Modeling and Simulation 建模与仿真, 2023, 12(2), 799-812
Published Online March 2023 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2023.122076

Hans汉斯

基于ELM状态预测的智能电网虚假数据检测

吴　京，李海英

上海理工大学机械工程学院，上海

收稿日期：2023年1月11日；录用日期：2023年3月1日；发布日期：2023年3月8日

摘　要

针对智能电网中虚假数据注入攻击(false data injection attack, FDIA)能够躲避传统坏数据检测的问题，本文研究了交流模型下研究FDI攻击方式，以历史状态数据间的内在关联为基础，构建了基于改进极限学习机(extreme learning machine, ELM)的预测模型。结合电网拓扑特定的电气关系，对比量测设备传输数据，对离群值进行类别标签。根据异常分布结合图论计算节点强度判定异常并检测攻击。在IEEE-14节点系统进行仿真，所提方法能快速检测并定位到异常节点，验证了所提方法的可行性和有效性。

关键词

状态估计，虚假数据，极限学习机，状态预测，节点强度

Smart Grid False Data Detection Based on ELM State Prediction

Jing Wu, Haiying Li

School of Mechanical Engineering, University of Shanghai for Science and Technology, Shanghai

Received: Jan. 11th, 2023; accepted: Mar. 1st, 2023; published: Mar. 8th, 2023

Abstract

To address the problem that false data injection attack (FDIA) can evade traditional bad data detection in smart grid, this paper investigates the way to study FDI attack under AC model and constructs an improved extreme learning machine (ELM) based on the intrinsic correlation between historical state data. The outliers are labeled with categories by comparing the transmission data of the measurement devices in combination with the electrical relations specific to the grid topol-

文章引用: 吴京, 李海英. 基于 ELM 状态预测的智能电网虚假数据检测[J]. 建模与仿真, 2023, 12(2): 799-812.
DOI: 10.12677/mos.2023.122076

ogy. Node strength is calculated based on the anomaly distribution combined with graph theory to determine anomalies and detect attacks. Simulations are performed on the IEEE-14 node system, and the proposed method can quickly detect and locate the anomalous nodes, which verifies the feasibility and effectiveness of the proposed method.

Keywords

State Estimation, Spurious Data, Extreme Learning Machine, State Prediction, Node Strength

1. 引言

随着电力信息物理系统(cyber physical system, CPS)的深度融合[1] [2] [3]，在实现电力系统整体运行性能最优化的同时，信息网络的安全漏洞也给电网带来潜在的威胁[4] [5]。虚假数据注入攻击(false data injection attacks, FDIA) [6]作为通过篡改量测数据破坏电网信息完整性的攻击方式，具有较强的隐蔽性与干扰性，影响控制中心的决策分析[7] [8]，是对电力系统威胁程度较高的攻击方式之一。因此，建立有效的攻击检测机制对系统的安全稳定具有重要意义。

现有的 FDIA 检测方法主要分为空间相关型检测和时间相关型检测两类[9]。空间相关型检测通过传感器件间的关联关系进行交叉验证，达到检测目的，在实际操作中难度较大；时间相关型检测利用系统过去时间的状态预测未来的状态，根据状态预测方法的不同可分为：基于无迹卡尔曼滤波的动态状态估计检测方法[10] [11] [12]和基于短期状态预测的检测方法[13] [14]。

文献[10] [11]采用无迹卡尔曼滤波与最小二乘法同时状态估计，通过两者状态量的差别检测 FDIA。文献[12]用无迹卡尔曼滤波状态估计与负荷预测以及潮流计算得到的状态量自适应混合预测，通过比较预测值与静态状态估计差值的分布检测攻击。但是基于 UKF 的动态估计检测方法预测步在状态量突变时效果不佳，需要通过量测值来修正，而被篡改量测将会导致检测偏差更大。文献[13]利用支持向量回归进行负荷预测，通过潮流计算得到的量测值与实际量测值的偏差来检测潜在的 FDIA。与直接预测量测相比，该方法的计算成本减少了，但工作量仍然较大。文献[14]展示了一种基于深度神经网络的状态预测策略，通过计算估计状态与预测值之间偏差检测攻击。上述检测方法的攻击检测部分大多是比较状态预测值与静态估计值之间的距离指标判断状态量是否受攻击，而在实际电网中状态估计的结果直接影响决策，对实时性要求较高。

针对上述问题，本文基于改进 ELM 状态预测算法提出一种虚假数据注入攻击检测与定位的方法。本文主要工作如下：

1) 充分利用历史数据不受虚假数据影响的优势采用状态预测的方法，进而得到量测预测值，降低了模型的复杂度。此外，采用 ELM 算法学习速率和泛化能力较一般前馈神经网络更具有优势，更符合电力系统大数据的实时性需求。

2) 将电网拓扑结构与图论相结合，可以更直观清晰的了解量测的异常情况，对判断攻击起了重要作用。

3) 利用节点强度判断是否受到攻击，检测攻击的同时可以定位到节点，在实践中识别攻击位置对快

速部署有效策略至关重要。

2. 问题描述

2.1. 状态估计

电力系统状态估计是通过各种智能仪表的监测数据，对当前系统运行状态评估的过程。其结果常用于经济调度、安全评估等。

在交流潮流模型中，非线性关系可表示为：

$$\boldsymbol{z}=h\left(\boldsymbol{x}\right)+\boldsymbol{e} \tag{1}$$

式中：$x\in\boldsymbol{R}^n$ 为状态变量，n 是状态变量的数量，$z\in\boldsymbol{R}^m$ 为智能监测仪表的量测，m 是量测的数量，$h(\cdot)$ 为量测与状态的非线性关系，$e\in\boldsymbol{R}^m$ 为量测误差，服从均值为 0 的高斯分布。

实际系统中各节点的电压幅值 U_i 和相角 θ_i 为状态量，节点注入有功功率 P_i、无功功率 Q_i 和线路上有功 P_{ij} 和无功功率 Q_{ij} 为测量值，关系如下：

$$P_i=V_i\sum_{j\in N_i}V_j\left(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}\right) \tag{2}$$

$$Q_i=V_i\sum_{j\in N_i}V_j\left(G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij}\right) \tag{3}$$

$$P_{\mathrm{ij}}=V_i^2G_{ij}-V_iV_j\left(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}\right) \tag{4}$$

$$Q_{ij}=-V_i^2B_{ij}-V_iV_j\left(G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij}\right) \tag{5}$$

式中：V_i、V_j 分别为节点 i、节点 j 的电压幅值；θ_{ij} 节点 i 与节点 j 的电压相角差；G_{ij}、B_{ij} 分别为节点 i 与节点 j 之间支路电导、电纳。

通常交流状态估计可以描述为一个二次优化问题，目标函数取得最小时的状态量即为最优估计。

$$J\left(\boldsymbol{x}\right)=\left[\boldsymbol{z}-h\left(\boldsymbol{x}\right)\right]^{\mathrm{T}}W\left[\boldsymbol{z}-h\left(\boldsymbol{x}\right)\right] \tag{6}$$

式中：W 为权重矩阵。

2.2. 智能电网虚假数据注入攻击

由于测量误差和通信的不稳定，传输数据偏离原有的真实值，为了确保状态估计结果的准确性，基于残差分析的传统坏数据检测器需要对不良数据检测和辨识。通过异常数据与正常数据的残差分析，误差超过阈值即判定为攻击数据[7]。假设量测变化为 a，引起状态量变化 c，此时残差表示为：

$$\begin{aligned}r_a&=\left\|\boldsymbol{z}+a-h\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right)\right\|_2\\&=\left\|\boldsymbol{z}-h\left(\hat{\boldsymbol{x}}\right)+a+h\left(\hat{\boldsymbol{x}}\right)-h\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right)\right\|_2\\&\le\left\|\boldsymbol{z}-h\left(\hat{\boldsymbol{x}}\right)\right\|_2+\left\|a+h\left(\hat{\boldsymbol{x}}\right)-h\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right)\right\|_2\\&=r+\tau_\alpha\end{aligned} \tag{7}$$

式中：r_a 和 r 分别表示有无攻击时的残差值，τ_a 表示残差增量，由公式(7)，当

$$a=h\left(\hat{\boldsymbol{x}}+\boldsymbol{c}\right)-h\left(\hat{\boldsymbol{x}}\right) \tag{8}$$

残差增量为 0，受到攻击时未引起残差的变化，当前系统无法检测到恶性数据[15]，FDIA 成功绕过不良数据检测。

由上述虚假数据注入原理，攻击者将虚假数据注入 AC 状态估计通常有两种方法：操纵系统状态变量和操纵特定的测量。根据功率平衡方程(2)~(5)，如果攻击者以状态变量为目标，依赖于该状态变量的所有量测都将受到影响。因此，一般是通过注入攻击篡改测值来达到改变状态量的目的。

3. 状态预测模型

3.1. 状态预测

极限学习机算法是由 Huang 等[16]提出的一种单层前馈神经网络学习算法，是对传统基于梯度前馈神经网络的改进，提升了学习效率并简化参数的设定。ELM 仅需要求解输出权重，是一个线性参数模型，学习过程易于在全局极小值处收敛，因此训练速度快，抗干扰能力强，在解决复杂问题上具有一定的优越性[17]。

极限学习机的组成包括输入层、隐含层和输出层，结构如下图 1 所示。

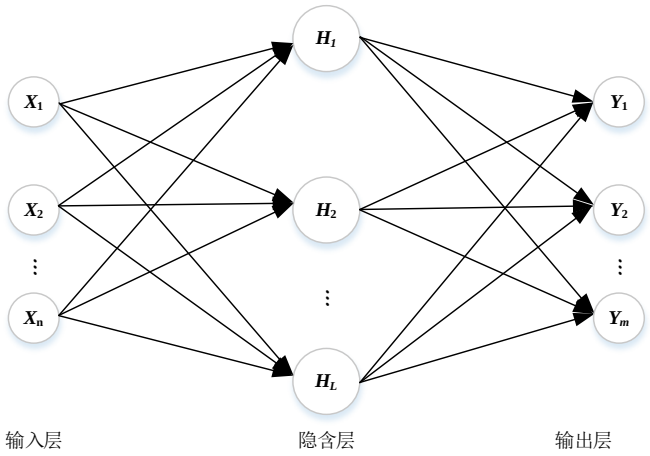

Figure 1. Network structure of the Extreme Learning Machine
图 1. 极限学习机的网络结构

给定一个包含 N 个不同数据样本$\left(x_i, y_k\right) \in R^n \times R^m$，$R$ 为实数，ELM 回归模型为：

$$f_L\left(x\right)=\sum_{i=1}^{L}\beta_i h_i\left(\boldsymbol{x}\right)=\sum_{i=1}^{L}\beta_i g_i\left(w\boldsymbol{x}+b\right) \tag{9}$$

式中：w_i 为输入层与隐含层的权重；β_i 为隐含层与输出层的权重；b_i 为隐含层的偏置；L 为隐含层的节点数；$h\left(\boldsymbol{x}\right)$ 为隐含层的输出；$g\left(x\right)$ 为隐含层的无限可微的激活函数，文中取 Sigmoid 函数。

隐含层输出矩阵为：

$$\boldsymbol{H}\left(x\right)=\left[h_1\left(\boldsymbol{x}\right), h_2\left(\boldsymbol{x}\right), \cdots, h_L\left(\boldsymbol{x}\right)\right] \tag{10}$$

在确定了权重 w 和隐含神经元阈值 b 之后，可求得隐藏层的输出矩阵 $\boldsymbol{H}$，ELM 训练的过程等价求解线性方程 $\boldsymbol{H\beta}=\boldsymbol{Y}$ 的最小二乘解，目标函数为：

$$\min\left\|\boldsymbol{H\beta}-\boldsymbol{Y}\right\|^2, \beta \in R^{L\times m} \tag{11}$$

其中，期望矩阵为

$$\boldsymbol{Y}=\left[Y_1, Y_2, \cdots, Y_m\right]^{\mathrm{T}} \tag{12}$$

解为 $\beta^*=\boldsymbol{H}^{\dagger}\boldsymbol{Y}$，其中 $\boldsymbol{H}^{\dagger}$ 为 $\boldsymbol{H}$ 的 Moore-Penrose 广义逆。

3.2. 参数优化

由前文可知，ELM 的初始权值和阈值都是随机产生的，每次产生都具有盲目性，本文利用麻雀搜索算法[18]对初始权值和阈值进行优化。

麻雀搜索算法(sparrow search algorithm, SSA)是 2020 年由 Xue 等[18]提出的一种群智能优化算法，具有寻优能力强、收敛速度快的特点。将麻雀群体分为发现者、加入者和预警者 3 部分，种群中适应值较高的作为发现者，负责寻找食物并为加入者提供觅食的方向。在每次迭代过程中，发现者位置按照如下公式更新：

$$X_{i,j}^{t+1}=\begin{cases}X_{i,j}\cdot\exp\left(-\dfrac{i}{\alpha\cdot iter_{\max}}\right), & R_2<ST\\ X_{i,j}+Q\cdot L, & \text{otherwise}\end{cases}\tag{13}$$

式中：t 表示当前迭代次数，$X_{i,j}$ 表示第 i 个麻雀种群在第 j 维中的位置信息，α 为 $(0,1]$ 之间随机数，$iter_{\max}$ 表示最大迭代次数，Q 为服从正态分布的随机数，L 是一个 $1\times d$ 并且元素全是 1 的矩阵，$R_2\in[0,1]$，$ST\in[0.5,1]$ 分别表示麻雀种群位置的预警值和安全值。

在觅食过程中，部分加入者会监视发现者，对其食物掠夺提高自己的适应度，从而成为发现者，加入位置按照下式更新：

$$X_{i,j}^{t+1}=\begin{cases}Q\cdot\exp\left(\dfrac{X_{worst}-X_{i,j}^{t}}{i^2}\right), & i>\dfrac{n}{2}\\ X_P^{t+1}+\left|X_{i,j}-X_P^{t+1}\right|\cdot A+L, & \text{otherwise}\end{cases}\tag{14}$$

式中：X_P^{t+1} 表示当前发现者所发现的最优位置，X_{worst} 表示当前全局最差的位置，A 表示其元素随机幅值为 1 或−1 的 $1\times d$ 的多维矩阵。

在麻雀种群中，意识到危险的麻雀数量占总数的 10%~20%，随机产生位置，按照以下公式更新：

$$X_{i,j}^{t+1}=\begin{cases}X_{best}^{t}+\beta\cdot\left|X_{i,j}^{t}-X_{\text{best}}^{t}\right|, & f_i>f_g\\ X_{i,j}^{t}+K\cdot\left[\dfrac{\left|X_{i,j}^{t}-X_{\text{best}}^{t}\right|}{(f_i-f_w)+\varepsilon}\right], & f_i=f_g\end{cases}\tag{15}$$

式中：X_{best} 是全局最优位置的个体，β 服从标准正态分布的随机数用来作为步长控制参数，f_i 表示当前麻雀个体 i 的适应度值，f_g，f_w 分别表示全局最佳适应值和最差适应值，$\varepsilon>0$，一般设为 10^{-8}，$K\in[0,1]$ 用来控制麻雀运动方向(图 2)。

使用均方根误差作为预测精度评判标准

$$RMSE=\sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\hat{d}_i-d_i\right)^2}\tag{16}$$

适应度函数选取训练后的均方根误差，值越小，表明预测的数据与原始数据重合度越高，最终优化的输出为最佳初始权值和阈值，再利用最佳权值和阈值训练的网络对测试数据集测试。

3.3. 检测与定位

由历史数据不受虚假数据攻击的影响，采用 SSA-ELM 算法对状态变量预测，结合网络拓扑结构和参数得到预测量测值，与系统量测仪表传输的数值比较，得出离群值，这里采用“3σ”准则，即几乎所有变量的观测值都应该在观测值平均值的 3σ 距离之内。因此，任何位于该距离之外的观测值都可以被认定为异常值。

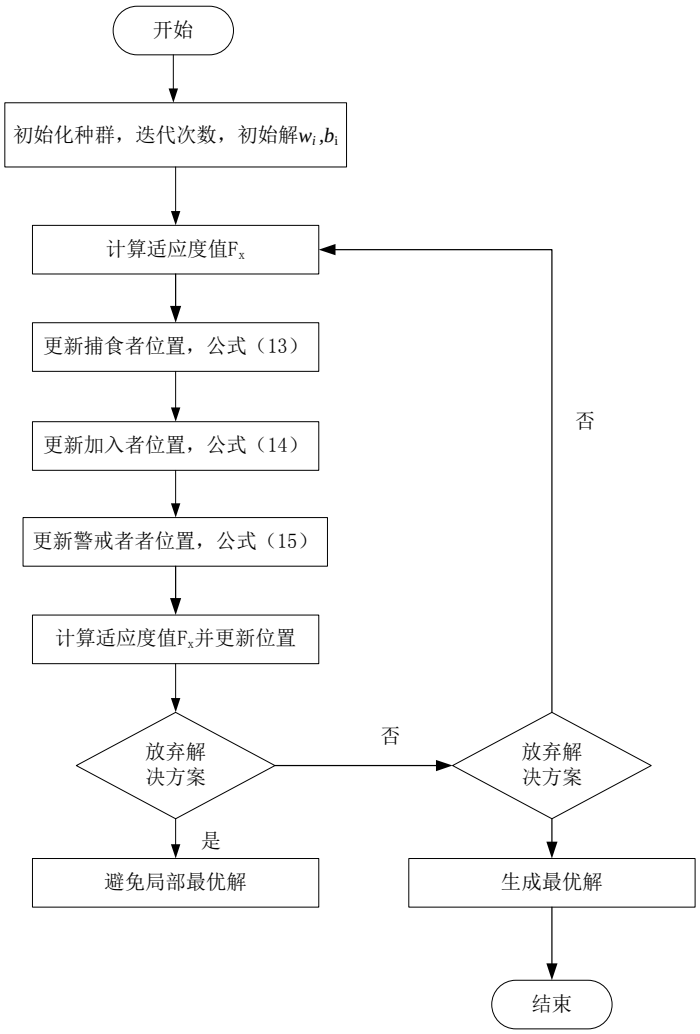

Figure 2. SSA-ELM algorithm framework
图 2. SSA-ELM 算法流程图

$$\begin{cases} \left|\boldsymbol{z}_i-\tilde{\boldsymbol{z}}_i\right| \le 3\sigma, \ \boldsymbol{z}_i \in \boldsymbol{z} \\ \left|\boldsymbol{z}_i-\tilde{\boldsymbol{z}}_i\right| > 3\sigma, \ \boldsymbol{z}_i \notin \boldsymbol{z} \end{cases} \tag{17}$$

电网实际上包含了两类拓扑结构：几何拓扑和物理拓扑。前者反映了电网设备的几何连接状态，后者体现电网元件物理上的电气耦合[19]。电力系统的拓扑可以用图$G \le V(G)$，E(G)>来表示，其中 V(G)为图 G 中包含的节点集合，E(G)为图 G 中包含的边集合[20]。

异常值的分布可以间接反映攻击的目标，针对筛选出来的异常值根据以下规则创建图：

1) 将量测分为两组：

A 组：电压幅值 U_i、相角 θ_i 和节点注入有功功率 P_i、无功功率 Q_i；

B 组：线路有功潮流 P_{ij} 和无功潮流 Q_{ij}；

2) 自边：各节点如果检测到至少一种 A 组类型的变量为异常，则将此节点添加到图中，用一条边连接到自身，并指定该边的权重为向量中 A 类型变量数量的一半，如图 3(b)；

3) 互边：如果检测到 B 类型的变量为异常值，则将代表此线路的两个端点添加到图中，用一条边连接这两个节点，并将该边的权重指定为 B 类型变量的数量，如图 3(c)。

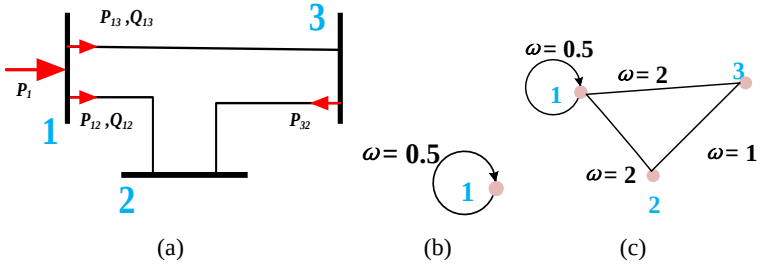

Figure 3. Schematic diagram of weighting map generation
图 3. 权重图生成示意图

创建图后，使用节点强度的概念衡量每个节点的重要性，图中一个节点的阶数简单的定义为直接连接到该节点的边数。这一定义在[21]中被推广到考虑加权强度 s_i 的加权图中的边的权重，定义如下：

$$s_i = \sum_{j \in N} a_{ij} \omega_{ij} \tag{18}$$

式中：a_{ij} 是图邻接矩阵的第(i, j)个元素，ω_{ij} 是分配给连接节点 i 和节点 j 的边的权重。

计算图中每个节点的 s_i 后，将根据以下规则最终决定向量 $\boldsymbol{z}$ 中检测到的异常值是否由网络攻击引起：如果图中至少可调数量的节点的 s_i 值大于预定义的阈值 ξ，则检测并定位攻击(图 4)。

$$\begin{cases} s_i > \xi, \text{ FDLA} \\ s_i \le \xi, \text{ normal} \end{cases} \tag{19}$$

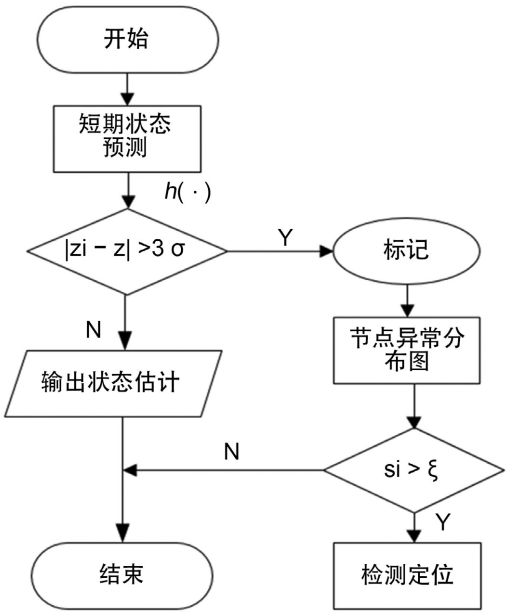

Figure 4. Block diagram of false data detection model
图 4. 虚假数据检测模型框图

4. 算例分析

4.1. 测试系统

本文测试系统中使用的负载数据来自纽约电力管理局公布的电力负荷数据(New York independent

system operator, NYISO) [22]。参考文献[23]将 NYISO 数据中如图 5 所示的 11 个负荷区域分别接入 IEEE-14 节点系统，该负荷数据的记录间隔为 5 分钟，图 6 为 CAPITL 区某三日符合波动情况。IEEE-14 节点测试系统的量测值和状态变量的 5 分钟间隔数据生成程序步骤如下：

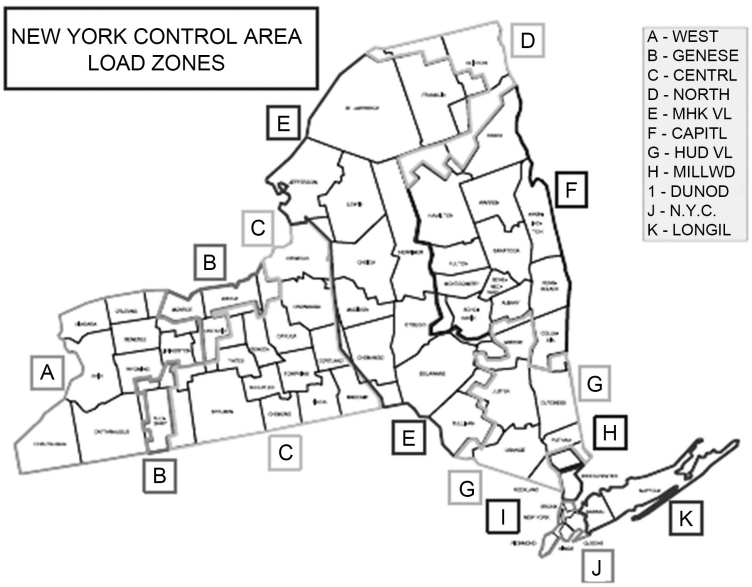

Figure 5. Map of actual electricity areas in 11 New York states
图 5. 纽约 11 州实际电力区域图

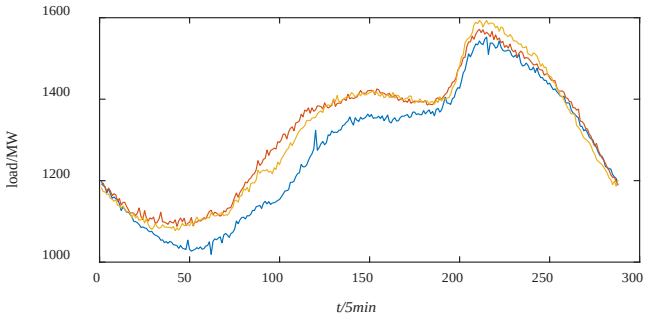

Figure 6. Daily load curve for the first 3 days of the CAPITL region in 2016
图 6. 2016 年 CAPITL 区域前 3 天的日负荷曲线

1) 将每个 NYISO 电网区域连接到 IEEE14 节点测试系统中的 11 条负荷总线之一，对应关系如下表 1；

2) 初始化 IEEE-14 节点有功负荷，基于各节点功率因数恒定的前提，算出对应的无功功率；

3) 累加新的负荷有功功率和无功功率，计算新的总有功和无功与相应初始值的比率，按比例增加每个发电机的发电量；

4) 每 5 分钟的时间间隔，在 IEEE14 节点系统上运行基于 MATPOWER 软件包，得到各节点每个时刻的电压相量值，并将其存储在历史数据库中。

4.2. 单节点攻击检测

根据初始节点和支路信息，运行潮流计算得到 14 个节点电压幅值和电压相角共 27 个系统状态值，其中 1 节点为平衡节点。

Table 1. Correspondence Table
表 1. 对应关系表

NYISO 实际负荷区域	NYISO 对应地图区域	IEEE-14 节点测试系统对应节点
WEST	A	2
GENESE	B	3
CENTRL	C	4
NORTH	D	5
MHK VL	E	6
CAPITL	F	9
HUD VL	G	10
MILLWD	H	11
DUNWWOD	I	12
N.Y.C	J	13
LONGIL	K	14

根据公式(2)~(5)得到系统的量测值，包括节点有功注入和无功注入，以及 20 条线路的有功功率和无功功率。通过每五分钟的实际负荷数据得到 68 个量测值，支路量测值如附录图 A2 所示。

假设电网在 11 月运行良好，在 12 月遭到攻击。从网络中采集了 8640 组正常样本。将 11 月份收集的数据按照 9：1 划分为训练集和测试集，初始种群数设置为 20，搜索最优神经元范围是 1~100，迭代次数大于 100 时寻优过程结束，对电压预测分析如下表 2，其中节点 14 电压相角和适应性曲线如图 7。

Table 2. IEEE-14 system voltage phase angle root-mean-square absolute error analysis
表 2. IEEE-14 系统电压相角均方根绝对误差分析

节点序号	**ELM**	**SSA-ELM** **($\times e^{-7}$)**
1	-	-
2	0.00018	1.6159
3	0.00048	2.8339
4	0.00035	1.1445
5	0.00030	1.1088
6	0.00049	0.1276
7	0.00045	0.1047
8	0.00045	0.1526
9	0.00049	0.1363
10	0.00050	0.0989
11	0.00050	9.4957
12	0.00052	0.08678
13	0.00052	1.8891
14	0.00055	2.2683

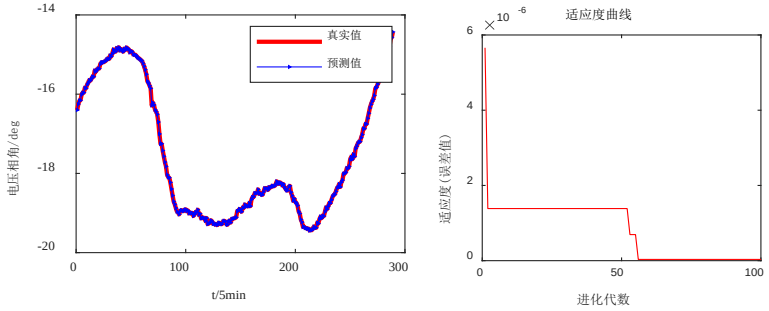

Figure 7. 14-node voltage phase angle prediction and its adaptability curve
图 7. 14 节点电压相角预测及其适应性曲线

在系统正常运行条件下，可以得到当前系统量测的近似真实值，攻击者在原始量测上强加的扰动将使被攻击量测值远离实际值。

如下图 8 所示，2 节点注入 1.1 倍原始电压相角值的攻击，检测到的异常值包含支路 1-2、2-3、2-4 和 2-5 两端的有功功率和无功功率，节点 1-2-3-4-5 注入的有功功率和无功功率，以及节点 2 的电压相角，节点 2 异常分布图生成过程如图 9 所示;针对节点 14 电压幅值的 1.1 倍原始值攻击确定的异常值包括支路 9-14 和 13-14 两端的有功功率和无功功率，节点 9、13 和 14 注入有功和无功功率，以及节点 14 的电压幅值。

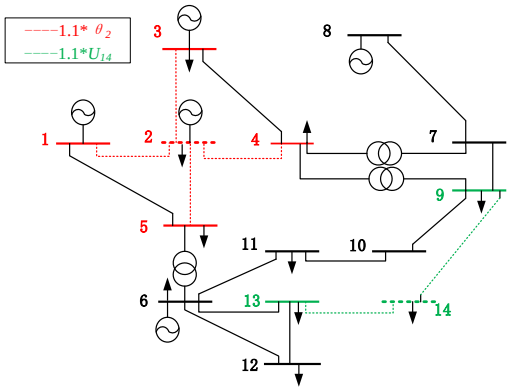

Figure 8. IEEE14 test system attack schematic
图 8. IEEE-14 测试系统攻击示意图

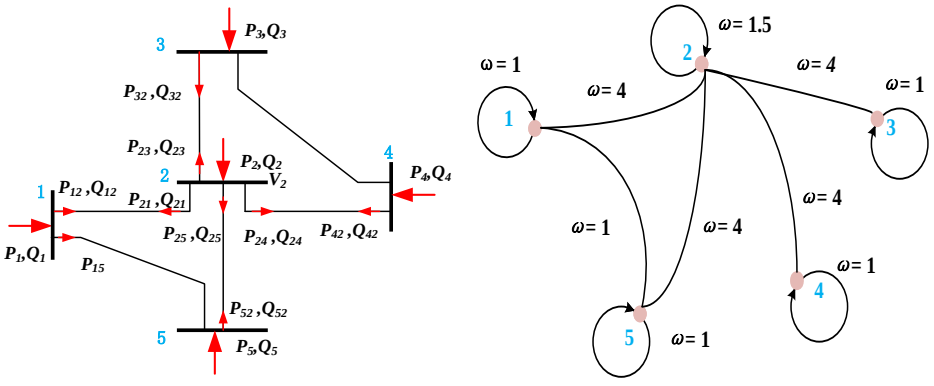

Figure 9. Node 2 outlier distribution weight map
图 9. 节点 2 异常值分布权重图

由检测结果表 3 和表 4 可以得出，这两种攻击将通过所提出方法检测和定位，因为他们各自的图形中至少包含一个强度为 10 或者更高的节点，如图 10、图 11 所示。

Table 3. 1.1*θ_2 attack detection results
表 3. 1.1*θ_2 攻击检测结果

节点	U_i	θ_i	P_i	Q_i	s_i
1	1.06	0	**2.47472**	**−0.20004**	6
2	1.045	**−0.096**	**−0.10138**	**0.39863**	**14**
3	1.01	−0.222	**−0.89985**	**0.0447**	5
4	1.018	−0.18	**−0.43226**	**0.01928**	6
5	1.02	−0.153	**−0.02895**	**−0.0347**	6
6	1.07	−0.248	−0.112	0.05231	1
7	1.062	−0.233	0	0	1
8	1.09	−0.233	0	0.17623	0
9	1.056	−0.261	−0.295	−0.166	0
10	1.051	−0.263	−0.09	−03058	0
11	1.057	−0.258	−0.035	−0.018	0
12	1.055	−0.263	−0.061	−0.016	0
13	1.05	−0.265	−0.135	−0.058	0
14	1.036	−0.28	−0.149	−0.05	0

Table 4. 1.1*U_{14} attack detection results
表 4. 1.1*U_{14} 攻击检测结果

节点	U_i	θ_i	P_i	Q_i	s_i
1	1.06	0	2.32393	−0.16549	0
2	1.045	−0.087	0.183	0.30857	0
3	1.01	−0.222	−0.942	0.06075	0
4	1.018	−0.18	−0.478	0.039	0
5	1.02	−0.153	−0.076	−0.016	0
6	1.07	−0.248	−0.112	0.0531	1
7	1.062	−0.233	0	0	1
8	1.09	−0.233	0	0.17623	0
9	1.056	−0.261	**−0.44435**	**−0.50013**	6
10	1.051	−0.263	−0.09	−0.058	2
11	1.057	−0.258	−0.035	−0.018	1
12	1.055	−0.263	−0.061	−0.016	2
13	1.05	−0.265	**−0.2548**	**−0.3116**	6
14	**1.139**	−0.28	**−0.13818**	**0.57536**	**11**

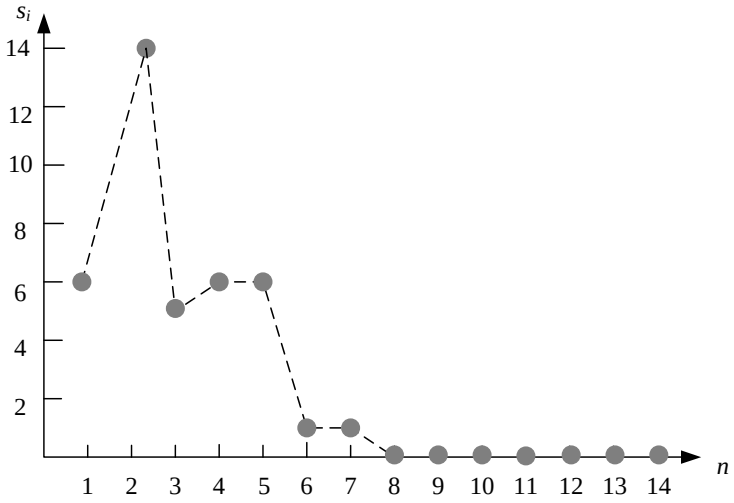

Figure 10. Node 2 attack detection strength map
图 10. 节点 2 攻击检测强度图

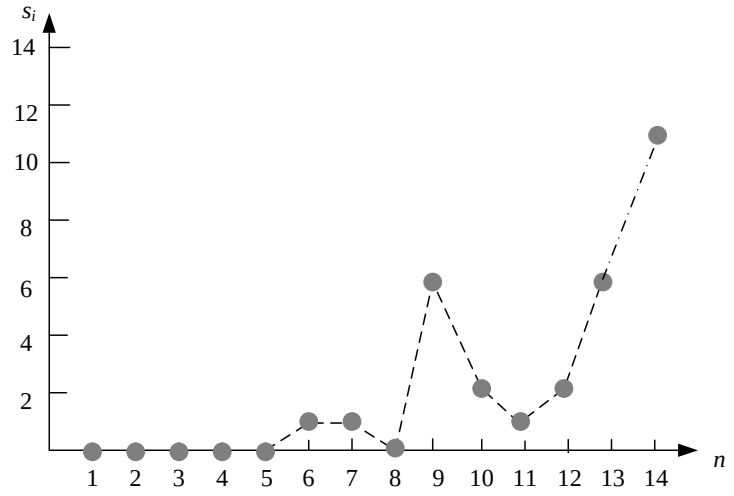

Figure 11. Node14attack detection strength map
图 11. 节点 14 攻击检测强度图

4.3. 全覆盖检测

为验证所用检测模型，对 IEEE-14 节点每个状态变量模拟攻击，在原始值上改变相应的比例，表 5 为检测结果。

本文采取五种攻击模式，对 27 个状态量模拟虚假数据注入攻击，攻击幅度分别为原始状态值的 90%、95%、100%、105%、110%，其中 100%代表状态值未遭受攻击。ND 为节点强度在阈值以上的被检测样本的个数，ND%为 ND 的百分数。采用当下攻击时刻前的 288 组数据，即样本总数据。

由原始值 90%和 110%的数据可知，当状态变量改变较大时，本文检测方法可以很好地检测到虚假数据的攻击；由原始值 95%和 105%的攻击数据可知，状态变量改变较小时，ND 会有所增加，这是因为其状态变量更加接近原始值，但是本文检测方法均有效检测到虚假数据的注入攻击。由于不同节点的强相关量测数目不一样，在相同攻击情况下，ND%会有所不同，如节点 8 等，由于其出线度仅为 1，即强相关量测较少，导致部分样本数据的关联度在阈值之上。

Table 5. False data injection attacks test results
表 5. 虚假数据注入攻击检测结果

攻击状态	90%		95%		100%		105%		110%	
	ND	ND%	ND	ND%	ND	ND%	ND	ND%	ND	ND%
θ_2	0	0	8	3	281	98	22	8	0	0
θ_3	0	1	13	5	285	99	18	6	5	2
θ_4	0	0	0	0	282	99	0	0	0	0
θ_5	2	0	0	0	281	98	0	0	0	0
θ_6	0	0	0	0	286	99	5	2	0	0
θ_7	4	1	15	5	285	99	12	5	3	1
θ_8	7	2	25	9	280	99	21	7	5	2
θ_9	0	0	8	3	283	99	14	5	0	0
θ_{10}	0	0	0	0	282	99	5	1	0	0
θ_{11}	2	1	20	7	285	99	0	0	0	0
θ_{12}	0	0	0	0	286	99	0	0	0	0
θ_{13}	0	0	0	0	280	98	0	0	0	0
θ_{14}	5	2	7	2	280	99	11	4	0	0
U_1	0	0	0	0	284	99	0	0	0	0
U_2	2	1	0	0	286	99	2	1	0	0
U_3	0	0	4	1	284	99	0	0	0	0
U_4	0	0	0	0	285	99	0	0	0	0
U_5	1	0	0	0	285	99	0	0	0	0
U_6	0	0	0	0	284	99	2	1	0	0
U_7	0	0	2	1	280	98	0	0	0	0
U_8	0	0	13	5	283	99	0	0	0	0
U_9	1	0	0	0	281	99	1	0	0	0
U_{10}	0	0	1	0	283	99	0	0	0	0
U_{11}	0	0	0	0	286	99	0	0	0	0
U_{12}	0	0	1	0	284	99	0	0	0	0
U_{13}	0	0	0	0	282	98	3	1	2	1
U_{14}	0	0	3	1	285	99	0	0	0	0

5. 结论

虚假数据的注入对电网的稳定性运行带来了巨大威胁，传统的不良数据检测无法判别。本文通过状态预测结合异常分布图在 IEEE-14 节点测试系统进行了仿真分析，提出了一种离线预测，在线检测的攻击检测方法，利用攻击前后的异常值分布求得节点强度变化来判断是否收到攻击，对单节点多节点进行实验证明模型的有效性。

参考文献

[1] 秦博雅, 刘东. 电网信息物理系统分析与控制的研究进展与展望[J]. 中国电机工程学报, 2020, 40(18): 5818-5826.

[2] 袁红团. 基于智能电网的安全监测云平台设计[J]. 自动化仪表, 2022, 43(3): 60-64.

[3] 白申义, 李建敏, 许圣龙, 朱云峰, 赵晓铎. 大电网实时快速安全稳定控制系统研制[J]. 自动化仪表, 2021, 42(8): 77-83.

[4] 石立宝, 简州. 基于动态攻防博弈的电力信息物理融合脆弱性评估[J]. 电力系统自动化, 2016, 40(17): 99-105.

[5] 汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化, 2016, 40(17): 59-69.

[6] Liu, Y., Ning, P. and Reiter, M.K. (2009) False Data Injection Attacks against State Estimation in Electric Power Grids. *Proceedings of the* 16*th ACM Conference on Computer and Communications Security*, Chicago, 9-13 November 2009, 21-32. https://doi.org/10.1145/1653662.1653666

[7] 朱杰, 张葛祥, 王涛, 等. 电力系统状态估计欺诈性数据攻击及防御综述[J]. 电网技术, 2016, 40(8): 2406-2415.

[8] 王琦, 邰伟, 汤奕, 倪明. 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(1): 72-83.

[9] 刘烃, 田决, 王稼舟, 等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报, 2019, 45(1): 5-24.

[10] 魏利胜, 张倩. 基于改进的 UKF 智能电网虚假数据攻击检测[J/OL]. 系统仿真学报. https://doi.org/10.16182/j.issn1004731x.joss.22-0292

[11] 王竞才, 李琰, 徐天奇. 基于扩展卡尔曼滤波的智能电网虚假数据检测[J] . 智慧电力, 2022, 50(3): 50-56.

[12] 刘鑫蕊, 常鹏, 孙秋野. 基于 XGBoost 和无迹卡尔曼滤波自适应混合预测的电网虚假数据注入攻击检测[J]. 中国电机工程学报, 2021, 41(16): 5462-5476.

[13] Deng, Y.Y., Zhu, K., *et al*. (2019) Real-Time Detection of False Date Injection Attacks Based on Load Forecasting in Smart Grid. 2019 *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, Beijing, 21-23 October 2019, 1-6. https://doi.org/10.1109/SmartGridComm.2019.8909811

[14] Mukherjee, D. (2021) Real-Time Identification of False Data Injection Attack in Smart Grid. 2021 *IEEE Region* 10 *Symposium* (*TENSYMP*), Jeju, 23-25 August 2021, 1-6. https://doi.org/10.1109/TENSYMP52854.2021.9550965

[15] 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(8): 2546-2559.

[16] Huang, G., Zhu, Q. and Siew, C. (2006) Extreme Learning Machine: Theory and Applications. *Neurocomputing*, **70**, 489-501. https://doi.org/10.1016/j.neucom.2005.12.126

[17] 张斌, 宫建锋, 郭宁, 靳盘龙, 韩一鸣. 基于改进核极限学习机的短期负荷预测全网模型设计[J]. 自动化仪表, 2021, 42(8): 64-67.

[18] Xue, J. and Shen, B. (2020) A Novel Swarm Intelligence Optimization Approach: Sparrow Search Algorithm. *System Science & Control Engineering*, **8**, 22-34. https://doi.org/10.1080/21642583.2019.1708830

[19] 杨雄平. 电力系统网络拓扑结构分析及运行方式组合研究[D]: [博士学位论文]. 武汉: 华中科技大学, 2007.

[20] 郎燕生, 李静, 罗雅迪, 伍凌云, 李强, 赵军, 王顺江. 基于图划分的大电网拓扑分析[J]. 电力系统保护与控制, 2017, 45(23): 108-115.

[21] Barrat, A. and Barthélemy, M. (2004) Modeling the Evolution of Weighted Networks. *Physical Review E*: *Statistical Nonlinear & Soft Matter Physics*, **70**, Article ID: 066149. https://doi.org/10.1103/PhysRevE.70.066149

[22] Load Data: Market and Operational Data (NYISO). http://www.energyonline.com/Data/GenericData.aspx?DataId=13&NYISO___Hourly_Actual_Load

[23] Gu, C.J., Panida, J. and Mehul, M. (2015) Detecting False Data Injection Attacks in AC State Estimation. *IEEE Transactions on Smart Grid*, **6**, 2476-2483. https://doi.org/10.1109/TSG.2015.2388545