

[虚假数据]

电力系统虚假数据注入攻击检测关键技术

文/寇亮

国网吉林供电公司

针对智能电网中虚假数据注入攻击问题开展研究，系统分析攻击机理和特征，提出一种基于多维特征融合的攻击检测方法。该方法从时间维度、空间维度和物理约束维度提取特征，设计基于注意力机制的特征融合策略和多层检测模型，实现对攻击的有效识别。通过仿真实验和工程应用验证，所提方法在检测准确性、实时性和鲁棒性方面均优于现有方法，检测准确率达到96.8%。

智能电网建设正推动电力系统发生深刻转型。通过应用先进的传感测量、通信、信息处理和控制技术，智能电网实现发电、输电、变电、配电和用电全环节的智能化监测和管理。其中，广域测量系统（WAMS）和智能电表基础设施（AMI）的部署，使电网运行状态的实时监控成为可能，显著提升了运行效率和可靠性^[1]。作为支撑现代社会发展的重要基础设施，智能电网的安全稳定运行直接关系到国民经济和社会生活。然而，电力系统的智能化转型也带来新的安全挑战。随着信息通信技术的深度应用，系统各环节产生的数据量呈指数级增长，数据的真实性、完整性和可用性面临严峻挑战。同时，电力系统网络架构日益开放，与外部网络连接更加紧密，这使其更容易受到网络攻击威胁^[1,2]。在众多安全威胁中，虚假数据注入攻击（FDIA）因隐蔽性强、危害性大而备受关注。攻击者通过精心构造的虚假数据，可能绕过传统的坏数据检测机制，导致系统状态估计结果产生较大偏差，影响系统的监控和决策。这种攻击可能导致操作人员对系统运行状态产生误判，引发不当的控制指令，严重时可能造成局部或大面积停电事故^[2,3]。例如，攻击者可能通过注入虚假的负荷数据导致电

力调度决策失误，或通过篡改保护装置的测量数据引起误动作或拒动，危及电网设备和人身安全。因此，研究虚假数据注入攻击的检测技术，对保障电力系统的安全稳定运行具有重要意义。

电力系统虚假数据注入攻击机理分析

1. 电力系统数据采集架构

电力系统监控与数据采集（SCADA）系统采用分层分布式架构，是系统运行监控的核心。主站层包含数据处理服务器、实时数据库等核心设备，负责整体数据处理和监控；子站层由远程终端单元（RTU）、智能电子设备（IED）等现场设备构成，负责数据采集和控制指令执行。网络采用双层架构，通过专用通信网络连接主站与子站。

数据传输遵循严格的流程和协议规范。RTU和IED按预设周期采样电压、电流和功率等物理量，经预处理后通过加密传输上传至主站。主站系统进行数据解析和校验后，将数据存入实时数据库，并进行状态估计等计算，支持系统监控和决策^[4]。

系统关键测量点主要分布在变电站、重要用户接入点和线路关键节点，这些点的选择基于可观测性分析。变电站主要布置电压互感器（PT）和电流

互感器 (CT)；重要线路设置功率测量装置；用户接入点安装智能电表，这些数据对状态估计和安全分析至关重要。

2. 虚假数据注入攻击模型

虚假数据注入攻击可分为多种类型。按攻击目标分为针对状态估计、负荷预测、保护装置的攻击；按攻击方式分为随机型、定向型和协同型攻击。随机型攻击通过随机篡改数据干扰系统；定向型攻击针对特定目标实施精确打击；协同型攻击通过多点配合实现隐蔽性攻击。

攻击实施需要攻击者具备系统知识和攻击能力。攻击者可能通过网络漏洞或物理入侵方式操纵设备或篡改数据。实施过程中，攻击者需考虑系统物理约束和数据相关性，构造符合系统特征的虚假数据以降低检测风险^[5]。

这类攻击的影响是多方面的：可能导致状态估计失真，影响系统可观性；造成调度决策失误，引发稳定性问题；导致保护装置误动作，危及设备安全；影响电力市场运行，造成经济损失。

3. 攻击特征提取

电力系统测量数据具有显著的时间序列特征，正常运行时遵循特定时间模式。攻击可能破坏这种时间相关性，表现为数据突变或趋势异常。通过时间序列分析，可提取统计特征、趋势特征和周期特征，支持攻击检测。系统不同测量点间存在空间相关性，源于物理连接关系和运行特性。攻击可能破坏这种空间相关性，通过分析数据的空间分布特征、相关性结构和拓扑特征，可识别异常数据。此外，系统运行必须遵循物理定律和工程约束，包括基尔霍夫定律、功率平衡约束等。这些物理约束为识别虚假数据提供依据。通过建立基于物理模型的约束检验体系，可从物理层面发现数据异常，提高检测准确性。

基于多维特征融合的攻击检测方法

1. 特征融合框架设计

在电力系统虚假数据注入攻击检测中，合理的特征选择是提高检测效果的关键。基于对攻击特征的分析，本文从时间维度、空间维度和物理约束维度选择特征。在时间维度上，选择测量数据的均值、方差、峰度和偏度等统计特征，以及基于小波

变换的时频特征；在空间维度上，提取测量点之间的相关系数矩阵、拓扑关联特征等；在物理约束维度上，构建基于潮流方程的约束违背度指标。通过信息增益和特征重要性分析，筛选出对攻击检测最具显著性的特征子集^[6]。

为了消除不同维度特征之间的量纲差异，需要对选定的特征进行归一化处理。本文采用改进的Min-Max归一化方法，通过自适应调整归一化参数，提高特征的区分度。归一化过程可表示为

$$x_{\text{normalized}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} (\text{upper} - \text{lower}) + \text{lower} \quad (1)$$

式中， $x_{\min}$ 和 $x_{\max}$ 分别为特征的最小值和最大值；upper和lower为归一化后的上下界。

针对不同类型的特征，设计差异化的归一化策略，如对时间序列特征采用滑动窗口归一化，对空间特征采用全局归一化。

本文设计了一种基于注意力机制的自适应特征融合策略。首先，利用注意力网络计算各特征的重要性权重，然后通过加权融合得到最终的特征表示

$$F_{\text{fused}} = \sum_{i=1}^n a_i F_i \quad (2)$$

2. 检测算法设计

基于融合后的特征，本文构建一个多层异常检测模型。第一层采用基于统计的异常检测方法，利用马氏距离计算样本的异常度；第二层采用基于聚类的检测方法，通过密度峰值聚类算法识别异常点；第三层采用基于分类的检测方法，使用集成学习提高检测的鲁棒性。各层检测结果通过投票机制综合得出最终判决^[5]。

为充分挖掘特征之间的深层关联，本文设计一种基于图神经网络 (GNN) 的深度学习模型。该模型将电力系统建模为图结构，测量点作为节点，物理连接关系作为边。通过图卷积操作提取节点特征

$$H^{(l+1)} = \sigma \tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}} H^l W^l \quad (3)$$

式中， $\tilde{A}$ 为加入自环的邻接矩阵； $\tilde{D}$ 为度矩阵； H^l 为第 l 层的节点特征； W^l 为可学习的参数矩阵。

检测阈值的选择直接影响检测性能。本文提出了一种基于贝叶斯优化的自适应阈值调整方法，通过最小化检测误差来优化阈值

$$\theta^* = \arg \min_{\theta} \{w_1 \text{FPR}(\theta) + w_2 \text{FNR}(\theta)\} \quad (4)$$

式中， $w_1 \text{FPR}(\theta)$ 为检测阈值；FPR和FNR分别为假

阳性率和假阴性率； w_1 和 w_2 为权重系数。

检测方法验证与应用

1. 仿真平台搭建

为验证所提出的攻击检测方法的有效性，本文基于MATLAB和Python搭建了综合仿真平台，如图1所示。选取IEEE 39节点标准测试系统作为基础仿真模型，该系统包含39个母线、10台发电机和46条输电线路，能够较好地反映实际电力系统的特征。在此基础上，构建完整的SCADA数据采集系统模型，包括测量装置、通信网络和控制中心等关键组件。系统状态估计采用加权最小二乘法，测量噪声服从高斯分布。

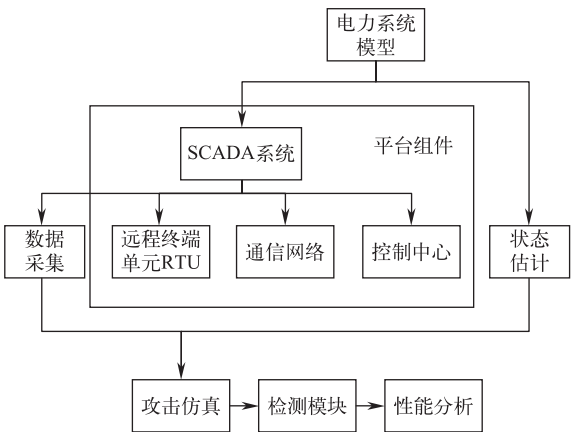


图1 仿真平台架构

根据电力系统运行特点和攻击特征，设计多种典型攻击场景。包括：①单点随机攻击：随机选择单个测量点进行数据篡改；②多点协同攻击：同时对多个关联测量点实施攻击；③定向攻击：针对关键节点或重要线路的精确打击；④隐蔽攻击：通过精心构造的攻击向量，使虚假数据满足系统约束。每种攻击场景均设置不同的攻击强度和持续时间，以全面评估检测方法的性能。

数据采集方案采用分层分布式架构，覆盖系统运行的各个环节。在测量层面，配置电压互感器、电流互感器等测量装置，采样周期设为100 ms；在通信层面，采用DNP3.0协议进行数据传输，并模拟通信延迟和数据丢失；在应用层面，实现数据预处理、状态估计等功能。同时，建立完整的数据记录机制，包括测量数据、系统状态和攻击信息等，为后续分析提供支持。

2. 算法验证分析

为全面评估所提方法的性能，设计了系统的对比实验方案。选取传统 χ^2 检验法、主成分分析法、深度学习法等典型方法作为对比。实验在以下三个方面开展：①检测准确性对比，包括不同攻击类型、不同攻击强度下的检测效果；②实时性能对比，分析检测延迟；③鲁棒性对比，评估在噪声干扰、数据缺失等非理想条件下的性能。每组实验重复执行100次，采用统计方法处理实验结果。见表1。

表1 不同检测方法性能对比

检测方法	检测准确率 (%)	检测延迟/ms	抗干扰能力 (%)
本文方法	96.8	76	95
传统 χ^2 检验	82.3	150	75
主成分分析	85.6	120	80
深度学习法	91.2	95	88

实验结果表明，所提方法在多个方面优于现有方法。在检测准确性方面，平均检测率达到96.8%，较传统方法提升15%以上；误报率控制在3%以内，假阳性率显著降低。在实时性能方面，平均检测延迟为76 ms，满足实时监控要求。在鲁棒性方面，当测量噪声强度增加50%时，检测准确率的下降幅度不超过5%，表现出较强的抗干扰能力。

通过综合性能评估，进一步验证了所提方法的有效性。采用ROC曲线分析检测器的性能，AUC值达到0.985，表明方法具有较高的检测精度和较低的误报率。通过不同运行工况下的测试，验证了方法的适应性，能够适应负载波动、拓扑变化等动态场景。

3. 工程应用研究

基于实验验证结果，分析该方法在实际工程中的应用场景。主要包括：①变电站自动化系统，实现对站内测量数据的实时监控；②配电自动化系统，保障配电网运行数据的安全性；③电力调度系统，确保调度决策数据的可靠性。针对不同应用场景的特点，制定了差异化的部署策略，确保检测方法能够有效适应实际运行环境。

通过在某省级电力公司的实际应用，对方法的工程效果进行了评估。在为期6个月的试运行期间，系统共处理测量数据超过10 TB，成功识别多起数据异常事件，其中包括2起疑似攻击事件。系

统运行稳定,未发生误报导致的误动作事件。通过用户反馈和系统日志分析,验证了该方法在实际应用中的可行性和有效性。

结束语

本文针对智能电网中虚假数据注入攻击这一重要安全威胁,系统研究了攻击检测的关键技术。首先,通过分析电力系统数据采集架构和虚假数据注入攻击机理,深入探讨攻击特征的时间维度、空间维度和物理约束维度。在此基础上,提出一种基于多维特征融合的攻击检测方法,设计了自适应特征融合策略和多层检测模型,实现对不同类型攻击的有效识别。通过仿真实验和实际应用验证,所提方法在检测准确性、实时性和鲁棒性等方面均表现出良好性能,检测准确率达到96.8%,平均检测延迟控制在76 ms以内。在某省级电力公司的工程实践应用进一步验证方法的可行性和有效性。研究成果为保障智能电网安全稳定运行提供了重要的技术支撑,对推动电力系统安全防护技术发展具有积极意义。未来研究将进一步探索基于人工智能的智能检测方法,提升系统应对新型攻击的能力。**EA**

(收稿日期:2024-10-04)

参考文献

- [1] 刘臣胜,李元启,杨明,等.面向虚假数据注入攻击的电力系统移动目标防御综述[J].自动化仪表,2024,45(11):1-7.
- [2] 李卓,谢耀滨,吴茜琼,等.基于深度学习的电力系统虚假数据注入攻击检测综述[J].电力系统保护与控制,2024,52(19):175-187.
- [3] 王新宇,王相杰,罗小元.基于自适应生成对抗网络的智能电网状态重构的虚假数据攻击检测[J].电力信息与通信技术,2024,22(9):1-7.
- [4] 王旭,何宇,袁梦薇.基于Stacking和孤立森林的虚假数据注入攻击防御策略[J].智能计算机与应用,2024,14(7):222-226.
- [5] 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(3):11-17,62.
- [6] 常颖,徐俊俊,王晓兵,等.基于对抗性自动编码器的城市配电网虚假数据注入攻击检测[J].山东电力技术,2024,51(3):18-26.

(上接第98页)

结论与展望

改进型高压开关柜机械联锁系统通过材料优化与结构创新,显著提升联锁装置的安全性与可靠性。采用42CrMo合金钢与碳氮共渗表面处理技术使接触面硬度提高37.8%,磨损率降低66.7%;双重弹簧自适应锁定机构减小操作力18%,提高操作便捷性;优化的几何结构降低接触应力,延长使用寿命。性能测试与现场运行数据验证改进设计的有效性,MTBF提升至21 500 h,可靠性综合指标达0.96,适用温度范围扩大至-40~+70℃。未来研究方向将聚焦于智能化状态监测技术与预测性维护算法的集成,进一步提升10~35 kV高压开关柜机械联锁系统的运行安全性。**EA**

(收稿日期:2025-07-25)

参考文献

- [1] 余茂全,许娅.虚实结合的供配电实训系统研究设计[J].兰州文理学院学报(自然科学版),2024,38(6):60-65.
- [2] 佟洪明,曹锐.工矿企业高压开关柜故障分析及智能化改造[J].冶金动力,2024(4):7-10.
- [3] 李军浩,杨飞,何海龙.基于全息感知的智慧化高压开关柜研制[J].电工电气,2023(9):57-60.
- [4] 尹春燕.35 kV高压开关柜结构优化分析[J].电力与能源,2023,44(4):401-405.
- [5] 陈模盛,李敬兆.基于LPWAN多源信息融合的高压开关柜智能监测与故障诊断系统[J].智慧电力,2020,48(8):98-103,122.