分类号：TM73　　学校代码：10363
密　级：公开　　学　　号：2220310112

安徽工程大学
Anhui Polytechnic University

硕士学位论文

题目　智能电网中虚假数据注入攻击的检测方法研究

论文作者　张国庆
指导教师　高文根
学科（专业）　电气工程
研究方向　电力系统稳定性分析

论文提交日期：2025 年 05 月 14 日

分类号：TM73　　单位代码：10363

密　级：公开　　学　　号：2220310112

题　　目 智能电网中虚假数据注入攻击的检测方法研究

题　　目 Research on Detection Approaches of False Data Injection Attacks in Smart Grids

论文作者：张国庆

校内导师：高文根教授

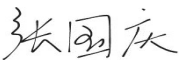
专　　业：电气工程

研究方向：电力系统稳定性分析

论文答辩日期：2025 年 04 月 29 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： 

日期：　　2025 年　05 月　14 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：张国庆 指导教师签名：高松根

日期： 2025 年 05 月 14 日　　日期： 2025 年 05 月 14 日

智能电网中虚假数据注入攻击的检测方法研究

摘 要

近年来，计算机技术、通信系统和自动控制的进步导致了网络物理系统(Cyber-Physical Systems, CPS)的出现，其中智能电网是最具代表性的应用之一。智能电网将物理电力传输、网络计算和通信深度融合，借助传感、通信和智能测量设备，提高了电力系统的运行可靠性。然而，这些网络技术的广泛应用也使电力系统面临潜在的网络攻击威胁，在众多网络攻击中，虚假数据注入攻击（False Data Injection Attacks, FDIAs）尤为值得关注。攻击者将虚假数据注入远程终端单元、数据传输通道和监控与数据采集(Supervisory Control and Data Acquisition, SCADA)系统，恶意地篡改状态估计，破坏电网信息的完整性，使控制中心的决策和调度受到干扰。目前，扩展卡尔曼滤波器(Extended Kalman Filter, EKF)算法被广泛用于 FDIAs 检测，EKF 算法引入的线性化误差往往被忽略，导致其估计精度下降，间接影响 FDIAs 检测。另外，基于状态估计的 FDIAs 定位方法复杂度高且局限性较大。针对现有研究中 FDIAs 检测和定位方法中的不足，本文主要开展以下工作：

(1)针对 FDIAs 的本质是攻击者通过篡改测量值，构建隐蔽的攻击向量来破坏系统的状态估计，建立了电力系统状态估计模型，依据此模型，对 FDIAs 的原理和向量构建进行了剖析和总结。首先，针对智能电网的非线性特征，建立了基于加权最小二乘(Weighted Least

Squares, WLS）的状态估计模型。其次，系统地描述了基于残差的不良数据检测(Bad Data Detection, BDD)原理。最后，在状态估计理论框架下研究了 FDIAs 的机理，重点对 FDIAs 向量的构造进行了深入分析。在 IEEE-14 节点和 IEEE-30 节点标准系统中进行了仿真实验，结果验证了 FDIAs 模型的有效性。

(2)针对基于 EKF 的 FDIAs 检测方法在检测过程中忽略泰勒级数的高阶项导致的线性化误差，提出了基于自适应插值扩展卡尔曼滤波器(Adaptive Interpolation Extended Kalman Filter, AIEKF)的 FDIAs 检测方法。首先，通过自适应插值策略在两个连续测量之间插入伪测量，从而减小线性化误差对估计精度以及 FDIAs 检测的影响。其次，考虑到 AIEKF 和 WLS 在 FDIAs 发生时所具有的不同性能，将两种估计器产生的偏差与预定的阈值进行比较，实现 FDIAs 的检测。最后，在 IEEE-14 节点和 IEEE-30 节点标准系统进行了仿真实验，结果表明该方法可以有效地提高 FDIAs 检测精度。

(3)针对基于状态估计的 FDIAs 定位方法过程复杂且具有较大局限性，提出了基于联合最大后验-最大似然估计(Joint Maximum a Posteriori-Maximum Likelihood, JMAP-ML)的 FDIAs 定位方法。首先，将虚假数据与测量数据误差归为一类，构建关于测量数据误差的高斯混合模型(Gaussian Mixture Model, GMM)。其次，利用基于 AIEKF 的 FDIAs 检测方法进行 FDIAs 检测和排除异常测量值，并将攻击发生时刻的测量数据导入 GMM 中，利用 JMAP-ML 算法求解模型参数。最后，在 IEEE-14 节点和 IEEE-30 节点标准系统上进行仿真实验，结

果表明该方法通过直接求解 GMM 参数实现 FDIAs 定位，简化了定位过程。

关键词：智能电网，虚假数据注入攻击，攻击检测，攻击定位，状态估计，联合最大后验-最大似然算法

RESEARCH ON DETECTION METHODS OF FALSE DATA INJECTION ATTACKS IN SMART GRIDS

ABSTRACT

In recent years, advancements in computer technology, communication systems, and automatic control have led to the emergence of Cyber-Physical Systems (CPS), with smart grids being one of the most representative applications. Smart grids deeply integrate physical power transmission, network computing, and communication technologies, leveraging sensing, communication, and intelligent measurement devices to enhance the operational reliability of power systems. However, the extensive application of these network technologies also exposes power systems to potential cybersecurity threats. Among various cyberattacks, False Data Injection Attacks (FDIAs) are particularly concerning. Attackers inject malicious data into remote terminal units, data transmission channels, and Supervisory Control and Data Acquisition (SCADA) systems, deliberately tampering with state estimation, compromising the integrity of power system information, and disrupting decision-making and scheduling at control centers. Currently, the Extended Kalman Filter (EKF) algorithm is widely employed for FDIAs detection. However, the linearization error introduced by EKF is often neglected, leading to reduced estimation accuracy and indirectly affecting FDIAs

detection performance. Additionally, existing state estimation-based FDIAs localization methods suffer from high complexity and significant limitations. To address these issues in FDIAs detection and localization, this study focuses on the following aspects:

(1)Considering that the essence of FDIAs lies in attackers manipulating measurement values to construct stealthy attack vectors that compromise state estimation in power systems, a state estimation model for power systems was established. Based on this model, the principles of FDIAs and the construction of attack vectors were analyzed and summarized. First, considering that smart grids exhibit nonlinear characteristics, a state estimation model based on Weighted Least Squares (WLS) was developed. Second, the principle of Bad Data Detection (BDD) based on residual analysis was systematically described. Finally, within the theoretical framework of state estimation, the mechanism of FDIAs was investigated, with a particular focus on the in-depth analysis of attack vector construction. Simulation experiments were conducted on the IEEE 14-bus and IEEE 30-bus standard systems, and the results verified the effectiveness of the FDIAs model.

(2)To address the linearization error introduced by the Taylor series approximation in EKF-based FDIAs detection, an FDIAs detection method based on the Adaptive Interpolation Extended Kalman Filter (AIEKF) is proposed. First, an adaptive interpolation strategy is employed to insert

pseudo-measurements between two consecutive measurements, reducing the impact of linearization error on estimation accuracy and FDIAs detection. Then, considering the different behaviors of AIEKF and WLS under FDIAs conditions, the bias between the two estimators is compared with a predefined threshold to detect FDIAs. Finally, simulation experiments on IEEE-14 and IEEE-30 standard test systems demonstrate that the proposed method significantly improves FDIAs detection accuracy.

(3)To address the high complexity and significant limitations of state estimation-based FDIAs localization methods, a Joint Maximum a Posteriori-Maximum Likelihood (JMAP-ML)-based FDIAs localization method is proposed. First, false data and measurement errors are classified into a single category, and a Gaussian Mixture Model (GMM) is constructed for measurement error representation. Second, the AIEKF-based FDIAs detection method is used to identify and remove anomalous measurements. The measurements at the time of attack occurrence are then fed into the GMM, and the JMAP-ML algorithm is employed to estimate the model parameters. Finally, simulation experiments on IEEE-14 and IEEE-30 bus systems demonstrate that the proposed method simplifies the localization process by directly solving GMM parameters, enhancing FDIAs localization efficiency.

KEY WORDS: smart grid, false data injection attacks, attack detection,

attack localization, state estimation, joint maximum a posteriori-maximum likelihood

目录

第1章 绪论

1.1 课题研究背景及意义

随着计算机技术、通信系统和自动控制技术在电力系统中的出现，电力网络物理系统(Cyber Physical Systems, CPS)逐渐形成并广泛应用[1][2]。图 1-1 是电力 CPS 的结构框架图。电力 CPS 作为计算域与物理域深度融合的智能化载体，是通过多维异构要素集成实现计算引擎、通信架构与控制逻辑深度耦合的新一代电力系统范式。该系统基于人机交互接口系统实现物理实体感知，依托网络化信息空间构建远程精准化、通信可靠化、响应实时化、操作安全化及决策协同化的多模态闭环管控机制[3]。智能电网是电力 CPS 的具体应用之一，通过集成传感器、通信网络和控制技术，实现了对电力生产、传输和消费的实时监控与管理。智能电网能够动态响应用户需求和环境变化，优化资源配置，提高电力系统的效率与可靠性，体现了 CPS 在智能决策与资源管理方面的优势[4]。

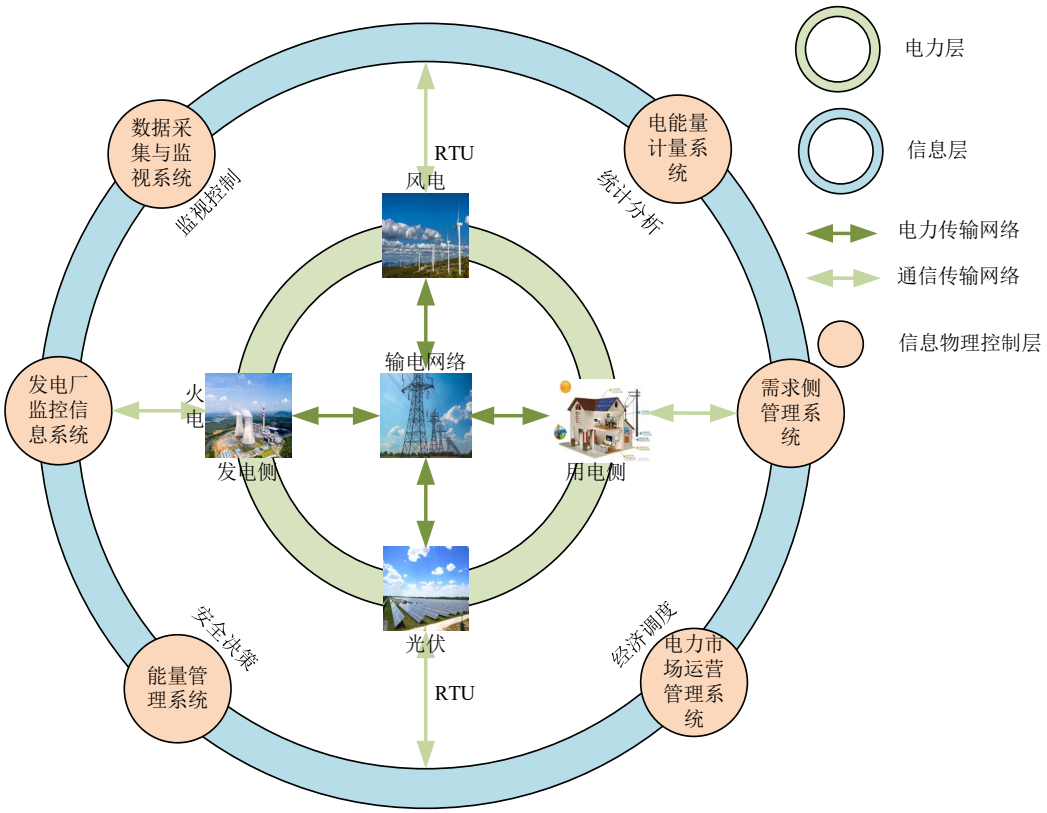


图 1-1 电力 CPS 结构

虽然这些网络技术，如传感、通信和智能测量设备，增强了电力系统的运行和可靠性，但也使系统暴露在潜在的网络攻击之下。针对智能电网的网络攻击是指在未获得授权的情况下，对智能电网的行为进行监视和分析，寻找出其漏洞和弱点，从而去破坏或削弱智能电网的功能。根据攻击目的进行分类，可以将这些攻击分为完整性攻击、可用性攻击和保密性攻击[5]。表 1-1 中总结了典型的攻击目标及其形式。其中，虚假数据注入攻击(False Data Injection Attacks, FDIAs)以其执行简单、隐蔽性高以及干扰控制中心正常运行的能力而著称[6]。这些虚假数据经过精心设计，以规避传统不良数据检测(Dad Data Detection, BDD)模块在状态估计过程中的识别。因此，被篡改的数据可能导致电力设备故障，甚至在极端情况下引发整个系统的崩溃，对电网的稳定运行构成重大威胁[7]。

表 1-1 针对智能电网的网络攻击

攻击分类	攻击目标	攻击形式
完整性攻击	电气量	虚假数据注入攻击
	电气量和开关量	拓扑篡改攻击
可用性攻击	时钟信号或授时协议	GPS 同步时钟伪造攻击
	计算、通信、存储资源	拒绝服务攻击
	通信通道	控制延时攻击
保密性攻击	密码、加密算法	密码破解
	通信通道	窃听

过去几十年内，全球范围内多次发生大规模电力网络安全事件，其中许多案例涉及利用数据篡改手段实施的攻击。1999 年，一名黑客利用特洛伊木马入侵了俄罗斯最大的天然气公司俄罗斯天然气工业股份公司。攻击者完全控制了负责监控通过管道的气体流量的中央配电盘[8]。2003 年，一种猛烈的蠕虫通过利用 MS-SQL 数据库的漏洞暴露了 SCADA。蠕虫从企业传播到 SCADA 网络，使安全监控系统瘫痪约 5 小时[9]。在 2010 年针对伊朗核设施的“奥运会(Olympic Game)”行动中，黑客通过“震网(Stuxnet)”蠕虫病毒，成功入侵并破坏伊朗核设施，严重迟滞了伊朗核计划，成为首个利用恶意代码对实体设施造成重大不可逆损坏的事件[10]。2015 年，乌克兰的电力基础设施遭到了精心策划的网络攻击，导致数十万用户在寒冷的冬季中断了电力供应。攻击者利用一种名为

BlackEnergy 的恶意软件渗透进电力公司的计算机网络，随后通过远程操作对关键控制系统进行破坏，最终导致电力断供[11]。2019 年 9 月，印度泰米尔纳德邦的 Kudankulam 核电站发生了内网感染恶意软件的事件，攻击者通过网络入侵成功将恶意软件植入核电站的内部网络，导致了关闭了一座反应堆[12]。诸如此类事件的发生严重影响了国民生活的正常进行。

从上述案件中可以看出，智能电网常常是攻击者首选的攻击目标，智能电网一旦遭受攻击，不仅会导致大范围的电力中断，还可能对工业生产等依赖电力的关键行业造成连锁反应，甚至危及国家安全和社会稳定[13]。智能电网的高互联性和数据驱动的特性，使其在面对 FDIAs 时尤为脆弱。攻击者可能将虚假数据注入远程终端单元、数据传输通道以及监控与数据采集(Supervisory Control and Data Acquisition, SCADA)系统中，恶意篡改各节点的状态，使得控制系统在错误状态的基础上发出指令，导致电力系统失衡、设备损坏或大范围停电[14][15]。因此，研究智能电网中 FDIAs 的检测问题具有十分重要的现实意义。

1.2 国内外研究现状

1.2.1 虚假数据注入攻击研究现状

FDIAs 的概念首先是由 Liu 等人在 2009 年提出的[16]，该研究表明，如果攻击者能够获取电网的配置信息并操控部分电表数据，其可以在不被现有算法检测到的情况下，向状态估计中注入任意错误。FDIAs 可以绕过现有的最大归一化残差(Largest Normalized Residual, LNR)检验、卡方检验等 BDD 机制[17-19]，破坏电力 CPS 中的核心设备，导致大规模停电。因此，为了确保智能电网的安全，许多研究人员致力于 FDIAs 的研究[20]。

早期研究聚焦于攻击策略的优化设计，文献[21]针对 FDIAs 在电力系统状态估计中的脆弱性问题，提出了最小化攻击成本的模型，并设计了优化算法来寻找对系统影响最大的攻击策略，为后续的研究奠定基础。文献[22]考虑了电力系统的物理特性，并将一般的 FDIAs 转化为负载再分配攻击模型。同时构建了双级混合整数线性规划模型，以确定最具破坏性的攻击策略。考虑到资源受限，攻击者很难拥有电力网络的完整拓扑结构和参数信息，文献[23]提出了一种通过获取

较少的网络信息来确定可行的攻击区域的 FDIAs 模型，攻击者只需针对攻击区域去获取局部信息参数，而对攻击以外的区域则不需过多关注。文献[24]在[23]的基础上进一步挖掘了不完全信息下的攻击建模机理，设计了基于机理驱动与图论搜索的攻击方案寻优算法。在攻击设计成功的基础上，攻击的隐蔽性至关重要，文献[25]提出了一种新的基于前后调度的双层假数据注入攻击模型，该模型在调度前最小化攻击前后上传量测值的差异以规避检测，在调度后通过安全约束经济调度引导系统进入非经济甚至不安全状态，显著提升了攻击的隐蔽性和破坏性。文献[26]提出了一种用于单线攻击的状态保留模型，在该模型中，攻击者可以通过在线路的终端总线上注入虚假电力来掩盖电网的拓扑结构，而不会被发现，进一步拓展了隐蔽攻击的应用场景。与此同时，为降低攻击实施的计算复杂度，文献[27]提出了一种基于紧缩投影逼近子空间跟踪算法的新型攻击方法，通过递推更新的方式构造出具备完整信息的雅可比矩阵，在降低矩阵计算量的基础上，缩短了攻击的发起过程。文献[28]则将攻击向量的设计转化为线性回归模型的子集选择问题，通过分析各量测数据对模型误差减少的贡献逐步选择攻击向量元素。

除了研究攻击策略，部分学者对防御机制也进行了一系列的研究。系统操作者与恶意攻击者之间的攻击防御互动，通常涉及有意识的思考，而且防御策略的有效性很大程度上取决于当前的攻击策略。文献[29]引入了一种图形方法作为防御机制，以防止 FDI 对电力系统进行攻击。其已经证明，如果安全地选择了电表测量的子集，则无法发起 FDIAs。文献[30]在[29]的基础上，提出了一种基于图论的拓扑优化算法，利用权值分配对网络拓扑进行等效变换，实现拓扑的优化选择，从而提高了系统的防御性能。与此同时，部分学者在采用博弈论框架研究攻击者与系统防御者之间的互动方面投入了越来越多的努力和兴趣。文献[31]提出了一种新的自适应马尔可夫博弈策略，针对任何静态攻击，该策略在满足理性与标准性的基础上将始终收敛到最佳响应防御策略。文献[32]针对在攻击发生时攻防双方需要不断改变各自策略以达到利益最大化，结合博弈论的思想优化现有的防御资源，从而完成对关键量测的保护。文献[33]通过海萨尼转换将不完全信息博弈转化为完全信息博弈，利用贝叶斯纳什均衡推断攻击者类型概率分布，然后构建多阶段动态博弈树，采用逆向归纳法求解均衡路径，确定攻防双方的最优策略。由于 FDIAs 依赖于物理系统的特性，已经出现了一部分工作利用物理系统来积

极防御这些攻击。文献[34]将移动目标防御与物理水印概念相结合，通过高斯水印扰动电抗，防止攻击者推断出新的系统参数。文献[35]提出了一种基于多项式的妥协弹性路由过滤方案，该方案可以通过过滤错误注入的数据来抵御攻击。文献[36]利用监视控制与数据采集和相量测量单元量测数据，提出了一种混合量测系统的多重匹配状态预测方法，其中心思想是在保证状态预测结果可靠的基础上实现 FDIAs 的在线防御。

1.2.2 虚假数据注入攻击检测研究现状

自从 FDIAs 的概念提出以来，有关 FDIAs 检测算法的问题受到了研究者的广泛关注。虽然 FDIAs 的检测算法各不相同，但主要可以分为系统模型和数据驱动两大类[37]，如图 1-2 所示。

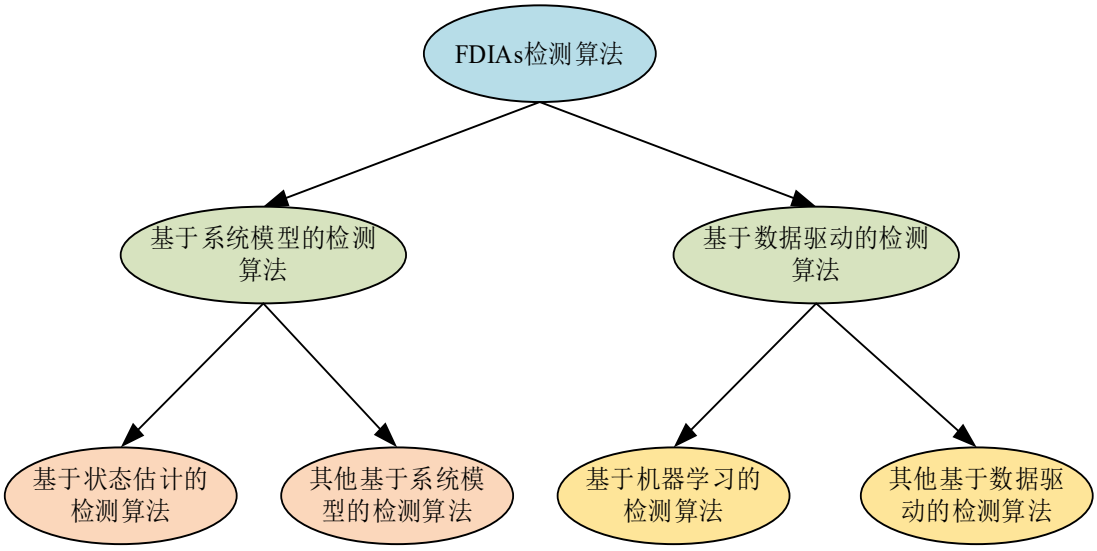


图 1-2 FDIAs 检测算法分类

基于系统模型的 FDIAs 检测算法主要思想是在电力系统自身模型或内部参数的基础上，对系统所收集到的数据进行分析处理计算出系统状态或系统内部参数，并结合相关判定方法[38-43]，将最终结果与设定的阈值进行比较，以此实现对 FDIAs 的检测。

状态估计分为静态估计和动态估计，由于智能电网是实时变化的，静态估计仅考虑当前时刻的量测数据，导致估计效果不佳，因此动态估计被引入到状态估计中。动态状态估计的核心是卡尔曼滤波器(Kalman Filter, KF)，通过预测步和更新步将历史时刻和当前时刻结合对系统状态进行实时估计。在攻击发生时刻，利

用动态估计与其他估计算法实时计算系统状态，结合欧式距离、余弦相似度等相关判定方法来检测 FDIAs，这一类检测算法都是基于这一思想，其他学者通过不断对 KF 算法进行改进，提高检测精度。文献[44]提出了一种基于偏差的 FDIAs 检测方法，该方法利用了加权最小二乘和卡尔曼滤波器的估计结果，在传统的卡尔曼滤波器中引入了指数加权函数使得两个估计量结果的差异增加，以此检测 FDIAs，但该方法只适用于直流系统。为了更好地拟合系统的非线性特征，部分学者提出扩展卡尔曼滤波器(Extend Kalman Filter, EKF)，EKF 算法通过对非线性系统方程进行一阶泰勒展开，将非线性系统线性化，用于交流状态估计。文献[45]和[46]利用 EKF 与其他算法的估计结果的差值进行 FDIAs 检测。由于 EKF 进行线性化时引入了线性化误差，导致滤波效果下降，文献[47]引入了无迹卡尔曼滤波器并对其进行了改进以检测 FDIAs，该方法通过自适应调节无迹卡尔曼滤波器 Sigma 点的选取，使得估计结果更加准确，更加有利于 FDIAs 的检测辨识，但没有考虑预测模型受负荷突变的影响，降低了模型预测精度。为了提高模型预测精度，文献[48]提出一种基于加权灰色关联分析和最小二乘支持向量机的日前负荷预测模型，结合无迹卡尔曼滤波的动态状态估计，自适应加权生成预测值，最终利用预测值与估计值的偏差检测 FDIAs。

FDIAs 发生后会造成系统数据的数理统计特性发生改变，一些学者开始研究如何利用系统数据的异常变化反应 FDIAs 的存在。文献[49]和[50]通过计算当前时间步与前一时间步的测量值变化，生成概率分布，并与历史数据的分布进行比较。利用 Kullback-Leibler 距离量化当前测量值分布与历史分布之间的差异，以此检测 FDIAs，但遭遇连续小规模攻击或重放攻击时，该方法检测效果不理想，尤其是当时间间隔较小时，难以区分正常变化与攻击。针对小规模攻击，文献[51]提出了一种基于 k 最小残差相似度的 FDIAs 检测算法，基本原理为在 FDIAs 发生前后，测量残差的概率分布发生变化，利用 Jensen-Shannon 距离精确量化测量残差分布的相似性，以此检测交流状态估计中的 FDIAs。针对传统的水印方法在检测重放攻击时，需要在检测率和控制性能之间进行权衡，文献[52]提出了一种基于水印和移动目标的 FDIAs 检测方案，该方法将带水印的信号与非线性静态辅助功能相结合，可检测出零动态攻击、重放攻击等多种类型的 FDIAs。

基于数据驱动的检测算法通常不需要对系统模型有任何了解，其中心思想是

利用历史数据训练学习，保存其数据特征，然后基于历史数据的特征对实时数据进行分析[53]，以此检测 FDIAs 的存在。

在 FDIAs 检测研究中，支持向量机(Support Vector Machines, SVM)因其较强的泛化能力和鲁棒性而备受关注，文献[54]提出了一种创新方法，将主成分分析与分布式高斯核 SVM 相结合，在维持高检测精度的同时有效降低了计算复杂度，但当系统规模较大或样本数目较多时，其较高的时间复杂度会导致训练过程耗时过长，并占用大量存储资源，并且该方法只适用于直流系统。由于系统状态不仅具有空间数据特征，还具有时间数据相关性，连续系统状态的时间依赖性实际上可以为系统操作员提供更多检测 FDIAs 的信息。而自动编码器(Autoencoder, AE)可以学习数据样本中的潜在相关结构，即时间维度和空间维度，可以学习有效的数据的缩减尺寸特征表示。于是文献[55]提出了一种基于自动编码器的 FDIAs 检测算法，该方法利用传感器数据在时间和空间上的相关性，任何会导致这些相关结构显著变化的攻击都可以被检测到，同时使用去噪自动编码器来清理损坏的数据，但是去噪自动编码器的泛化能力有限。文献[56]提出了一种基于离散小波变换和深度神经网络(Deep Neural Networks, DNN)的 FDIAs 检测方法，在现有的 DNN 单元构建了一个循环神经网络(Recurrent Neural Network, RNN)模型。该网络通过学习由离散小波变换提取的时间-空间系统状态特征，旨在区分攻击事件和正常电力系统运行事件。但是单向门控循环单元不能很好地提取小波变换中的有效特征，并且有出现梯度爆炸的可能。针对 DNN 的“黑盒”属性降低了检测模型的可解释性，导致检测结果缺乏可信度，文献[57]提出了一种基于多头图注意力网络和时间卷积网络模型的 FDIAs 检测算法。该方法分别利用多头图注意力网络和时间卷积网络提出测量数据空间和时序特征，增强了模型空间特征和时间维度上的可解释性，但是其训练时间较长，计算资源消耗大，并且对训练所需的数据质量和完整性要求较高。针对在 FDIAs 检测过程中 DNN 在训练过程中出现过拟合问题，文献[58]提出了一种基于残差神经网络结构的多通道融合的 FDIAs 检测算法，该方法利用一维卷积神经网络和长短期记忆网络对时间序列进行提取融合，然后利用残差神经网络搭建更深层的网络模型，从而更好地学习 FDIAs 的特征。然而，该方法需要借助大规模的数据集来开展训练工作，否则就难以实现高效且精准的检测。

除了上述的机器学习方法外，一些学者通过利用量测数据的隐藏特征，将受FDIAs影响的数据与正常数据分为不同类别，从而实现FDIAs的检测。文献[59]提出了一种基于循环图(Recurrence Plots, RPs)和视觉几何群网络(Visual Geometry Group Network, VGGNet)的维度扩展数据驱动新型检测算法，该方法利用递归图将实时一维时间序列智能电表数据增强为二维图像数据，然后使用 VGGNet 对增强的二维数据进行区分真实和受污染的智能电表数据，但 VGGNet 作为深度模型计算复杂度较高，可能难以满足智能电表实时检测的需求。K均值聚类算法由于实现简单，算法复杂度低，广泛用于聚类问题，但由于K均值对初始质心的选取比较敏感，模糊K均值聚类算法便被由于FDIAs检测。在文献[60]和[61]中，一个样本不再固定属于某一类别，而是计算出样本属于某个类别的概率，即受FDIAs影响的样本概率为a，则正常样本的概率为$1-a$，利用模糊K均值聚类成功地检测了FDIAs。与上述思想类似，文献[62]从统计学习的角度将FDIAs发生后的量测数据建模为高斯混合模型，假设攻击数据和正常数据位于特征空间的不同区域，通过融合不同分布特性，能够逼近任意复杂的数据分布，从而实现FDIAs的检测。

1.2.3 研究现状分析

在 FDIAs 方面，研究通常分为攻击者模型和防御模型两大类。攻击者模型描述了攻击者如何获取电网敏感信息并篡改或注入虚假数据。攻击者可以是完全知情或部分知情型，利用数据冗余、测量误差和通信漏洞干扰电网运行。主要挑战在于准确描述攻击者行为，尤其是在信息不完全时，或者如何识别大规模电网中的潜在攻击目标及路径。未来研究需关注电网状态变化时，攻击者行为的适应性调整。防御模型则通过多种策略提升电网安全性，采用图论、博弈论等方法设计灵活有效的防御机制。尽管已有进展，防御策略仍面临两个问题：一是适应性和实时性不足，传统方法难以应对动态攻击；二是攻击行为动态变化，现有方法假设攻击可预测，因此防御系统的响应要求更高。未来研究应聚焦于提高自适应性、结合智能技术应对动态攻击，并探索防御策略的协同机制，以增强电网系统的整体防护能力。

在 FDIAs 检测方面，现有的基于系统模型和机器学习的检测算法虽然不断

发展，但在目前的检测算法中仍然存在系统模型简化、复杂环境下识别能力受限、算法可扩展性不足等问题。具体来说，一方面，在基于状态估计的 FDIAs 检测算法中，EKF 算法被广泛使用，为了提高 EKF 算法的估计精度，相继产生了迭代 EKF、指数加权 EKF 等算法，但这些改进的算法却忽略了 EKF 算法的本质，EKF 算法产生的线性化误差没有得到解决，这会造成随着电力系统维度的上升，EKF 算法的估计性能下降，而基于状态估计的 FDIAs 检测算法核心就是算法估计，算法的估计精度间接影响 FDIAs 的检测效果。另一方面，在检测受攻击的节点时，即 FDIAs 的定位，利用状态估计的思想对 FDIAs 进行定位，其过程中比较复杂且有一定局限性。基于机器学习的 FDIAs 定位算法虽然可以对受攻击的节点进行定位，但是所利用的算法需要大量的数据进行训练，甚至训练过程中可能出现过拟合的情况。相比之下，利用统计学习思想拟合 FDIAs 发生前后数据的分布特性，构建测量数据的混合分布模型，在利用相关算法求解模型参数的基础上对受攻击的节点进行定位更有优势。因此，未来的研究需要在多个方面进行改进：首先，在适应性方面，现有检测方法大多集中在输电网，未来应扩展到配电网、微网、用户储能和智能电表等多样化的电力系统，以适应不断变化的系统环境。其次，在鲁棒性方面，检测算法需要应对更加复杂的场景，如不确定性电力输出、量测噪声、负荷波动以及拓扑变化等。最后，在时效性方面，现有研究主要集中在小规模系统，未来需要开发适用于大规模电力系统的实时检测算法，如何在保证检测精度的同时减少计算复杂度并缩短检测时间，将成为一项重要挑战。

综上所述，虽然针对 FDIAs 的攻击向量的构造、攻击的防御以及攻击检测方面取得了一定的成效，但对于 FDIAs 的研究仍处于初级阶段，特别是针对 FDIAs 检测算法方面仍存在一些不足之处。因此，针对智能电网下虚假数据注入攻击检测的研究具有重要的意义。

1.3 主要研究内容及创新点

FDIAs 是一种针对智能电网的网络攻击方式，攻击者通过向系统中注入虚假的测量数据，旨在篡改系统的状态估计、影响决策过程，甚至使电网系统出现故障或无法正常运行。本文主要围绕 FDIAs 的检测展开研究。首先分析了 FDIAs

的原理及模型构建，其次在此基础上利用自适应插值扩展卡尔曼滤波器进行FDIAs检测，最后利用联合最大后验-最大似然估计算法进行FDIAs定位，全文的主要框架如图1-3所示，具体如下：

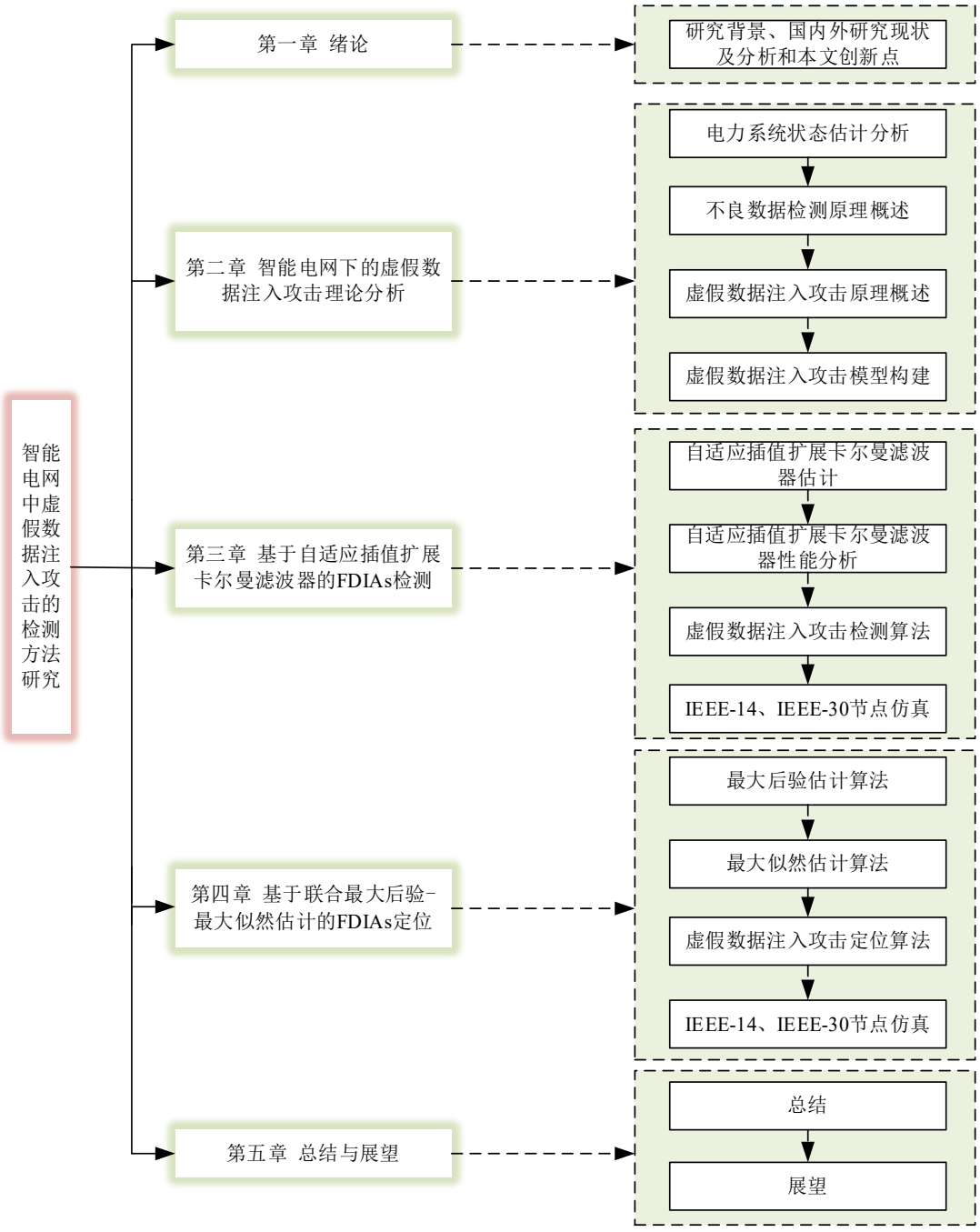


图1-3 研究内容框架图

第一章为绪论。首先，阐述了开展FDIAs检测的背景及意义；其次，从攻击者和防御者两个角度介绍了国内外针对FDIAs本身开展的研究的现状，在此基础上，重点阐述了国内外针对FDIAs检测方法的研究现状，并对现状进行了分

析；最后，介绍了本文的研究内容及创新点。

第二章为智能电网下虚假数据注入攻击理论分析。首先，建立了电力系统的状态估计模型，并阐述了不良数据检测的基本原理；其次，详细分析了 FDIAs 的生成过程，包括攻击的基本原理及其构建方法；最后，在状态估计的框架下构建了攻击向量模型，并在 IEEE-14 节点和 IEEE-30 节点的标准系统上进行了有效性验证。

第三章为基于自适应扩展卡尔曼滤波器的 FDIAs 检测。首先，将自适应插值策略引入 EKF 中，形成 AIEKF 算法；其次，将 AIEKF 与 WLS 算法相结合，利用两者在面对 FDIAs 时的不同响应，并使用欧氏距离作为检测指标来识别 FDIAs；最后，在 IEEE-14 节点和 IEEE-30 节点标准系统上进行了仿真实验，结果显示 AIEKF 算法误差较小，检测效果较好。

第四章为基于联合最大后验-最大似然估计的 FDIAs 定位。首先，将攻击向量与测量噪声视作一体，构建关于测量噪声的高斯混合模型；其次，在上一章检测的基础上，进行 FDIAs 检测并排除异常测量值，将攻击发生时刻的测量值导入 GMM，利用 JMAP-ML 算法求解模型参数，定位出受到篡改的测量值，通过分析测量值之间的相关性实现 FDIAs 的定位；最后，在 IEEE-14 节点和 IEEE-30 节点标准系统上进行了仿真实验，结果表明 JMAP-ML 算法直接通过求解 GMM 参数实现 FDIAs 定位，简化了定位过程。

第五章为总结与展望。对本课题开展的研究内容进行了总结，分析了课题当前研究内容的不足之处，并且阐述了本课题未来需要改进的方向。

本文主要创新点如下：

(1)提出了一种基于自适应插值扩展卡尔曼滤波器的 FDIAs 检测方法。针对传统扩展卡尔曼滤波器在状态估计时会忽略高阶项，导致线性化误差，因此引入自适应插值策略对其进行优化。通过在连续测量间进行线性化插值，使状态估计更加精确。在此基础上，将 AIEKF 与 WLS 相结合，利用两者在面对 FDIAs 时的不同响应，并使用欧氏距离作为检测指标来识别 FDIAs。

(2)提出了一种基于联合最大后验和最大似然估计的 FDIAs 定位方法。针对传统基于状态估计的方法在定位受攻击的节点时过程比较复杂且局限性较大，因此引入统计学习思想，将攻击向量与测量噪声可以视作一体，构建关于测量噪声

的 GMM。在此基础上，利用 JMAP-ML 算法求解模型参数，对攻击发生时刻的测量值进行二分类，定位出受到篡改的测量值。通过分析测量值之间的相关性，实现 FDIAs 的定位。

第2章 智能电网下的虚假数据注入攻击理论分析

2.1 引言

状态估计在电力系统中的重要性不可忽视，其作为电力调度和控制的基础环节，对电力系统安全稳定运行产生直接影响。准确的状态估计为能量管理系统(Energy Management System, EMS)提供了关键的实时数据支持，确保负荷预测、经济调度、最优潮流计算等功能能够高效、可靠地执行。同时，状态估计的准确性对故障诊断和应急响应至关重要，能够有效防止电力系统运行过程中潜在的风险和异常情况。反之，若状态估计存在偏差或错误，可能导致调度策略失误，甚至引发系统不稳定和大规模停电事故。

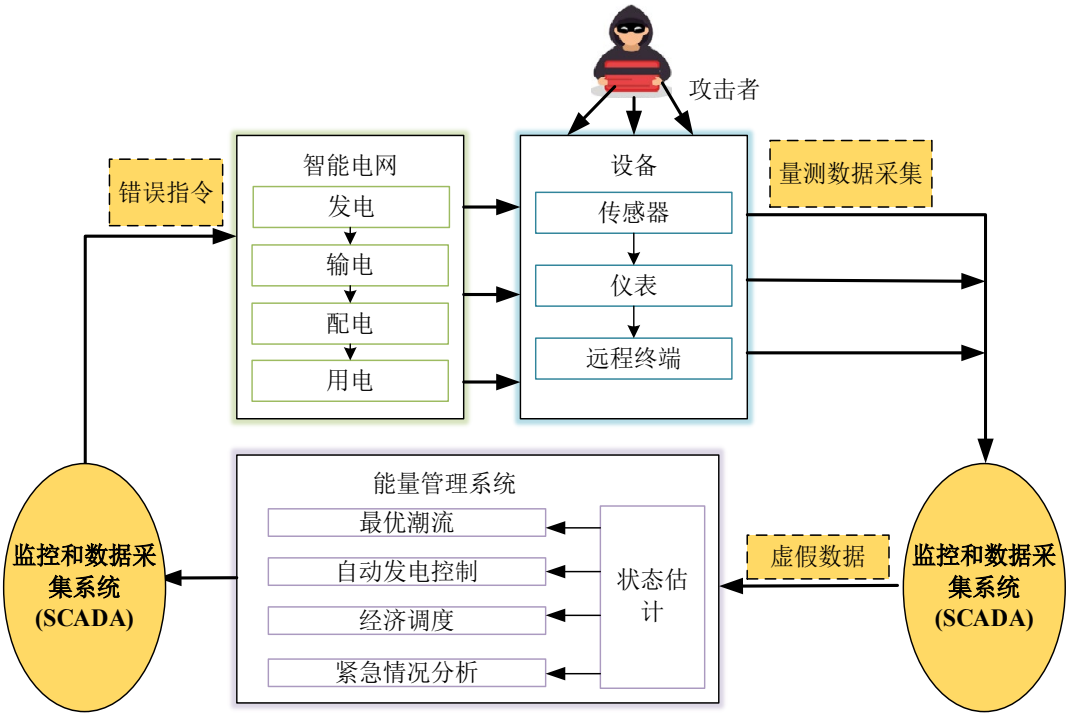


图 2-1 智能电网中虚假数据注入攻击示意图

FDIAs 是一种专门针对 CPS 中状态估计数据完整性的新型攻击方法，其攻击示意图如图 2-1 所示，攻击者将虚假数据注入到智能电网传感器、控制器、远程控制单元中，以此实现隐蔽地恶意篡改状态估计。这些数据经过精心设计，可以躲过传统电力系统中的 BDD 模块，可能导致电网设备出现故障，严重时可能导致电网完全瘫痪，对电网安全构成重大威胁。因此，对围绕 FDIAs 本身以及与

其相关的理论基础进行深入研究具有一定的现实意义。

2.2 电力系统状态估计

电力系统状态估计是电网实时运行的核心分析工具，通过电压互感器、电流互感器等传感器采集母线电压、线路电流及功率等实时量测数据，经功率变换器处理、模/数转换器数字化后，借助通信通道传输至调度中心。

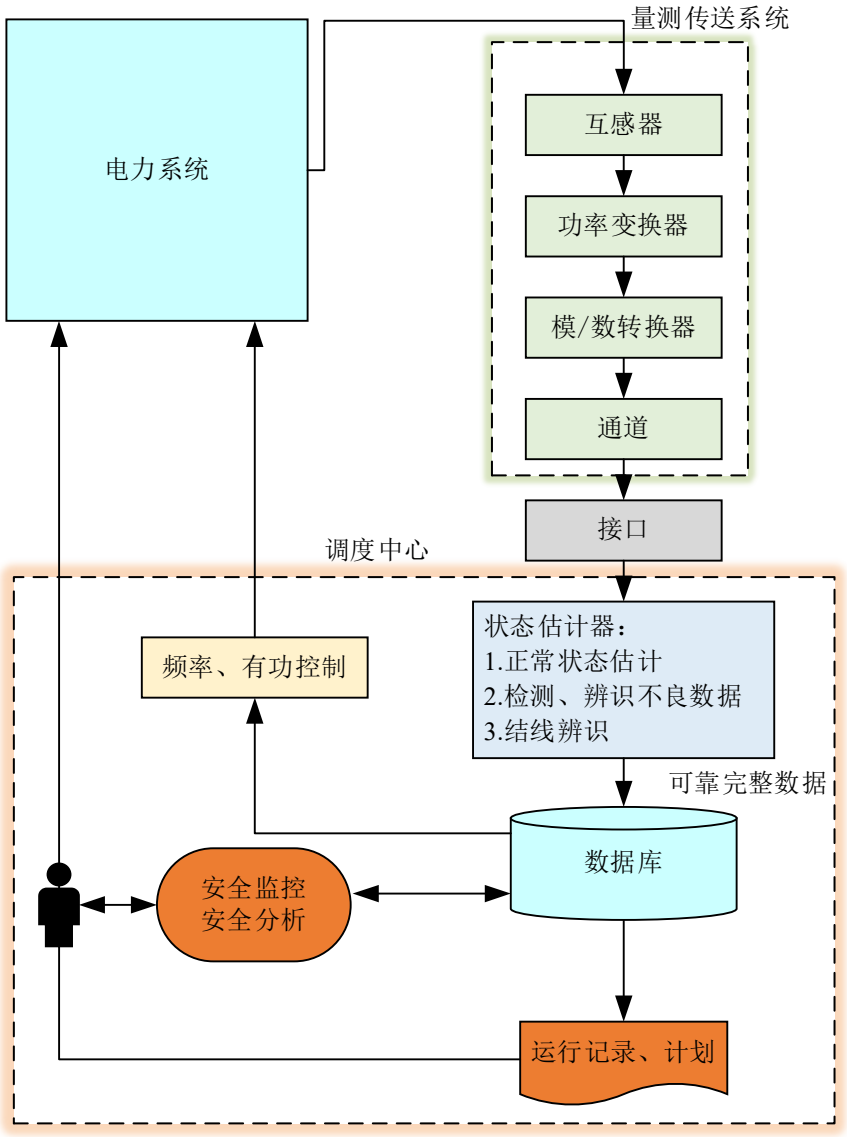


图 2-2 电力系统结构工作示意图

由图 2-2 可知，状态估计器通过相关算法计算出电网节点电压幅值、相角等关键状态量，并同步完成异常数据检测与剔除，确保数据可靠性；同时结合开关量信息动态辨识电网拓扑结构，修正网络模型与实际连接的偏差。其输出的高精

度状态数据不仅支撑实时安全监视和风险预判，还为频率调节、有功控制等闭环控制提供决策依据，并与历史数据库联动，优化电网运行记录分析与长期规划。这一过程深度融合了数据采集、模型校核与动态优化，是电力系统稳定运行的关键保障。

在交流潮流状态估计中，潮流与电压幅值和电压角度之间存在非线性依赖关系[63]，从而产生如下非线性数学依赖关系:

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{2-1}$$

式中，$\boldsymbol{z}$是测量值矢量，包括有功和无功功率流、有功和无功功率注入、电压幅度和相角；$\boldsymbol{x}$是状态变量矢量，包括电压幅值和相角；$\boldsymbol{e}$是测量误差矢量，一般假设$\boldsymbol{e}\sim\mathcal{N}\left(\boldsymbol{0},\boldsymbol{R}\right)$；$\boldsymbol{h}(.)$是测量值和状态变量之间建立依赖关系的函数向量，即：

$$\boldsymbol{h(x)}=\begin{bmatrix} V_i \\ P_i\left(\theta_i,\theta_j,V_i,V_j\right) \\ Q_i\left(\theta_i,\theta_j,V_i,V_j\right) \\ P_{ij}\left(\theta_i,\theta_j,V_i,V_j\right) \\ Q_{ij}\left(\theta_i,\theta_j,V_i,V_j\right) \end{bmatrix} \tag{2-2}$$

式中，P_i、Q_i、P_{ij}、Q_{ij}均为与电压幅值和相角相关的方程，具体表达式如下：

$$\begin{aligned} P_i &= V_i\sum_{j\in T}V_j\left[G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}\right] \\ Q_i &= V_i\sum_{j\in T}V_j\left[G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij}\right] \\ P_{ij} &= V_i^2G_{ij}-V_iV_j\left[G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}\right] \\ Q_{ij} &= -V_i^2B_{ij}-V_iV_j\left[G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij}\right] \end{aligned} \tag{2-3}$$

式中，V_i和V_j分别为i和j处的电压幅值；P_i、Q_i分别表示i母线的有功功率注入和无功功率注入；P_{ij}和Q_{ij}分别表示母线i到母线j的有功潮流和无功潮流；G_{ij}和B_{ij}分别表示母线i到母线j的电导和电纳；θ_{ij}表示从母线i到母线j的线电压相位角差；$\boldsymbol{T}$表示与i相邻的总线集合。

WLS 是电力系统中广泛使用的状态估计方法[64]，其利用权重反映不同测量数据的可靠性。该方法通过构建目标函数$J(\hat{\boldsymbol{x}})$，最小化测量值与测量值的估计值

之差的加权平方和，从而得到最接近系统的真实状态 $\boldsymbol{x}$ 的最优解。根据 WLS，最终状态变量的求解转化为下式：

$$\hat{\boldsymbol{x}} = \arg\min\left[\boldsymbol{z} - \boldsymbol{h}\left(\hat{\boldsymbol{x}}\right)\right]^T \boldsymbol{R}^{-1}\left[\boldsymbol{z} - \boldsymbol{h}\left(\hat{\boldsymbol{x}}\right)\right] \tag{2-4}$$

式中，$\boldsymbol{R}$ 为测量误差的协方差矩阵

加权最小二乘法的状态估计过程首先需要初始化状态向量 $\boldsymbol{x}$，通常可以使用平衡潮流解作为初始值。在状态向量初始化后，需要计算测量方程 $\boldsymbol{h}(\boldsymbol{x})$ 关于状态向量 $\boldsymbol{x}$ 的雅可比矩阵 $\boldsymbol{H}$，其元素定义为 $\boldsymbol{H}_{ij} = \dfrac{\partial \boldsymbol{h}_i(\boldsymbol{x})}{\partial \boldsymbol{x}_j}$。这个雅可比矩阵反映了测量方程对状态变量的敏感度，是后续迭代更新状态的重要基础。在状态估计过程中，通过线性化近似，可将测量方程表示为：

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{2-5}$$

然后，通过以下正规方程来更新状态变量 $\boldsymbol{x}$：

$$\boldsymbol{x}^{k+1} = \boldsymbol{x}^k + \left(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^k\right)\right) \tag{2-6}$$

式中，$\boldsymbol{x}^k$ 为第 k 次迭代的状态估计值。根据式(2-6)进行不断的迭代修正，这个迭代过程会不断更新状态向量，直到满足预定的收敛标准 ε，即：

$$\left\|\boldsymbol{x}^{k+1} - \boldsymbol{x}^k\right\| < \varepsilon \tag{2-7}$$

此时，$\boldsymbol{x} = \boldsymbol{x}^k$ 为系统最优状态估计值。

2.3 不良数据检测算法基本概述

电力系统的 BDD 估计过程中不可或缺的一部分，其主要目的是在状态估计过程中识别并排除可能影响估计精度的错误测量数据。电力系统的运行依赖于大量实时测量的数据，这些数据通常由各种传感器和测量设备采集，经过多级传输和处理后，最终汇总至调度中心。然而，由于测量设备可能发生故障、数据传输过程中可能受到噪声干扰，甚至可能出现通信链路的故障或丢包，电力系统中获取的测量数据往往会包含不良数据。这些不良数据，如果未经检测和处理，可能导致状态估计结果的严重偏差，从而影响系统的正常运行和安全稳定性。为了保证状态估计的准确性，电力系统需要有效的 BDD 数据的过程通常包括：首先，

通过分析测量数据与状态估计值之间的残差来发现异常；其次，使用不同的检测方法，例如残差极值函数检测法、加权残差检测法、标准残差检测法等，以进一步确认不良数据的存在。

WLS 方法旨在通过最小化加权残差平方和(目标函数$J(\hat{\boldsymbol{x}})$)来确定状态变量$\boldsymbol{x}$。然而，当测量数据中存在不良数据时，某些测量值的残差会大幅度增加，导致这些残差在目标函数中的贡献远高于正常范围，从而使得目标函数$J(\hat{\boldsymbol{x}})$值显著偏离正常水平。因此，通过观察目标函数值的变化，可以检测到不良数据的存在。

具体而言，首先计算测量值与基于当前状态估计的计算值之间的差异，这些差异称为残差，残差$\boldsymbol{r}$可以表示为：

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}\right) \tag{2-8}$$

在使用目标函数极值法检测不良数据时，通常采用假设性检验，即：

$$\begin{cases} J\left(\hat{\boldsymbol{x}}\right)>\chi^2_{(m-n),p}, & H_0\text{为真，接受}H_0 \\ J\left(\hat{\boldsymbol{x}}\right)\le\chi^2_{(m-n),p}, & H_0\text{为假，接受}H_1 \end{cases} \tag{2-9}$$

式中，H_0为原始性假设，即存在不良数据；H_1为选择性假设，即不存在不良数据；$\chi^2_{(m-n),p}$为卡方检验阈值；p为置信度水平，$m-n$为自由度。

2.4 智能电网下的虚假数据注入攻击

FDIAs 念首先是由 Liu Y 于 2011 年提出，之后便引发了广大学者的关注。与不良数据的形成不同，FDIAs 是由人为因素造成的。FDIAs 作为一种网络攻击形式，通过篡改传感器数据或测量数据，误导电力系统的状态估计，进而可能导致错误的调度决策，甚至引发大范围的电力中断。更具挑战性的是，FDIAs 往往能够绕过常规的 BDD 机制，这使得其检测变得更加复杂。因此，深入了解 FDIAs 的原理及其模型构建过程，有助于 FDIAs 发生时制定有效的检测和定位方法，从而提高电力系统的稳定性。

2.4.1 虚假数据注入攻击原理概述

为了最小化攻击 SCADA 系统所需的努力，避免被检测并维持欺骗，攻击者通常会在传输电网中寻找攻击点，这些点需要修改的测量数量最少或对测量值的更改最小。攻击者还需要电网拓扑结构信息，以便他能够以避免被 BDD 机制发现和消除的方式修改测量值。

隐藏攻击的一般规则是攻击者必须更改数据，以便测量结果能够合理地对应系统的物理属性。如果潮流方程没有可行的解，那么 BDD 将把 FDIAs 检测为超过某个可接受限度的值。如式(2-3)所示，每个总线的功率注入和总线之间的功率流都是状态变量的函数。因此，如果攻击者的目标是改变任何功率注入或功率流测量的感知值，攻击者需要调整出现在该测量的函数中的状态变量的估计值。换句话说，为了使所有的测量都符合功率流方程，攻击者必须调整与该状态变量相关的所有测量值[65]。

经过以上分析，隐蔽的 FDIAs 需要满足以下约束：

(1)如果对线路上的所有功率流和功率注入都进行了测量，攻击者需要攻击以功率注入总线为界的子图中的所有测量值，以隐藏其攻击。

(2)潮流注入变化加上功率损耗变化之和必须为零，即：

$$\sum_i \Delta P_i + \Delta P_{loss} = 0 \tag{2-10}$$

$$\sum_i \Delta Q_i + \Delta Q_{loss} = 0 \tag{2-11}$$

(3)攻击者为隐藏攻击而必须改变的最小测量值在很大程度上取决于网络拓扑结构、总线类型的组成(带和不带发电机注入的总线)、现有的测量值。

2.4.2 虚假数据注入攻击模型构建

根据上一节所描述，构建一个 FDIAs 向量，攻击者必须充分了解电网的拓扑结构，并掌握相关的信息。为了向状态估计器隐藏攻击，需要获得破坏的最小测量值数目。利用系统的雅可比矩阵，可以推导出来状态变量与测量值之间的关系。只需要考虑雅可比矩阵的每一列中具有非零值的行，通过确定该列中非零元素的数量，最小测量值数目就会确定，即矩阵提供了哪个测量依赖于哪个状态变量的信息，即元件的非零值表示该值是状态的直接函数。为了隐藏被攻击状态变

量的值，需要直接对依赖这个状态变量的所有测量值进行操作。由于在电力系统中，状态变量与测量值之间的关系是非线性的，由式(2-1)给出。系统的雅可比矩阵 $\boldsymbol{J}_h$ 为：

$$\boldsymbol{J}_h=\begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_{n-1}} & \frac{\partial h_1}{\partial x_n} \\ \frac{\partial h_2}{\partial x_1} & \frac{\partial h_2}{\partial x_2} & \cdots & \frac{\partial h_2}{\partial x_{n-1}} & \frac{\partial h_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial h_{m-1}}{\partial x_1} & \frac{\partial h_{m-1}}{\partial x_2} & \cdots & \frac{\partial h_{m-1}}{\partial x_{n-1}} & \frac{\partial h_{m-1}}{\partial x_n} \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_{n-1}} & \frac{\partial h_m}{\partial x_n} \end{bmatrix} \tag{2-12}$$

式中， m 为测量值的维数； n 为状态变量的维数。

在确定了必须更改哪些测量值之后，下一步要做的就是将这些测量值更改成更改为哪些值。假设攻击者确定了要攻击的状态变量 V_i，那么就需要改变母线 i 和 j 上的潮流，为了找到产生期望潮流的电压幅值，必须求解式(2-3)获得相关的信息。

令 $\boldsymbol{a}=\left[a_1,a_2,\cdots,a_{m-1},a_m\right]^T$ 为攻击向量，将 $\boldsymbol{a}$ 注入到系统后，正常的系统测量值 $\boldsymbol{z}$ 变为 $\boldsymbol{z}_F=\boldsymbol{z}+\boldsymbol{a}$。假设 $\boldsymbol{c}=\left[c_1,c_2,\cdots,c_{n-1},c_n\right]^T$ 为虚假数据攻击向量 $\boldsymbol{a}$ 引起的状态变量的变化量，则攻击发生后的状态估计量变为 $\hat{\boldsymbol{x}}_F=\hat{\boldsymbol{x}}+\boldsymbol{c}$。在攻击发生后，对应的残差 $\boldsymbol{r}_F$ 可以表示为：

$$\begin{aligned} \boldsymbol{r}_F&=\boldsymbol{z}_F-\boldsymbol{h}\left(\hat{\boldsymbol{x}}_F\right) \\ &=\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right) \\ &=\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}\right)+\boldsymbol{a} \\ &=\boldsymbol{z}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}\right) \\ &=\boldsymbol{r} \end{aligned} \tag{2-13}$$

不难发现，在 FDIAs 发生前后，系统残差不发生改变，因此，传统的 BDD 方法无法检测出 FDIAs。

为了进一步说明 FDIAs 的过程，本文通过 IEEE-14 节点和 IEEE-30 节点标

准系统进行仿真验证。

本文所用到的系统数据来源于 Matpwer 7.1，状态变量的真值在潮流方程的基础上利用潮流计算得到最优潮流结果。在模拟阶段的测量中加入标准差为 0.01 的高斯噪声作为测量值。通过对测量数据注入虚假数据，最后利用 WLS 对系统状态该进行估计。

2.4.3 IEEE-14 节点标准系统单节点攻击

电力系统 IEEE-14 节点结构如图 2-3 所示，这里共有 41 个测量值和 27 个状态变量，在正常操作条件下，在确定 BDD 的阈值时，将置信水平设置为 p=0.95，自由度设置为 $m-n$=14，然后使用卡方分布计算检测阈值，得到值为 23.68。

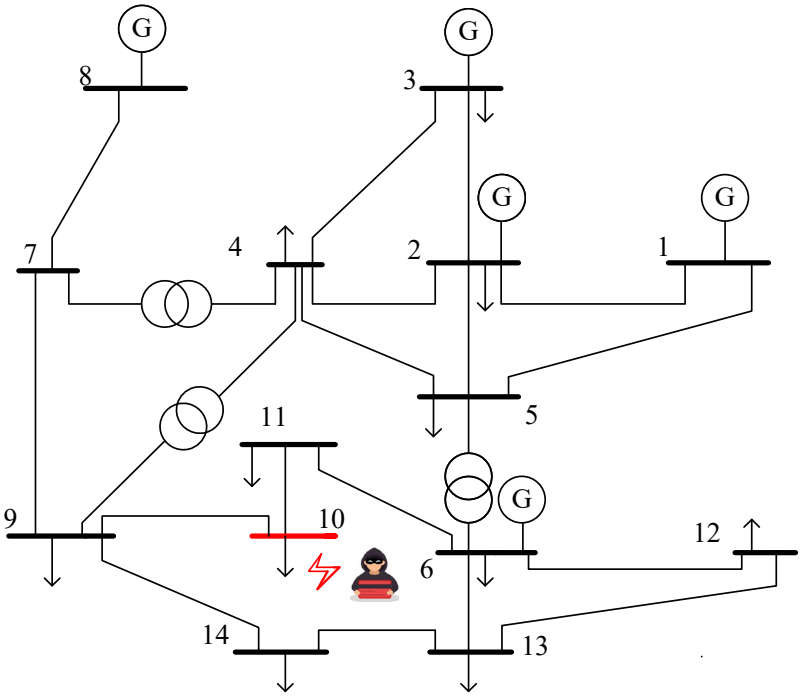


图 2-3 IEEE-14 节点标准系统接线图

在 IEEE-14 节点标准电力系统中，在 $t=200s\sim400s$ 之间，发动单状态攻击，对节点 10 的电压幅值进行攻击，攻击强度为 0.4p.u.。根据式(2-12)确定与 V_{10} 相关的收集到的测量值有 4 个，分别为 P_{10}、P_{11}、Q_{10}、Q_{11}。在对相关测量值进行篡改后，系统中所收集到的测量值分布发生变化，结果如图 2-4 所示。然后根据所收集到的测量值利用 WLS 进行状态估计，结果如图 2-5 和图 2-6 所示。在图 2-5 中，节点 10 的电压幅值发生改变，增大了 0.4p.u.。而在图 2-6 中，系统节点

的相角没有发生明显变化，实现了所设计的攻击目标。

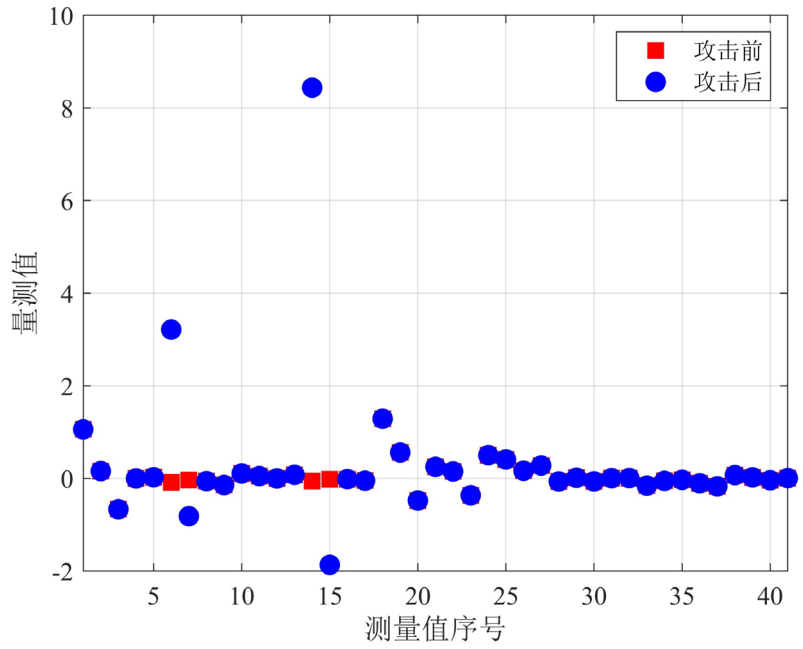


图 2-4 IEEE-14 节点攻击前后测量值分布图

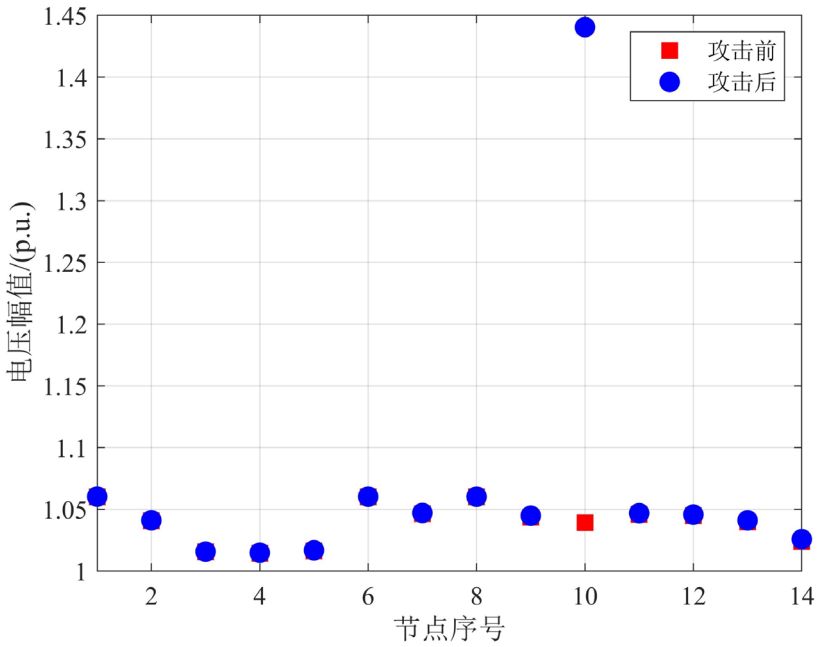


图 2-5 IEEE-14 节点攻击前后电压幅值分布图

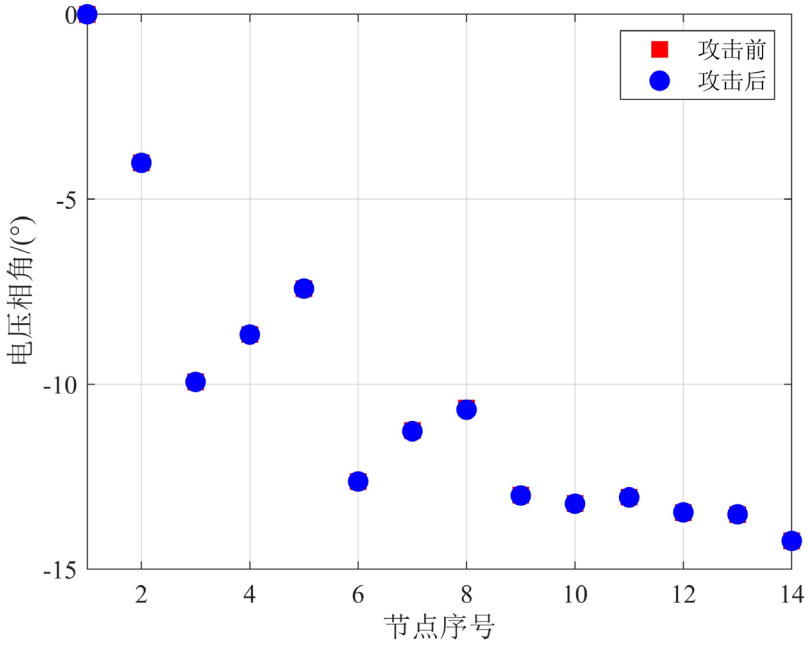


图 2-6 IEEE-14 节点攻击前后电压相角分布图

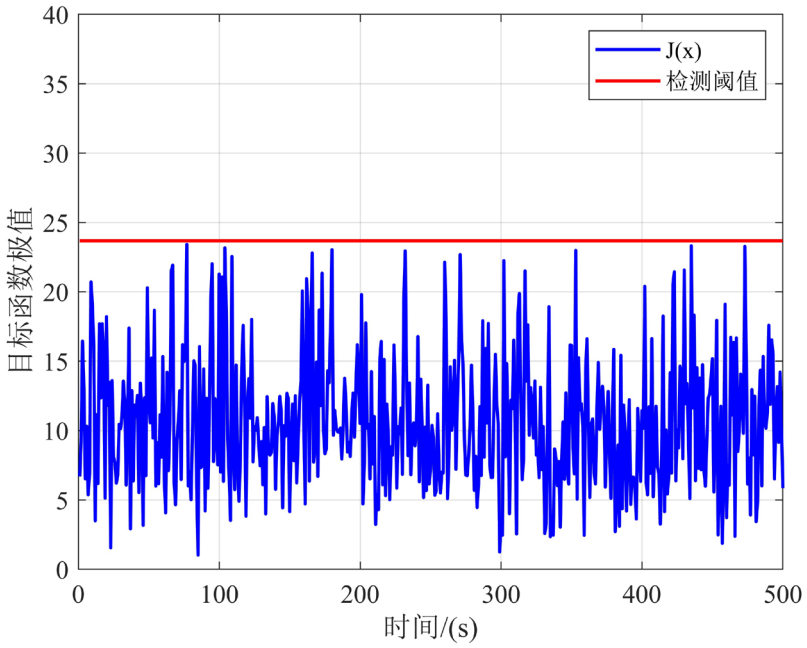


图 2-7 IEEE-14 节点目标函数值变化图

系统发生 FDIAs 后，利用 BDD 机制进行检测，检测结果如图 2-7 所示，在 $t=200s\sim400s$ 之间，目标函数值与攻击发生前分布相同，没有超过其检测阈值，从而说明成功地向系统注入了虚假数据，而 BDD 机制无法检测出系统存在的 FDIAs。

2.4.4 IEEE-30 节点标准系统多节点攻击

对于多状态攻击来说，攻击者需要篡改更多的测量值以此来改变相关的状态量，电力系统 IEEE-30 节点结构如图 2-8 所示，这里共有 93 个测量值和 59 个状态变量，在正常操作条件下，在确定坏数据检验的阈值时，将置信水平设置为 p=0.95，自由度设置为 $m-n$=34，然后使用卡方分布计算检测阈值，得到值为 48.602。

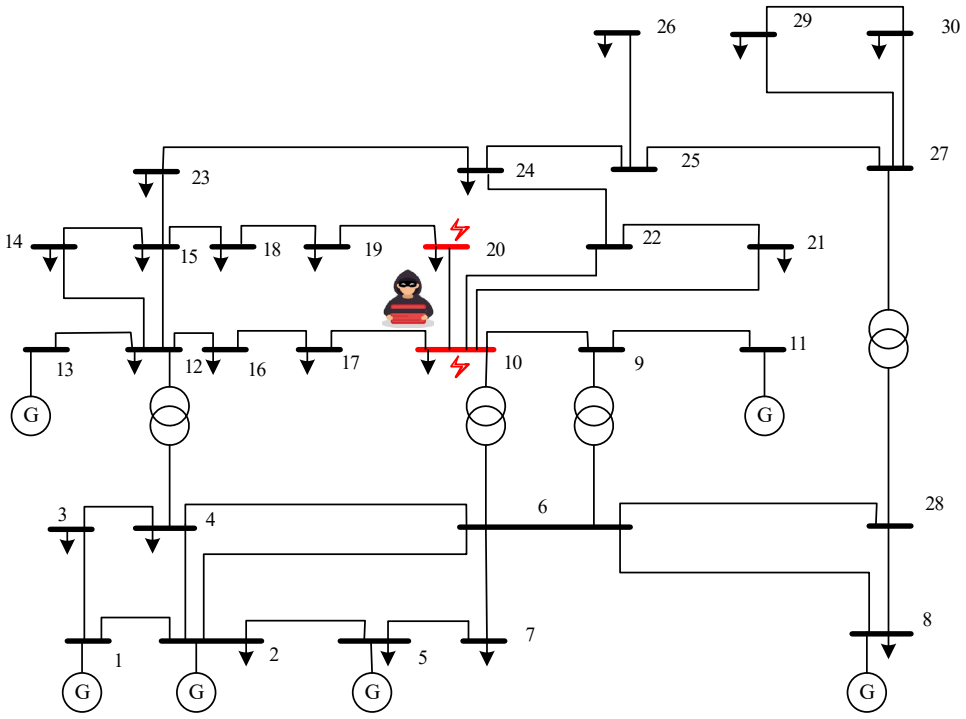


图 2-8 IEEE-30 节点标准系统接线图

在 IEEE-30 节点标准电力系统中，在 $t=200s\sim400s$ 之间，发动多状态攻击，对节点 10 和节点 20 的电压幅值进行攻击，攻击强度为 0.28p.u.。由单节点攻击转向多节点攻击的过程中，随着状态的增多，使得攻击者需要篡改的测量值数目也会增多，这更需要攻击者精心构造攻击向量，隐藏攻击的发生。根据式(2-12)确定与 V_{10}、V_{20} 相关的收集到的测量值有 17 个，分别为 P_{10}、P_{20}、P_{21}、Q_{6}、Q_{10}、Q_{20}、Q_{21}、$P_{17\text{-}10}$、$P_{19\text{-}20}$、$P_{21\text{-}10}$、$P_{22\text{-}10}$、$Q_{10\text{-}6}$、$Q_{10\text{-}9}$、$Q_{17\text{-}10}$、$Q_{19\text{-}20}$、$Q_{21\text{-}10}$、$Q_{22\text{-}10}$。在对相关测量值进行篡改后，系统中所收集到的测量值分布发生变化，结果如图 2-9 所示。然后根据所收集到的测量值利用 WLS 进行状态估计，结果如图 2-10 和图 2-11 所示。在图 2-10 中，节点 10 和节点 20 的电压幅值发生

改变，增大了 0.28p.u.。而在图 2-11 中，系统节点的相角没有发生明显变化，实现了所设计的攻击目标。

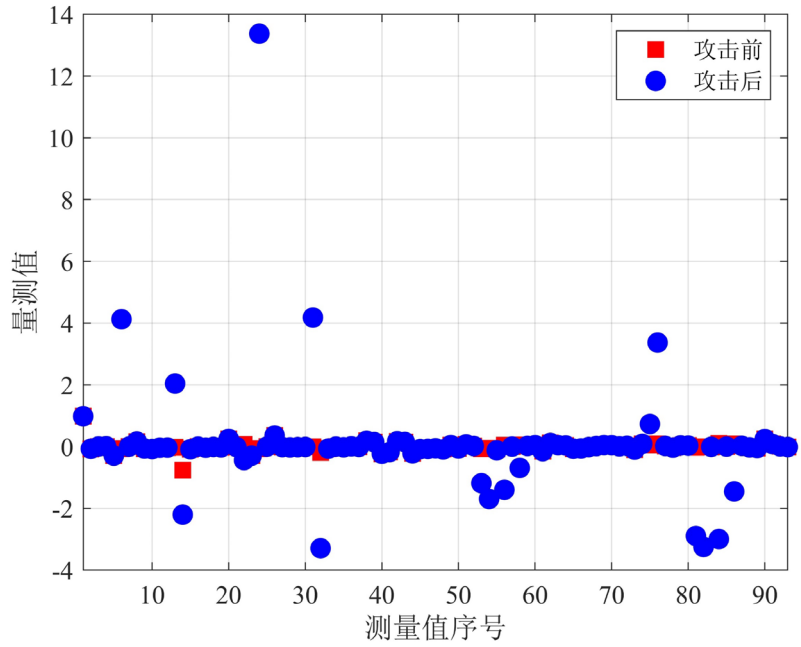


图 2-9 IEEE-30 节点攻击前后测量值分布图

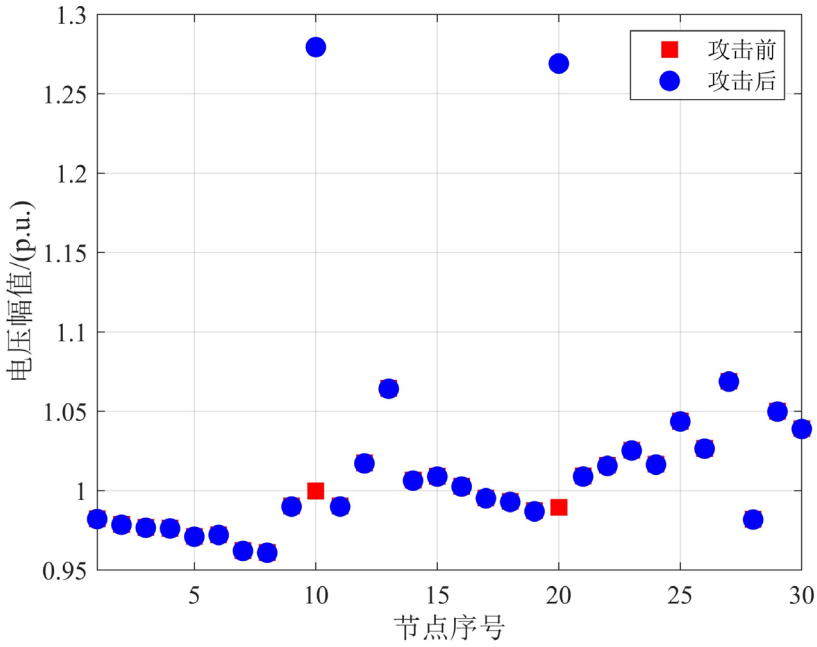


图 2-10 IEEE-30 节点攻击前后电压幅值分布图

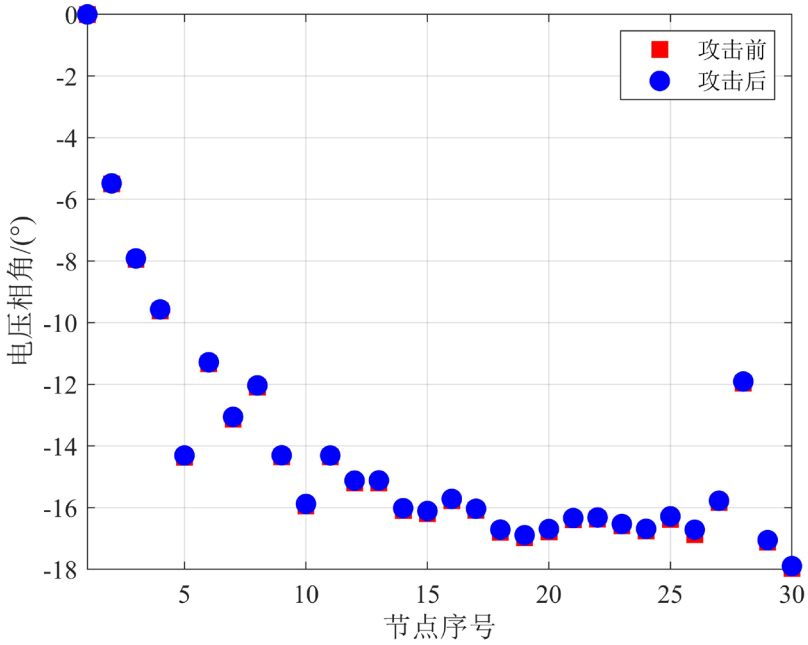


图 2-11 IEEE-30 节点攻击前后电压相角分布图

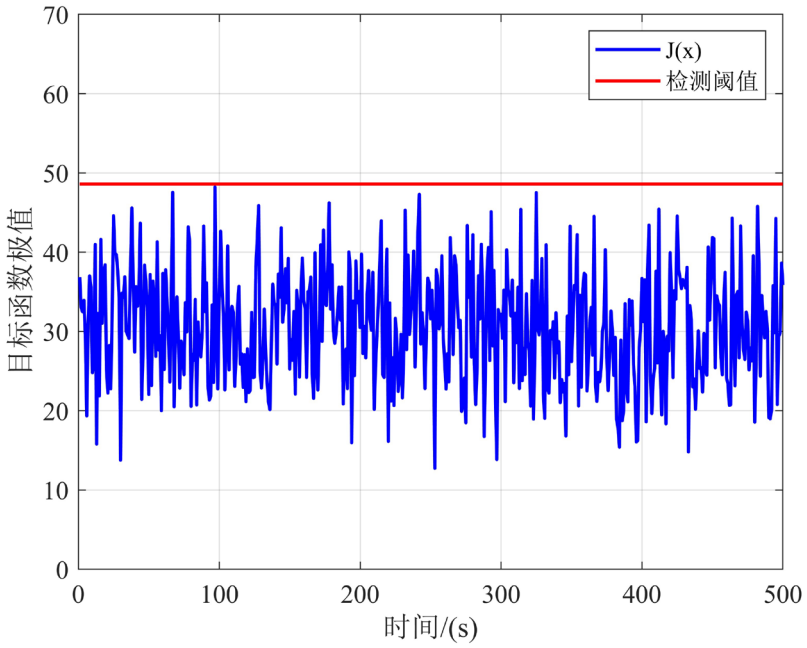


图 2-12 IEEE-30 节点目标函数值变化图

系统发生 FDIAs 后，利用 BDD 机制进行检测，检测结果如图 2-12 所示，在 $t=200s\sim400s$ 之间，目标函数值与攻击发生前分布相同，没有超过其检测阈值，从而说明成功地向系统注入了虚假数据，而 BDD 机制无法检测出系统存在的 FDIAs。

2.5 本章小结

本章建立了电力系统的状态估计模型，阐述了 BDD 机制并分析了 FDIAs 的原理和模型构建。首先，推导了基于 WLS 的电力系统状态估计模型。其次，在完成状态估计的基础上，阐述了 BDD 的原理。最后，阐述了 FDIAs 的原理，从攻击者的角度出发，构建了基于拓扑完整性的 FDIAs 模型，并在 IEEE-14 节点和 IEEE-30 节点标准系统进行不同场景的攻击模拟，以此验证模型的有效性。为后续研究 FDIAs 的检测和定位提供了理论基础。

第3章 基于自适应插值扩展卡尔曼滤波器的 FDIAs 检测

3.1 引言

FDIAs 作为一种针对状态估计的新型网络攻击，攻击者通过操纵传感器、测量设备或数据传输过程中的信息，向系统注入虚假的数据，从而误导系统的状态估计与决策过程。第二章中已经介绍了其攻击原理，并在对其模型的构建进行了深入研究，同时解释了其可以绕过传统的 BDD 机制。因此，当系统遭受 FDIAs 时，如何快速地检测成为保障智能电网稳定运行的重要挑战。

考虑到状态估计是电力系统运行与控制的核心技术，本章使用了基于状态估计的 FDIAs 检测方法。针对传统的 EKF 在进行电力系统状态估计时其估计精度被系统的非线性程度制约，进而影响 FDIAs 的检测问题，提出了一种基于自适应插值扩展卡尔曼滤波器(Adaptive Interpolation Extended Kalman Filter, AIEKF)的 FDIAs 检测方法。通过状态方程和量测方程的非线性程度大小，在此基础上自适应调整在连续测量之间添加的伪测量的数目，减小了非线性对 EKF 估计精度的负面影响。在高度非线性的电力系统中，AIEKF 能够更为准确地估计系统状态。当系统遭受 FDIAs 时，AIEKF 和 WLS 两种估计器的收敛速度不同，利用两者之间的时间差异性，并引入欧式距离作为检测指标，从而来检测 FDIAs。最后，在 IEEE-14 节点和 IEEE-30 节点标准电力系统进行仿真测试，以此来验证所提方法的有效性。

3.2 基于自适应插值扩展卡尔曼滤波器的状态估计

3.2.1 扩展卡尔曼滤波原理

电力系统本质上是一个高度复杂的非线性系统，其动态行为受电压、电流、功率等多种变量的非线性相互作用影响。在这种系统中，状态变量与系统输入输出之间的关系通常难以用线性方程描述。因此，为了准确反映电力系统的动态特性，状态估计需要基于非线性状态方程和测量方程来建模，使得状态估计更具准确性和实用性，具体可以形式化为：

$$\boldsymbol{x}_k = \boldsymbol{f}(\boldsymbol{x}_{k-1}) + \boldsymbol{\omega}_{k-1} \tag{3-1}$$

$$\boldsymbol{z}_k = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{e}_k \tag{3-2}$$

式中，$\boldsymbol{x}_k$ 和 $\boldsymbol{z}_k$ 分别为 k 时刻状态向量和测量向量；$\boldsymbol{f}(.)$ 和 $\boldsymbol{h}(.)$ 分别为状态传递函数和测量函数；$\boldsymbol{\omega}_{k-1}$ 和 $\boldsymbol{e}_k$ 分别为过程噪声和测量噪声，且 $\boldsymbol{\omega}_{k-1} \sim \mathcal{N}(\boldsymbol{0},\boldsymbol{Q})$ 和 $\boldsymbol{e}_k \sim \mathcal{N}(\boldsymbol{0},\boldsymbol{R})$。

在多维且非线性的电力系统中，状态转移函数 $\boldsymbol{f}(.)$ 的确定往往非常困难。在本章中，采用 Holt's 双指数平滑法。Holt's 方法的核心思想是通过平滑技术减小随机噪声对预测结果的影响，从而准确捕捉状态变量的变化趋势，并进行后续的预测。该方法可描述为：

$$\begin{cases} \tilde{\boldsymbol{x}}_{k+1} = \boldsymbol{a}_k + \boldsymbol{b}_k \\ \boldsymbol{a}_k = \alpha \hat{\boldsymbol{x}}_k + (1-\alpha)\tilde{\boldsymbol{x}}_k \\ \boldsymbol{b}_k = \beta\left(\boldsymbol{a}_k - \boldsymbol{a}_{k-1}\right) + (1-\beta)\boldsymbol{b}_{k-1} \end{cases} \tag{3-3}$$

式中，$\boldsymbol{a}_k$ 是水平分量；$\boldsymbol{b}_k$ 是倾斜分量；$\tilde{\boldsymbol{x}}_{k+1}$ 为 $k+1$ 时刻的状态预测量；$\hat{\boldsymbol{x}}_k$ 为 k 时刻的状态估计量；α 和 β 是一对平滑参数，在本章中，设置为 $\alpha = 0.9$，$\beta = 0.4$。

电力系统中的测量函数 $\boldsymbol{h}(.)$ 是用来描述系统的测量值(如电压、电流、功率等)与系统状态变量(如节点电压幅值和相角)之间的关系的数学表达式。测量函数通常是非线性的，因为电力系统的物理特性本质上是非线性的。测量函数在状态估计中扮演着关键角色，将实际测量的数据与系统状态联系起来，使得状态估计器能够根据测量值推算出系统的状态，可以根据上一章式(2-2)获得。

由于 KF 算法只能用于线性系统，不适用于电力系统等非线性问题，因此衍生了 EKF 算法。EKF 算法首先通过泰勒级数展开完成非线性系统的线性化操作，然后使用 KF 算法的相关公式对非线性系统进行估计。具体来说，状态方程式(3-1)在状态估计量 $\hat{\boldsymbol{x}}_{k-1}$ 处进行泰勒级数展开，忽略二次级及以上的项。同样，测量方程式(3-2)在状态预测量 $\tilde{\boldsymbol{x}}_k$ 处进行泰勒级数展开，忽略二次级及以上的项。线性化模型表示为:

$$\begin{aligned}\boldsymbol{x}_k &\approx \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)+\left.\frac{\partial \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)}{\partial \hat{\boldsymbol{x}}_{k-1}}\right|_{\hat{\boldsymbol{x}}_{k-1}}\left(\boldsymbol{x}_{k-1}-\hat{\boldsymbol{x}}_{k-1}\right)+\boldsymbol{\omega}_{k-1} \\ &=\boldsymbol{F}_{k-1}\boldsymbol{x}_{k-1}+\boldsymbol{\omega}_{k-1}+\boldsymbol{u}_{k-1}\end{aligned} \tag{3-4}$$

$$\begin{aligned}\boldsymbol{z}_k &\approx \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)+\left.\frac{\partial \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)}{\partial \tilde{\boldsymbol{x}}_k}\right|_{\tilde{\boldsymbol{x}}_k}\left(\boldsymbol{x}_k-\tilde{\boldsymbol{x}}_k\right)+\boldsymbol{e}_k \\ &=\boldsymbol{H}_k\boldsymbol{x}_k+\boldsymbol{e}_k+\boldsymbol{y}_k\end{aligned} \tag{3-5}$$

式中，$\boldsymbol{F}_{k-1}=\left.\frac{\partial \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)}{\partial \hat{\boldsymbol{x}}_{k-1}}\right|_{\hat{\boldsymbol{x}}_{k-1}}$ 和 $\boldsymbol{H}_k=\left.\frac{\partial \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)}{\partial \tilde{\boldsymbol{x}}_k}\right|_{\tilde{\boldsymbol{x}}_k}$ 分别是 $\boldsymbol{f}(.)$ 和 $\boldsymbol{h}(.)$ 的雅可比矩阵；

$\boldsymbol{u}_{k-1}=\boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)-\left.\frac{\partial \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)}{\partial \hat{\boldsymbol{x}}_{k-1}}\right|_{\hat{\boldsymbol{x}}_{k-1}}\hat{\boldsymbol{x}}_{k-1}$ 和 $\boldsymbol{y}_k=\boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)-\left.\frac{\partial \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)}{\partial \tilde{\boldsymbol{x}}_k}\right|_{\tilde{\boldsymbol{x}}_k}\tilde{\boldsymbol{x}}_k$ 均为外作用项。

经过式(3-4)和(3-5)就完成了系统的线性化。接着，利用 KF 的步骤进行状态估计，便可得到 EKF 的滤波步骤。EKF 滤波公式具体如下：

- 预测步骤：

$$\tilde{\boldsymbol{x}}_{k|k-1}=\boldsymbol{F}_{k-1}\hat{\boldsymbol{x}}_{k-1} \tag{3-6}$$

$$\tilde{\boldsymbol{P}}_{k|k-1}=\boldsymbol{F}_{k-1}\hat{\boldsymbol{P}}_{k-1}\boldsymbol{F}_{k-1}^{T}+\boldsymbol{Q}_{k-1} \tag{3-7}$$

- 更新步骤：

$$\boldsymbol{K}_k=\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{H}_k{}^{T}(\boldsymbol{H}_k\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{H}_k{}^{T}+\boldsymbol{R}_k)^{-1} \tag{3-8}$$

$$\hat{\boldsymbol{x}}_k=\tilde{\boldsymbol{x}}_{k|k-1}+\boldsymbol{K}_k\left[\boldsymbol{z}_k-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right] \tag{3-9}$$

$$\hat{\boldsymbol{P}}_k=\left(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H}_k\right)\tilde{\boldsymbol{P}}_{k|k-1} \tag{3-10}$$

式中，$\tilde{\boldsymbol{x}}$ 和 $\hat{\boldsymbol{x}}$ 分别表示状态变量的预测量和估计量；$\boldsymbol{I}$ 是单位矩阵；$\tilde{\boldsymbol{P}}$ 和 $\hat{\boldsymbol{P}}$ 分别表示状态协方差矩阵的预测量和估计量；$\boldsymbol{Q}$ 和 $\boldsymbol{R}$ 分别是过程噪声和测量噪声误差向量的协方差矩阵；$\boldsymbol{K}$ 是卡尔曼增益。

由于忽略泰勒级数中的高阶项所引入的线性化误差，只有状态转移函数 $\boldsymbol{f}(.)$ 和测量函数 $\boldsymbol{h}(.)$ 为线性或拟线性时，EKF 才倾向于保持其最优估计精度。对于一

个被认为是线性或准线性的系统，线性化误差与过程和测量噪声的方差相比应该是微不足道的。然而，当电力系统的非线性严重时，由于 EKF 算法忽略了泰勒展开过程中的高阶项，从而导致线性化过程带来较大误差，使得估计效果下降[66]。

3.2.2 自适应插值策略

本节引入了一种自适应插值策略，该方法根据非线性水平自适应调整插值因子，具体来说，当非线性程度较高时，增大插值因子 r 提高估计精度，当系统非线性较低时，减小插值因子 r，在减少计算时间的前提下保持估计精度。该策略包括三个关键步骤。首先，使用非线性指标量化状态转移函数 $\boldsymbol{f}(.)$ 和测量函数 $\boldsymbol{h}(.)$ 的非线性水平。在下一步中，根据第一步中计算的非线性指标，利用有限状态机(Finite State Machine, FSM)模型确定插值因子 r。最后，通过线性插值在两次实际测量之间插入伪测量，以减轻非线性的不利影响。

根据式(3-4)，状态转移函数 $\boldsymbol{f}(\boldsymbol{x})$ 的非线性指标 η_f 为：

$$\boldsymbol{\varepsilon}_f = \boldsymbol{x}_k - \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right) - \left.\frac{\partial \boldsymbol{f}\left(\hat{\boldsymbol{x}}_{k-1}\right)}{\partial \hat{\boldsymbol{x}}_{k-1}}\right|_{\hat{\boldsymbol{x}}_{k-1}} \left(\boldsymbol{x}_{k-1} - \hat{\boldsymbol{x}}_{k-1}\right) \tag{3-11}$$

$$\eta_f = \boldsymbol{\varepsilon}_f{}^T \boldsymbol{Q}_k^{-1} \boldsymbol{\varepsilon}_f \tag{3-12}$$

式中，$\boldsymbol{\varepsilon}_f$ 是状态转移函数 $\boldsymbol{f}(\boldsymbol{x})$ 泰勒展开时忽略的误差。

类似地，根据式(3-5)，测量函数 $\boldsymbol{h}(\boldsymbol{x})$ 的非线性指标 η_h 为：

$$\boldsymbol{\varepsilon}_h = \boldsymbol{z}_k - \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right) - \left.\frac{\partial \boldsymbol{h}\left(\tilde{\boldsymbol{x}}_k\right)}{\partial \tilde{\boldsymbol{x}}_k}\right|_{\tilde{\boldsymbol{x}}_k} \left(\boldsymbol{x}_k - \tilde{\boldsymbol{x}}_k\right) \tag{3-13}$$

$$\eta_h = \boldsymbol{\varepsilon}_h{}^T \boldsymbol{R}_k^{-1} \boldsymbol{\varepsilon}_h \tag{3-14}$$

式中，$\boldsymbol{\varepsilon}_h$ 是测量函数 $\boldsymbol{h}(\boldsymbol{x})$ 泰勒展开时忽略的误差。

如式(3-12)和式(3-14)所示，$\boldsymbol{\varepsilon}_f$ 和 $\boldsymbol{\varepsilon}_h$ 被 $\boldsymbol{Q}_k$ 和 $\boldsymbol{R}_k$ 归一化。在此过程中，η_f 和 η_h 在数值上是非负的。因此，当 $\boldsymbol{\varepsilon}_f \ll \boldsymbol{Q}_k$ 和 $\boldsymbol{\varepsilon}_h \ll \boldsymbol{R}_k$，则 $\eta_f \ll 1$ 和 $\eta_h \ll 1$，此时可以认

为状态转移函数和测量函数是准线性的。否则，必须根据插值因子r的大小，添加伪测量值。需要注意的是，当添加伪测量值时，采样率会增加，从而使得状态量的扰动减小，因此系统的非线性程度减小。

综上所述，自适应插值策略包括以下三个子步骤：

(1)利用式(3-11)-(3-14)进行计算状态转移函数和测量函数的非线性指标。

(2)根据η_f和η_h确定插值因子并利用 FSM 进行管理。

(3)通过线性插值在两个连续的测量之间插入r个伪测量值。

在第二个步骤中，本文以一个四状态的 FSM 模型来阐述基本原理，需要注意的是，为了将非线性指标带入预先设定的范围，FSM 的状态可以有任何多个。如图 3-1 所示，是一个四状态的 FSM 模型，设i为 FSM 的状态索引，在有限状态机每个状态i中，均包含三个参数，分别为插值因子r_i、阈值上限U_i、阈值下限L_i。

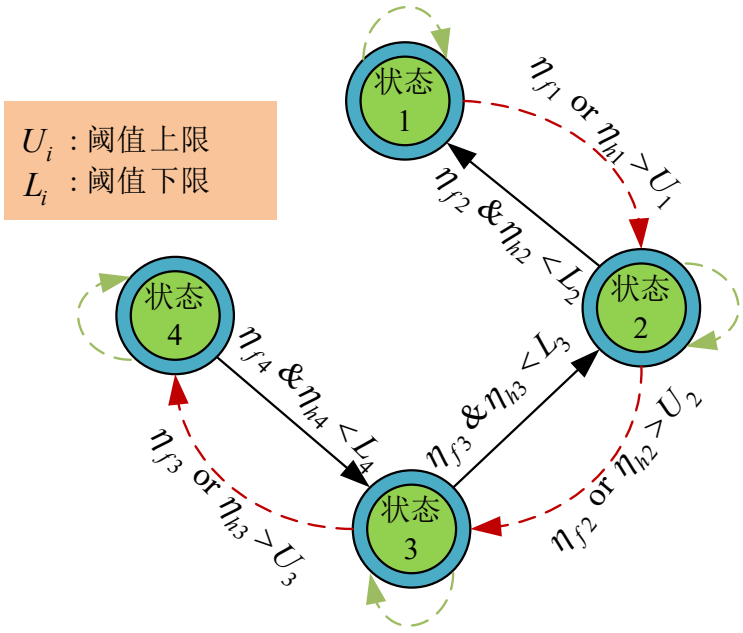


图 3-1 有限状态机(四个状态)

其中，η_{fi}和η_{hi}分别为状态方程和测量方程的非线性指标，这两个非线性指标可能是不相关的。

在任意一个状态i，阈值之间的关系都应满足阈值上限大于阈值下限，即

$U_i > L_i$，且不同状态的插值因子应满足$r_{i+1} > r_i$，状态i越高，关联的插值因子r越大。插值因子r与η_f和η_h的大小密切相关，非线性指标η_f和η_h越大，插值因子r越大。相反，非线性指标η_f和η_h越小，插值因子r较小。需要强调的是，当$\eta_f = 0$和$\eta_h = 0$，表明系统为线性系统，不需要进行插值。插值因子r的选择伪代码如表 3-1 所示

表 3-1 插值因子选择的伪代码

算法：选择插值因子
状态i　　$r = r_i$
if $\eta_{fi} > U_i$ or $\eta_{hi} > U_i$ then
前往下一个状态 $i+1$
else
$\eta_{fi} < L_i$ and $\eta_{hi} < L_i$
前往上一个状态 $i-1$
end if
保持当前状态i

如果要运行 FSM，应该从 FSM 的状态 1 开始，计算状态非线性指标η_f和测量非线性指标η_h。如果两者都小于U_i，则 FSM 将停留在状态 1。否则，FSM 将向前移动一步到状态 2，有一个更大的r来减少η_f和η_h。r可以这样设置，即 FSM 每向前移动一步，有效采样率就会翻倍。FSM 将继续加倍有效采样率，直到η_f和η_h都低于U_i或达到最大采样率。当考虑计算时间时，可用计算资源允许的最大采样率决定允许的最大r。

另一方面，如果η_f和η_h都小于L_i，则 FSM 将后退一步到具有较小r的状态，这将使有效采样率降低 50%。这是运行 FSM 的一种工程方法，可以根据其应用程序和可用计算资源的需要对其进行调整，根据文献[66]中的定义，各状态下的

r 的具体值见表 3-2。

表 3-2 四个不同状态下的插值数目

状态 i	插值因子 r	阈值下限 L	阈值上限 U
$i=1$	1	L_1	U_1
$i=2$	3	L_2	U_2
$i=3$	7	L_3	U_3
$i=4$	15	L_4	U_4

3.2.3 基于自适应插值扩展卡尔曼滤波器的状态估计

AIEKF 结合了传统的 EKF 和自适应插值策略，可以有效地平衡计算时间和估计精度，从而提高 EKF 在电力系统中的估计精度。AIEKF 的算法流程图如图 3-2 所示，包括自适应插值步骤和 EKF 算法步骤：

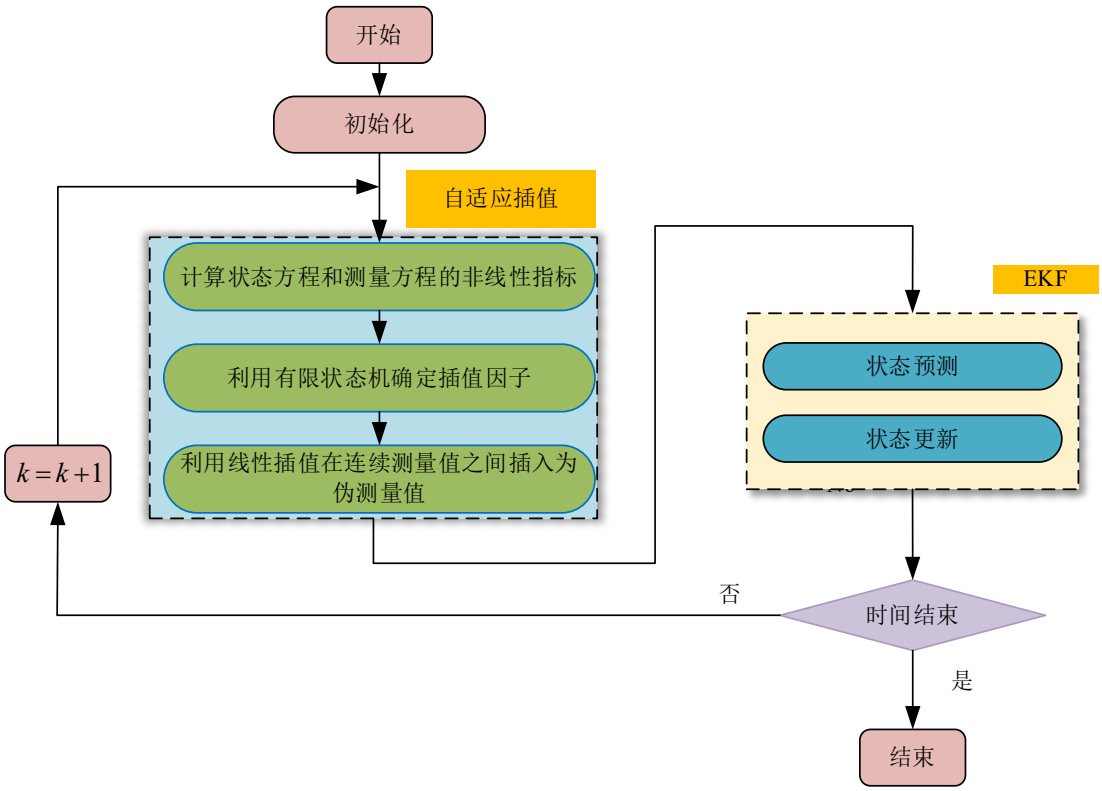


图 3-2 AIEKF 算法流程图

(1)初始化：设置初始状态变量 $\hat{\boldsymbol{x}}_0$ 和状态协方差矩阵 $\hat{\boldsymbol{P}}_0$ 。

(2)自适应插值：为了在计算效率和估计精度之间取得折衷，该算法引入了自

适应插值策略，该策略包括三个关键步骤。首先，分别使用式(3-11)-(3-14)计算状态转移函数和测量函数的非线性指标η_f和η_h。在下一步中，在四状态的 FSM 模型的基础上确定插值因子r。最后，通过线性插值在两次实际测量之间引入r次伪测量，以减轻非线性的不利影响。

(3)在确定插值因子个数r的基础上，利用 EKF 算法对电力系统进行估计。首先，利用$k-1$时刻的状态及其协方差矩阵，根据式(3-6)和式(3-7)推导出k时刻的先验估计。其次，对先验估计进行校正，根据式(3-8)-(3-10)得到后验估计。

3.3 算法收敛性分析

AIEKF 通过计算两个非线性指标η_f和η_h，量化系统的非线性程度。在系统接近线性或准线性时，EKF 线性化展开引入的误差相对较小，从而使得 EKF 更能准确地跟踪系统的真实状态，避免因误差累积导致估计结果偏离真实值，为滤波的收敛创造了有利条件。

当η_f或η_h大于U_i时，AIEKF 算法会在连续实际测量值之间添加更多伪测量值。从信息论的角度看，当r增大时，有效采样率高，即相当于增加了系统的观测信息，滤波器获得了更多关于系统状态的信息，最终使得系统状态的扰动减小，系统更接近线性情况，有利于滤波收敛。

设$\varsigma_k=\boldsymbol{x}_k-\hat{\boldsymbol{x}}_k$为状态估计偏差，构建李雅普诺夫函数$\boldsymbol{V}\left(\varsigma_k\right)=\varsigma_k^T\boldsymbol{P}_k^{-1}\varsigma_k$，利用李雅普诺夫函数衡量系统状态偏离平衡状态。

对李雅普诺夫函数求关于时间的导数$\dot{\boldsymbol{V}}\left(\varsigma_k\right)$，首先把$\varsigma_k=\boldsymbol{x}_k-\hat{\boldsymbol{x}}_k$展开：

$$\varsigma_k=\boldsymbol{x}_k-\tilde{\boldsymbol{x}}_{k|k-1}+\boldsymbol{K}_k\left[z_k-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]=\varsigma_{k|k-1}-\boldsymbol{K}_k\left[\boldsymbol{h}(\boldsymbol{x}_k)+\boldsymbol{e}_k-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right] \tag{3-15}$$

然后计算$\boldsymbol{V}\left(\varsigma_k\right)$：

$$\begin{aligned}\boldsymbol{V}\left(\varsigma_k\right)=&\left(\varsigma_{k|k-1}-\boldsymbol{K}_k\left[\boldsymbol{h}(\boldsymbol{x}_k)+\boldsymbol{e}_k-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]\right)^T\left(\left(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H}_k\right)\tilde{\boldsymbol{P}}_{k|k-1}\right)^{-1}\\&\left(\varsigma_{k|k-1}-\boldsymbol{K}_k\left[\boldsymbol{h}(\boldsymbol{x}_k)+\boldsymbol{e}_k-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]\right)\end{aligned} \tag{3-16}$$

利用矩阵求逆原理可得：

$$\left(\left(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H}_k\right)\tilde{\boldsymbol{P}}_{k|k-1}\right)^{-1}=\tilde{\boldsymbol{P}}_{k|k-1}^{-1}+\tilde{\boldsymbol{P}}_{k|k-1}^{-1}\boldsymbol{K}_k\left(\boldsymbol{I}-\boldsymbol{H}_k\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{K}_k\right)^{-1}\tilde{\boldsymbol{P}}_{k|k-1}^{-1} \tag{3-17}$$

将其带入式(3-16)，同时考虑到测量噪声 $\boldsymbol{e}_k$ 的性质（$E\left(\boldsymbol{e}_k\right)=0, E\left(\boldsymbol{e}_k\boldsymbol{e}_k^T\right)=\boldsymbol{R}_k$）以及卡尔曼增益 $\boldsymbol{K}$ 的性质，经过一系列推导可得：

$$\begin{aligned}\boldsymbol{V}\left(\varsigma_k\right)-\boldsymbol{V}\left(\varsigma_{k|k-1}\right)=&-\left[\boldsymbol{h}(\boldsymbol{x}_k)-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]^T\left(\boldsymbol{H}_k\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{H}_k^T+\boldsymbol{R}_k\right)^{-1}\\&\left[\boldsymbol{h}(\boldsymbol{x}_k)-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]-tr\left(\boldsymbol{K}_k\boldsymbol{R}_k\boldsymbol{K}_k^T\tilde{\boldsymbol{P}}_{k|k-1}^{-1}\right)\end{aligned} \tag{3-18}$$

由于 $\left(\boldsymbol{H}_k\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{H}_k^T+\boldsymbol{R}_k\right)^{-1}$ 和 $\tilde{\boldsymbol{P}}_{k|k-1}^{-1}$ 都是正定矩阵，且 $\left[\boldsymbol{h}(\boldsymbol{x}_k)-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]^T\left(\boldsymbol{H}_k\tilde{\boldsymbol{P}}_{k|k-1}\boldsymbol{H}_k^T+\boldsymbol{R}_k\right)^{-1}\left[\boldsymbol{h}(\boldsymbol{x}_k)-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}\right]\geq 0$，$tr\left(\boldsymbol{K}_k\boldsymbol{R}_k\boldsymbol{K}_k^T\tilde{\boldsymbol{P}}_{k|k-1}^{-1}\right)\geq 0$，所以可得：

$$\boldsymbol{V}\left(\varsigma_k\right)-\boldsymbol{V}\left(\varsigma_{k|k-1}\right)\leq 0 \tag{3-19}$$

当且仅当 $\boldsymbol{h}(\boldsymbol{x}_k)-\boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}$ 且 $\boldsymbol{K}_k=0$ (理想状态)时取等号，即：

$$\boldsymbol{V}\left(\varsigma_k\right)<\boldsymbol{V}\left(\varsigma_{k|k-1}\right) \tag{3-20}$$

从而，

$$\dot{\boldsymbol{V}}\left(\varsigma_k\right)<0 \tag{3-21}$$

这表明随着时间推移，李亚普诺函数值不断减小。根据李亚普诺稳定性理论，稳定系统的状态会趋向于平衡状态，即在滤波器中估计误差趋向于零，即 AIEKF 的估计结果收敛到真实状态。

3.4 基于自适应插值扩展卡尔曼滤波器的 FDIAs 检测

在电力系统的正常运行中，由于设备故障、传输误差或其他偶然因素引发的数据异常，通常会通过基于残差分析的 BDD 方法被有效识别和剔除。这是因为在系统故障或误差发生时，残差值会出现明显的偏离，传统的 BDD 算法能够通过监测这一偏差来准确定位异常数据。然而，FDIAs 经过精心设计，其攻击向量可以使得量测数据在攻击前后所产生的残差几乎保持不变，从而使得残差检测方法难以察觉到异常。由于攻击者能够操控量测数据使得残差依旧在正常范围内，传统的基于残差的检测手段无法有效区分正常误差和攻击行为，这使得 FDIAs 能

够绕过经典的 BDD 机制，对电力系统的安全性构成重大威胁。

智能电网具有高度非线性特征，WLS 和 EKF 等状态估计方法的估计精度会有所下降。为了提高检测算法的准确性，利用所提出的 AIEKF 算法求解系统中各节点的状态变量。一旦攻击者开始对测量仪器进行篡改，式(3-9)的结果与之前的结果不同，表示为：

$$\begin{aligned}\hat{\boldsymbol{x}}_k^f &= \tilde{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k + \boldsymbol{a}_k - \boldsymbol{H}_k\tilde{\boldsymbol{x}}_{k|k-1}] \\ &= \hat{\boldsymbol{x}}_k + \boldsymbol{K}_k\boldsymbol{a}_k\end{aligned} \tag{3-22}$$

式中，$\hat{\boldsymbol{x}}_k^f$ 为 FDIAs 后的估计状态。为了更好地方便估计，引入 $\boldsymbol{c}_k = \hat{\boldsymbol{x}}_k^f - \hat{\boldsymbol{x}}_k$。那么，对于下一时刻 $k+1$，可以表示为：

$$\begin{aligned}\hat{\boldsymbol{x}}_{k+1}^f &= \tilde{\boldsymbol{x}}_{k+1|k}^f + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1}^f - \boldsymbol{H}_{k+1}\tilde{\boldsymbol{x}}_{k+1|k}^f] \\ &= \tilde{\boldsymbol{x}}_{k+1|k}^f + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1} + \boldsymbol{a}_{k+1} - \boldsymbol{H}_{k+1}\tilde{\boldsymbol{x}}_{k+1|k}^f] \\ &= \hat{\boldsymbol{x}}_{k+1} + \left[\boldsymbol{I} - \boldsymbol{K}_{k+1}\boldsymbol{H}_{k+1}\right]\boldsymbol{F}_k\boldsymbol{c}_k + \boldsymbol{K}_{k+1}\boldsymbol{a}_{k+1}\end{aligned} \tag{3-23}$$

从公式可以看出，电力系统的状态估计不仅取决于当前时刻注入的虚假数据 $\boldsymbol{a}_k$，还受到之前估计状态中的偏差 $\boldsymbol{c}_k$ 的影响。具体来说，在更新后的状态估计公式中，虚假数据注入产生的偏差会通过卡尔曼增益矩阵进行整合，并与之前的估计状态进行叠加。因此，注入偏差不仅是当前时刻单次注入行为的结果，更是多次注入积累的体现。随着时间的推移，注入的虚假数据偏差将逐渐影响系统的整体状态估计，最终导致系统的估计状态偏离真实状态。

WLS 和 AIEKF 作为电网状态估计的两种常用方法，虽然在应用场景中都有良好的表现，但静态估计与动态估计的内在机理存在显著差异。WLS 通过对当前系统的测量数据进行加权最小化处理，实时估计电网状态，其核心思想是在每个时间步基于当前的测量值得到一个最优估计。当 FDIAs 发生时，由于 WLS 直接依赖于当前量测值，其估计量将会迅速受到注入数据的影响，导致估计结果偏离实际状态，向攻击后的状态变量快速收敛。这种对量测数据的高依赖性使得 WLS 在面对 FDIAs 时，容易受到干扰，且估计结果会随机波动，难以抵御攻击的影响。

与此不同，AIEKF 不仅依赖于当前的观测数据，还结合了历史信息所生成的预测数据，从而对系统状态进行实时动态估计。AIEKF 的滤波过程在每个时间步

中将系统的先验估计(即预测值)与实时量测数据(即观测值)进行综合处理，更新后的状态估计值由这两者共同决定。因此，当 FDIAs 发生时，AIEKF 的估计量不会立刻完全偏向被攻击的状态值，而是会由于先验估计的影响，保持一定的延迟和缓冲，使得攻击的影响在短期内被部分抑制。这种机理使得 AIEKF 在面对虚假数据注入时表现出一定的抗干扰能力，尤其是在攻击初期，能够减缓估计值向攻击状态偏移的速度。

基于 WLS 和 AIEKF 在面对 FDIAs 时不同的响应特性，可以提出一种基于 AIEKF 的 FDIAs 检测方法。具体而言，由于 WLS 在攻击发生后迅速对攻击数据做出反应，而 AIEKF 则因为综合考虑了预测值和观测值，表现出相对的延迟性，这种时间上的差异为 FDIAs 的检测提供了一个有效的信号。通过监控两种估计器在同一时刻对状态估计的反应，并分析其估计结果之间的偏差，可以及时识别出 FDIAs 的发生。

在一致性检验中，引入欧氏距离作为判别依据，可以显著提升检测的准确性和可靠性。欧氏距离是一种衡量两个点之间距离的标准度量工具，通过计算 WLS 估计值与 AIEKF 估计值之间的欧氏距离，可以量化两者在不同时间步的估计差异。当系统处于正常运行状态时，由于两种估计方法都能够有效反映电网的真实状态，其估计值应当非常接近，对应的欧氏距离也应较小。然而，当 FDIAs 发生时，由于 WLS 估计量受到虚假数据的快速影响，而 AIEKF 具有一定的延迟和缓冲，两者的估计结果将产生显著差异，从而导致欧氏距离急剧增大，这种欧氏距离的动态变化可以作为检测 FDIAs 的重要指标，定义 k 时刻的欧式距离如下所示：

$$d\left(k\right)=\sqrt{\sum_{i=1}^{n}\left(\hat{\boldsymbol{x}}_{i,k}^{WLS}-\hat{\boldsymbol{x}}_{i,k}^{AIEKF}\right)^{2}} \tag{3-24}$$

式中，$\hat{\boldsymbol{x}}_{i,k}^{WLS}$ 是 k 时刻 WLS 的估计值；$\hat{\boldsymbol{x}}_{i,k}^{AIEKF}$ 是 k 时刻 AIEKF 的估计值；n 是状态向量的维数。

通过对比状态量之间欧氏距离 $d\left(k\right)$ 与一致性检测阈值 τ，当 $d\left(k\right)\geq\tau$ 时，判定系统发生 FDIAs；相反，当 $d\left(k\right)<\tau$ 时，则认为没有发生 FDIAs。

在 3.2.1 小节中提到，AIEKF 的预测值采用 Holt's 两参数法计算，当系统中

出现发电机或负荷突变时，可能会导致$d\left(k\right)\geq\tau$，增加系统的误报。因此，在一致性检验步骤后增加 BDD，可以使得 FDIAs 的检测更加准确，与传统的 BDD 不同，其公式如下：

$$J(k)=\left\|\boldsymbol{z}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}^{AIEKF}\right)\right\|_2 \tag{3-25}$$

在一致性检验的基础上，通过将$J(k)$与 BDD 阈值τ_b进行比较，以此来判定系统是否发生 FDIAs。当$d\left(k\right)\geq\tau$，且$J(k)\geq\tau_b$时，系统存在 FDIAs。反之，当$d\left(k\right)\geq\tau$，且$J(k)<\tau_b$，系统不存在 FDIAs，间接说明系统存在发电机或负载突变等不良数据。基于 AIEKF 的 FDIAs 检测流程图如图 3-3 所示。

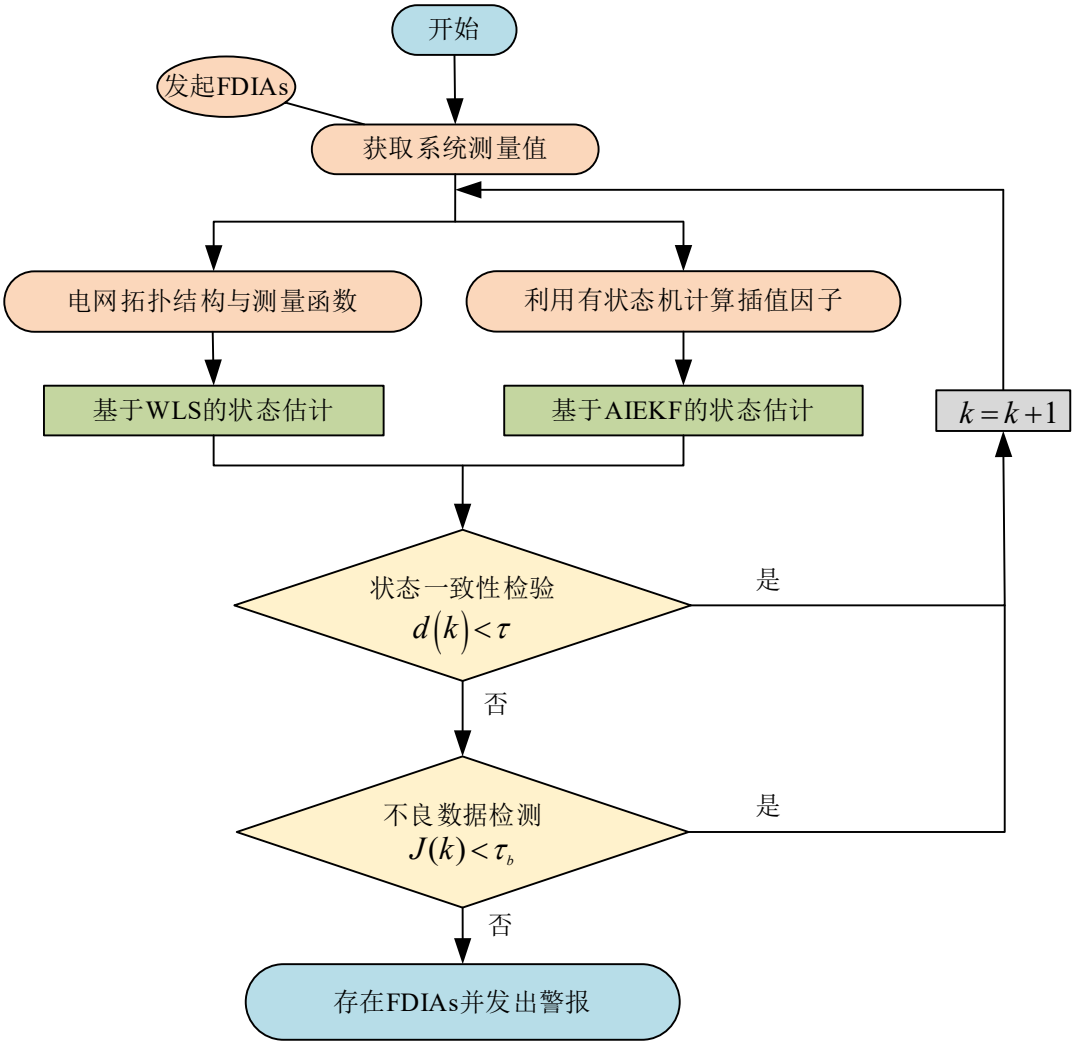


图 3-3 基于 AIEKF 的 FDIAs 检测流程图

3.5 仿真设计与结果分析

本章利用 Matlab2021b 和 Matpower 7.1 进行仿真分析。Matpower 通过构建电力系统的潮流方程(基于节点导纳矩阵和功率平衡方程)来计算各节点的状态。这些方程将系统的拓扑结构、线路参数、发电机输出和负荷需求联系在一起。主要采用牛顿-拉夫森法等迭代算法来求解这些非线性方程。算法从初始猜测的电压值开始，通过迭代调整节点的电压幅值和相位角，逐步减少功率不平衡，直到达到收敛条件，最终计算出各节点电压幅值与电压相角。在此基础上，叠加均值为零的高斯白噪声作为量测数据。

实验内容分为两个部分：AIEKF 性能分析和 IEEE 系统的 FDIAs 检测验证。首先，分析 AIEKF 的估计性能是为了说明其估计的准确性，准确的状态估计更有利于 FDIAs 的检测；接着，在 IEEE-14 节点和 IEEE-30 节点标准电力系统进行 FDIAs 检验的验证，从而说明本文所算法的有效性。

3.5.1 AIEKF 性能分析

为了验证本文引入的 AIEKF 算法在状态估计中的有效性，使用均方根误差(Root Mean Square Error, RMSE)作为度量来评估算法估计的准确性。均方根误差的计算公式如下：

$$RMSE=\sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\boldsymbol{x}_i-\hat{\boldsymbol{x}}_i\right)^2} \tag{3-26}$$

式中，$\boldsymbol{x}_i$ 是状态变量真值的第 i 个分量，$\hat{\boldsymbol{x}}_i$ 是状态变量估计的第 i 个分量，N 是状态变量的维数。

在电网正常运行时，负荷是不断变化的。为了模拟实时电网状态，在 Matlab 中修改负荷数据，从而使得节点状态是不断波动的。在 IEEE-14 节点标准电力系统中采用不同算法进行状态估计，采样时间为 60min，每隔 1min 做一次状态估计并统计其估计结果。为了更清晰地观察估计结果，随机选取节点 11 进行分析。在电网正常运行下，分别利用 WLS、EKF、AIEKF 对节点状态进行状态估计，结果如图 3-4 和图 3-5 所示。

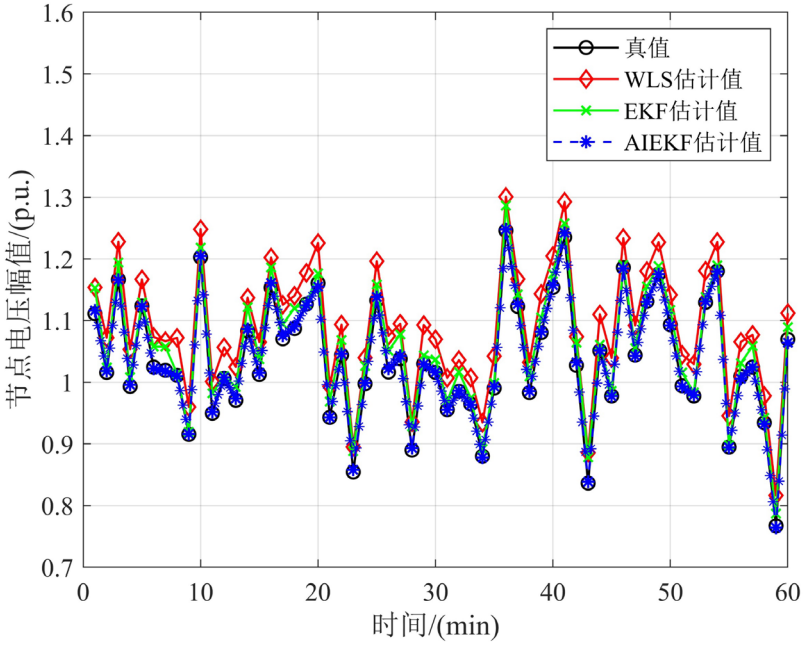


图 3-4 节点 11 电压幅值估计结果

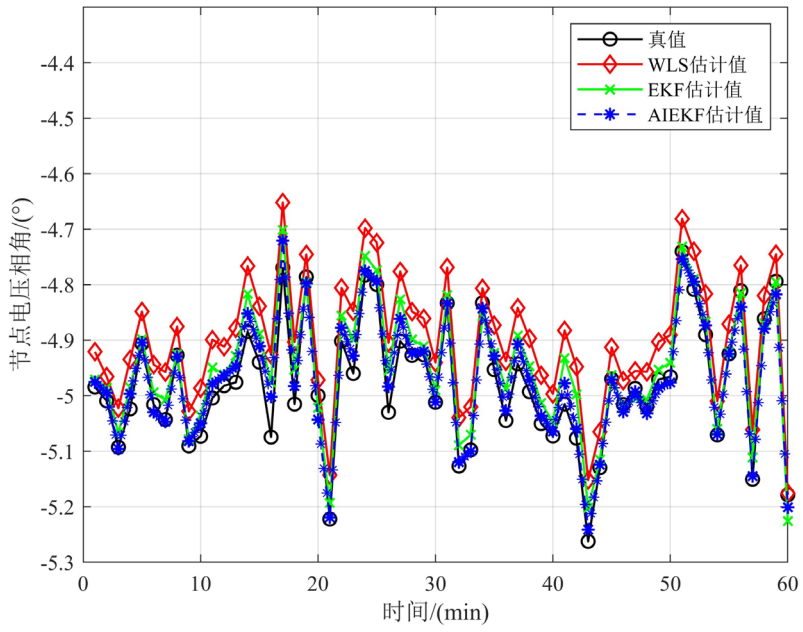


图 3-5 节点 11 电压相角估计结果

RMSE 是衡量某个节点状态量估计精度的关键指标，其数值大小与算法性能呈负相关。为客观评价不同算法的估计性能差异，在系统达到稳态后随机选取状态估计样本点，统计、整理实验数据如表 3-3 所示。

表 3-3 三种算法的性能对比

算法	RMSE	仿真时间(s)
WLS	0.069	1.36
EKF	0.033	1.67
AIEKF	0.016	2.25

由图 3-4、图 3-5 可知以及表 3-3 可知，AIEKF 算法的性能要优于 WLS 和 EKF。虽然 AIEKF 算法所用的仿真时间相对于 EKF 来说较长，但是相差不大。因此，在当进行 FDIAs 检测时，AIEKF 能提供更精确的估计，从而提高 FDIAs 检测精度。

3.5.2 IEEE-14 节点标准系统的 FDIAs 检测

本节所使用的 FDIAs 向量是根据第二章所介绍的原理生成，利用本章提出的算法在 IEEE-14 节点标准电力系统中进行 FDIAs 检测。IEEE-14 节点标准电力系统如图 2-3 所示，共有 14 个节点，5 个发电机，20 条支路，其中支路数据如表 3-4 所示。

表 3-4 IEEE-14 节点标准电力系统支路数据表

起始节点	终止节点	电阻(R)	电抗(X)	电纳(B/2)
1	2	1.938×10^{-2}	5.917×10^{-2}	2.64×10^{-2}
1	5	5.403×10^{-2}	2.2304×10^{-1}	2.64×10^{-2}
2	3	4.699×10^{-2}	1.9797×10^{-1}	2.192×10^{-2}
2	4	5.811×10^{-2}	1.7632×10^{-1}	1.87×10^{-2}
2	5	5.695×10^{-2}	1.7388×10^{-1}	1.7×10^{-2}
3	4	6.701×10^{-2}	1.7103×10^{-1}	1.73×10^{-2}
4	5	1.335×10^{-2}	4.211×10^{-2}	6.4×10^{-3}
4	7	0	2.0912×10^{-1}	0
4	9	0	5.5618×10^{-1}	0
5	6	0	2.5202×10^{-1}	0
6	11	9.498×10^{-2}	1.989×10^{-1}	0
6	12	1.2291×10^{-1}	2.5581×10^{-1}	0

续表 3-4 IEEE-14 节点标准电力系统支路数据表

6	13	6.615×10^{-2}	1.3027×10^{-1}	0
7	8	0	1.7615×10^{-1}	0
7	9	0	1.1001×10^{-1}	0
9	10	3.181×10^{-2}	8.45×10^{-2}	0
9	14	1.2771×10^{-1}	2.7038×10^{-1}	0
10	11	8.205×10^{-2}	1.9207×10^{-1}	0
12	13	2.2092×10^{-1}	1.9988×10^{-1}	0
13	14	1.7093×10^{-1}	3.4802×10^{-1}	0

假设系统前 75min 内正常运行，在第 75min 时 11 节点持续遭 FDIAs，观察假数据注入攻击发生前后节点电压幅值和相角的变化。采用 WLS 和 AIEKF 算法对系统总线进行状态估计。图 3-6 和图 3-7 分别是是 150 个采样时刻的两种算法的电压幅值和相角的估计结果，如图所示，系统在第 75min 遭受 FDIAs，两种算法在不同的时刻收敛于受攻击后的状态值。WLS 在攻击发生时，迅速收敛于 FDIAs 后的状态值，AIEKF 则是经过多个时刻逐渐收敛到攻击后的状态值，两种算法之间的时间差正是检测 FDIAs 的关键之处。

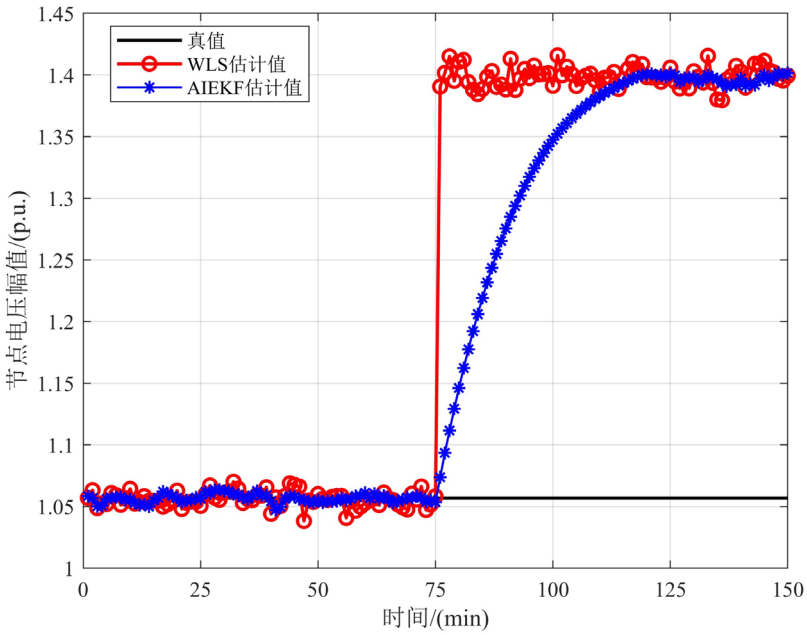


图 3-6 FDIAs 前后节点 11 电压幅值

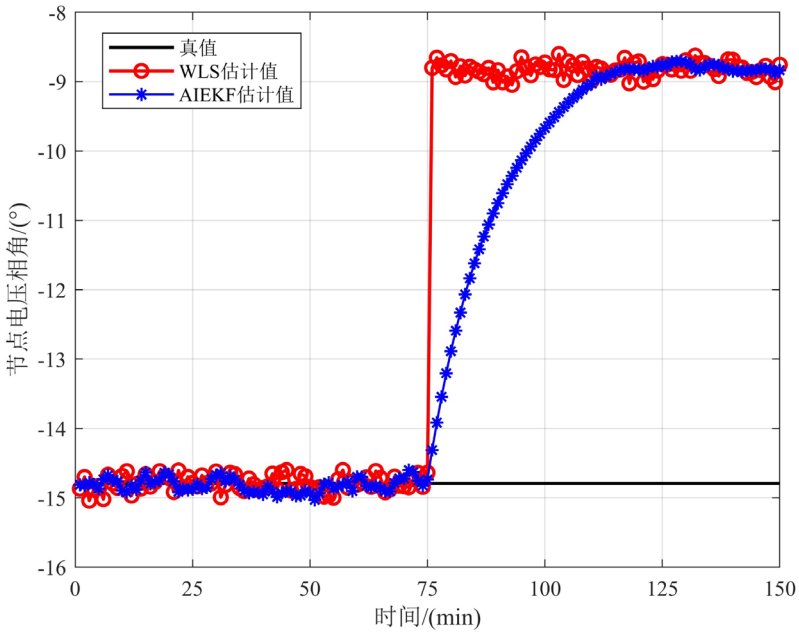


图 3-7 FDIAs 前后节点 11 电压相角

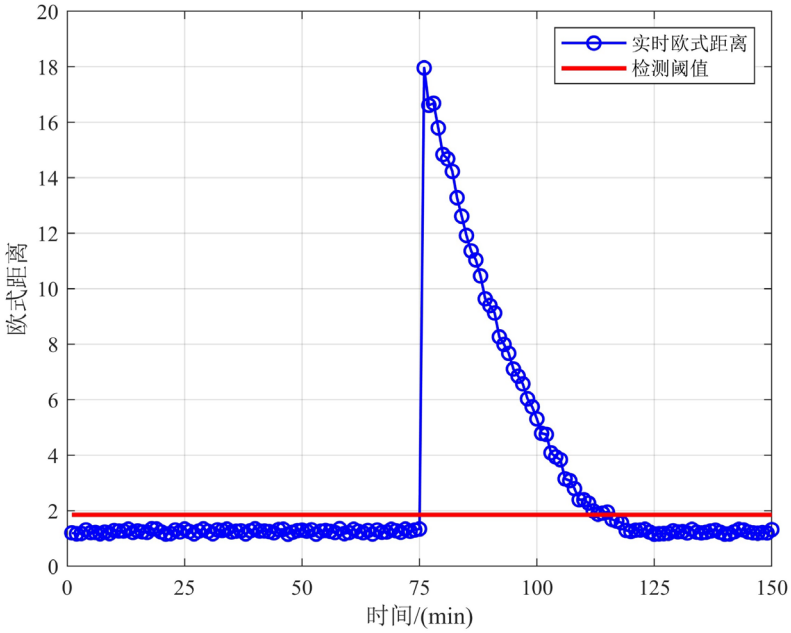


图 3-8 FDIAs 前后实时欧氏距离变化

在利用两种算法进行完状态估计之后，根据式(3-17)计算两者之间的欧式距离。采用蒙特卡罗模拟，通过 1000 个独立的实验，可以得到正常情况下的欧氏距离分布。为了防止检测系统在正常情况下，由于数据的微小波动而触发误报，在得出最大值后需要加上一定的裕量，最终经过模拟后的检测阈值为$\tau=1.85$。

为了更清晰地观察欧氏距离的变化趋势，图 3-8 给出了实时欧氏距离的变化趋势图。

从图 3-8 可知，在系统发生 FDIAs 前，欧式距离 $d(k)$ 在 1.25 附近波动，但并未超出阈值。但在第 75 分钟时，系统发生 FDIAs，此时欧氏距离 $d(k)$ 变为 17.9856。为了进一步排除由其他事件引起的误检测，紧接着需要进行 BDD。在 IEEE-14 节点标准电力系统中，卡方检验中的各元素分别为：$m=41$、$n=27$、$p=0.95$，BDD 阈值为 $J(k)=23.68$。在 FDIAs 后，$J(k)=29.358$，大于检测阈值，说明系统确实发生了 FDIAs。

为了评估所提出方法的检测性能，假设系统遭受了 200 个采样时刻的攻击，将本节所提出的算法与基于 EKF 检测方法[67]和基于短期状态预测的检测方法[68]进行比较，检测效果的量化采用两个指标：真阳率(True Positive Rate, TPR)和假阳率(False Positive Rate, FPR)，具体的公式如下：

$$TPR=\frac{TP}{TP+FN} \tag{3-27}$$

$$FPR=\frac{FP}{FP+TN} \tag{3-28}$$

式中 TP 表示成功检测到攻击的次数；TN 表示成功检测到正常数据的次数；FP 表示正常数据被检测为异常的次数；FN 表示异常数据被检测为正常数据的次数。

表 3-5 三种算法的 TPR 和 FPR

算法	TPR	FPR
EKF	87.5%	9.67%
短时状态预测	90.0%	8.0%
AIEKF	92.5%	5.33%

检测结果对比见表 3-5，从表中可以看出，本节所提出的基于 AIEKF 的 FDIAs 检测方法相比于 EKF 检测方法和短时状态预测检测方法具有高 TPR 和低 FPR，从而说明 AIEKF 算法能够提高 FDIAs 的检测精度，为下一章节实现 FDIAs 的定位提供了更准确的检测能力。

3.5.3 IEEE-30 节点标准系统的 FDIAs 检测

为了更好地验基于 AIEKF 的 FDIAs 检测方法的有效性，本小节在 IEEE-30

节点标准电力系统中进行 FDIAs 检测，IEEE-30 节点标准电力系统如图 2-8 所示，共有 30 个节点，6 个发电机，41 条支路，其中支路数据如表 3-6 所示。

表 3-6 IEEE-30 节点标准电力系统支路数据表

起始节点	终止节点	电阻(R)	电抗(X)	电纳(B/2)
1	2	1.92×10^{-2}	5.75×10^{-2}	2.64×10^{-2}
1	3	4.52×10^{-2}	1.652×10^{-1}	2.04×10^{-2}
2	4	5.7×10^{-2}	1.737×10^{-1}	1.84×10^{-2}
3	4	1.32×10^{-2}	3.79×10^{-2}	4.2×10^{-3}
2	5	4.72×10^{-2}	1.983×10^{-1}	2.09×10^{-2}
2	6	5.81×10^{-2}	1.763×10^{-1}	1.87×10^{-2}
4	6	1.19×10^{-2}	4.14×10^{-2}	4.5×10^{-3}
5	7	4.6×10^{-2}	1.16×10^{-1}	1.02×10^{-2}
6	7	2.67×10^{-2}	8.2×10^{-2}	8.5×10^{-3}
6	8	1.2×10^{-2}	4.2×10^{-2}	4.5×10^{-3}
6	9	0	2.08×10^{-1}	0
6	10	0	5.56×10^{-1}	0
9	11	0	2.08×10^{-1}	0
9	10	0	1.1×10^{-1}	0
4	12	0	2.56×10^{-1}	0
12	13	0	1.4×10^{-1}	0
12	14	1.231×10^{-1}	2.559×10^{-1}	0
12	15	6.62×10^{-2}	1.304×10^{-1}	0
12	16	9.45×10^{-2}	1.987×10^{-1}	0
14	15	2.21×10^{-1}	1.997×10^{-1}	0
16	17	5.24×10^{-2}	1.923×10^{-1}	0
15	18	1.073×10^{-1}	2.185×10^{-1}	0
18	19	6.39×10^{-2}	1.292×10^{-1}	0
19	20	3.4×10^{-2}	6.8×10^{-2}	0
10	20	9.36×10^{-2}	2.09×10^{-1}	0

续表 3-6 IEEE-30 节点标准电力系统支路数据表

10	17	3.24×10^{-2}	8.45×10^{-2}	0
10	21	3.48×10^{-2}	7.49×10^{-2}	0
10	22	7.27×10^{-2}	1.499×10^{-1}	0
21	22	1.16×10^{-2}	2.36×10^{-2}	0
15	23	1×10^{-1}	2.02×10^{-1}	0
22	24	1.15×10^{-1}	1.79×10^{-1}	0
23	24	1.32×10^{-1}	2.7×10^{-1}	0
24	25	1.885×10^{-1}	3.292×10^{-1}	0
25	26	2.544×10^{-1}	3.8×10^{-1}	0
25	27	1.093×10^{-1}	2.087×10^{-1}	0
28	27	0	3.96×10^{-1}	0
27	29	2.198×10^{-1}	4.153×10^{-1}	0
27	30	3.202×10^{-1}	6.207×10^{-1}	0
29	30	2.399×10^{-1}	4.533×10^{-1}	0
8	28	6.36×10^{-2}	2×10^{-1}	2.14×10^{-2}
6	28	1.69×10^{-2}	5.99×10^{-2}	6.5×10^{-3}

图 3-9 和图 3-10 为 FDIAs 发生后，使用 WLS 和 AIEKF 对各个节点状态进行状态估计的结果。从图中可以看出，虽然 FDIAs 使得系统节点电压幅值和相角发生改变，但是攻击后的算法估计结果分布与攻击发生前大致相同。由于是根据第二章的原理构建的 FDIAs 向量，因此在攻击发生前后，系统残差并没有明显变化。利用式(3-17)计算正常情况下的欧氏距离 $d(k)$，可得到一致性检验的阈值为 $\tau=2.58$。当系统发生 FDIAs 后，$d(k)=19.8732$，明显超过了检测阈值。

为了进一步排除由其他事件引起的误检测，紧接着需要进行 BDD。在 IEEE-30 节点标准电力系统中，卡方检验中的各元素分别为：$m=93$、$n=59$、$p=0.95$，BDD 阈值为 $J(k)=48.602$。在 FDIAs 发生后，$J(k)=53.658$，大于检测阈值，说明系统确实发生了 FDIAs。

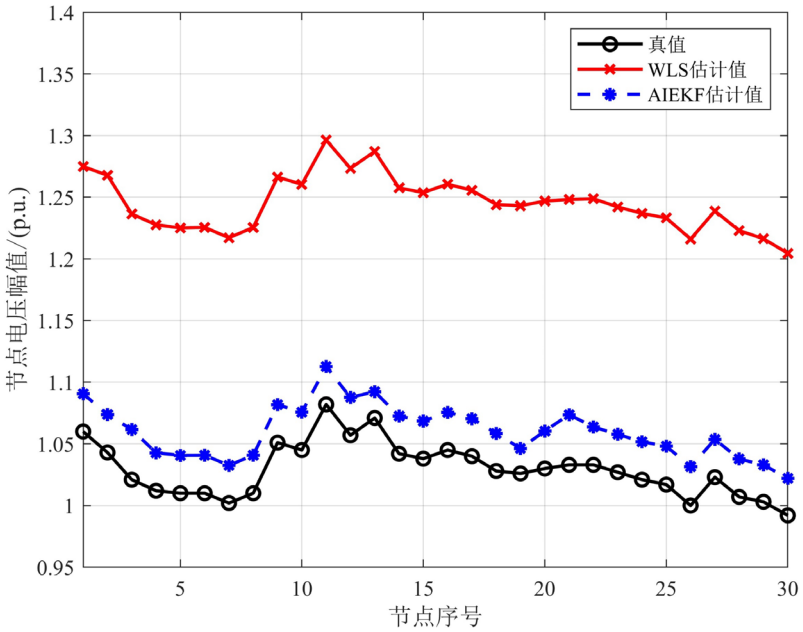


图 3-9 FDIAs 后系统节点电压幅值变化

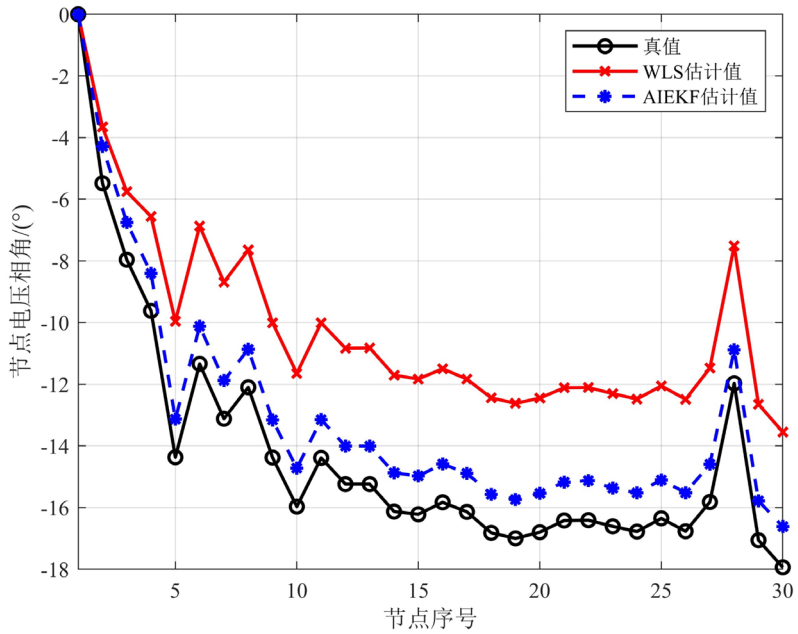


图 3-10 FDIAs 后系统节点电压相角变化

与上一小节类似，为了评估所提出方法的检测性能，假设系统遭受了 200 个采样时刻的攻击，将本节所提出的算法与基于 EKF 检测方法和基于短期状态预测的检测方法进行比较，比较结果见表 3-7。

表 3-7 三种算法的 TPR 和 FPR

算法	TPR	FPR
EKF	89.5%	10.33%
短时状态预测	91.5%	8.67%
AIEKF	93.5%	8.0%

从表中可以看出，本节所提出的基于 AIEKF 的 FDIAs 检测方法相比于 EKF 检测方法和短时状态预测检测方法具有高 TPR 和低 FPR，从而说明在多节点系统中 AIEKF 算法同样可以提高 FDIAs 的检测精度，为下一章节实现 FDIAs 的定位提供了更准确的检测能力。

3.6 本章小结

本章提出了基于 AIEKF 的智能电网 FDIAs 检测算法。首先介绍了传统的 EKF 算法，并分析了其缺点，以此为基础引入了自适应插值策略，从而提出了基于 AIEKF 的电力系统状态估计；其次，阐述了基于 AIEKF 的 FDIAs 检测过程；最后，实验仿真分为两个部分，分析了 AIEKF 的估计性能，并在 IEEE-14 节点和 IEEE-30 节点标准电力系统上进行 FDIAs 检测，仿真结果表明，AIEKF 提高了状态估计的精度，并提高了 FDIAs 的检测能力，为下一章的定位奠定了基础。

第4章 基于联合最大后验-最大似然估计的 FDIAs 定位

4.1 引言

对于电力系统的控制中心而言，定位受攻击的节点至关重要。如果控制中心能够确定攻击的具体位置，就可以迅速采取措施对该节点进行隔离，从而有效地阻止攻击者继续通过该节点向电网注入虚假数据。定位攻击节点的能力不仅能够增强防御系统的准确性，还可以为后续的恢复工作提供重要的信息依据。

利用第三章提出的基于状态估计的算法检测智能电网中存在的 FDIAs 后，需要进一步检测出具体的受攻击的节点，即所谓的 FDIAs 定位。基于状态估计的算法进行 FDIAs 定位需要将电力系统划分成不同的区域，然后在每个分区内进行 FDIAs 检测，直至分区不能进一步划分。在这个过程中需要对每个分区检测阈值进行设定，而阈值的选取精度又决定着检测精度，阈值选取的困难使得该方法具有较大的局限性，不能满足需要对 FDIAs 进行精准定位的需求，这一不足在实际应用中可能会限制系统应对攻击的能力。

本章以系统收集到的传感器测量数据为基础，考虑到 FDIAs 发生前后传感器测量数据误差的分布特性，假设测量数据误差服从于高斯分布，而攻击发生后的测量数据误差也服从于高斯分布，从而构成高斯混合模型(Gaussian Mixture Model, GMM)，这一模型结合了正常状态和攻击状态下的误差分布特征。为了对 GMM 的参数进行准确估计，本文提出了联合最大似然-最大后验(Joint Maximum a Posteriori - Maximum Likelihood, JMAP-ML)算法。在参数估计的基础上，利用 GMM 分类结果以及测量数据之间的相关性实现对 FDIAs 的定位。最后，在 IEEE-14 节点和 IEEE-30 节点标准电力系统进行仿真测试，以此来验证所提方法的有效性。

4.2 状态估计的 FDIAs 定位原理概述

在利用第三章提出的算法对系统进行 FDIAs 全局检测后，将电力系统进行划分为不同的区域，在每个区域内进行 FDIAs 检测。之后将检测出 FDIAs 的区域在进行划分，直至定位出受攻击的节点。

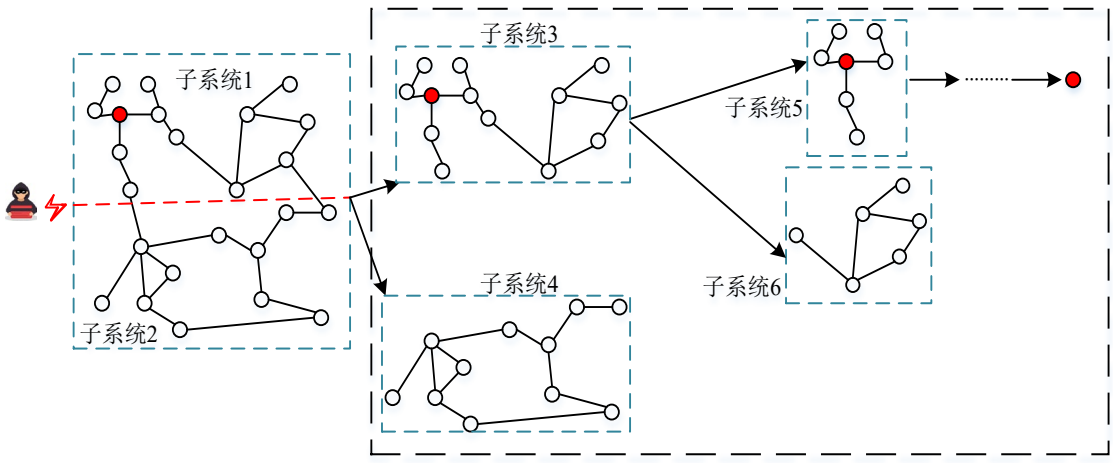


图 4-1 基于系统划分定位攻击示意图

如图 4-1 所示，左边为电力系统连接图，其中圆圈代表系统节点，黑线代表节点之间的连接线，红色代表该节点受到攻击。为了定位出受攻击的节点，需要对系统进行二划分，分为子系统 1 和子系统 2。之后在子系统 1 和子系统 2 中分别进行 FDIAs 检测，在检测出受攻击的子系统 1 中，继续将子系统 1 进行划分，分为子系统 3 和子系统 4，以此类推，直至单独划分出红色节点。在系统划分的过程中，需要构建逻辑定位矩阵。在定位矩阵的基础上进行检测，构成检测矩阵，将逻辑定位矩阵与检测矩阵进行逻辑与操作，可实现对攻击节点的定位。

表 4-1 逻辑定位矩阵

	1	2	⋯	$n-1$	n
$\left(1,\cdots,\frac{n}{2}\right)\middle\vert\left(\frac{n}{2}+1,\cdots,n\right)$	$1\vert 0$	$1\vert 0$	⋯	$0\vert 1$	$0\vert 1$
$\left(1,\cdots,\frac{n}{4}\right)\middle\vert\left(\frac{n}{4}+1,\cdots,\frac{n}{2}\right)$	$1\vert 0$	$0\vert 1$	⋯	$0\vert 0$	$0\vert 0$
⋮	⋮	⋮	⋮	⋮	⋮
$(n-1)\vert n$	$0\vert 0$	$0\vert 0$	⋯	$1\vert 0$	$0\vert 1$

假设系统中有 n 个节点，根据上述原理构建的逻辑定位矩阵如表 4-1 所示，其中矩阵的列数等于系统中的总线数 n，列标题是总线的名称。矩阵的行数等于 $n-1$，行标题由二分法确定。第一行为标题为 $\left(1,\cdots,\frac{n}{2}\right)\middle\vert\left(\frac{n}{2}+1,\cdots,n\right)$，最后一行标题为 $(n-1)\vert n$。另外，当传感器 j 受到攻击的事实并不意味着其他传感器不会受到攻

击。因此，当行 i 的标题不包含列 j 的标题时，行 i 和列 j 用 0 表示。而在检测矩阵的元素组成中，检测出 FDIAs 记为 1，否则为 0，构成一个 $n-1$ 行的列矩阵。

当单节点 n 受到攻击时，包含节点 n 的所有分区检测结果均为 1。将逻辑定位矩阵的元素与检测矩阵中元素进行逻辑与操作，当逻辑定位矩阵的行和列标题仅包含 n 这个节点时，并且与操作后结果为 1，即可定位受攻击的 n 节点。而当系统发生多节点攻击时，重复上述操作即可，以上就是基于状态估计的 FDIAs 定位过程。

但由于每个区域进行 FDIAs 检测时，都需要一个检测阈值，导致定位过程较为复杂，具有较大的局限性。而在本节所提出的基于 JMAP-ML 的 FDIAs 定位方法中，无需设定检测阈值，并且定位过程充分利用量测数据的分布特性，无需多次划分系统，简化了定位过程，具有较高的定位精度。

4.3 联合最大后验-最大似然估计算法概述

JMAP-ML 是一种结合最大后验估计(Maximum a Posteriori, MAP)和最大似然估计(Maximum Likelihood, ML)的方法，主要用于同时估计模型参数和潜在变量。在传统的 ML 估计中，目标是找到使观测数据出现概率最大的参数，即通过最大化似然函数来进行估计。然而，ML 估计并没有考虑先验信息，可能在数据稀缺或噪声较大的情况下表现不佳。MAP 估计通过引入先验知识，结合数据和先验信息，最大化后验概率，从而在参数估计中引入了对先验分布的考虑。而在实际问题中，往往不仅需要估计模型参数，还需要同时估计潜在变量，比如在高斯混合模型应用场景中。JMAP-ML 方法通过最大化观测数据的似然函数与模型参数及潜在变量的联合后验概率，能够有效地处理这种问题。

4.3.1 高斯混合模型的构建

根据第二章的描述，考虑了一个具有 m 个测量值，n 个状态变量的电力系统，两者之间的关系为：

$$\boldsymbol{z}=\underbrace{\boldsymbol{h}(\boldsymbol{x})}_{\boldsymbol{y}}+\boldsymbol{e} \tag{4-1}$$

式中，$\boldsymbol{z}$为原始测量向量；$\boldsymbol{y}$为无噪声测量向量；$\boldsymbol{e}$为测量误差向量。

在电力系统运行过程中，在 SCADA 系统收集的K组测量数据中，假设为实现 FDIAs，测量向量$\boldsymbol{z}$中m个测量值中的f个测量值被篡改，则相应的测量值误差的样本来自两部分：一部分是正常测量$m-f$的误差样本，一部分是被篡改的测量f误差的样本。为便于理解，将K组测量数据向量融合为一个整体矢量，其表达式为：

$$\boldsymbol{Z}=\boldsymbol{Y}+\boldsymbol{E} \tag{4-2}$$

式中，列向量$\boldsymbol{Z}$、$\boldsymbol{Y}$和$\boldsymbol{E}$的维数均为$mK\times1$，各自的表达式为：

$$\boldsymbol{Z}=\left[z_{1,1},\cdots,z_{1,K},\cdots,z_{m,1},z_{m,K}\right]^{T} \tag{4-3}$$

$$\boldsymbol{Y}=\left[y_{1,1},\cdots,y_{1,K},\cdots,y_{m,1},y_{m,K}\right]^{T} \tag{4-4}$$

$$\boldsymbol{E}=\left[e_{1,1},\cdots,e_{1,K},\cdots,e_{m,1},e_{m,K}\right]^{T} \tag{4-5}$$

在式(4-2)中，将实际得到的第k个测量向量$\boldsymbol{z}_k$的第i次测量表示为：

$$z_{i,k}=y_{i,k}+e_{i,k} \tag{4-6}$$

式中，$e_{i,k}$服从高斯分布，可分为两种情况：正常测量数据误差的分布为$p_e^{(1)}=\left(e;\mu_1,\sigma_1^2\right)$；篡改后的测量数据误差的分布为$p_e^{(2)}=\left(e;\mu_2,\sigma_2^2\right)$。

在本章中，使用 GMM 来表示测量误差，从而简化了这个问题。高斯混合模型可表示为：

$$p(e;\boldsymbol{\theta})=\sum_{l=1}^{2}\alpha_l p_e^{(l)}(e;\mu_l,\sigma_l^2) \tag{4-7}$$

式中，α_l为未知参数，表示各组分的比例。假设测量向量$\boldsymbol{z}$中m个测量值中的f个测量值被篡改，则$\alpha_1=\frac{m-f}{m}$，$\alpha_2=\frac{f}{m}$。与此同时，$\alpha_1+\alpha_2=1$。GMM 的主要挑战是求解各部分分布参数$\boldsymbol{\theta}=\left[\alpha_1,\alpha_2,\mu_1,\mu_2,\sigma_1^2,\sigma_2^2\right]^{T}$，通过使用 JMAP-ML 算法可以实现对模型参数的估计。

4.3.2 基于联合最大后验-最大似然算法的参数估计

基于式(4-2)的测量模型和式(4-7)高斯混合分布，$\boldsymbol{\theta}=\left[\alpha_1,\alpha_2,\mu_1,\mu_2,\sigma_1^2,\sigma_2^2\right]^T$ 的对数似然函数为：

$$\begin{aligned}\mathcal{L}_I\left(\boldsymbol{\theta};\boldsymbol{E}\right)&=\ln\left[p\left(\boldsymbol{E};\boldsymbol{\theta}\right)\right]\\&=\ln\left[\prod_{i=1}^{m}\prod_{k=1}^{K}p\left(e_{i,k},\boldsymbol{\theta}\right)\right]\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\ln\left[\sum_{l=1}^{2}\alpha_l p_e^{(l)}\left(e_{i,k};\mu_l,\sigma_l^2\right)\right]\end{aligned}\tag{4-8}$$

相关参数$\hat{\boldsymbol{\theta}}$的最大似然估计量可通过以下问题得到解决，

$$\begin{aligned}&\underset{\boldsymbol{\theta}}{\text{argmax}}\ \mathcal{L}_I(\boldsymbol{\theta};\boldsymbol{E})\\&\text{s.t. }\alpha_1\geq 0,\quad \alpha_2\geq 0,\\&\alpha_1+\alpha_2=1\end{aligned}\tag{4-9}$$

对于上述问题，解决式(4-8)中的代价函数是复杂的，本质上，JMAP-ML 算法是 MLE 的近似值。因此，为了简化成本函数的复杂性，引入了一个完整的数据集$\boldsymbol{o}=\left\{\boldsymbol{\kappa},\boldsymbol{E}\right\}$，$\boldsymbol{\kappa}$是随机变量(也称为潜在变量)的向量，定义为$\boldsymbol{\kappa}=\left[\kappa_{1,1},\cdots,\kappa_{1,K},\cdots,\kappa_{m,1},\cdots,\kappa_{m,K}\right]^T$，$\boldsymbol{\kappa}$的值指出哪个混合成分产生了相应的测量误差。更具体地说，

$$\kappa_{i,k}=\begin{cases}1, & e_{i,k}\in p_e^{(1)}\left(e;\mu_1,\sigma_1^2\right)\\2, & e_{i,k}\in p_e^{(2)}\left(e;\mu_2,\sigma_2^2\right)\end{cases}\tag{4-10}$$

为了避免歧义，定义$\left\{\boldsymbol{E};\boldsymbol{\theta}\right\}$为不完整数据，$\left\{\boldsymbol{E},\kappa;\boldsymbol{\theta}\right\}$为完整数据。完整数据的对数似然函数表示为：

$$\begin{aligned}\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)&=\ln\left[p\left(\boldsymbol{\kappa},\boldsymbol{E};\boldsymbol{\theta}\right)\right]\\&=\ln\left[\prod_{i=1}^{m}\prod_{k=1}^{K}p\left(e_{i,k},\kappa_{i,k};\boldsymbol{\theta}\right)\right]\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\ln\left(\alpha_{\kappa_{i,k}}p_e^{\left(\kappa_{i,k}\right)}\left(e_{i,k};\mu_{\kappa_{i,k}},\sigma_{\kappa_{i,k}}^2\right)\right)\end{aligned}\tag{4-11}$$

很明显，新引入的完整数据对数似然函数具有更易于处理的形式，可以通过

JMAP-ML 算法来近似 MLE，式(4-9)转化为另外一种形式，其表达式为：

$$\begin{aligned} &\arg\max_{\boldsymbol{\theta}} \mathcal{L}_I(\boldsymbol{\theta};\boldsymbol{\kappa},\boldsymbol{E}) \\ &\text{subject to } \alpha_1 \geq 0, \quad \alpha_2 \geq 0, \\ &\alpha_1 + \alpha_2 = 1 \end{aligned} \tag{4-12}$$

作为逼近 MLE 的均值，采用 MLE 的思想对数据进行处理，即完整数据对数似然函数 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$ 对 $\boldsymbol{\theta}$ 和 $\boldsymbol{\kappa}$ 都直接最大化，即：

$$\arg\max_{\boldsymbol{\theta},\boldsymbol{\kappa}} \mathcal{L}_C(\boldsymbol{\theta};\boldsymbol{\kappa},\boldsymbol{E}) = \arg\max_{\boldsymbol{\theta}} \left\{ \arg\max_{\boldsymbol{\kappa}} \mathcal{L}_C(\boldsymbol{\theta};\boldsymbol{\kappa},\boldsymbol{E}) \right\} \tag{4-13}$$

JMAP-ML 标准包含一个 MAP 估计步骤(根据潜在变量 $\boldsymbol{\kappa}$)和一个 ML 估计步骤(根据确定性参数 $\boldsymbol{\theta}$)。通常，基于 JMAP-ML 标准开发的算法从精心选择的初始值 $\boldsymbol{\theta}^{(0)}$ 开始，并且在迭代过程中上述两个步骤之间交替进行。关于这两个步骤的详细信息将在后续部分中给出。

4.3.3 最大后验估计步骤公式化

参数 $\boldsymbol{\kappa}$ 的估计是 JMAP-ML 算法的第一步。为了方便求解，需要对似然函数进行如下变换：

$$\mathcal{L}_C(\boldsymbol{\theta};\boldsymbol{\kappa},\boldsymbol{E}) = \ln p(\boldsymbol{\kappa},\boldsymbol{E};\boldsymbol{\theta}) = \ln p(\boldsymbol{\kappa}\,|\,\boldsymbol{E};\boldsymbol{\theta}) + \ln p(\boldsymbol{E};\boldsymbol{\theta}) \tag{4-14}$$

式中，$\ln p(\boldsymbol{E};\boldsymbol{\theta})$ 与 $\boldsymbol{\kappa}$ 无关，因此可以将式(4-14)的极值替换为前条件概率函数的极值，如下所示：

$$\arg\max_{\boldsymbol{\kappa}} \ln p(\boldsymbol{\kappa}\,|\,\boldsymbol{E};\boldsymbol{\theta}) \tag{4-15}$$

将参数 $\boldsymbol{\theta}$ 的第 η 次迭代值 $\boldsymbol{\theta}^{(\eta)}$ 带入上式，求解 $\boldsymbol{\kappa}$ 的 MAP 估计，产生下式：

$$\boldsymbol{\kappa}^{(\eta+1)} = \arg\max_{\boldsymbol{\kappa}} \ln p(\boldsymbol{\kappa}\,|\,\boldsymbol{E};\boldsymbol{\theta}^{(\eta)}) \tag{4-16}$$

式(4-16)可以分为 mK 个简单的部分：

$$\kappa_{i,k}{}^{(\eta+1)} = \arg\max_{\kappa_{i,k}} \ln p(\kappa_{i,k}\,|\,e_{i,k};\boldsymbol{\theta}^{(\eta)}) \tag{4-17}$$

式中，$\forall(i,k) \in P \triangleq \left[(1,1),\cdots,(1,K),\cdots(m,1),\cdots,(m,K)\right]$。$p(\kappa_{i,k}\,|\,e_{i,k};\boldsymbol{\theta}^{(\eta)})$ 通过贝叶斯规则计算，具体公式为：

$$p\left(\kappa_{i,k}=l\left|e_{i,k},\boldsymbol{\theta}^{(\eta)}\right.\right)=\frac{\alpha_l^{(\eta)}p_e^{(l)}\left(e_{i,k};\mu_l^{(\eta)},\sigma_l^{2,(\eta)}\right)}{p\left(e_{i,k};\boldsymbol{\theta}^{(\eta)}\right)} \tag{4-18}$$

式中，$p\left(e_{i,k};\boldsymbol{\theta}^{(\eta)}\right)=\sum_{l=1}^{2}\alpha_l^{(\eta)}p_e^{(l)}\left(e_{i,k};\mu_l^{(\eta)},\sigma_l^{2,(\eta)}\right)$。

由于$\kappa_{i,k}$是离散值，因此式(4-17)的全局最优解必须是$\{\kappa_{i,k}=1,2\}$中最大化$\ln p(\kappa_{i,k}|e_{i,k};\boldsymbol{\theta}^{(\eta)})$的解。通过定义：

$$\Gamma_{i,k,l}^{(\eta)}\triangleq\alpha_l^{(\eta)}p_e^{(l)}\left(e_{i,k};\mu_l^{(\eta)},\sigma_l^{2,(\eta)}\right),\quad l=1,2 \tag{4-19}$$

由于 ln(.)是单调函数，只需比较$\Gamma_{i,k,l}^{(\eta)}$的值，给出 MAP 估计如下：

$$\kappa_{i,k}^{(\eta)}=\begin{cases}1, & \Gamma_{i,k,1}^{(\eta)}\geq\Gamma_{i,k,2}^{(\eta)}\\ 2, & \Gamma_{i,k,1}^{(\eta)}<\Gamma_{i,k,2}^{(\eta)}\end{cases} \tag{4-20}$$

经过上述步骤便完成了最大后验估计，实现了对测量数据的分类。

4.3.4 最大似然估计步骤公式化

参数$\boldsymbol{\theta}$的估计是 JMAP-ML 算法的第二步。通过将估计的$\boldsymbol{\kappa}^{(\eta+1)}$代入完全对数似然函数$\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$，则完整对数似然函数可重新表述为：

$$\begin{aligned}\mathcal{L}_c\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}^{(\eta+1)}\right)&=\ln\left[p\left(\boldsymbol{E},\boldsymbol{\kappa}^{(\eta+1)};\boldsymbol{\theta}\right)\right]\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\ln\left(\alpha_{\kappa_{i,k}^{(\eta+1)}}p_e^{\left(\kappa_{i,k}^{(\eta+1)}\right)}\left(e_{i,k};\mu_l,\sigma_l^2\right)\right)\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\sum_{l=1}^{2}\ln\left(\alpha_l p_e^{(l)}\left(e_{i,k};\mu_l,\sigma_l^2\right)\right)\delta\left(l-\kappa_{i,k}^{(\eta+1)}\right)\end{aligned} \tag{4-21}$$

式中，$\delta(.)$是脉冲函数，其表达式为：

$$\delta\left(l-\kappa_{i,k}^{(\eta+1)}\right)=\begin{cases}1, & if\quad l=\kappa_{i,k}^{(\eta+1)}\\ 0, & otherwise\end{cases} \tag{4-22}$$

在接下来的步骤中，对$\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}\right)$最大化求解$\boldsymbol{\theta}$，从而得到$\boldsymbol{\theta}$的第$(\eta+1)$次

迭代：

$$\boldsymbol{\theta}^{(\eta+1)}=\arg\max_{\boldsymbol{\theta}}\mathcal{L}_C(\boldsymbol{\theta};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}) \tag{4-23}$$

为了方便计算，本节引入权重函数 $\omega_{i,k,l}$。因此，式(4-21)可以转化为另一种形式：

$$\begin{aligned}\mathcal{L}_c^{(\eta)}\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}^{(\eta+1)}\right)&=\ln\left[p\left(\boldsymbol{E},\boldsymbol{\kappa}^{(\eta+1)};\boldsymbol{\theta}\right)\right]\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\sum_{l=1}^{2}\omega_{i,k,l}^{(\eta)}\ln\left[\alpha_l p_e^{(l)}\left(e_{i,k};\mu_l,\sigma_l^2\right)\right]\\&=\sum_{i=1}^{m}\sum_{k=1}^{K}\left(\omega_{i,k,1}^{(\eta)}\ln\alpha_1+\omega_{i,k,2}^{(\eta)}\ln\alpha_2\right)\\&+\sum_{i=1}^{m}\sum_{k=1}^{K}\left(\omega_{i,k,1}^{(\eta)}\ln p_e^{(1)}\left(e_{i,k};\mu_1,\sigma_1^2\right)\right)\\&+\sum_{i=1}^{m}\sum_{k=1}^{K}\left(\omega_{i,k,2}^{(\eta)}\ln p_e^{(2)}\left(e_{i,k};\mu_2,\sigma_2^2\right)\right)\end{aligned} \tag{4-24}$$

式中，权重函数 $\omega_{i,k,l}$ 定义为：

$$\omega_{i,k,l}=\delta\left(l-\kappa_{i,k}^{(\eta+1)}\right) \tag{4-25}$$

为了方便理解，对式(4-24)进行简化，转化为以下形式：

$$\mathcal{L}_c^{(\eta)}\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}^{(\eta+1)}\right)=\mathcal{L}_0^{(\eta)}\left(\alpha_1,\alpha_2\right)+\sum_{l=1}^{2}\mathcal{L}_l^{(\eta)}\left(\mu_l,\sigma_l^2\right) \tag{4-26}$$

式中，

$$\mathcal{L}_0^{(\eta)}\left(\alpha_1,\alpha_2\right)\triangleq\sum_{i=1}^{m}\sum_{k=1}^{K}\left(\omega_{i,k,1}^{(\eta)}\ln\alpha_1+\omega_{i,k,2}^{(\eta)}\ln\alpha_2\right) \tag{4-27}$$

$$\mathcal{L}_l^{(\eta)}\left(\mu_l,\sigma_l^2\right)\triangleq\sum_{i=1}^{m}\sum_{k=1}^{K}\ln\left(p_e^{(l)}\left(e_{i,k};\mu_l,\sigma_l^2\right)\right)\omega_{i,k,l}^{(\eta)} \tag{4-28}$$

按照文献[69]的技术路线求解混合模型和参数，对 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$ 最大化。更精确地说，求解以下方程：

$$\frac{\partial}{\partial\alpha_l}\left[\mathcal{L}_0^{(\eta)}\left(\alpha_1,\alpha_2\right)+\lambda\left(\sum_{l=1}^{2}\alpha_l-1\right)\right]=0 \tag{4-29}$$

$$\frac{\partial}{\partial \mu_l}\left[\mathcal{L}_l^{(\eta)}\left(\mu_l,\sigma_l^2\right)\right]=0 \tag{4-30}$$

$$\frac{\partial}{\partial \sigma_l^2}\left[\mathcal{L}_l^{(\eta)}\left(\mu_l^{(\eta+1)},\sigma_l^2\right)\right]=0 \tag{4-31}$$

式中，λ是拉格朗日乘子。通过求解上述封闭方程，各参数的最终表达式如下：

$$\alpha_l^{(\eta+1)}=\frac{1}{mK}\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)} \tag{4-32}$$

$$\mu_l^{(\eta+1)}=\frac{\sum_{i=1}^{m}\sum_{k=1}^{K}\left(z_{i,k}-y_{i,k}\right)\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{4-33}$$

$$\sigma_l^{2,(\eta+1)}=\frac{\sum_{i=1}^{m}\sum_{k=1}^{K}\left(z_{i,k}-y_{i,k}-\mu_l^{(\eta+1)}\right)^2\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{4-34}$$

为了更好地理解 JMAP-ML 算法，表 4-2 总结了该算法的流程，如下所示：

表 4-2 GMM 参数估计的 JMAP-ML 算法流程图

步骤	流程
1.	输入测量数据 $\boldsymbol{z}$
2.	选择收敛容差Δ和最大迭代次数 $N_{itr}^{\max}$；设置迭代索引 $\eta=0$；选择初始值 $\boldsymbol{\theta}^{(0)}=\left[\alpha_1^{(0)},\alpha_2^{(0)},\mu_1^{(0)},\mu_2^{(0)},\sigma_1^{2,(0)},\sigma_2^{2,(0)}\right]^T$
3.	第η次迭代
4.	根据式(4.20)计算 $\kappa_{i,k}^{(\eta)}$
5.	根据式(4.25)计算 $\omega_{i,k,l}^{(\eta)}$
6.	求解 $\boldsymbol{\theta}^{(\eta+1)}$ 使得式(4.26)最大化
7.	如果对数似然函数值的增量小于Δ或者达到最大迭代次数 $N_{itr}^{\max}$，终止算法；否则，令 $\eta\rightarrow\eta+1$，并返回步骤 2
8.	输出 $\boldsymbol{\theta}^{(\eta+1)}$

4.4 算法分析

4.4.1 收敛性分析

如表 4-2 所示，JMAP-ML 算法是一种迭代算法。因此，有必要保证算法的收敛性，即 JMAP-ML 算法最终单调收敛于完整数据对数似然函数的某驻点 $\mathcal{L}_C^*$。为了验证这个问题，进行了相关分析。

在 JMAP-ML 算法的第一步中，对于给定的先验参数估计 $\boldsymbol{\theta}^{(\eta)}$，最大化 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$ 相对于 $\boldsymbol{\kappa}$。由于 $\boldsymbol{\kappa}^{(\eta+1)}$ 是全局最优解，由此可得出下式：

$$\mathcal{L}_C\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}\right)\geq\mathcal{L}_C\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\kappa}^{(\eta)},\boldsymbol{E}\right) \tag{4-35}$$

式中，对其参数空间的任意 $\boldsymbol{\kappa}^{(\eta)}$ 均成立。

第二步，最大化 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}\right)$ 关于 $\boldsymbol{\theta}$。与期望最大化(Expectation Maximization，EM)算法类似，这里需要考虑 Q 函数：

$$Q\left(\boldsymbol{\theta},\boldsymbol{\theta}^{(\eta)}\right)=\sum_{\boldsymbol{\kappa}}\ln\left[p\left(\boldsymbol{\kappa},\boldsymbol{E};\boldsymbol{\theta}\right)\right]p\left(\boldsymbol{\kappa}\middle|\boldsymbol{E};\boldsymbol{\theta}^{(\eta)}\right) \tag{4-36}$$

然后，需要证明 $Q\left(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{\theta}^{(\eta)}\right)\geq Q\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\theta}^{(\eta)}\right)$ 对其参数空间中的任意 $\boldsymbol{\theta}^{(\eta)}$ 成立。

在 EM 算法中，M 步可以推导出 $\boldsymbol{\theta}^{(\eta+1)}=\arg\max_{\boldsymbol{\theta}}Q(\boldsymbol{\theta},\boldsymbol{\theta}^{(\eta)})$，因此上述关系是可以证明的。对于高斯分布，文献 [70] 和文献 [71] 证明了更新参数 $\alpha_1^{(\eta+1)},\alpha_2^{(\eta+1)},\mu_1^{(\eta+1)},\mu_2^{(\eta+1)},\sigma_1^{2,(\eta+1)},\sigma_2^{2,(\eta+1)}$ 是相应最大化问题的全局最优解。基于此，可以很容易地证明：

$$\mathcal{L}_C\left(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}\right)\geq\mathcal{L}_C\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\kappa}^{(\eta+1)},\boldsymbol{E}\right) \tag{4-37}$$

这意味着 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$ 在迭代过程中单调递增。由于 $\mathcal{L}_C\left(\boldsymbol{\theta};\boldsymbol{E},\boldsymbol{\kappa}\right)$ 有上边界，则保证收敛于某平稳点 $\mathcal{L}_C^*$。

4.4.2 复杂度分析

在复杂度分析中，需要更关注 JMAP-ML 算法的迭代过程，因为其消耗的计算能力最大。复杂度是根据浮点运算(Floating Point Operations Per Second, FLOPs)来计算的，将一些基本操作所需的 FLOPs 定义如下：

(1) ε_{add}：用于加法运算的 FLOPs；

(2) ε_{sub}：用于减法运算的 FLOPs；

(3) ε_{mul}：用于乘法运算的 FLOPs；

(4) ε_{div}：用于除法运算的 FLOPs；

(5) ε_{exp}：用于指数运算的 FLOPs；

(6) ε_{pow}：用于平方运算的 FLOPs；

(7) ε_{sqrt}：用于开方运算的 FLOPs；

(8) ε_{com}：用于比较运算的 FLOPs；

请注意，上述操作所需的实际 FLOPs 可能因处理器而异。

由于 JMAP-ML 算法本质上是迭代的，因此将分析集中在一次 JMAP-ML 迭代中，例如第$(\eta+1)$次迭代。估计步骤从$\omega_{i,k,l}=\delta\left(l-\kappa_{i,k}^{(\eta+1)}\right)$开始，给定先验参数估计$\boldsymbol{\theta}^{(\eta)}$。这需要计算

$$e_{i,k}=z_{i,k}-y_{i,k} \tag{4-38}$$

$$\Gamma_{i,k,l}=\frac{\alpha_l^{(\eta)}}{\sqrt{2\pi\sigma_l^{2,(\eta)}}}.\exp\left[\frac{\left(e_{i,k}-\mu_l^{(\eta)}\right)}{-2\sigma_l^{2,(\eta)}}\right] \tag{4-39}$$

其中，$i=1,2,\cdots,m$；$k=1,2,\cdots,K$；$l=1,2$。

显然，式(4-38)需要$mK\varepsilon_{sub}$ FLOP，式(4-39)需要$2\left(\left(mK+3\right)\varepsilon_{mul}+\left(mK+1\right)\varepsilon_{pow}+mK\varepsilon_{sub}+mK\varepsilon_{div}+mK\varepsilon_{exp}\right)$FLOPs。为了得到$\kappa_{i,k}$，还

需要 $mK\varepsilon_{com}$ FLOPs。

获得 $\delta\left(l-\kappa_{i,k}^{(\eta+1)}\right)$ 之后，需要计算下式：

$$\alpha_l^{(\eta+1)}=\frac{1}{mK}\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)} \tag{4-40}$$

$$\mu_l^{(\eta+1)}=\frac{\sum_{i=1}^{m}\sum_{k=1}^{K}\left(z_{i,k}-y_{i,k}\right)\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{4-41}$$

$$\sigma_l^{2,(\eta+1)}=\frac{\sum_{i=1}^{m}\sum_{k=1}^{K}\left(z_{i,k}-y_{i,k}-\mu_l^{(\eta+1)}\right)^2\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{4-42}$$

很容易验证式(4-40)计算 $\alpha_l^{(\eta+1)}$ 需要 $\left(mK-1\right)\varepsilon_{add}+1\varepsilon_{div}+1\varepsilon_{sub}$ FLOPs，式(4-41)计算 $\mu_l^{(\eta+1)}$ 需要 $2\left(mK\varepsilon_{mul}+\left(mK-1\right)\varepsilon_{add}+\varepsilon_{div}\right)$ FLOPs，式(4-42)计算 $\sigma_l^{2,(\eta+1)}$ 需要 $2\left(mK\varepsilon_{mul}+\left(mK+1\right)\varepsilon_{pow}+\varepsilon_{sub}+\varepsilon_{div}+\left(mK-1\right)\varepsilon_{add}\right)$。定义 $FL\left(\boldsymbol{\theta}\right)$ 为在一次 JMAP-ML 迭代中估计 $\boldsymbol{\theta}$ 所消耗的 FLOPs 总数，则其等于总的 FLOPs。

$$\begin{aligned}FL\left(\boldsymbol{\theta}\right)=&\left(5mK-5\right)\varepsilon_{add}+(3mK+3)\varepsilon_{sub}\\&+\left(6mK+6\right)\varepsilon_{mul}+\left(2mK+5\right)\varepsilon_{div}\\&+2mK\varepsilon_{exp}+\left(4mK+4\right)\varepsilon_{pow}+mK\varepsilon_{com}\end{aligned} \tag{4-43}$$

最后，设 $N_{itr}^{JMAP-ML}$ 为达到 JMAP-ML 算法收敛的迭代次数，则最终 JMAP-ML 估计值的总 FLOPs 为：

$$FL_{JMAP-ML}\approx N_{iter}^{JMAP-ML}FL(\boldsymbol{\theta}) \tag{4-44}$$

4.5 基于联合最大后验-最大似然估计的 FDIAs 定位

在智能电网中，FDIAs 的定位是一项关键任务。为了有效地定位这些攻击，本文提出了一种基于 JMAP-ML 的算法来求解 GMM 参数。本章在第三章的基础上，将基于 AIEKF 的 FDIAs 检测方法作为全局检测，当检测到系统中存在 FDIAs

后，在利用 JMAP-ML 算法对受到攻击的测量数据进行定位，筛选出受到篡改的数据。JMAP-ML 算法的定位原理为基于对潜在变量数值的分析，即 1 代表测量值为正常，2 则表示测量值受到攻击。正如第二章中所讨论的，攻击者若想成功地改变某一节点的状态估计值，必须对与该状态相关的所有测量值进行篡改。这意味着，状态估计值的变化不仅依赖于单一测量值的变化，而是涉及到整个测量值集合的协同作用。因此，攻击的实施需要攻击者具备对多个测量值进行同步操控的能力。本章所利用的思想正是基于这一特性，通过分析测量值之间的相关性，可以精确地定位出受攻击的节点。

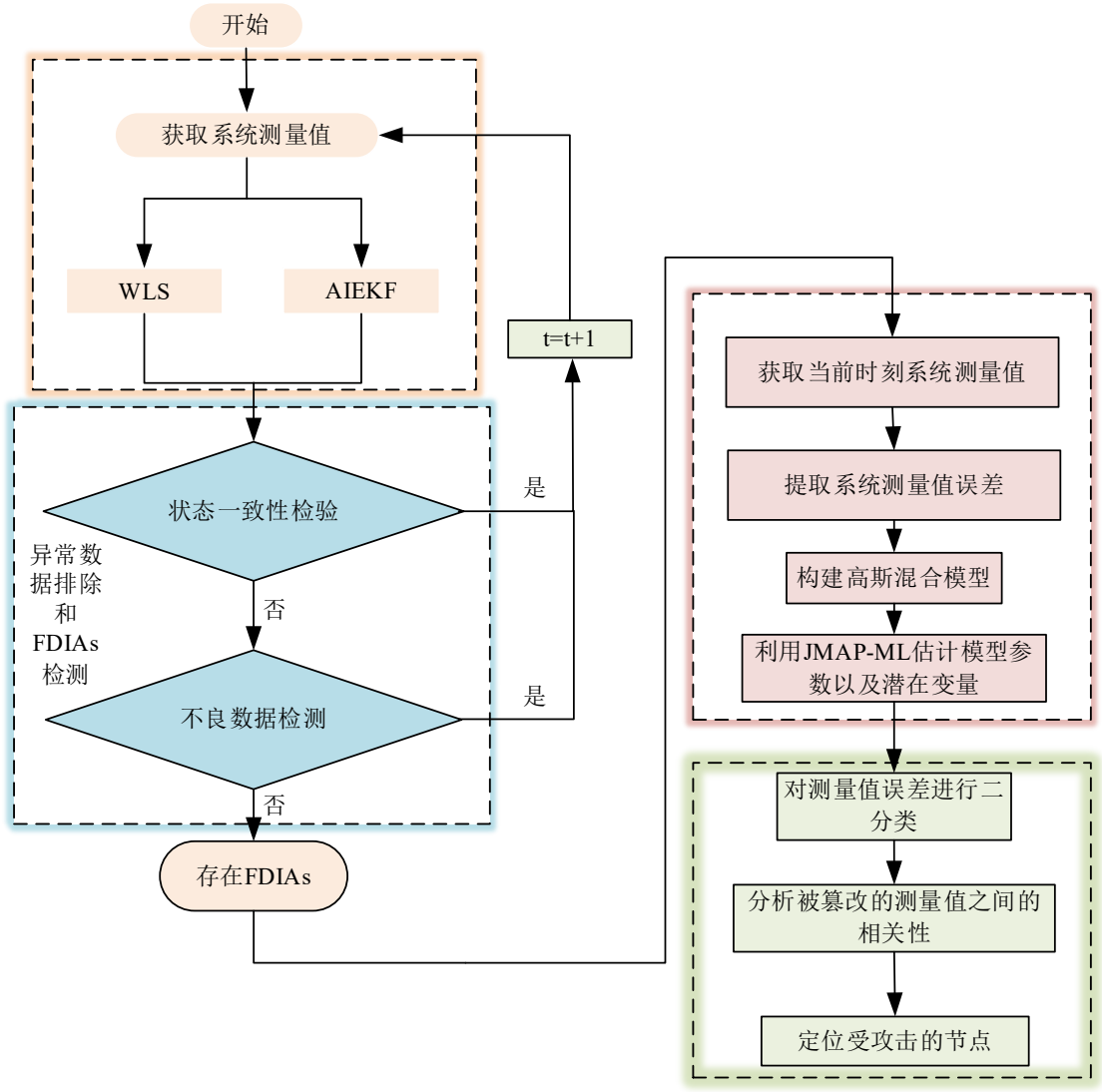


图 4-2 基于 JMAP-ML 的 FDIAs 定位流程图

图 4-2 是基于 JMAP-ML 算法的 FDIAs 定位流程图。首先，利用基于 AIEKF 的 FDIAs 检测算法进行全局检测。在检测到 FDIAs 后，提取该时刻的系统测量

值误差，并带入 GMM 中，利用 JAMP-ML 算法求解模型参数，即在 MAP 步和 ML 步的相互迭代中，求解潜在变量κ和模型参数θ。潜在变量κ的具体数值标志着该测量值是否收到攻击，利用得到的潜在变量κ的值确定受到篡改的测量值，然后通过分析这些测量值之间的相关性，定位出受攻击的节点。

利用 JMAP-ML 算法求解 GMM 的参数以此实现 FDIAs 定位的过程，也可以同步实现 FDIAs 的检测，但是当系统中发生负载或发电机突变或者测量值噪声过大时，可能使得 JMAP-ML 分类结果不准确，从而降低对 FDIAs 定位的精度，而基于 AIEKF 的 FDIAs 检测方法可以将上述情况排除在外。另外，基于状态估计的 FDIAs 定位方法在定位过程中，进行全局检测的次数远远小于构建检测矩阵而进行区域检测的次数。因此，为了定位出具体的攻击节点，将第三章所提出的方法作为全局检测，检测出 FDIAs 后，利用本章所提出的 FDIAs 定位方法进行定位，在实时检测的基础上，实现准确地定位。

4.6 仿真设计与结果分析

在本节中，通过 IEEE-14 节点标准系统和 IEEE-30 节点标准系统验证了所提出算法的可行性。与上一章使用的仿真软件相同，本章在 Matlab2021b 软件中进行仿真，并使用 Matpower 7.1 功率仿真包计算出最优潮流，得到了真实的测量值。然后，将高斯白噪声作为传感器测量值进行叠加，作为传感器测量值。在不同攻击场景下设计不同的攻击向量，并与传感器测量值进行叠加，作为 FDIAs 发生后系统所接收的测量值。利用基于 JMAP-ML 算法的定位方法进行仿真测试，以此来验证本章所提出方法的有效性。

4.6.1 IEEE-14 节点标准系统的 FDIAs 定位

IEEE-14 节点标准系统的结构图如图 2-3 所示，这里便不再给出。表 4-3 总结了在 IEEE-14 节点标准系统仿真时设定的模拟参数。表中相关参数说明如下：m 为测量值向量的维数；K 表示测量组数；α_1 和 α_2 为各成分的比例系数；μ_1 和 μ_2 分别为高斯混合模型中的均值;σ_1 和 σ_2 表示高斯混合模型中的方差；Δ 为收敛容差；$N_{itr}^{\max}$ 是最大迭代次数。

表 4-3 仿真参数设置

参数	值
m	41
K	40
α_1	0.8
α_2	0 .2
μ_1	0
μ_2	0.03
σ_1	0.1
σ_2	0.05
Δ	10^{-6}
$N_{itr}^{\max}$	50

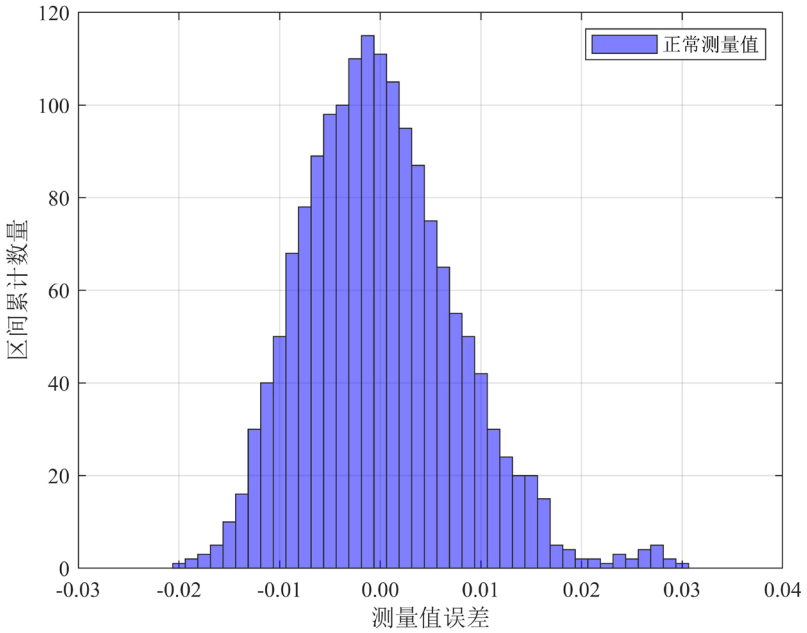


图 4-3 正常情况下测量值误差分布

图 4-3 模拟了 40 组测量值误差所包含的 1640 个测量值误差的分布，从图中可以看出，正常情况下测量值误差e_i是具有高斯分布特性，即$e_i \sim \mathcal{N}\left(\mu_1,\sigma_1^2\right)$。然而，当系统受到 FDIAs 时，部分测量值误差会发生变化，即从e_i变为e_i+a_i，与

原先相比，攻击后的测量值误差服从于新的高斯分布，即 $e_i + a_i \sim \mathcal{N}\left(\mu_2, \sigma_2^2\right)$，图 4-4 给出了攻击后的系统测量值误差分布特性，从图 4-4 可以看出，攻击后的系统测量值误差发生了变化，使得收受到攻击的测量值与未受到攻击的测量值具有不同特性的高斯分布，构成了 GMM。

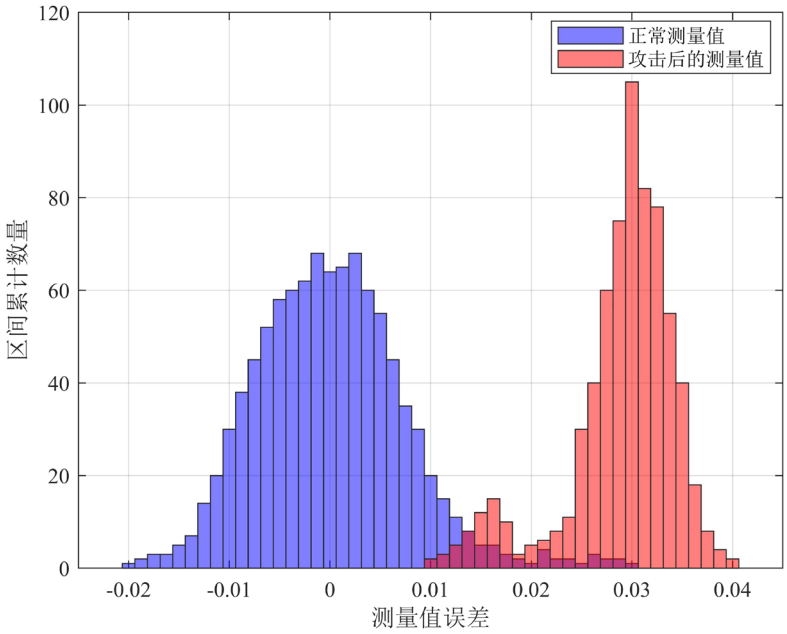


图 4-4 FDIAs 下的测量值误差分布

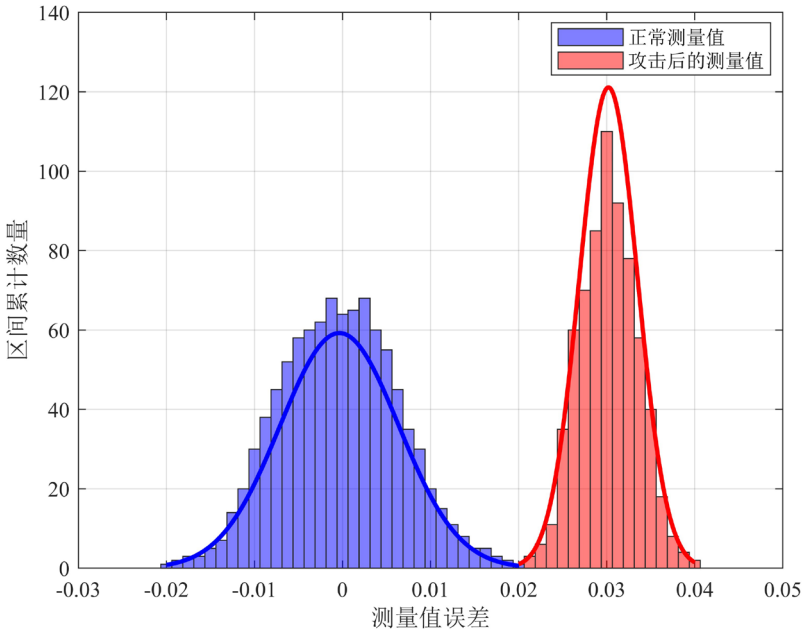


图 4-5 JMAP-ML 算法下攻击后的测量值误差分布

紧接着，为了验证所提出算法的有效性，使用 JMAP-ML 算法对 40 组包含攻击的量测值误差进行分类，为了直观地看出其特性，对分类的误差分布进行了拟合，最终结果如图 4-5 所示。从图 4-5 可以看出，攻击后的测量值误差满足不同特性的高斯分布，JMAP-ML 算法具有很好的分类效果。

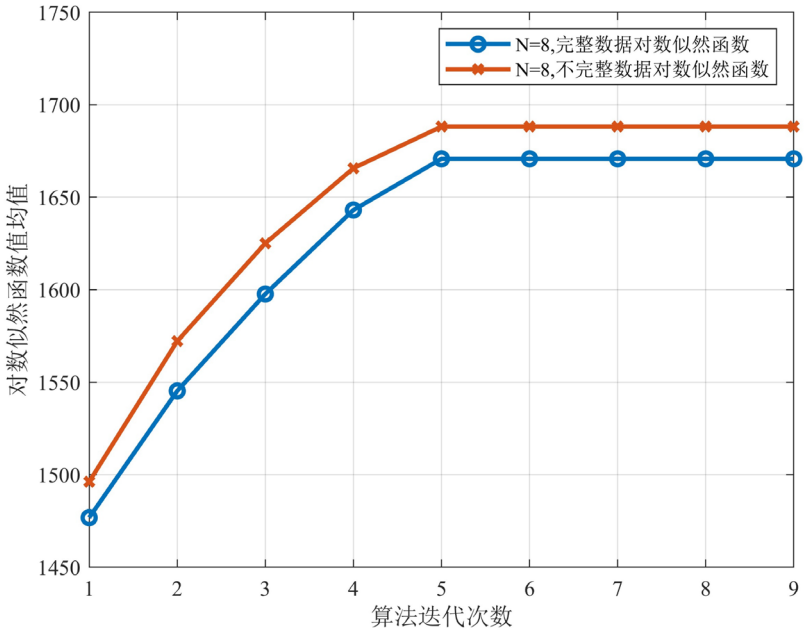


图 4-6 JMAP-ML 算法下对数似然函数与迭代次数的关系

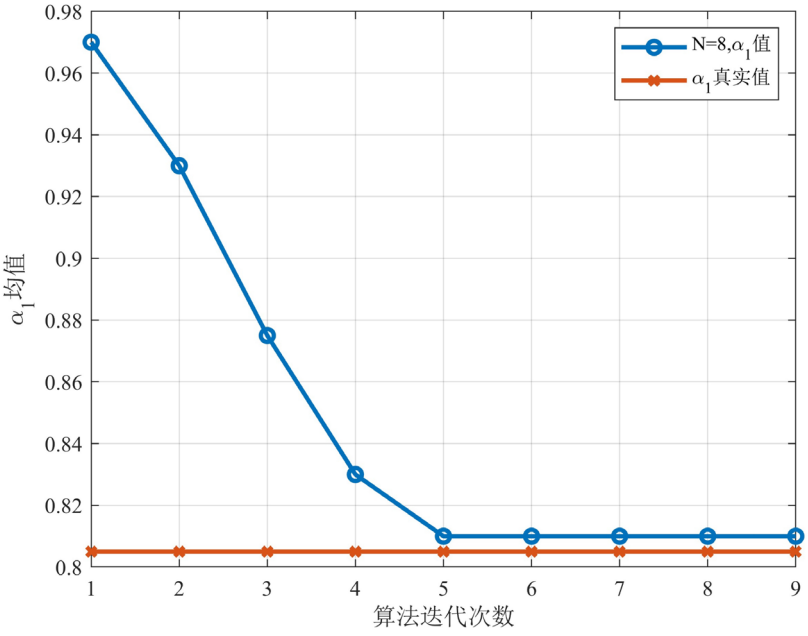


图 4-7 α_1 均值与迭代次数关系变化图

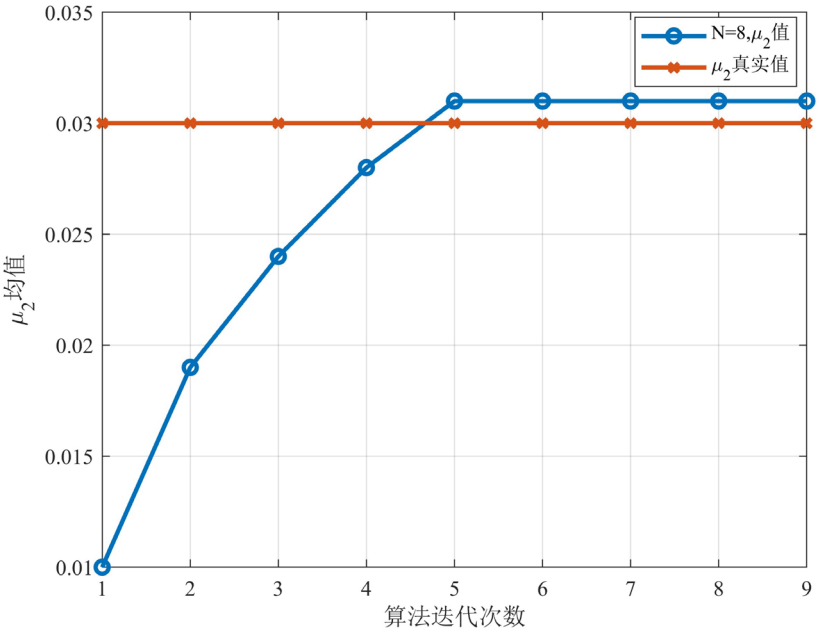


图 4-8 μ_2 均值与迭代次数关系变化图

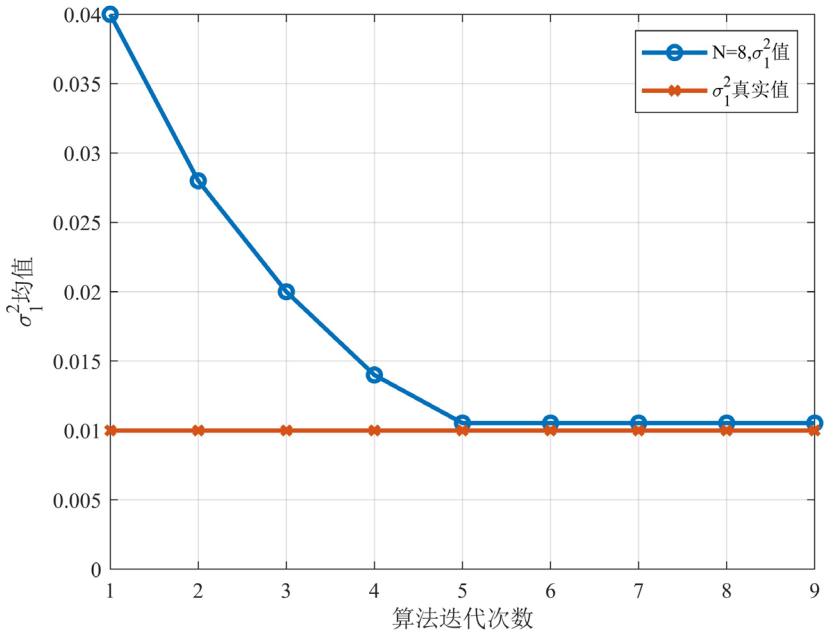


图 4-9 σ_1^2 均值与迭代次数关系变化图

为了证明算法的快速收敛性，假设攻击的测量值数量 $f=8$，并使用蒙特卡罗方法进行 1200 个独立实验。同时，记录不完整数据 $\mathcal{L}_I$ 和完整数据 $\mathcal{L}_C$ 的对数似然函数值均值的变化过程。图 4-6 展示了两者的均值与迭代次数之间的关系。同

时计算混合参数估计$\boldsymbol{\theta}$的均值，图 4-7、图 4-8 和图 4-9 展示了混合参数均值与迭代次数的关系。由于空间有限，只给出了α_1、μ_2、σ_1^2三个参数随迭代次数变化过程图，此外图中给出了α_1、μ_2、σ_1^2的真实值。

将上述图中的一些重要结论解释如下：

(1)从图 4-6 中可以看出，不完整数据和完整数据对数似然单调地增加迭代，直到满足收敛条件，这与上述的理论证明是一致的。

(2)从图 4-7、图 4-8 和图 4-9 可以看出，JMAP-ML 算法生成了一个有偏估计器，其可以高精度地估计相关参数。

(3)经过 5 次迭代，JMAP-ML 算法收敛。

在迭代算法中，样本数目决定了参数的估计精度，其随着样本数目的增加而增高。假设系统中正常测量值为正样本，被攻击的测量值为负样本，在正负样本组成的高斯混合模型中，各自的分布参数的估计精度受样本数目的影响。当受攻击的节点增加时，测量值中需要篡改的测量值数目就越多，正样本的高斯分布参数的估计精度随着样本数目的减少而下降，相反，负样本的高斯分布参数的估计精度随着样本数目的增加而增高。

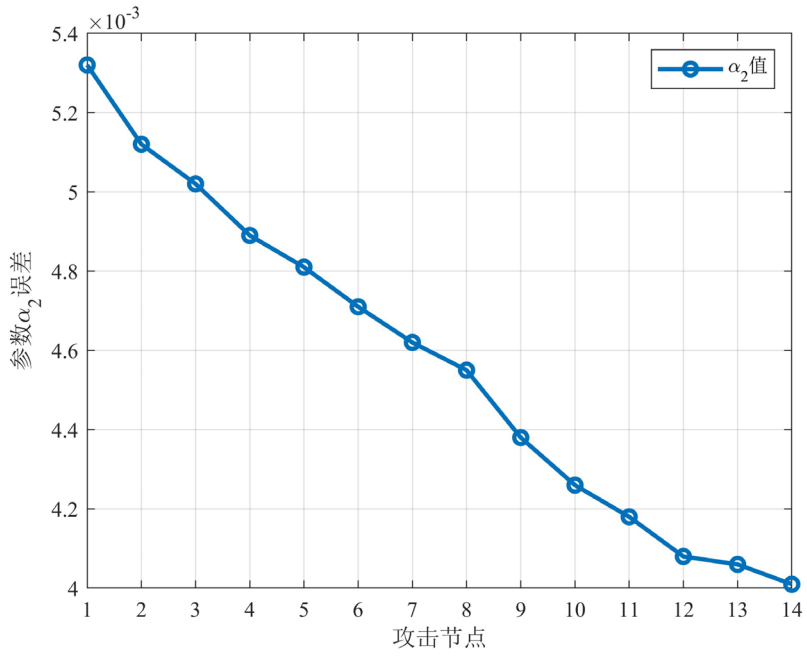


图 4-10 α_2 估计精度与受攻击节点数目关系图

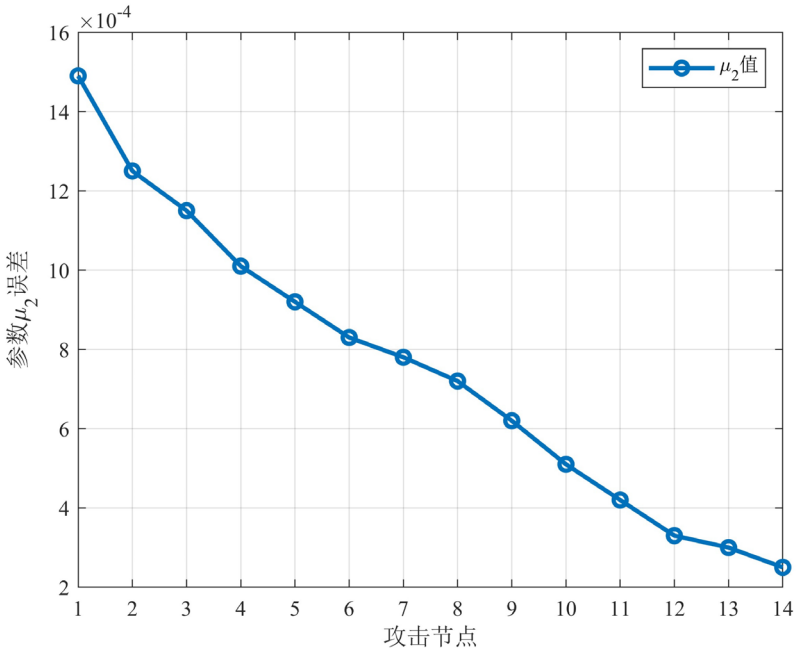


图 4-11 μ_2 估计精度与受攻击节点数目关系图

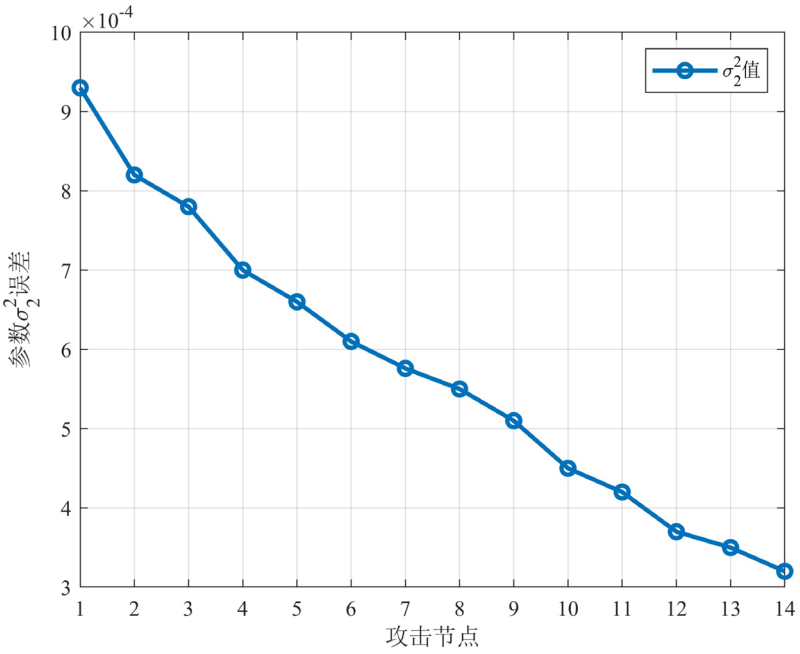


图 4-12 σ_2^2 估计精度与受攻击节点数目关系图

为了更好地突出 JMAP-ML 算法的估计性能，不同的攻击场景在仿真实验中被模拟，并使用该算法估计了混合模型的相关参数。由于空间有限，只给出了参数 α_2、μ_2、σ_2^2 的仿真结果图。从图 4-10、图 4-11 和图 4-12 中可以看出，随着

被攻击节点的增加，导致系统接收到的测量值中被篡改的测量值数目越来越多，即系统中负样本的数目增加。由于 JMAP-ML 算法是一个迭代算法，样本数目决定了参数估计的精度，因此，参数α_2、μ_2、σ_2^2的估计精度随着攻击节点数目的增加而增高。

使用 JMAP-ML 算法进行 GMM 参数估计后，利用潜在变量κ数值的不同可以定位出受攻击的测量值，之后利用测量值之间的相关性可定位出受攻击的节点。本章采用受试者工作特征(Receiver Operating Characteristic, ROC)曲线进行分析。ROC 曲线以 TPR 为纵坐标，以 FPR 为横坐标，ROC 曲线表征 TPR 和 FPR 之间的权衡。

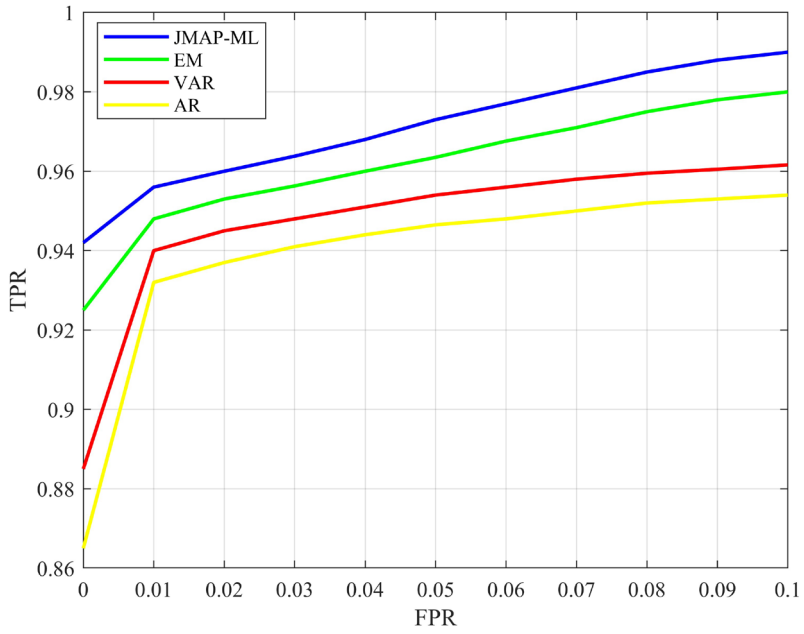


图 4-13 四种算法的 ROC 曲线

将本文提出的 JMAP-ML 算法与先前提出的基于自回归(Autoregression, AR)的定位算法、基于向量自回归(Vector Autoregressive, VAR)[72]的定位算法和基于 EM[73]的定位算法的性能进行了比较。为了保证算法的性能不受测量值数据的影响，将相同的测量值数据用于四种算法仿真过程。

在 FDIAs 存在的情况下，四种方法的 ROC 曲线如图 4-13 所示。从图中可以看出，随着 FPR 的增大，四种算法的 TPR 也不断增加。但本文提出的 JMAP-ML 算法的 TPR 是四种方法中最高的。具体来说，当 FPR 为 5%时，JMAP-ML

算法的 TPR 为 97.6%，EM 算法的 TPR 为 96.2%，VAR 算法的 TPR 为 95.3%，AR 算法的 TPR 为 94.7%，从而说明 JMAP-ML 算法的 FPR 低，TPR 高。在利用潜在变量的值定位到被篡改的测量值之后，通过分析被篡改的测量值之间的相关性，可以检测出受到攻击的节点，即 FDIAs 定位。

4.6.2 IEEE-30 节点标准系统的 FDIAs 定位

对于智能电网来说，FDIAs 的定位是在电网节点上进行的。根据识别出的相邻且相互关联的异常测量值，定位出系统中被攻击的节点。下面以 IEEE-30 节点标准系统为例，对本章所提出算法的性能进一步进行分析。IEEE-30 节点标准系统的结构图如图 2-8 所示，这里便不再给出。

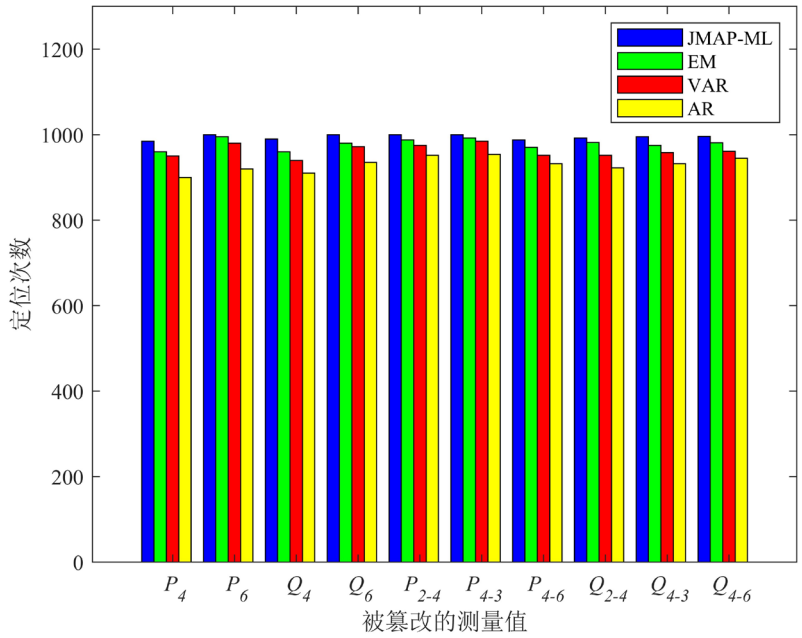


图 4-14 四种算法下被篡改的测量值的定位结果图

在模拟仿真中，FDIAs 同时发生在节点 4 和节点 10 上，对两个节点的电压幅值进行篡改。正如第 2 章所讲，攻击者要实现 FDIAs，必须修改与节点 4 和节点 10 上电压幅值相关的系统所接收的所有测量值。由于空间有限，没有提供关于总线 10 电压幅值的测量值定位情况。当总线 4 电压幅值被攻击时，需要篡改的测量值为P_4、P_6、Q_4、Q_6、P_{2-4}、P_{4-3}、P_{4-6}、Q_{2-4}、Q_{4-3}、Q_{4-6}。利用蒙特卡洛模拟 1000 次独立实验，记录四种算法的定位结果，相关结果如图 4-14 所

示。从图中可以看出，与其他三种算法相比，JMAP-ML 算法具有更好的定位性能。在定位出被篡改的测量值后，不难发现，测量值 P_4、P_6、Q_4、Q_6、P_{2-4}、P_{4-3}、P_{4-6}、Q_{2-4}、Q_{4-3}、Q_{4-6} 均与节点 4 相关，利用测量值之间的相关性，定位出受攻击的节点，定位结果如图 4-15 所示。如图所示，AR 算法的定位准确率为 90%，VAR 算法的定位准确率为 94.2%，EM 算法的定位准确率为 96.3，而 JMAP-ML 算法相比于其他三种定位算法具有最高的定位准确率，高达 98.8%。

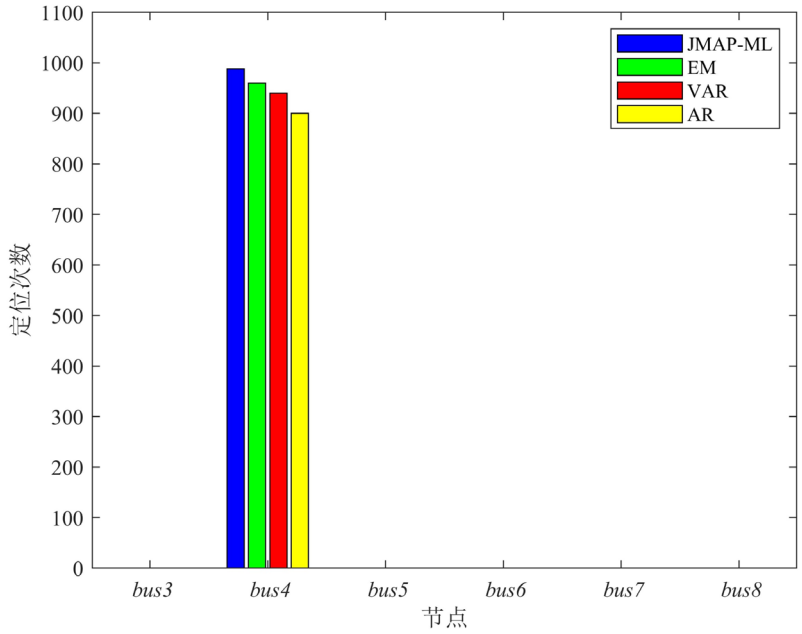


图 4-15 四种算法下被攻击节点的定位结果图

4.7 本章小结

在第三章基于自适应插值扩展卡尔曼滤波器的 FDIAs 检测算法实现异常测量值的排除和 FDIAs 的检测后，本章提出了基于 JMAP-ML 算法的智能电网 FDIAs 定位算法。首先，考虑到 FDIAs 的产生是以篡改系统接收到的测量值为基础，本章将测量值误差模型重新建模为 GMM，并在 GMM 中引入潜在变量以此来简化模型参数求解问题。其次，提出了使用 JMAP-ML 算法求解 GMM 参数，将攻击时刻的测量数据导入 GMM 中，在混合模型参数的基础上实现了对 FDIAs 的定位。最后，在 IEEE-14 节点和 IEEE-30 节点标准系统上对 FDIAs 进行定位，

仿真结果表明，不同于状态估计定位方法的复杂过程，JAMP-ML 算法直接通过求解 GMM 参数实现了 FDIAs 的定位。

第5章 总结与展望

5.1 全文总结

随着电力系统智能化转型进程加速，以智能计量装置与传感终端为代表的物联网设备已深度渗透至发、输、变、配全环节，通过信息物理深度耦合构建了具备多维感知与协同控制特征的智能电网。虽然这些网络技术，如传感、通信和智能测量设备，增强了电力系统的运行和可靠性，但也使系统暴露在潜在的网络攻击之下，对智能电网的网络攻击会危及信息的可用性、完整性和机密性。FDIAs是一种专门针对智能电网中状态估计数据完整性的新型攻击方法。攻击者通过智能电网传感器、控制器、远程控制单元注入虚假数据，影响潮流计算、控制决策等，篡改电网原始数据。这种情况可能导致电网设备出现故障，严重时可能导致电网完全瘫痪，不仅对电网安全造成严重威胁，而且还可能造成巨大的经济损失。因此，为保障智能电网的稳定运行，针对 FDIAs 开展检测工作具有重大意义。本文从 FDIAs 的检测入手，主要完成了以下几部分工作：

(1)研究了智能电网中 FDIAs 的原理与建模。首先描述了电力系统状态估计模型，在状态估计理论的基础上对 BDD 原理进行了描述。接着，对 FDIAs 的形成过程进行了详细分析，其中包括 FDIAs 的原理以及其构建。最后在状态估计的基础上构造出攻击向量并在 IEEE-14 节点和 IEEE-30 节点标准系统中验证了其有效性。

(2)提出了一种基于自适应插值扩展卡尔曼滤波器的 FDIAs 检测方法。针对 EKF 进行状态估计时，忽略了高阶项，造成了线性化误差。引入自适应插值策略，对 EKF 进行优化，通过在连续测量之间进行线性化插值，实现更为准确的状态估计。在此基础上，将 AIEKF 与 WLS 进行结合，利用两种估计器在面对 FDIAs 时不同的反应(WLS 立即变化，AIEKF 是逐渐发生变化，最终二者都会收敛到攻击后的状态值)，引入欧式距离作为检测指标，以此检测 FDIAs。最后在 IEEE-14 节点和 IEEE-30 节点标准系统中进行了仿真实验，结果表明 AIEKF 算法误差更小，检测效果较好。

(3)提出了一种基于联合最大后验-最大似然估计的 FDIAs 定位方法。针对传

统的基于状态估计的方法在定位出受攻击的节点时过程比较复杂且局限性较大，利用统计学习的思想，将攻击向量可以和测量噪声视为一个整体，构建关于测量噪声的 GMM。通过基于 AIEKF 的 FDIAs 检测方法进行全局检测，检测出 FDIAs 并排除异常测量值，将攻击发生时刻的测量值导入 GMM，利用 JMAP-ML 算法求解 GMM 的分布参数，对测量值进行二分类，定位出受到篡改的测量值。通过分析测量值的相关性，实现 FDIAs 定位。最后在 IEEE-14 节点和 IEEE-30 节点标准系统中进行了仿真实验，结果表明 JMAP-ML 算法直接通过求解 GMM 参数实现 FDIAs 的定位，简化了定位过程。

5.2 未来展望

本文主要针对智能电网中虚假数据注入攻击检测问题展开了研究，虽然取得了一定成效，但是研究中仍然存在一些不足之处，需要进一步讨论分析，如：

(1)在本文中，关于测量噪声模型均建模为高斯噪声，然而在实际的智能电网中可能存在各种各样的测量噪声。文中所使用的算法，如 WLS、AIEKF 和 JMAP-ML 算法均是基于高斯噪声展开的，这三种算法面对其他噪声时的估计性能有待进一步验证。

(2)本文所使用的 IEEE-14 节点和 IEEE-30 节点标准系统中均是 Matpower 中的模拟仿真系统，与真实的电力系统有一定区别，未来的研究应当在实际电网中测试并对本文提出的算法进行实时改进。

(3)本文只考虑了在 FDIAs 发生后如何去检测，此时已经对电网造成了一定的损失。未来的研究应该着眼于如何防御 FDIAs，开发出一套防御方案，从源头上阻止 FDIAs 的发生。

参考文献

[1] Wang P, Govindarasu M. Multi-agent based attack-resilient system integrity protection for smart grid[J]. IEEE Transactions on Smart Grid, 2020, 11(4): 3447-3456.

[2] 赵俊华, 文福拴, 薛禹胜, 等. 电力 CPS 的架构及其实现技术与挑战[J]. 电力系统自动化, 2010, 34(16): 1-7.

[3] 吴在军, 徐东亮, 徐俊俊, 等. 信息物理多重攻击下配电网状态估计关键技术评述[J]. 电力系统自动化, 2024, 48(06): 127-138.

[4] Wang X, Luo X, Zhang M, et al. Detection and isolation of false data injection attacks in smart grid via unknown input interval observer[J]. IEEE Internet of Things Journal, 2020, 7(4): 3214-3229.

[5] 王琦, 李梦雅, 汤奕, 等. 电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J]. 电力系统自动化, 2019, 43(09): 9-21.

[6] 杨玉泽, 刘文霞, 李承泽, 等. 面向电力 SCADA 系统的 FDIA 检测方法综述[J]. 中国电机工程学报, 2023, 43(22): 8602-8622.

[7] Zhuang P, Deng R, Liang H. False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 6000-6013.

[8] Alanazi M, Mahmood A, Mohammad J. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues[J]. Computers & Security, 2023, 125: 103028.

[9] Zhou J, Chen B, Yu L. Intermediate-variable-based estimation for FDI attacks in cyber-physical systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs. 2020, 67(11): 2762-2766.

[10] Tian J, Tan R, Guan X, et al. Moving target defense approach to detecting Stuxnet-like attacks[J]. IEEE Transactions on Smart Grid, 2020, 11(1): 291-300.

[11] Liang G, Weller S, 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.

[12] Pang Z, Fan L, Dong Z, et al. False data injection attacks against partial sensor measurements of networked control systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(1): 149-153.

[13] 王琦, 郜伟, 汤奕, 等. 面向电力信息物理系统的虚假数据注入攻击研究综述[J], 自动化学报, 2019, 45(01): 72-83.

[14] 王先培, 田猛, 董政呈, 等. 输电网虚假数据攻击研究综述[J]. 电网技术, 2016, 40(11): 3406-3414.

[15] 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, 2018, 4(1): 48-59.

[16] Liu Y, Ning P, Reiter M. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2011, 14(1): 1-33.

[17] Mukherjee D. Data-driven false data injection attack: A low-rank approach[J]. IEEE Transactions on Smart Grid, 2022, 13(3): 2479–2482.

[18] 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 of Things Journal, 2022, 9(9): 6893–6904.

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

[20] 彭大天, 董建敏, 蔡忠闽, 等. 假数据注入攻击下信息物理融合系统的稳定性研究[J]. 自动化学报, 2019, 45(01): 198-207.

[21] Yang Q, Yang J, Yu W, et al. On false data-injection attacks against power system state estimation: modeling and countermeasures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(3):717-729.

[22] Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems[J].

IEEE Transactions on Smart Grid, 2011, 2(2):382-390.

[23] Liu X, Bao Z, Lu D, et al. Modeling of local false data injection attacks with reduced network information[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686-1696.

[24] 杨玉泽, 刘文霞, 刘耕铭, 等. 不完全信息下计及残差污染的虚假数据注入攻击研究[J/OL]. 中国电机工程学报, 1-14[2024-10-18].

[25] Gao S, Lei J, Wei X, et al. A novel bilevel false data injection attack model based on pre- and post- dispatch[J]. IEEE Transactions on Smart Grid, 2022, 13(3): 2487-2490.

[26] Kim J, Tong L. On topology attack of a smart grid: undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(7): 1294-1305.

[27] 邓彬, 饶爽, 胡亚荣, 等. 基于子空间跟踪算法的盲虚假数据攻击[J]. 电气自动化, 2023, 45(02): 82-84.

[28] 李雪, 钟慧欣, 孙庆, 等. 基于快速回归算法的虚假数据攻击构造新方法[J]. 仪器仪表学报, 2018, 39(03): 179-189.

[29] Bi S, Zhang Y. Graphical methods for defense against false-data injection attacks on power system state estimation[J]. IEEE Transactions on Smart Grid, 2014, 5(3): 1216-1227.

[30] 罗小元, 何俊楠, 王新宇, 等. 智能电网虚假数据注入攻击弹性防御策略的拓扑优化[J]. 自动化学报, 2023, 49(06): 1326-1338.

[31] Hao J, Kang E, Sun J, et al. An adaptive Markov strategy for defending smart grid false data injection from malicious attackers[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 2398-2408.

[32] 蔡星浦, 王琦, 邰伟, 等. 基于多阶段博弈的电力 CPS 虚假数据注入攻击防御方法[J]. 电力建设, 2019, 40(05): 48-54.

[33] 李军, 李韬. 基于贝叶斯序贯博弈模型的智能电网信息物理安全分析[J]. 自动化学报, 2019, 45(01): 98-109.

[34] Higgins M, Teng F, Parisini T. Stealthy MTD against unsupervised learning-based

blind FDI attacks in power systems[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1275-1287.

[35] Yang X, Lin J, Moulema P, et al. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems[C]// 2012 IEEE 32nd International Conference on Distributed Computing Systems, Macau, China, 2012: 92-101.

[36] 刘鑫蕊, 吴泽群. 面向智能电网的空间隐蔽型恶性数据注入攻击在线防御研究[J]. 中国电机工程学报, 2020, 40(08): 2546-2559.

[37] Guo H, Sun J, Pang H, et al. Event-based optimal stealthy false data-injection attacks against remote state estimation systems [J]. IEEE Transactions on Cybernetics, 2023, 53(10): 6714-6724.

[38] Zhao J, Zhang G, La M, et al. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1580-1590.

[39] Kurt M, Yılmaz Y, Wang X. Distributed quickest detection of cyber-attacks in smart grid[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2015-2030.

[40] Khalaf M, Youssef A, El-Saadany E. Joint detection and mitigation of false data injection attacks in AGC systems[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 4985-4995.

[41] Manandhar K, Cao X, Hu F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter[J]. IEEE Transactions on Control of Network Systems, 2014, 1(4): 370-379.

[42] 庞清乐, 韩松易, 周泰, 等. 基于 ASRUKF 和 IMC 算法的电力信息物理系统虚假数据注入攻击检测[J]. 智慧电力, 2024, 52(07): 111-118.

[43] 常梦言, 刘永慧. 虚假数据注入攻击下基于容积卡尔曼滤波的电力系统状态估计[J]. 电力科学与技术学报, 2024, 39(03): 10-18.

[44] 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.

[45] 何耀，周聪，郑凌月，等. 基于扩展卡尔曼滤波的虚假数据攻击检测方法[J]. 中国电力，2017，50(10)：35-40.

[46] KARIMIPOUR H，DINAVAHI V．Robust massively parallel dynamic state estimation of power systems against cyber-attack[J]．IEEE Access，2017，6：2984-2995.

[47] 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.

[48] 束洪春, 杨永银, 赵红芳, 等. 基于自适应加权混合预测的电网虚假数据注入攻击检测[J/OL]. 电网技术, 1-10[2024-11-12].

[49] Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in AC state estimation [J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2476-2483.

[50] SINGH S K, KHANNA K, BOSE R, et al. Joint-transformation-based detection of false data injection attacks in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(1): 89-97.

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

[52] Ghaderi M, Gheitasi K, Lucia W. A blended active detection strategy for false data injection attacks in cyber-physical systems[J]. IEEE Transactions on Control of Network Systems, 2021, 8(1): 168-176.

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

[54] Esmalifalak M, Liu L, Nguyen N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2017, 11(3): 1644-1652.

[55] Aboelwafa M, Seddik K, Eldefrawy M, et al. A machine-learning-based technique for false data injection attacks detection in industrial IoT[J]. IEEE Internet of Things Journal, 2020, 7(9): 8462-8471.

[56] Yu J, Hou Y, Li V. Online false data injection attack detection with wavelet

transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271-3280.

[57] 苏向敬, 邓超, 栗风永, 等. 基于 MGAT-TCN 模型的可解释电网虚假数据注入攻击检测方法[J]. 电力系统自动化, 2024, 48(02): 118-127.

[58] 方正刚. 基于通道融合的 Res-CNN-LSTM 电网虚假数据注入攻击检测[J]. 电气技术, 2024, 25(03): 11-17+62.

[59] Du Z, Yan Z, Xu Y. A dimensional augmentation-based data-driven method for detecting false data injection in smart meters[J]. IEEE Transactions on Smart Grid, 2024, 15(1): 1180-1183.

[60] Mohammadpourfard M, Sami A, Seifi A R. A statistical unsupervised method against false data injection attacks: A visualization-based approach[J]. Expert Systems with Applications, 2017, 84: 242-261.

[61] Mohammadpourfard M, Sami A, Weng Y. Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations [J]. IEEE Transactions on Sustainable Energy, 2018, 9(3): 1349-1364.

[62] Foroutan S A, Salmasi, F R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method[J]. IET Cyber-Physical Systems: Theory & Applications, 2017, 2(4): 161-171.

[63] Deng R, Zhuang P, Liang H. False data injection attacks against state estimation in power distribution systems[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 2871-2881.

[64] Yuan C, Zhou Y, Liu G, et al. Graph computing-based WLS fast decoupled state estimation[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2440-2451.

[65] Hug G, Giampapa J. 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.

[66] Akhlaghi S, Zhou N, Huang Z. A multi-step adaptive interpolation approach to

mitigating the impact of nonlinearity on dynamic state estimation[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 3102-3111.

[67] Hu P, Gao W, Li Y, 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.

[68] Xu R, Wang R, Guan Z, et al. Achieving efficient detection against false data injection attacks in smart grid[J]. IEEE Access, 2017, 5: 13787-13798.

[69] Yin F, Fritsche C, Gustafsson F, et al. EM- and JMAP-ML based joint estimation algorithms for robust wireless geolocation in mixed LOS/NLOS environments[J]. IEEE Transactions on Signal Processing, 2014, 62(1): 168-182.

[70] Gupta M, Chen Y. Theory and use of the EM algorithm[J], Now Foundations and Trends, 2010, 4(3): 223-296.

[71] Boyd S, Vandenberghe L. Convex optimization[M]. New York, USA: Cambridge University Press, 2004.

[72] Shi W, Wang Y, Jin Q, et al. PDL: An efficient prediction-based false data injection attack detection and location in smart grid[C]// 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018: 676-681.

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

攻读硕士期间取得的学术成果

[1] Zhang G, Gao W, Li Y, et al. Detection of false data injection attacks in a smart grid based on WLS and an adaptive interpolation extended Kalman filter[J]. Energies 2023, 16(20): 7203.

[2] Zhang G, Gao W, Li Y, et al. Detection and localization of false data injection attacks in smart grid based on joint maximum a posteriori-maximum likelihood[J]. IEEE Access, 2023, 11: 133867-133878.

[3] Zhang G, Gao W, Li Y, et al. Joint detection and localization of false data injection attacks in smart grids: An enhanced state estimation approach[J]. Computers and Electrical Engineering, 2024, 120: 109834.

[4] Zhang G, Gao W, Li Y, et al. A two-stage recovery strategy against false data injection attacks in smart grids[J]. Electric Power Systems Research, 2025, 245: 111632.

致谢

蒙天赐良缘，幸得三载寒窗，学有所成，倍感欣慰。光阴荏苒，似水流年；踟蹰回首，百感交集。思往昔，求学路上，坎坷难行；幸得诸师长、同窗、亲友相助，方能迎难而上，终有所获。值此论文完稿之际，不禁感怀至深，谨以此文，略表谢意。

首先，谨谢恩师高文根教授，恩德深重，教诲良多。先生博学多识，治学严谨，凡于论文研讨之际，必循循善诱，析疑释难。每临困顿时，先生不辞劳苦，倾力相助，使弟子得以豁然开朗，行有所成。若无恩师之引领，焉能至今日之成果？此恩此情，铭刻于心，永志不忘。

其次，感怀同门诸君，皆学术良友，共砺共勉。谢师兄师姐、师弟师妹及同届诸同学，携手共进，昼夜相伴；谢师弟师妹，承欢共读，探讨研学。思彼时，共探术理，激扬文字，乃学问精进之基；同室而居，齐心协力，共克难关，乃友情倍增之助。此情此景，没齿难忘。

尤感知己，情深义重。感怀挚爱女友静雨，伴我左右，共度艰辛。无论风雨阴晴，皆慰藉之言，倍增信心。承蒙之情，何以为报？惟愿今后执手共行，长相厮守。

又谢同窗友朋，室友浩哥、康哥、宏伟，及挚友阿乐等，三载相伴，欢声笑语共度。曾与尔等夜话长谈，畅论天地；携手并肩，共享光阴。汝等之情，铭刻于心，虽天南地北，仍愿情谊常在。

再谢家人父母，教养恩深，矢志不忘。昔年慈母抚育，含辛茹苦，严父教诲，字字珠玑。点滴亲情，铭刻心间；寸草之心，难报春晖。家之恩情，万死莫能忘。

末了，谨谢母校与各位良师，安徽工程大学之教诲，电气工程学院之关怀，皆使弟子获益匪浅。愿母校繁荣昌盛，桃李满天下；愿恩师康健长寿，学问日隆！

万语千言，不足为表；但愿此心，君子共知。愿我辈学子，学无止境，勇攀高峰！

尚德教学　唯实惟新