DOI:10.20033/j.1003-7241.(2025)05-0085-05.

基于梯度提升决策树的网络虚假数据注入攻击检测方法

郭敬东，刘文亮，罗富财，沈立翔，林少钧

(国网福建省电力有限公司,福建 福州 350003)

摘 要: 针对虚假数据攻击向量可避开网络不良数据检测机制现状,提出基于梯度提升决策树的网络虚假数据注入攻击检测方法。采用孤立森林算法提取遭受虚假数据注入攻击后网络量测数据的异常分值特征,采用局部线性嵌入算法降维处理异常分值提取后量测数据,提取其属性特征,将两种特征作为样本数据输入基于梯度提升决策树的攻击检测模型,实现虚假数据注入攻击检测。实验结果表明,该方法可准确提取网络量测数据特征,当二叉树数量为120,数据维度为3,邻居节点数为8时,特征提取结果精度更高;可实现虚假数据注入攻击检测,并具有突出检测效果。

关键词: 孤立森林算法;虚假数据;梯度提升;决策树;异常分值;攻击检测

中图分类号:TP391;TM761 文献标识码:A 文章编号:1003-7241(2025)05-0085-05

Detection Method of Network False Data Injection Attacks Based on Gradient Lifting Decision Tree

GUO Jing-dong, LIU Wen-liang, LUO Fu-cai, SHEN Li-xiang, LIN Shao-jun

(State Grid Fujian Electric Power Co., Ltd., Fuzhou 350003 China)

Abstract: Aiming at the fact that false data attack vectors can avoid the detection mechanism of network bad data, a detection method of network false data injection attack based on gradient lifting decision tree is proposed. The isolated forest algorithm is used to extract the abnormal score features of the network measurement data after being attacked by false data injection, and the local linear embedding algorithm is used to reduce the dimension to deal with the abnormal score of the extracted measurement data, extract its attribute features, and input the two features as sample data into the attack detection model based on the ladder lifting decision tree to achieve false data injection attack detection. The experimental results show that this method can accurately extract the features of network measurement data. When the number of binary trees is 120, the data dimension is 3, and the number of neighbor nodes is 8, the accuracy of feature extraction is higher. It can realize false data injection attack detection and has outstanding detection effect.

Keywords: isolated forest algorithm; false data; gradient lifting; decision tree; abnormal score; attack detection

0 引言

随着国家经济实力的不断增强,中国信息化呈现出突飞猛进的发展势头,信息技术已应用到社会各个领域,融合智能化技术的现代生产网络大大提高了办公效率和全局调配能力的同时,也给网络安全带来了诸多威胁。虚假数据注入攻击(false data injection attack,FDIA)是当下较为普遍的攻击方式[1],它通过注入攻击向量来改变网络原始量测数据,影响网络的正常运行,甚至能够将攻击者的意愿作为网络运行依据。FDIA具有隐蔽性特点,可长时间潜伏于网络中,对网络的稳定运行进行持续性破坏,造成不可挽回的损失[2]。FDIA危害性极高,采用有效措施实现虚假数据注入攻击的准确、实时检测,对维护网络安全、降低网络风险具有积极意义。

刘鑫蕊等人针对电力信息物理系统中存在的虚假数据注入攻击威胁,提出在确定相似日的基础上,采用基于极限梯度提升算法(extreme gradient boosting,XGBoost的预测模型完成日前负荷量的预估后,通过潮流计算确定负荷的状态量,结合无迹卡尔曼滤波确定的状态量完成自适应混合FDIA检测模型的构建,根据中心极限定量的基本原理实现FDIA检测。该方法的FDIA检测效果会因状态量预测误差而大受影响[3];杨杉等人针对新能源互联网数据共享程度较高容易遭受攻击问题,提出利用两个互补马尔科夫链模型获取新能源互联网的运行状态信息,确定预估状态值与实际值之间的误差,以此构建虚假数据注入攻击检测器,实现新能源互联网是否存在虚假数据注入攻击的判断,但该方法构建的FDIA检测器对强度低的注入攻击向量不敏感[4]。梯度提升决策树是集成学习中具有广泛应用的智能分类模型[5],它以回归树作

*基金项目:国网福建省电力有限公司2020年科技项目(52130419002F)

收稿日期:2023-12-01

为基分类器，选择对数损失函数对前一次模型的负梯度进行不断处理，以达到损失最低目标。通过构建强分类器可有效提升模型检测的准确度。因此，本文提出基于梯度提升决策树的网络虚假数据注入攻击检测方法，增强对低强度、隐蔽性FDIA检测的敏感度，提升虚假数据注入攻击检测效果。

1 网络虚假数据注入攻击检测

1.1 网络虚假数据注入攻击问题描述

虚假数据注入攻击是威胁网络信息安全的一把利刃，网络一旦遭受虚假数据注入攻击，可能造成严重的后果、难以估量的损失。假定网络量测数据集合表示为v，a为攻击向量，对于其内第i个元素，用a_i表示，将a注入到网络量测数据集合v后，网络的量测数据z_i可通过下式进行描述：

$$z_i=\begin{cases}z_i'+a_i, i\in v\\ z_i', i\notin v\end{cases} \tag{1}$$

式中，攻击注入前的量测数据为z_i'。

根据网络不良数据检测机制，若网络无不良数据，则有$\|\delta\|_2<\tau$，τ为设定的检测阈值，网络的量测偏差为δ。设定网络无不良数据，利用攻击向量a攻击网络，当a符合条件$\|a-h(x+c)+h(x)\|_2\leqslant\tau-\|\delta\|_2$，即遭受虚假数据注入攻击后的网络偏差$\delta'$符合$\|\delta'\|_2<\tau$条件时，攻击向量$a$可躲避过网络不良数据检测机制。网络量测函数可通过$h(\cdot)$描述，用于反映状态变量$x$与量测数据$z$间的关联性，则有$z=h(x)+\varepsilon$，量测干扰为$\varepsilon$，$c$为网络状态变量偏差。

1.2 网络数据异常特征提取

攻击者对网络进行虚假数据注入攻击后，会对网络量测数据进行篡改，准确获取虚假数据注入攻击后网络量测数据的异常特征是实现网络虚假数据注入攻击检测的前提。

1.2.1 孤立森林提取网络量测数据异常分值特征

在孤立森林算法中，将远离数据群体的离散点视为异常数据，其具备稀疏性特点[6-7]。采用孤立森林算法获取FDIA产生后网络量测数据异常分值的原理是，基于网络目标量测数据进行任意二叉树的构造，根据任意选取的属性值把一定区域内网络量测数据分成两组，按照相同规则进行循环划分，当网络量测数据均分割完成或二叉树高度满足设定条件后结束。异常网络量测数据由于具有稀疏性特点，因此会被快速分配在叶子节点上，其在二叉树的深度较小。利用叶子、根节点间的距离长度可完成网络量测数据的异常分析。基于孤立森林的FDIA网络量测数据异常分值提取过程为：

(1) 对网络量测数据二叉树iTree进行构造，将其作为基本单元，t棵二叉树即可构成孤立森林iForest。用v描述遭受虚假数据注入攻击的网络量测数据集，z为网络量测数据，其属性为f，z、f数量分别为n、s。任意选取ϕ个网络量测数据，将其作为二叉树的根节点。任意选择某一维度网络量测数据子集，从其极大、极小值中任选切割点p，将其作为中心构建一个超平面，R为子集内的随机记录，当$R<p$时，则将其作为二叉树的左子节点，当$R>p$，则将其作为二叉树的右子节点，不断循环确定各子节点，当v中的网络量测数据均分割完成或二叉树高度满足设定条件后即可成功建立一棵二叉树。

(2) FDIA网络量测数据异常分值的计算。建立t棵二叉树iTree即可完成孤立森林iForest的构造。确定网络量测数据的iTree和iForest后，通过遍历各个iTree，计算每个网络量测数据z在各iTree的遍历深度均值$B(z)$即可实现FDIA后网络量测数据异常分值的提取。当其值较小时，z具有较高的异常分值，反之，其异常分值低。数量为n的网络量测数据z，$B(n)$表示其在iTree上的路径长度，路径长度均值$c(n)$可通过下式计算：

$$c(n)=2H(n-1)-\frac{2(n-1)}{n} \tag{2}$$

式中：谐波数表示为$H(n-1)$。

遭受FDIA后网络量测数据的异常分值特征$s(z,n)$可通过下式进行描述：

$$s(z,n)=2^{-\frac{E(B(z))}{c(n)}} \tag{3}$$

式中：$B(z)$的期望表示为$E(B(z))$。

对$s(z,n)$作归一化处理，以使其在[0,1]区间取值。

1.2.2 基于LLE的网络量测数据属性特征提取

实现异常分值提取后的网络量测数据维数较大，且具有较大噪声，因此，需通过局部线性嵌入(LLE)对其作降维处理[8]，以利于网络量测数据属性特征的提取。本文采用局部线性嵌入算法，将维度大的网络量测数据映射至低维空间内，以达到降维目标。在v数据集内，z_i为任意一个网络量测数据，选取$k(k<n)$个数据点，将其视为邻居节点。计算各网络量测数据z_i至邻居节点间的距离d_{ij}，其描述公式为：

$$d_{ij}=\left[\sum\left(z_{ik}-z_{jk}\right)^2\right]^{\frac{1}{2}} \tag{4}$$

设定W为局部重建权值矩阵，在任何局域空间内，邻居节点与网络量测数据点大致视为线性结构，$P(W)$为其误差，构建下式目标函数以使误差为最低：

$$\min P(W)=\sum_{i=1}^{N}\left|z_i-\sum_{j=1}^{k}w_{ij}z_{ij}\right|^2,\quad j=(1,2,\cdots,k) \tag{5}$$

式中：对于任何一个网络量测数据z_i，其邻居节点为z_{ij}，网络量测数据间的权值表示为w_{ij}，并且符合条件$\sum_{j=1}^{k} w_{ij}=1$。对于任何一个网络量测数据z_i，其误差可通过下式描述：

$$e=\left|z_i-\sum_{j=1}^{k} w_{ij}z_{ij}\right|^2=\left|\sum_{j=1}^{k} w_{ij}\left(z_i-z_j\right)\right|^2 =\sum_{j=1}^{k}\sum_{o=1}^{k} w_{ij}w_{io}Q_{jo}^{i} \tag{6}$$

$$Q_{jo}^{i}=\left(z_i-z_j\right)^T\left(z_i-z_o\right) \tag{7}$$

式中：局部协方差矩阵表示为Q_{jo}^{i}。对于任意邻居节点z_o，其中z_i与z_j间的权值表示为w_{jo}。

基于拉格朗日乘子法可实现局部重建权值的确定，其公式描述为：

$$w_{ij}=\frac{\sum_{o=1}^{k}\left(Q^i\right)_{jo}^{-1}}{\sum_{p=1}^{k}\sum_{q=1}^{k}\left(Q^i\right)_{pq}^{-1}} \tag{8}$$

式中，Q^i是正则化处理后的奇异矩阵，其阶数为$p\times q$，正则化处理公式描述为：

$$Q^i=\tilde{Q}^i+\lambda I \tag{9}$$

式中：正则化处理前的奇异矩阵为$\tilde{Q}^i$，正则化系数表示为λ，单位矩阵表示为I。

FDIA网络量测数据降维需满足误差最低条件，其公式描述为：

$$\min P(Y)=\sum_{i=1}^{N}\left|y_i-\sum_{j=1}^{k} w_{ij}y_{ij}\right|^2=\sum_{i=1}^{N}\sum_{j=1}^{N} D_{ij}y_i^T y_j \tag{10}$$

式中：对于FDIA网络量测数据z_i、z_j，其在低维空间的映射为y_i、y_j；D为对称矩阵，阶数为$N\times N$，设$D=(I-W)^{\mathrm{T}}(I-W)$，$W$表示$N\times N$阶矩阵。

通过拉格朗日乘子法可实现FDIA网络量测数据降维结果的确定，即：

$$DY^T=\mu Y^T \tag{11}$$

式中：μ为系数，Y为FDIA网络量测数据在低维空间的输出值，为矩阵D的最小特征值所对的特征向量。

在降维后的低维空间中，获取属性特征r个，属性特征用$f_1,f_2,\cdots,f_r$表示。

1.2.3 异常特征提取结果表示

本文采用孤立森林算法获取遭受FDIA后网络量测数据的异常分值特征后，通过局部线性嵌入算法对异常分值提取后的网络量测数据作降维处理，以完成其新属性特征的提取，确定的网络量测数据异常特征为$A=[ID, s(z,n),f_1,f_2,\cdots,f_r]$，其中，网络量测数据样本序号表示为$ID$，对网络量测数据进行降维处理后，其新属性表示为$f_1,f_2,\cdots,f_r$。

1.3 基于梯度提升决策树的网络FDIA检测模型

网络虚假数据注入攻击是有计划、有预谋的攻击行为，表现为隐蔽性强的特点，攻击者将设计好的虚假数据序列注入到网络中，意图避开网络的状态估计检测机制，隐秘地篡改网络量测数据，这对网络虚假数据注入攻击检测效果提出了更高的要求[9]。梯度提升决策树算法(gradient boosting decision tree，GBDT)将回归树作为基础分类器，利用前次迭代确定的负梯度不断对模型进行优化，在误差下降的梯度方向不断构造新回归树，在反复循环过程中增强分类器的识别能力。因此，本文采用梯度提升决策树方法构建FDIA检测模型，实现网络FDIA的高精度检测。$\{(A_i,u_i)\}(i=1,2,\cdots,n)$描述基于梯度提升决策树的网络FDIA检测模型的数据样本，用于检测网络量测数据中的虚假数据注入攻击。损失函数对虚假数据注入攻击检测精度具有决定性作用，为使虚假数据注入攻击检测模型具有突出检测效果，本文选取对数损失函数，其公式描述为：

$$L\left(u,F(A)\right)=2\sum_{i=1}^{\eta}\log\left(1+\exp\left(-2u_ig_i\right)\right) \tag{12}$$

式中：FDIA网络量测数据异常特征样本为$A_i=(A_{1i},A_{2i},\cdots,A_{\eta i})$，其对应真实标签表示为$u_i$，预测标签表示为$g_i$，网络量测数据特征总数为$\eta$。

基于梯度提升决策树的网络虚假数据注入攻击检测流程为：

第一步：对FDIA检测模型进行初始设置，对满足最小损失的常数β进行预估，初始FDIA检测模型通过下式进行描述：

$$F_0(A)=\arg\min_{\beta}\sum_{i=1}^{n} L\left(u_i,\beta\right) \tag{13}$$

第二步：利用前次迭代确定的负梯度不断对模型进行优化，按照梯度变小方向完成FDIA检测模型的优化。

(1) 基于当前迭代次数下的FDIA检测模型，确定其损失函数的负梯度值，将其视为误差χ_{im}的预估结果，其公式描述为：

$$\chi_{im}=-\left[\frac{\partial L\left(u_i,F\left(A_i\right)\right)}{\partial F\left(A_i\right)}\right]_{F_m(A)=F_{m-1}(A)} \tag{14}$$

其中：循环次数为m。

(2) 根据公式(15)的计算结果进行新回归树的构建，并计算其叶子节点范围$R_{j,m}$，$j=1,2,\cdots,J$。

(3) 将最小损失函数作为优化目标，对梯度减小方向的最佳步长ψ_{jm}进行计算，公式描述为：

$$\psi_{jm}=\arg\min_{\beta}\sum_{A_i\in R_{j,m}}^{n} L\left(u_i,F_{m-1}(A)+\beta\right) \tag{15}$$

(4) 对当前迭代下的FDIA检测模型进行修正，公式描述为：

$$F_m(A)=F_{m-1}(A)+\sum_{j=1}^{J}\beta_{jm}I,\ A\in R_{j,m} \tag{16}$$

第三步：停止迭代循环，确定最终的FDIA检测模型，其公式描述为：

$$F_{\mathrm{M}}(P)=\sum_{m=1}^{M}\sum_{j=1}^{J}\beta_{jm}I,\ A\in R_{j,m} \tag{17}$$

其中：M为总循环数量。

第四步：网络量测数据样本遭受虚假数据注入攻击的概率为$\mathbb{R}_{+}(A)$，未受到FDIA的概率为$\mathbb{R}_{-}(A)$，其公式描述为：

$$\begin{cases}\mathbb{R}_{+}(A)=\mathbb{R}_{\chi}(u=1|A)=\dfrac{1}{1+e^{-2F_M(A)}}\\ \mathbb{R}_{-}(A)=\mathbb{R}_{\chi}(u=-1|A)=\dfrac{1}{1+e^{2F_M(A)}}\end{cases} \tag{18}$$

按照下式完成网络量测数据样本标签$u(A)$的识别，公式为：

$$u(A)=2*l\{\sigma(-1,1)\mathbb{R}_{+}(A)>\sigma(-1,1)\mathbb{R}_{-}(A)\}-1 \tag{19}$$

式中：代价函数通过$\sigma(-1,1)$表示，若实际结果为1，预测结果为−1；通过函数$l\{\}$，可将布尔值变换为{0,1}。

将获取的FDIA网络量测数据特征输入到基于梯度提升决策树的FDIA检测模型中，输出的虚假数据攻击检测结果为1或0，前者为数据遭受虚假数据注入攻击；后者为数据未遭受虚假数据注入攻击。

2 实验结果与分析

以配电网的电力信息物理系统网络作为研究对象，向其注入攻击向量以对非完全网络拓扑下的虚假数据注入攻击进行仿真模拟，获得网络虚假数据注入攻击样本集，其中含有正常网络量测数据2 500条，异常注入攻击数据300条，以3∶1比例选择训练、测试样本，采用本文方法对网络虚假数据注入攻击进行检测，分析本文方法的检测性能。

FDIA产生后，网络量测数据异常分值的提取是实现网络虚假数据注入攻击检测的前提，孤立森林中二叉树的构建数量对异常分值特征的提取精度具有直接影响。采用本文方法对FDIA训练样本集进行异常分值提取，通过不同数量二叉树的受试者工作特征曲线(receiver operating characteristic curve，ROC)曲线的变化分析网络量测数据异常分值特征提取效果，实验结果如图1所示。分析图1可知，查全率反映虚假数据注入攻击样本准确识别为异常的概率，随着构建的二叉树数量的不断增多，网络量测数据异常分值提取的查全率呈先增后减趋势变化，当二叉树数量仅为30时，加大了虚假数据注入攻击异常样本的区分难度，异常样本难以完全孤立，从而降低了查全率指标值；当二叉树增加至120时，查全率指标上升至最大值，可达到93%左右，继续构建二叉树，查全率指标开始下降，当建立的二叉树达到400棵时，查全率指标值与30棵二叉树接近。实验结果表明，构造120棵二叉树有利于虚假数据注入攻击异常样本的孤立，异常分值提取结果更为精确。

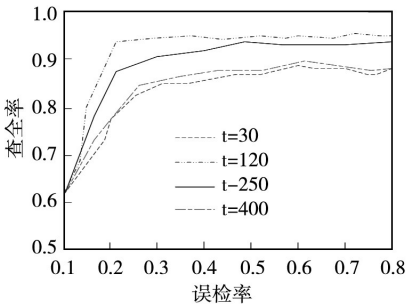

图1 不同二叉树数量下的ROC曲线分析

将本文方法应用于网络虚假数据注入攻击训练样本集的异常分值提取中，选取的其中异常分值最高的前10个提取结果如表1所示。通过分析异常分值提取结果及其在样本集的分布分析本文方法的异常特征提取能力。分析表1可知，采用本文方法对虚假数据注入攻击训练样本集的量测数据进行特征提取，能够确定电量数据的异常分值。

表1 网络量测数据异常分值提取结果

日期	时间	电量/kW·h	异常得分
2019/7/8	17:15:14	634	0.83
2019/7/8	20:33:20	698	0.80
2019/7/8	13:37:56	704	0.78
2019/7/8	20:34:15	1 534	0.77
2019/7/8	20:34:57	1 475	0.75
2019/7/8	20:34:45	1 431	0.74
2019/7/10	6:11:52	1 467	0.73
2019/7/10	6:12:41	756	0.72
2019/7/10	8:23:31	760	0.71
2019/7/10	9:23:50	755	0.71

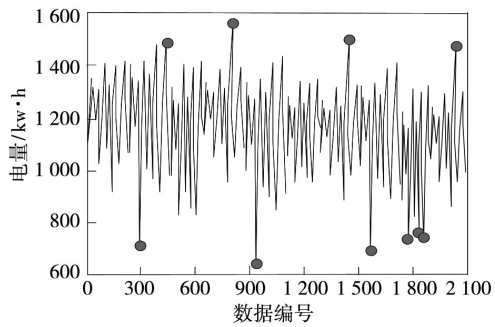

图2 选取电量数据在样本集中的分布分析

表1中数据在虚假数据注入攻击样本集中的分布如图2所示。图2中红色圆圈标记的即为提取到的异常分值较高的10个电量数据，从图中可看出，这10个数据与正常电量数据间的差异性较大，通过本文方法可实现异常电量数据的孤立，完成其异常分值特征的提取。

数据降维对FDIA网络量测数据特征提取的准确度具有重要影响，数据维度、邻居点数量的选择起决定性作用。采用本文方法对FDIA训练样本集进行检测，通过对不同数据维度下的虚假数据注入攻击检测效果实现数据维度、邻居节点数目的确定，实验结果如图3所示。分析图3可知，随着邻居节点数的不断地增多，网络虚假数据注入攻击检测率呈先增后减趋势变化，当邻居节点数目为8时，网络虚假数据注入攻击检测率达到最大值，即92%，继续增加邻居节点数目，虚假数据注入攻击检测能力下降。当邻居节点数目一定时，虚假数据注入攻击检测率随着数据维度的降低而不断增大。当数据维度为3时，虚假数据注入攻击检测率最高。因此，当数据维度为3、邻居节点数为8时，虚假数据注入攻击样本特征提取能力最强。

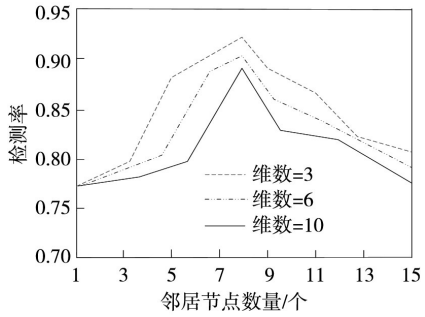

图3 不同维度下的虚假数据注入攻击检测效果分析

采用本文方法对FDIA检测模型进行训练后，利用训练好的FDIA检测模型完成FDIA检测样本的虚假数据注入攻击检测，检测样本数量为700条，其中正常样本数量和虚假数据攻击样本数量分别为620条和80条。通过统计分析本文方法的虚假数据注入攻击检测输出结果，验证本文方法的检测能力，实验结果如表2所示。分析表2可知，采用本文方法对网络FDIA训练样本数据进行虚假数据注入攻击检测，检测到有622个正常样本、78个FDIA样本，结合实际样本情况得出，仅有2个FDIA样本未被成功检测出，检测成功率高达97.5%。实验结果表明，本文方法能够对虚假数据注入攻击进行检测，并具有较好的检测效果。

表2 虚假数据注入攻击检测结果分析

检测输出结果	样本数量/条
1	622
0	78

3 结束语

应用本文方法对配电网某信息融合管理网络的虚假数据注入攻击进行检测，通过FDIA检测样本数据集的异常分值特征提取结果、不同数据维度的FDIA检测率的变化分析本文方法的FDIA检测性能。实验结果表明：(1)构造的二叉树数量为120时，FDIA检测样本数据集异常分值特征提取更精准；(2)数据维度为3、邻居节点数为8时，本文方法的特征提取性能最优；(3)本文方法可实现网络虚假数据注入攻击检测，FDIA检测成功率很高。

参考文献：

[1] 曹扬，胡飞飞，张思拓，等.基于OPNET的电力调度数据网络仿真[J].自动化技术与应用，2023，42(5)：144-145，149.

[2] 杨杉，谭博，郭静波.基于双马尔科夫链的新型能源互联网虚假数据注入攻击检测[J].电力自动化设备，2021，41(2)：131-137.

[3] 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.

[4] 谷云东，马冬芬，程红超.基于相似数据选取和改进梯度提升决策树的电力负荷预测[J].电力系统及其自动化学报，2019，31(5)：64-69.

[5] 周杰英，贺鹏飞，邱荣发，等.融合随机森林和梯度提升树的入侵检测研究[J].软件学报，2021，32(10)：3254-3265.

[6] 李新鹏，高欣，阎博，等.基于孤立森林算法的电力调度流数据异常检测方法[J].电网技术，2019，43(4)：1447-1456.

[7] 宋勇，齐迹.基于随机森林的电子档案资源快速分类研究[J].自动化技术与应用，2024，43(5)：102-105.

[8] 席亮，蒋涛，张凤斌.基于局部线性嵌入的免疫检测器优化生成算法[J].控制与决策，2019，34(5)：1032-1036.

[9] 赵子源，邢宏伟.基于大数据的电力监控系统网络安全监测系统设计[J].能源与环保，2022，44(1)：242-24，255.

作者简介：郭敬东(1968-)，男，硕士，高级工程师，研究方向：电力信息安全。