

DOI: 10.19783/j.cnki.pspc.211659

## 基于深度自编码器高斯混合模型的窃电行为检测

刘钊瑞<sup>1</sup>, 高云鹏<sup>1</sup>, 郭建波<sup>2</sup>, 李云峰<sup>1</sup>, 顾德喜<sup>1</sup>, 文一章<sup>1</sup>

(1. 湖南大学电气与信息工程学院, 湖南 长沙 410082; 2. 杭州海兴电力科技股份有限公司, 浙江 杭州 310011)

**摘要:** 针对用户侧窃电检测背景下无监督方法的适用性, 研究如何解决特征提取和异常检测间的解耦问题, 提出基于深度自编码器高斯混合模型(Deep Auto-encoder Gaussian Mixture Model, DAGMM)的用户窃电行为检测方法。首先对数据进行增广迪基-福勒检验, 获取具有平稳性的用电数据维度。然后通过压缩网络提取数据潜在特征, 利用估计网络及高斯混合模型获取反映异常程度的样本能量。最后基于端对端的学习方式对网络参数联合优化以避免模型解耦, 将样本能量超过异常阈值的用户识别为窃电, 据此实现用户窃电行为检测。实验结果表明, 基于深度自编码器高斯混合模型的窃电行为检测方法受窃电样本影响小, 提取的特征可有效反映用户用电规律, 具有更高的检测准确率。相比于现有方法, 其检出率、误检率、F1 测度及 AUC 等评价指标均有显著提高。

**关键词:** 窃电行为; 无监督学习; 深度自编码器高斯混合模型; 增广迪基-福勒检验; 解耦

### Abnormal detection of electricity theft using a deep auto-encoder Gaussian mixture model

LIU Zhaorui<sup>1</sup>, GAO Yunpeng<sup>1</sup>, GUO Jianbo<sup>2</sup>, LI Yunfeng<sup>1</sup>, GU Dexi<sup>1</sup>, WEN Yizhang<sup>1</sup>

(1. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China;

2. Hangzhou Haixing Electrical Co., Ltd, Hangzhou 310011, China)

**Abstract:** Considering the applicability of unsupervised methods for user-side electricity theft detection, this paper studies how to solve the decoupling problem between feature extraction and anomaly detection. It proposes a user-side electricity theft detection method based on the deep auto encoder Gaussian mixture model (DAGMM). First, the electricity consumption data dimension with stationarity is obtained according to the augmented Dickey Fuller test. Then, potential characteristics of data are extracted by compressing the network. An estimation network and Gaussian mixture model are used to obtain sample energy. This reflects the degree of anomaly. Finally, network parameters are optimized jointly based on end-to-end learning to avoid model decoupling, and identify users whose sample energy exceeds the abnormal threshold as electricity thief. In this way theft of electricity can be detected. The experimental results show that the detection method based on DAGMM is less affected by the sample of electricity theft, and the extracted features can effectively reflect the user's electricity consumption law with higher detection accuracy. Compared with the existing methods, the detection rate, false detection rate, F1 measurement and AUC of the proposed method are significantly improved.

This work is supported by the National Natural Science Foundation of China (No. 51777061).

**Key words:** stealing electricity; unsupervised learning; deep auto-encoder Gaussian mixture model; augmented Dickey Fuller test; decoupling

## 0 引言

随着我国电力市场化进程不断推进以及用户对电能可靠性和质量要求不断提升, 智能电网安全稳

定运行的需求日益增强<sup>[1-2]</sup>。对用户侧数据进行深入研究有利于降低供电企业非技术性损失, 提高电力系统稳定性<sup>[3]</sup>。窃电行为是造成电网非技术性损失的主要原因之一, 其对电力企业经济利益、电力系统稳定运行造成巨大的威胁<sup>[4-5]</sup>。因此, 研究提高窃电检测效果的方法对社会经济发展具有重要价值与意义<sup>[6]</sup>。

**基金项目:** 国家自然科学基金项目资助(51777061); 广西电网科技项目资助(GXKJXM20200020)

传统窃电检测主要依靠人工稽查, 该方式存在盲目性, 具有检测效率低、消耗大量人力资源、增加电网运营成本等缺点<sup>[7]</sup>。随着电力系统智能化程度不断提高, 泛在物联网建设发展使电力公司获得指数级增长的数据量, 为数据驱动方法提供有力支撑<sup>[8-10]</sup>。基于数据驱动的窃电行为检测方法主要可分为有监督学习<sup>[11-13]</sup>和无监督学习<sup>[14]</sup>两类。有监督学习需对大量已知用户是否窃电的标签数据进行学习, 而实际应用中已知窃电用户量通常很小, 不足以支撑有监督模型训练, 且有监督学习在用电习惯及窃电手段发生变化的情况下检测效果降低。无监督学习因不需要标签数据训练, 对数据量的要求不高, 相比有监督学习, 无监督学习具有高时效性, 适用范围更加广泛<sup>[15]</sup>。

当前, 国内外学者基于无监督方法对窃电行为检测技术展开了一定的研究。文献[14]利用异常样本与典型负荷曲线的相似程度低, 采用模糊聚类提取特征曲线, 通过待测曲线与特征曲线比较初步确定疑似窃电用户。文献[16]从异常点影响聚类结果及用户用电习惯随季节等因素变化的角度出发, 提出流式密度聚类算法快速检测窃电用户。文献[17]考虑电网数据洁净度与用户类别不平衡, 通过迭代筛选提取相对最大密度类群以提高窃电检测精度。文献[18]考虑到用户日负荷具有随机性, 对多次由密度峰值聚类算法识别为窃电的用户进行稽查以降低误检率。文献[19]结合形状和密度信息, 采用最大信息系数作为评价相似性指标, 以更好地描述用户用电习惯的相似性。然而, 由于用户用电习惯受季节、经济等多种因素影响, 负荷曲线形态复杂且具有随机波动性, 相似的两条曲线可能存在时移, 导致欧式距离等作为评价相似性指标失效<sup>[20]</sup>, 用电负荷数据的高维特性使其在原始特征空间中进行密度估计较为困难, 随着数据维度增加, 密度预测时间复杂度急剧增加<sup>[21]</sup>, 因此, 利用负荷曲线表示用户用电规律在某些情况下可能失效, 提取合适的负荷特征表示用电习惯对窃电行为准确检测具有重要价值。

为此, 文献[22]考虑时段负荷波动性, 提出用电量变化指标和小时内用电模式变化指标等时段负荷变化特征表征用户用电规律。文献[15]考虑日用电量变化趋势及随季节波动特性, 提取趋势指标、变动性指标、波动性指标等用户长期负荷特征, 通过主成分分析对特征降维, 利用网格化局部离群因子检测窃电用户。文献[23]采用同文献[15]的特征, 提出基于高斯核函数的局部离群因子算法以降低数据分布差异对窃电检测性能的影响。文献[24]考虑

各特征重要程度不同, 采用层次分析法确定各指标权重, 通过加权的离群点检测算法识别异常。目前, 基于无监督方法对窃电行为检测的研究, 在特征提取和异常检测上均独立进行, 而实际负荷曲线形态复杂, 现有提取时段特征方法只适用符合正常用户用电基本平稳假设的窃电行为检测<sup>[25]</sup>, 当数据不符合上述情况时, 特征提取方法将失效, 提取用户长期用电特征时, 若所选时长不合适, 检测效果也将变差, 特征提取后不再对特征进行优化的异常检测方法易丢失关键信息, 使特征提取与异常检测间解耦, 导致无监督方法在窃电行为检测上适用性较低。

针对上述问题, 本文提出基于深度自编码器高斯混合模型(Deep Auto-encoder Gaussian Mixture Model, DAGMM)的窃电行为检测方法。首先根据推广迪基-福勒检验选取具有平稳性的用电数据维度, 通过 DAGMM 压缩网络提取负荷压缩编码和重构误差特征, 在高斯混合模型框架下使用估计网络进行密度估计, 并通过高斯混合模型获取反映异常程度的样本能量, 将重构误差、样本能量及避免局部最优和奇点问题引入的正则项作为代价损失, 再基于端对端的学习方式对网络参数联合优化, 通过箱线图设置异常阈值, 将样本能量超过阈值的用户识别为窃电, 据此实现用户窃电行为检测。最后通过大量实验对本文提出方法的准确性和有效性进行验证分析。

## 1 用电数据分析与预处理

### 1.1 数据预处理

电网数据采集过程中存在软硬件故障、特殊事件等, 易导致采集数据存在缺失<sup>[26]</sup>, 据此本文按缺失比例不同对数据采用不同方式预处理。当某用户缺失数据占比超过5%时, 认为非偶然因素导致用户数据缺失, 将该用户单独进行用电异常排查, 否则对邻近两天同时段负荷均值进行修正, 由此构建修正公式为

$$f(x_{ij}^k) = \frac{1}{2}(x_{ij}^{k-1} + x_{ij}^{k+1}) \quad (1)$$

式中,  $x_{ij}^k$  为第  $i$  个用户第  $k$  天第  $j$  个采样点的负荷。

电力负荷包括基荷和变动负荷, 为突出变动负荷走势, 同时避免数量级相差较大的影响, 通过归一化去掉基荷。对每日负荷进行归一化, 可减弱具有临界峰值或错误数据注入的异常天数和季节的影响<sup>[27]</sup>, 本文对每日负荷采用 min-max 归一化处理, 有

$$x_{ij}^k = \frac{x_{ij}^k - x_{\min}^k}{x_{\max}^k - x_{\min}^k} \quad (2)$$

式中： $x_{\min}^k$  为第  $i$  个用户第  $k$  天负荷的最小值； $x_{\max}^k$  为第  $i$  个用户第  $k$  天负荷的最大值。

### 1.2 用电数据维度选取

用户日负荷具有随机波动性，易受季节、经济等多种因素影响，采用日负荷进行分析具有不稳定性。较长用电量数据隐含较多信息，有利于模型学习潜在用电规律，但过长负荷数据使模型复杂性增加，同时使模型学习难度提升。为减少数据维度对窃电检测方法的影响，可选择平稳的多日负荷进行分析。

增广迪基-福勒检验(Augmented Dickey-Fuller test, ADF)可排除自相关影响，通过对单位根检验判断数据是否存在趋势性及季节性特征。本文实验对训练集用户负荷数据计算 ADF 检验值，根据赤池信息准则(Akaike Information Criterion, AIC)确定滞后数目，各置信度下平稳性检验结果如图 1 所示。

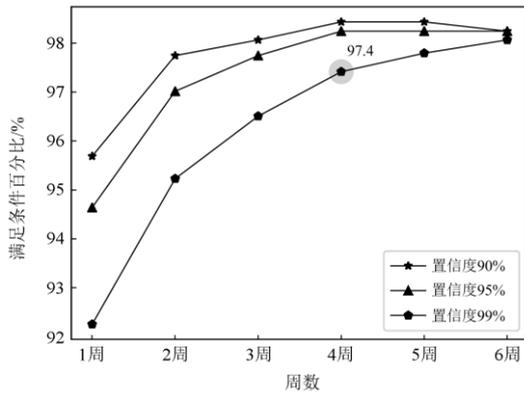


图 1 各置信度下平稳性检验结果

Fig. 1 Results of stationarity test at each confidence level

由图 1 可知，当选择 4 周负荷数据进行平稳性分析时，97.4%的数据有大于 99%的置信度为平稳

序列，故本文选取每个用户 4 周负荷数据作为输入。

## 2 基于 DAGMM 的窃电检测方法

### 2.1 深度自编码器高斯混合模型构建

深度自编码器高斯混合模型由压缩网络和估计网络组成。其中压缩网络提取数据的潜在特征，估计网络在高斯混合模型框架下对潜在特征进行密度估计，并通过高斯混合模型得到反映异常程度的样本能量，样本能量超过阈值识别为异常，其结构如图 2 所示。

由图 2 可知，窃电检测中每个样本的特征向量为单个电力用户 4 周用电负荷序列  $x$ ，压缩网络的任务是使  $x$  与其重构所得序列  $x'$  尽可能相似，同时获得最显著的编码特征，并从多种相似性角度提取重构误差特征，更好地表征用电负荷序列特点。由于大多数用户为正常用户，为获得更小的重构误差，压缩网络参数偏向拟合正常用户的负荷数据，进而使正常与窃电用户的特征有较大差异。压缩网络通过深度自编码器和重构误差单元提取负荷序列的压缩编码和重构误差特征，压缩编码为

$$z_c = h(x; \theta_e) \quad (3)$$

式中： $h(\cdot)$ 为编码器函数； $\theta_e$ 为编码器参数。

通过解码器对  $z_c$  进行重构得到重构向量，即

$$x' = g(z_c; \theta_d) \quad (4)$$

式中： $g(\cdot)$ 为解码器函数； $\theta_d$ 为解码器参数。

利用重构误差特征函数  $f(\cdot, \cdot)$ ，提取样本  $x$  和重构向量  $x'$  的重构误差特征为

$$z_r = f(x, x') \quad (5)$$

由此，将  $z_c$  和  $z_r$  组成样本低维特征  $z$  输入估计网络。

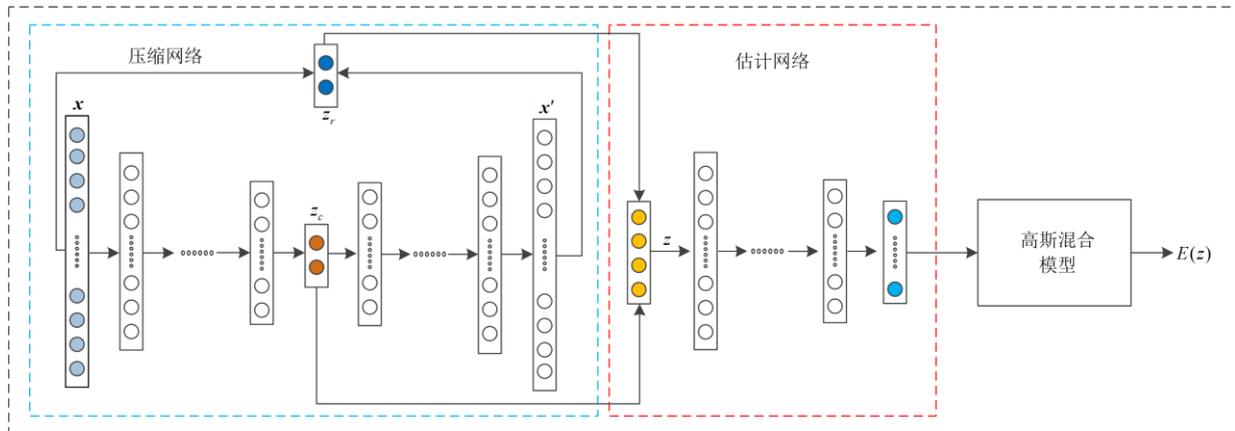


图 2 深度自编码器高斯混合模型结构图

Fig. 2 Structure of deep auto-encoder Gaussian mixture mode



估计网络的任务是在高斯混合模型框架下对压缩网络提取的特征进行密度估计, 获取高斯混合模型参数并通过高斯混合模型得到样本能量。基于大部分用户为正常用户及正常用户具有相似用电规律的假设, 窃电用户符合某个高斯混合成分的概率较小, 其样本能量值较高, 样本能量越高该样本异常的可能性越大, 将低维特征  $\mathbf{z}$  输入估计网络得到输出向量, 有

$$\mathbf{p} = MLN(\mathbf{z}; \boldsymbol{\theta}_m) \quad (6)$$

式中:  $MLN(\cdot)$  为多层神经网络函数;  $\boldsymbol{\theta}_m$  为多层神经网络参数。

输出层神经元数  $n$  为假设的高斯混合成分数  $K$ , 将输出  $\mathbf{p}$  通过 softmax 激活函数得到样本归属于各高斯混合成分的  $K$  维概率, 即

$$\boldsymbol{\gamma} = \text{softmax}(\mathbf{p}) \quad (7)$$

估计网络将多层神经网络与 EM 算法有机结合, 通过概率  $\boldsymbol{\gamma}$  和低维特征  $\mathbf{z}$  可估算高斯混合模型的均值  $\boldsymbol{\mu} = [\boldsymbol{\mu}_1 \boldsymbol{\mu}_2 \text{L} \boldsymbol{\mu}_K]$ 、分量分布  $\boldsymbol{\varphi} = [\varphi_1 \varphi_2 \text{L} \varphi_K]$  和协方差  $\mathbf{C} = [\mathbf{C}_1 \mathbf{C}_2 \text{L} \mathbf{C}_K]$ , 可得

$$\boldsymbol{\mu}_k = \frac{\sum_{i=1}^N \gamma_{ik} \mathbf{z}_i}{\sum_{i=1}^N \gamma_{ik}} \quad k = 1, 2, \text{L}, K \quad (8)$$

$$\varphi_k = \frac{\sum_{i=1}^N \gamma_{ik}}{N} \quad k = 1, 2, \text{L}, K \quad (9)$$

$$\mathbf{C}_k = \frac{\sum_{i=1}^N \gamma_{ik} (\mathbf{z}_i - \boldsymbol{\mu}_k)(\mathbf{z}_i - \boldsymbol{\mu}_k)^T}{\sum_{i=1}^N \gamma_{ik}} \quad k = 1, 2, \text{L}, K \quad (10)$$

式中,  $N$  为样本总数。

利用估计出的高斯混合模型参数计算样本能量表达式为

$$E(\mathbf{z}) = -\log\left(\sum_{k=1}^K \varphi_k \frac{\exp(-\frac{1}{2}(\mathbf{z} - \boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k^{-1}(\mathbf{z} - \boldsymbol{\mu}_k))}{\sqrt{|\mathbf{C}_k|}}\right) \quad (11)$$

DAGMM 总代价函数包括三部分, 分别为压缩网络的重构误差损失  $L(\mathbf{x}, \mathbf{x}')$ 、估计网络的样本能量以及避免局部最优和奇点问题引入的正则项。总代价函数可表示为

$$J(\theta_e, \theta_d, \theta_m) = \frac{1}{N} \sum_{i=1}^N L(\mathbf{x}_i, \mathbf{x}'_i) + \frac{\tau_1}{N} \sum_{i=1}^N E(\mathbf{z}_i) + \tau_2 \sum_{k=1}^K \sum_{j=1}^d \frac{1}{C_{kij}} \quad (12)$$

式中:  $\tau_1$  为估计网络代价参数;  $\tau_2$  为正则项参数;  $d$  为样本维数。

DAGMM 整体训练过程为压缩网络提取数据低维特征, 估计网络获取高斯混合模型参数, 通过高斯混合模型计算样本能量, 根据代价损失函数得到代价损失值, 并通过梯度下降法求代价损失最小值, 更新压缩网络和估计网络参数。

## 2.2 DAGMM 参数选取

本文通过对用电负荷数据分析进行窃电行为检测, 由于负荷数据中包含冗余信息, 采用欠完备自编码器作为压缩网络编码器, 网络的激活函数对算法性能有较大影响, 本文压缩网络采用 softplus 激活函数, 估计网络采用 tanh 激活函数, 其计算式分别为

$$\text{softplus}(y) = \log(1 + e^y) \quad (13)$$

$$\tanh(y) = \frac{e^y - e^{-y}}{e^y + e^{-y}} \quad (14)$$

softplus 激活函数用来解决梯度消失问题, 具有单侧抑制和稀疏灵活特性, 其具有相对宽阔的兴奋边界, 可有效避免大部分神经元死亡现象的发生。tanh 激活函数关于原点对称, 在原点附近梯度较大, 可使模型快速收敛。因此, 选取 softplus 函数作为压缩网络激活函数使模型参数稀疏化, 模型可有效学习复杂的用电规律; 选取 tanh 函数作为估计网络激活函数, 可加快模型学习速度, 使算法更快达到较好的检测性能。

重构误差特征可反映样本与其他用户用电习惯间的差异, 本文从距离和形态两个角度进行重构误差特征提取。针对距离特征, 由于高维时间序列数据在平方以上的高次方运算中出现截断误差<sup>[28]</sup>, 且曼哈顿距离在计算速度上优于欧几里得距离, 同时为避免特征值过大, 采用相对曼哈顿距离提取样本与重构向量间的距离误差, 可得

$$D_{\text{Manhattan}}(\mathbf{x}_i, \mathbf{x}'_i) = \frac{\sum_{j=1}^d |x_{ij} - x'_{ij}|}{\sum_{j=1}^d |x_{ij}| + \varepsilon} \quad (15)$$

式中:  $\varepsilon$  为防止分母为 0 的附加项;  $x_{ij}$  表示第  $i$  个用户第  $j$  个采样点负荷;  $x'_{ij}$  表示重构的第  $i$  个用户第  $j$  个采样点负荷。

采用余弦相似度衡量样本与重构向量间的形态误差, 其计算式为

$$D_{\text{cos}}(x_i, x'_i) = 1 - \frac{\sum_{j=1}^d (x_{ij} x'_{ij})}{\sqrt{\sum_{j=1}^d (x_{ij})^2} \sqrt{\sum_{j=1}^d (x'_{ij})^2} + \varepsilon} \quad (16)$$

对于 DAGMM 结构的设计, 本文最终确定网络结构参数如表 1 所示。

表 1 DAGMM 结构参数

Table 1 Structural parameters of DAGMM

结构	参数
压缩网络	编码部分: 1344/168/64/4
	解码部分: 64/168/1344
	激活函数: softplus
估计网络	网络结构: 6/26/13
	激活函数: tanh
其余参数	$\lambda_1$ : 0.1
	$\lambda_2$ : 0.001
	迭代次数: 50
	学习率: 0.001
优化器: AdamOptimizer	

### 2.3 窃电行为检测阈值设定

为保证本文所提方法检出更多窃电用户的同时减少误判, 需设置合理检测阈值, 本文将样本能量超过所设阈值的用户判定为较大窃电嫌疑, 提出利用箱线图设定窃电行为检测阈值, 箱线图异常阈值选取原理图如图 3 所示。箱线图作为可显示数据分散情况的统计图, 其利用数据的 5 个统计量, 即最小值、第一四分位数、中位数、第三四分位数和最大值来描述数据分布, 认为离群值为数据序列中的极端值。

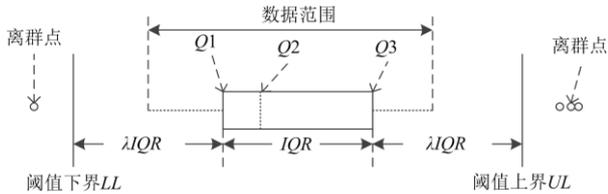


图 3 箱线图异常阈值选取

Fig. 3 Selection of abnormal threshold for boxplot

如图 3 所示, 定义第一四分位数  $Q1$ , 第三四分位数  $Q3$ , 四分位距为  $IQR = Q3 - Q1$ , 阈值上界为  $UL = Q3 + \lambda \cdot IQR$ , 阈值下界为  $LL = Q1 - \lambda \cdot IQR$ , 取阈值上界作为窃电行为检测阈值, 经实验测试  $\lambda$  设为 1.5 时截取的检出率和误检率位于 ROC 曲线的拐点, 故  $\lambda$  设为 1.5 最为合理。利用箱线图选取的阈值完全依靠实际数据, 不需假定数据服从某种特定分布, 真实直观地反映数据自身特性,  $IQR$  反映处于 25%~75% 的数据分布, 具有良好的抗噪性, 极端数据也不会影响  $IQR$  和  $Q3$ , 因此, 箱线图的阈值上界作为检测阈值更加准确客观。

### 2.4 算法流程

本文提出的基于深度自编码器高斯混合模型的用户侧窃电行为检测方法, 实现流程如图 4 所示。

如图 4 所示, 本文检测方法的具体实现步骤如下。

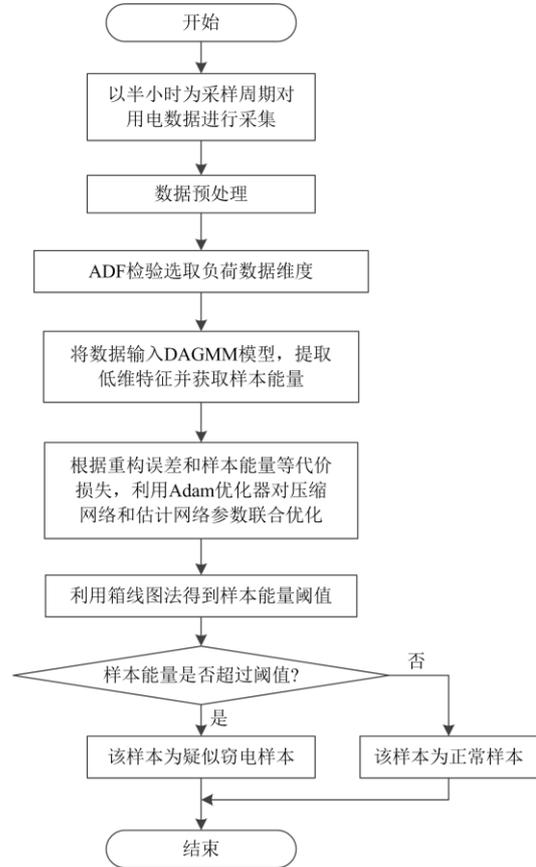


图 4 基于 DAGMM 的窃电行为检测流程图

Fig. 4 Flow chart of electric theft behavior detection based on DAGMM

1) 以半小时为采样周期, 采集各用户历史 6 周的用电负荷数据作为原始数据;

2) 对数据进行预处理, 针对缺失值进行填补和剔除后, 对每日负荷进行 min-max 归一化处理, 去除基荷并减弱某日异常数据对归一化的影响;

3) 对数据进行平稳性分析, 基于 AIC 准则确定滞后数目, 选取使多数用户满足 99% 置信度下的 ADF 数据长度为输入维度;

4) 将样本输入 DAGMM 模型进行训练, 利用压缩网络得到用户用电习惯的低维表示, 并基于余弦相似度、相对曼哈顿距离获得用户的重构误差特征, 通过估计网络在高斯混合模型框架下进行特征密度估计, 利用高斯混合模型获得样本能量;

5) 基于 AdamOptimizer 优化器和总代价损失对 DAGMM 的压缩网络和估计网络参数联合优化, 利用优化后的 DAGMM 重新计算样本能量;

6) 通过箱线图得出样本能量异常阈值, 将样本能量超过阈值的用户识别为窃电, 据此实现用户窃电行为检测。

### 3 仿真实验与分析

本文实验平台使用 AMD Ryzen 7 4800U with Radeon Graphics CPU@1.80 GHz, 在 python3.7 环境下进行分析, 深度学习框架选取 TensorFlow。

#### 3.1 数据集构建与评价指标

##### 3.1.1 数据集构建

本文采用爱尔兰电力公司和爱尔兰可持续能源局发布的真实用电数据作为数据集, 该数据集包含超过 5000 个爱尔兰居民和商业用户 535 天的用电记录(以半小时为采样间隔), 本文选取其中 2500 个居民用户 42 天的负荷记录作为研究对象。由于数据集中各居民用户同意将采集数据用于研究使用, 设所有用户均为正常用户。随机选取部分正常用户用电记录构造窃电样本, 构造算式为

$$\left\{ \begin{array}{l} h_1(x_{ij}) = \alpha x_{ij}, \alpha = \text{random}(0.1, 0.8) \\ h_2(x_{ij}) = \begin{cases} x_{ij}, & \text{if } x_{ij} \leq \eta \\ \eta, & \text{if } x_{ij} > \eta \end{cases}, \eta = \text{random}(0, 1) \\ h_3(x_{ij}) = \max\{x_{ij} - \eta, 0\} \\ \eta = \text{random}(0, 1) \times x_{i\max} \\ h_4(x_{ij}) = 0 \\ h_5(x_{ij}) = \alpha_j x_{ij}, \alpha_j = \text{random}(0.1, 0.8) \\ h_6(x_{ij}) = \alpha_j \text{mean}(x_i), \alpha_j = \text{random}(0.1, 0.8) \\ h_7(x_{ij}) = x_{i(49-j)} \end{array} \right. \quad (17)$$

式中:  $h_1(\cdot)$  表示持续按固定比例减小计量电量, 更换互感器、分压分流等窃电手段;  $h_2(\cdot)$  表示按动态分数降低电表计量, 将超出阈值的电量拦截上报的窃电手段;  $h_3(\cdot)$  表示可控开关间断性报告零电量, 在无稽查风险时窃电;  $h_4(\cdot)$  表示全时段零电量, 包括电表开路、断开电压表连接片、无表法等窃电手段;  $h_5(\cdot)$ 、 $h_6(\cdot)$  分别表示持续按变比例随机减少计量电量和在用户电量均值基础上按随机变比减少电量, 篡改电表软件的智能化窃电;  $h_7(\cdot)$  表示根据分时电价颠倒用电时序, 降低电费成本的窃电手段。

##### 3.1.2 评价指标

考虑实际检测中大多数用户为正常用户, 只有极少数用户存在窃电行为, 故对窃电检测模型不能只使用准确率作为评价指标, 为对模型进行有效评估, 本文基于表 2 所示的混淆矩阵进行评价。

表 2 混淆矩阵

Table 2 Confusion matrix

用户类型	检测为窃电用户	检测为正常用户
实际为窃电用户	TP	FN
实际为正常用户	FP	TN

如表 2 所示, 利用混淆矩阵获得多个评价指标, 本文选择准确率 ACC、检出率 TPR、误检率 FPR 和 F1 测度进行评价, 其定义分别为  $\text{ACC} = \text{TP} / (\text{TP} + \text{FP})$ 、 $\text{TPR} = \text{TP} / (\text{TP} + \text{FN})$ 、 $\text{FPR} = \text{FP} / (\text{FP} + \text{FN})$ 、 $\text{F1} = 2\text{TP} / (2\text{TP} + \text{FN} + \text{FP})$ 。其中, TPR 表示检出真实窃电用户占总窃电用户的比例, FPR 表示正常用户被误判为窃电用户占所有正常用户总数的比例。由于窃电稽查成本高, TPR 和 FPR 为主要关注的评价指标, F1 测度为 TPR 和 FPR 的调和平均数, 其兼顾模型的 TPR 和 FPR, F1 越高模型性能越好。

ROC 曲线以 FPR 为横轴, TPR 为纵轴, 反映 FPR 和 TPR 两个指标增长速率的相对关系, AUC 为 ROC 曲线下的面积, 作为衡量学习器优劣的性能指标。AUC 的值越高, 该分类器的效果越好, 故将 ROC 曲线和 AUC 用于窃电检测模型评估。

#### 3.2 检测结果分析

本文将数据随机分为 80% 的训练集和 20% 的测试集, 以用户 4 周负荷数据为输入, 定义窃电用户数占总用户数的比例为窃电比例, 随机选取 5%、10%、20% 的正常用户构造窃电样本, 检测结果如表 3 所示。

表 3 窃电行为检测结果

Table 3 Result of electricity theft detection

窃电比例/%	ACC/%	TPR/%	FPR/%	F1	AUC
5	92.70	69.61	6.10	0.9608	0.8490
10	91.48	67.72	6.27	0.9526	0.8220
20	88.32	50.75	4.14	0.9318	0.7898

由表 3 可知, 在 10% 窃电比例下, 基于本文提出方法的 TPR 为 0.6772, FPR 为 0.0627, 即正常用户被误判的概率为 6.27% 时, 可检出 67.72% 的窃电用户, 具有较好的检测性能。在 5% 和 10% 低窃电比例下, 基于本文方法检测的 AUC 均在 0.82 以上, 同时具有较高的 F1 测度, 由箱线图阈值得到的 TPR 较高, 同时 FPR 较低。随窃电比例增加, 当窃电比例达到 20%, TPR 约为 50% 时, 检测性能略有下降。分析可知, 本文检测方法本质为基于重构的异常检测, 其要求数据符合大部分正常用户具有相似用电规律的假设, 只有少数异常用户具有与正常用户相差较大的用电习惯。当窃电比例较高时, 不符合大多数样本为正常样本的基本假设, 导致模型训练受窃电样本影响变大, 不能偏向拟合正常样本的数据分布。

以 10% 窃电比例展开分析, 训练集各类窃电样本数分别为 32、19、28、23、27、28 和 32, 本文所提方法对各窃电类型检出百分比分别为 9.38%、89.47%、96.43%、100.00%、0%、100.00% 和 93.75%。

通过对 5%、10% 和 20% 窃电比例下各类窃电手段检测情况的分析, 本文所提方法对  $h_4$ 、 $h_6$  对应的窃电手段能全部检出, 大概率检测出  $h_2$ 、 $h_3$  和  $h_7$  造成的窃电现象, 对  $h_1$  和  $h_5$  对应的窃电手段无法有效检测。

多维标度法(Multidimensional Scaling, MDS)降维保证所有数据点在低维和高维空间中的欧式距离相等。用户数据基于 MDS 映射到二维平面的散点图如图 5 所示。

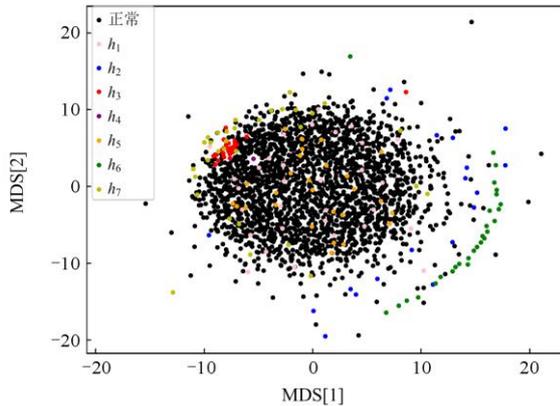


图 5 用户数据映射到二维平面的散点图

Fig. 5 Scatter diagram for customers after mapping

由图 5 可知,  $h_1$ 、 $h_5$  生成的窃电样本与正常样本分布相近, 且由  $h_1$  表达式可知, 其标准化后与生成该窃电原样本一致, 故窃电方式  $h_1$  较难识别。由各窃电算式定义可知,  $h_4$  的值一直保持不变,  $h_2$ 、 $h_3$  和  $h_6$  导致负荷波动性较大,  $h_7$  与大多数正常样本的峰值相反, 由于编码器能学习到位置信息,  $h_7$  重构时误差较大, 窃电用户识别结果如图 6 所示。

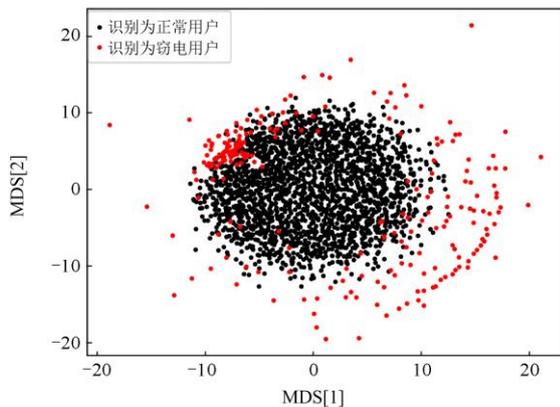


图 6 窃电用户识别结果

Fig. 6 Electricity stealing user identification result

由图 6 可知, 本文所提方法将远离大多数正常样本的正常用户误判为异常用户, 对有多个相似用电规律的用户类型几乎不会误判。因此, 本文所提方法能较为准确地检出窃电用户, 当出现离群正常

用户的现象时, 仍能有效检测出离群用户。

### 3.3 算法性能影响分析

#### 3.3.1 数据维度影响分析

日用电负荷具有随机波动性, 易造成误判, 过长负荷数据具有较高的模型复杂度和学习难度。本文针对数据维度对算法性能影响进行实验, 不同输入数据维度下本文所提方法的 ROC 曲线如图 7 所示。

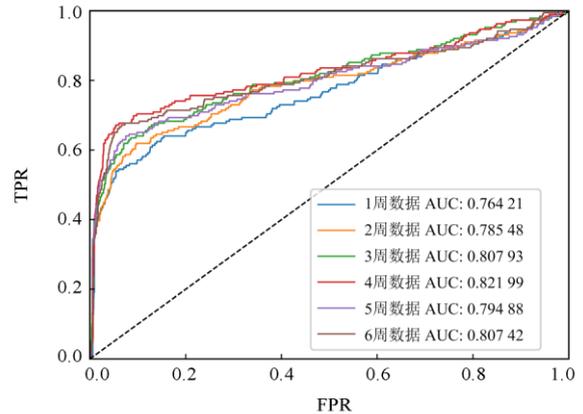


图 7 不同输入维度 ROC 曲线

Fig. 7 ROC curve for different input dimensions

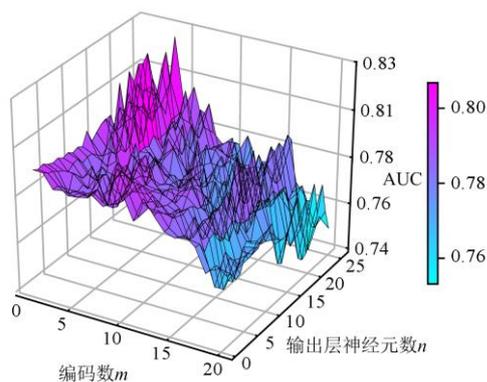
由图 7 可知, 当采用 1 周、2 周用电量数据分析时, 本文提出方法的 AUC 在 0.79 以下, 输入数据信息量相对较少, 导致模型学习信息不足, 检测性能相对较差。当采用 5 周、6 周用电量数据分析时, 本文方法的 AUC 在 0.8 左右, 数据包含足够信息量, 增大数据维度对算法性能的提升不显著, 同时模型复杂度增加, 数据重构难度增大, 算法性能相对降低。经平稳性分析可知, 多数用户 4 周负荷数据不受季节和趋势信息影响, 数据长度相对较短, 使模型具有相对较少的参数, 其作为输入的 AUC 为 0.822, 相较其他维度更为合理, 因此, 综合数据平稳性分析有效选取数据输入维度, 可使本文方法具有更高的检测准确率。

#### 3.3.2 DAGMM 参数影响分析

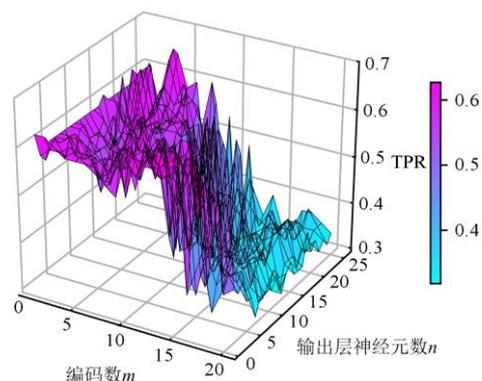
DAGMM 的参数对窃电行为检测性能有较大影响, 其中, 编码器编码数影响负荷数据的压缩程度和方向, 估计网络输出神经元数为假设的高斯混合成分数, 其影响样本能量计算结果, 本文针对编码数  $m$  和输出层神经元数  $n$  对算法性能的影响进行实验, 设置估计网络结构为  $(m+2)/2n/n$ , 其他参数保持不变, 不同参数下各评价指标表面图如图 8 所示。

由图 8(a)可知, 当编码数  $m$  为 4 时, 输出层神经元数  $n$  在 13~25 均具有较高的 AUC, 当  $m$  较小且  $n$  取不同值时, 本文方法的 AUC 在 0.78 以上,

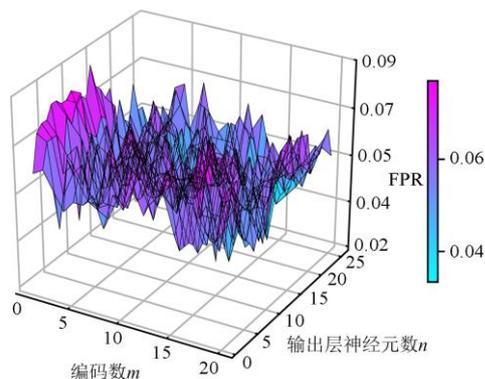
当  $m$  取值较高时, AUC 降低。分析可知, 当  $m$  较大时, 提取的特征包含次要信息过多, 导致算法性能下降。由图 8(b)和图 8(c)可见, 当  $m$  较小  $n$  较大时, 测试集的 TPR 较高同时 FPR 相对较低, 低误检率下能检测出大多数窃电用户。因此, 当选取较低  $m$  和相对较大  $n$  时, 本文方法具有较高检测准确率。



(a) AUC表面图



(b) 测试集TPR表面图



(c) 测试集FPR表面图

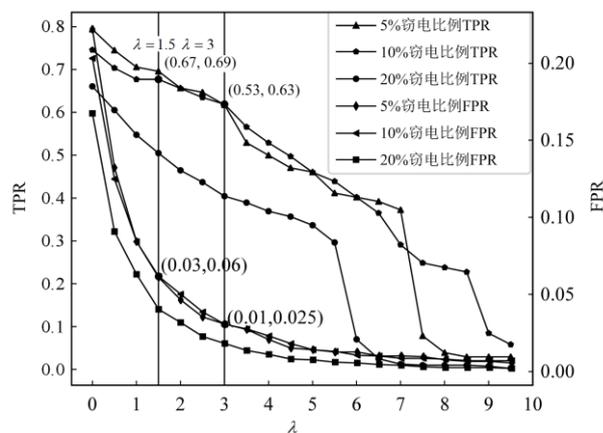
图 8 不同参数下方法性能

Fig. 8 Algorithm performance of different parameters

### 3.3.3 箱线图参数影响分析

本文利用箱线图设定异常阈值, 阈值计算式为

$UL = Q3 + \lambda \cdot IQR$ , 参数  $\lambda$  影响本文方法的检测结果。本文对 5%、10% 和 20% 窃电比例下样本展开实验, 参数  $\lambda$  对方法性能的影响如图 9 所示。

图 9 参数  $\lambda$  对方法性能的影响Fig. 9 Influence of parameter  $\lambda$  on algorithm performance

由图 9 可知, 随着  $\lambda$  增加, FPR 下降幅度减缓, 当  $\lambda$  取值为 1.5 时, FPR 接近拐点且在 7% 以下, 同时具有较高的 TPR。当  $\lambda$  取值为 3 时, FPR 在 4% 以下, 低窃电比例下 TPR 在 60% 左右, 继续增加  $\lambda$ , FPR 下降幅度平缓, 检测性能变差。

不同窃电比例下本文方法的 ROC 曲线如图 10 所示。

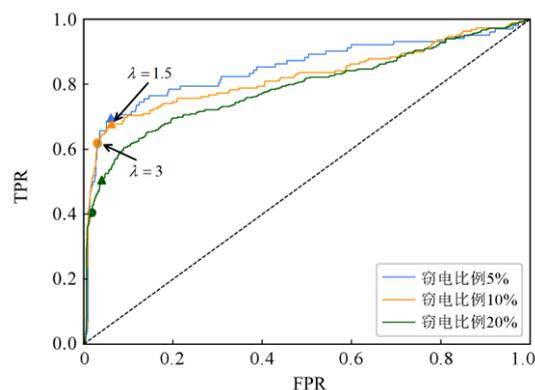


图 10 不同窃电比例下本文方法的 ROC 曲线

Fig. 10 ROC curves of the proposed method under different electricity-stealing ratios

由图 10 可知, 在低窃电比例下,  $\lambda$  设为 1.5 和 3 分别对应 ROC 曲线的两个转折点, 因此将  $\lambda$  设为 1.5~3 之间较为合理。

### 3.4 与现有方法比较

为了验证本文方法的有效性, 比较现有的同结构压缩网络 (Compression Network, CN) 结合 LOF (Local Outlier Factor)、OCSVM (one class support

vector machine)、GMM(Gaussian Mixed Model)、KNN(K-Nearest Neighbor)、iForest(Isolation Forest)及同结构自编码器(Autoencoder, AE)结合 GMM 等几种方法,各方法参数设置如表 4 所示,各方法检测结果如表 5 所示。

由表 5 可知,本文方法的各评价指标均优于 CN\_GMM,本文方法端对端的学习方式对压缩网络和估计网络参数联合优化,使模型参数更加合理。AE\_GMM 比 CN\_GMM 的 AUC 低 0.076,对重构误差进行特征提取可挖掘出更多代表数据是否正常的信息。本文所提方法的 AUC 为 0.82, CN 结合其他分类器的 AUC 值为 0.76 左右,除 AE\_GMM 的 FPR 较高,在各方法 FPR 相近的情况下,本文所提方法的 TPR 为 67.72%,其他方法的 TPR 在 50%左右,在特征提取方式相同的情况下,其他各无监督检测算法性能相似,本文方法检测性能远优于其他。

表 4 检测方法与参数设置

方法	模型参数
CN_LOF	邻居数: 300, 叶子数: 20
	距离度量: 欧式距离
	按异常比例 10%选取阈值
CN_OCSVM	训练误差分数上界: 0.1
	核函数: RBF
	gamma: 0.25
CN_GMM	高斯混合成分数: 6
	阈值: 0.2
CN_KNN	邻居数: 300
	采用箱线图选取阈值
	最大样本数: 256
CN_iForest	估计器数: 100, 最大特征数: 2
	按窃电比例 10%选取阈值
AE_GMM	高斯混合成分数: 4
	阈值: 0.8

表 5 不同方法窃电行为检测结果

方法	ACC/%	TPR/%	FPR/%	F1	AUC
CN_LOF	90.29	51.85	6.07	0.9464	0.7662
CN_OCSVM	89.92	49.21	6.22	0.9444	0.7045
CN_GMM	89.97	50.26	6.27	0.9447	0.7661
CN_KNN	90.01	55.56	6.72	0.9446	0.7834
CN_iForest	90.38	52.38	6.02	0.9469	0.7639
AE_GMM	86.17	40.21	9.48	0.9228	0.6897
DAGMM	91.48	67.72	6.27	0.9526	0.8220

不同检测方法的 ROC 曲线如图 11 所示。

如图 11 所示,本文方法的 ROC 曲线在低 FPR 下具有相对较高的 TPR,即在误检用户数相同的情

况下,可检测出更多窃电用户,有效减少不必要的稽查,节约人力物力成本的同时可查处大部分窃电用户,相比于其他方法,本文所提方法具有更高的检测准确度。

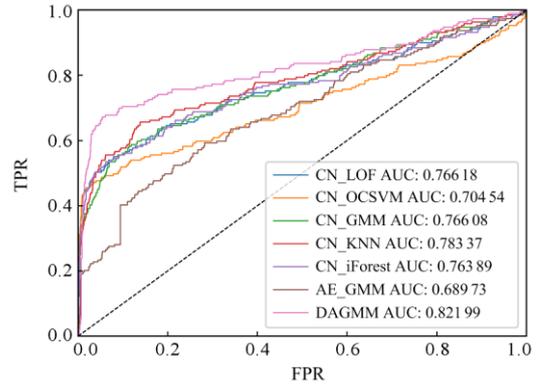


图 11 不同检测方法的 ROC 曲线对比图

Fig. 11 Comparison of ROC curves of different methods

不同检测方法对各窃电类型的检出率如图 12 所示。

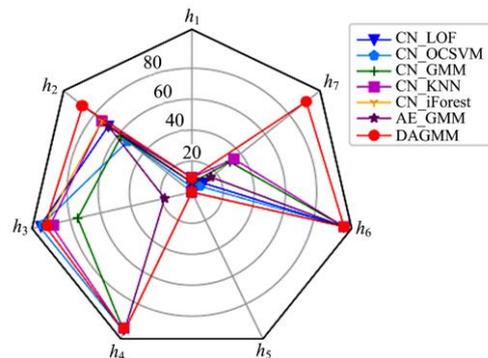


图 12 不同检测方法对各窃电类型的检出率

Fig. 12 Detection rate of different methods for each type of electric theft

由图 12 可知,各方法均能检出  $h_2$ 、 $h_3$ 、 $h_4$  和  $h_6$  四类窃电,而相比于现有方法,本文方法检测  $h_7$  时,性能远优于其他现有方法,可更准确实现窃电行为识别。

## 4 结论

本文针对用户侧窃电检测背景下因模型解耦导致的无监督方法适用性低的问题,提出了一种基于深度自编码器高斯混合模型的窃电行为检测方法。仿真与实验结果表明:利用自编码器和重构误差单元提取用户用电特征,减少了数据冗余性并偏向拟合正常用户用电习惯,有效获取了区分正常和窃电用户的行为特征;利用高斯混合模型进行异常检测,

对出现概率低的窃电用户可有效识别; 基于端对端的模型学习方式, 对特征提取与异常检测模型参数的联合优化克服了解耦问题, 提高了模型检测准确度; 同时采用箱线图设定窃电检测阈值, 提高了模型检测精度; 相比于现有检测方法, 本文所提方法受窃电样本影响小, 具有更高的检测准确率, 对窃电用户可准确识别, 为用户侧窃电行为准确检测与分析提供了全新有效的解决方案。

## 参考文献

- [1] LEON C, BISCARRI F, MONEDERO I, et al. Variability and trend-based generalized rule induction model to NTL detection in power companies[J]. *IEEE Transactions on Power Systems*, 2011, 26(4): 1798-1807.
- [2] 余斌, 孟庆强, 周卫华, 等. 大型电池储能电站系统运行控制策略研究[J]. *供用电*, 2021, 38(3): 78-83.  
YU Bin, MENG Qingqiang, ZHOU Weihua, et al. Study on operation control strategy of large battery energy storage power station system[J]. *Distribution & Utilization*, 2021, 38(3): 78-83.
- [3] PUNMIYA R, CHOE S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing[J]. *IEEE Transactions on Smart Grid*, 2019, 10(2): 2326-2329.
- [4] GUERRERO J I, MONEDERO I, BISCARRI F, et al. Non-technical losses reduction by improving the inspections accuracy in a power utility[J]. *IEEE Transactions on Power Systems*, 2017, 33(2): 1209-1218.
- [5] 招景明, 唐捷, 潘峰, 等. 基于 SDAE 和双模型联合训练的低压用户窃电检测方法[J]. *电测与仪表*, 2021, 58(12): 161-168.  
ZHAO Jingming, TANG Jie, PAN Feng, et al. Detection method of electricity theft for low-voltage users based on SDAE and double-model joint training[J]. *Electrical Measurement & Instrumentation*, 2021, 58(12): 161-168.
- [6] 陈启鑫, 郑可迪, 康重庆, 等. 异常用电的检测方法: 评述与展望[J]. *电力系统自动化*, 2018, 42(17): 189-199.  
CHEN Qixin, ZHENG Kedi, KANG Chongqing, et al. Detection methods of abnormal electricity use: review and prospect[J]. *Automation of Electric Power Systems*, 2018, 42(17): 189-199.
- [7] 程超, 张汉敬, 景志敏, 等. 基于离群点算法和用电信息采集系统的反窃电研究[J]. *电力系统保护与控制*, 2015, 43(17): 69-74.  
CHENG Chao, ZHANG Hanjing, JING Zhimin, et al. Study on the anti-electricity stealing based on outlier algorithm and the electricity information acquisition system[J]. *Power System Protection and Control*, 2015, 43(17): 69-74.
- [8] 李欣悦, 李凤婷, 尹纯亚, 等. 直流双极闭锁故障下送端系统暂态过电压计算方法[J]. *电力系统保护与控制*, 2021, 49(1): 1-8.  
LI Xinyue, LI Fengting, YIN Chunya, et al. Transient overvoltage calculation method of HVDC sending-end system under DC bipolar blocking[J]. *Power System Protection and Control*, 2021, 49(1): 1-8.
- [9] ASHA K S, JAYA L A. Data mining for classification of power quality problems using WEKA and the effect of attributes on classification accuracy[J]. *Protection and Control of Modern Power Systems*, 2018, 3(3): 303-314.
- [10] 孙立明, 杨博. 蓄电池/超导混合储能系统非线性鲁棒分数阶控制[J]. *电力系统保护与控制*, 2020, 48(22): 76-83.  
SUN Liming, YANG Bo. Nonlinear robust fractional-order control of battery/ SMES hybrid energy storage systems[J]. *Power System Protection and Control*, 2020, 48(22): 76-83.
- [11] 游文霞, 申坤, 杨楠, 等. 基于 AdaBoost 集成学习的窃电检测研究[J]. *电力系统保护与控制*, 2020, 48(19): 151-159.  
YOU Wenxia, SHEN Kun, YANG Nan, et al. Research on electricity theft detection based on AdaBoost ensemble learning[J]. *Power System Protection and Control*, 2020, 48(19): 151-159.
- [12] SUN Q, SHI L, NI Y, et al. An enhanced cascading failure model integrating data mining technique[J]. *Protection and Control of Modern Power Systems*, 2017, 2(1): 19-28.
- [13] JINDAL A, DUA A, KAUR K, et al. Decision tree and SVM-based data analytics for theft detection in smart grid[J]. *IEEE Transactions on Industrial Informatics*, 2016, 12(3): 1005-1016.
- [14] 康宁宁, 李川, 曾虎, 等. 采用 FCM 聚类与改进 SVR 模型的窃电行为检测[J]. *电子测量与仪器学报*, 2017, 31(12): 2023-2029.  
KANG Ningning, LI Chuan, ZENG Hu, et al. Using FCM clustering and improved SVR model to detect electric theft behavior[J]. *Journal of Electronic Measurement and Instrumentation*, 2017, 31(12): 2023-2029.
- [15] 庄池杰, 张斌, 胡军, 等. 基于无监督学习的电力用户异常用电模式检测[J]. *中国电机工程学报*, 2016, 36(2): 379-387.  
ZHUANG Chijie, ZHANG Bin, HU Jun, et al. Abnormal power consumption pattern detection of power users

- based on unsupervised learning[J]. Proceedings of the CSEE, 2016, 36(2): 379-387.
- [16] 王桂兰, 周国亮, 赵洪山, 等. 大规模用电数据流的快速聚类 and 异常检测技术[J]. 电力系统自动化, 2016, 40(24): 27-33.  
WANG Guilian, ZHOU Guoliang, ZHAO Hongshan, et al. Fast clustering and anomaly detection of large-scale electricity data stream[J]. Automation of Electric Power Systems, 2016, 40(24): 27-33.
- [17] 洪刚, 朱庆波, 楼越焕. 基于密度峰值估计的用电异常检测算法[C] // 2017 智能电网发展研讨会论文集, 2017 年 7 月 25 日, 中国, 北京: 565-571.  
HONG Gang, ZHU Qingbo, LOU Yuehuan. Electricity anomaly detection algorithm based on density peak estimation[C] // 2017 Smart Grid Development Symposium Proceedings, July 25, 2017, Beijing, China: 565-571.
- [18] ZHENG K, WANG Y, CHEN Q, et al. Electricity theft detecting based on density-clustering method[C] // 2017 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia), December 4-7, 2017, Auckland, New Zealand: 1-6.
- [19] ZHENG K, CHEN Q, WANG Y, et al. A novel combined data-driven approach for electricity theft detection[J]. IEEE Transactions on Industrial Informatics, 2019, 15(3): 1809-1819.
- [20] 宋军英, 崔益伟, 李欣然, 等. 改进分段线性表示与动态时间弯曲相结合的负荷曲线聚类方法[J]. 电力系统自动化, 2021, 45(2): 89-96.  
SONG Junying, CUI Yiwei, LI Xinran, et al. Improved piecewise linear representation combined with dynamic time bending load curve clustering method[J]. Automation of Electric Power Systems, 2021, 45(2): 89-96.
- [21] 单洪明, 张军平. 实值多变量维数约简: 综述[J]. 自动化学报, 2018, 44(2): 193-215.  
SHAN Hongming, ZHANG Junping. Real-valued multivariate dimension reduction: a survey[J]. Acta Automatica Sinica, 2018, 44(2): 193-215.
- [22] 郑思达, 梁琪琳, 彭鑫霞, 等. 基于模糊聚类的异常用电行为识别研究[J]. 电测与仪表, 2020, 57(19): 40-44.  
ZHENG Sida, LIANG Qilin, PENG Xinxia, et al. Research on recognition of abnormal electricity use behavior based on fuzzy clustering[J]. Electrical Measurement & Instrumentation, 2020, 57(19): 40-44.
- [23] 孙毅, 李世豪, 崔灿, 等. 基于高斯核函数改进的电力用户用电数据离群点检测方法[J]. 电网技术, 2018, 42(5): 1595-1606.  
SUN Yi, LI Shihao, CUI Can, et al. An improved outlier detection method for power user data based on Gaussian kernel function[J]. Power System Technology, 2018, 42(5): 1595-1606.
- [24] 王毅, 丁力, 侯兴哲, 等. 基于层次分析法的加权力线窃电检测方法[J]. 科学技术与工程, 2017, 17(33): 96-103.  
WANG Yi, DING Li, HOU Xingzhe, et al. Power theft detection method based on the analytic hierarchy process[J]. Science Technology and Engineering, 2017, 17(33): 96-103.
- [25] 陈建华, 戴铁潮, 张宁, 等. 确定性合同分解中异常负荷数据的识别与修正[J]. 电力系统自动化, 2009, 33(6): 21-24, 43.  
CHEN Jianhua, DAI Tiechao, ZHANG Ning, et al. Identification and correction of abnormal load data in deterministic contract decomposition[J]. Automation of Electric Power Systems, 2009, 33(6): 21-24, 43.
- [26] 金晟, 苏盛, 薛阳, 等. 数据驱动窃电检测方法综述与低误报率研究展望[J]. 电力系统自动化, 2022, 46(1): 3-14.  
JIN Sheng, SU Sheng, XUE Yang, et al. Review of data-driven electric theft detection methods and research prospect of low false positive rate[J]. Automation of Electric Power Systems, 2022, 46(1): 3-14.
- [27] WANG Y, CHEN Q, KANG C, et al. Clustering of electricity consumption behavior dynamics toward big data applications[J]. IEEE Transactions on Smart Grid, 2016, 7(5): 2437-2447.
- [28] 冉冉, 陈硕, 刘颖, 等. 基于聚类分析的用电模式判别研究[J]. 电力大数据, 2019, 22(4): 43-49.  
RAN Ran, CHEN Shuo, LIU Ying, et al. Study on power consumption pattern discrimination based on cluster analysis[J]. Power Systems and Big Data, 2019, 22(4): 43-49.

收稿日期: 2021-12-06; 修回日期: 2022-01-19

作者简介:

刘钊瑞(1997—), 女, 硕士研究生, 主要研究方向为数据挖掘、模式识别; E-mail: Liuzr594@hnu.edu.cn

高云鹏(1978—), 男, 通信作者, 博士后, 教授, 主要研究方向为模式识别、电力系统自动化与智能信息处理等; E-mail: gfront@126.com

郭建波(1973—), 男, 硕士研究生, 高级工程师, 主要研究方向为电力大数据应用分析和人工智能等。E-mail: jianbo.guo@hxgroup.com

(编辑 许威)