窃电行为检测方法研究综述

肖 宇[1],叶 志[1],黄 瑞[1],刘谋海[1],夏 睿[2],高云鹏[2]

(1.国网湖南省电力有限公司,湖南 长沙 410004; 2.湖南大学电气与信息工程学院,湖南 长沙 410082)

摘 要:电力系统中因窃电行为对电网公司造成的非技术损失一直是电网公司迫切解决的难题。伴随电网大量部署智能电表,利用电力计量自动化系统采集的用户侧数据开展窃电行为准确检测受到研究者和电网公司的普遍关注。首先,介绍用户窃电行为基本分类情况、评价指标与现有窃电检测数据集;然后,从基于电网状态分析、机器学习、博弈论以及硬件4个方面对现有窃电行为检测方法进行全方面整理、剖析与对比,总结出各方法基本思路和优缺点;最后,对当前窃电行为检测领域研究中存在的挑战深入分析,并对未来研究工作重点进行展望。

关 键 词:非技术损失;窃电检测;电网状态;机器学习;博弈论

DOI:10.19781/j.issn.1673-9140.2023.04.001 **中图分类号**:TM715 **文章编号**:1673-9140(2023)04-0001-14

Summary of research on electricity theft behavior detection methods

XIAO Yu[1], YE Zhi[1], HUANG Rui[1], LIU Mouhai[1], XIA Rui[2], GAO Yunpeng[2]

(1.State Grid Hunan Electric Power Co.,Ltd.,Changsha 410004, China; 2. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China.)

Abstract: The non-technical losses caused by electricity theft in the power system have always been a pressing issue for power grid companies to urgently address. With the deployment of a large number of smart meters in the power grid, the use of user-side data collected by the power metering automation system to accurately detect electricity theft has attracted widespread attention from researchers and power grid companies. Firstly, the basic classification of users′ electricity stealing behavior, evaluation indicators and existing electricity theft detection data sets are introduced. Then, from the four aspects of grid state analysis, machine learning, game theory and hardware, the existing detection methods of electricity theft behavior are comprehensively sorted, analyzed and compared, and the basic ideas, advantages and disadvantages of each method are summarized. Finally, the current challenges in the field of electricity theft behavior detection are deeply analyzed, and a prospective outlook on the focus of future research work is provided.

Key words: non-technical losses; electricity theft detection; grid status; machine learning; game theory

电力资源作为中国最广泛使用的能源之一,其在社会经济发展和居民日常生计中起着举足轻重的作用,而且其安全稳定的供给与人民的生活水平和国家安全稳定息息相关[1]。早在1899年,美国爱迪生照明公司协会(AEIC)针对用户窃电行为提出了具体反窃电措施[2]。随后,基于AEIC委员会提

收稿日期:2022-07-28;修回日期:2022-10-04

基金项目:国网湖南省电力有限公司科技项目(5216AG21001T);国家自然科学基金(51777061)

通信作者:高云鹏(1978—),男,教授,博士生导师,主要从事电能计量、智能信息处理方面的研究;E-mail: gfront@126.com

出的反窃电方案，美国通用电气公司(GE)于1968年研制出I-70S，Schlumberger公司于1984年开发了J5S电能表[3]。印度于2017年研制了一款基于Arduino和Rasberry Pi的智能电表，可通过监测用户负载曲线骤降等异常数据对窃电用户进行定位[4]。而在中国，青岛鼎信通讯所研制了智能管理单元读取集中器，其采集的数据配合检测装置内置算法可以判断异常电流值、电压波动和表计开盖记录等，并通过后台系统实时监控各台区异常用电情况，为高损台区检测和窃电定位提供了重要数据支撑[5]。

中国福建省年均因人为偷电直接引起的经济损失接近1亿元[6]；2019年5月，江苏镇江警方查获特大盗电“挖”比特币案件，该团伙累计窃电价值近2 000万元[7]。而全世界范围内因偷电造成的损失接近960亿美元[8]，如美国、加拿大和英国每年因窃电造成的经济损失分别为60、1.73、1亿美元[9-10]；印度、巴西和俄罗斯每年因窃电造成的经济损失分别为60、105、51亿美元[11]。据此可知，每年因窃电造成的经济损失在发展中国家和发达国家均异常严重。因此，对窃电用户进行准确检测，对维护电力市场的正常运转，保障供电企业的经济利益具有重要的现实意义和社会价值。

传统窃电检测主要依赖于人工排查，不仅效率低下，且难以精准定位到台区下的窃电用户[12]。同时，物理手段仍然无法应对网络攻击等高级手段对电表实施的人为干预。伴随智能电表在电网中大面积展开，高级量测体系(advanced metering infrastructure，AMI)已在智能电网中日趋成熟。AMI简化架构如图1所示。

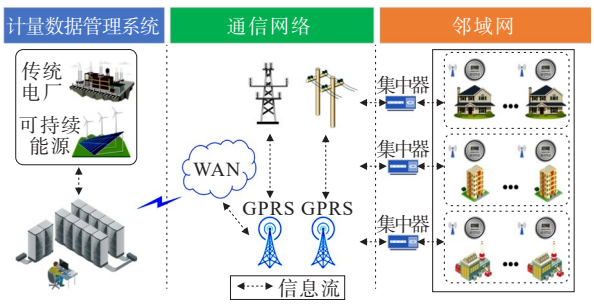

图1 AMI简化结构

Figure 1 Simplified architecture of AMI

高级量测体系支持双向通信仪表以更高的频率读取耗电量，可实时处理并发送信号以管理需求，其为智能电网不可或缺的重要一环，也是实现网络双向通信，提高资源配置和保障信息安全的重要支撑。AMI通常由通信网络、智能电表、集中器和计量数据管理系统构成。在AMI下，涌现了许多基于机器学习算法的窃电用户检测方法，通过建立机器学习模型分析用户的历史用电数据信息，挖掘隐含的用电行为模式。据某电网公司的实际测试结果显示，经过布置智能电表的配电区域其窃电检测率较之前明显提升[13]。因此，从供电公司角度，不仅需提高智能电表本身抗物理攻击的性能，还应进一步基于现有电力计量自动化系统建立窃电检测体系，充分利用AMI提供的数据构建台区窃电用户检测模型，分析用户用电数据信息，有效检测窃电用户，以保障电网利益和电力系统的安全稳定运行。

本文内容框架如图2所示，首先结合电表接线方式介绍不同窃电手段的实现方式和物理意义，并详细描述检测方法的评价指标和各研究成果所采

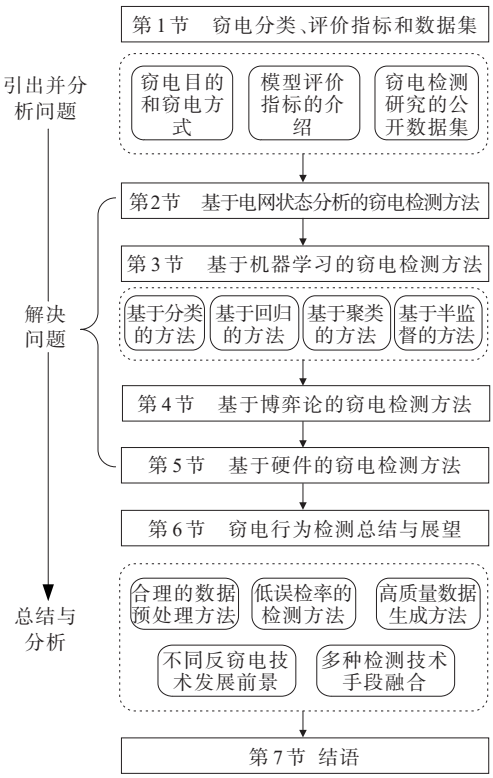

图2 本文内容框架

Figure 2 Article content structure

用的数据集;然后分别从基于电网状态分析、机器学习、博弈论和硬件4个方面详细对现有窃电行为检测方法进行全面整理、分析与对比,总结各方法基本思路和优缺点;最后对当前窃电行为检测研究领域中存在的挑战和问题进行深入分析和总结,并对未来研究工作重点进行展望。

1　窃电分类、评价指标和数据集

当窃电检测完成对用户的分类后,还需要对检测方法的准确性进行评估,以此衡量各方法的优劣,因此需对模型评价指标进行介绍。最后,对各检测方法中采用的数据集扼要罗列,此为实施用窃电行为检测的必要组成部分。

1.1　窃电分类

根据电路基础,电能表计量的功率计算公式[14]为

$$P = UI\cos\varphi \tag{1}$$

式中,U为电压值;I为流入电能表的电流值;$\cos\varphi$为功率因数。

窃电用户意图减少原本应支付的电费,从而获取不法利益,而其只需更改电压、电流以及功率因数三者中的至少一个变量,就能使电能表少计甚至不计量,从而实现窃电。设在一个时间段t内,经修改后电表测量的用户用电量为x_t,对应该时刻单位电价为p_t,而用户实际的用电量为x_t^*,计及某时间段内的电费,T为该计价时段集合,则有

$$\sum_{t\in T} p_t x_t \leqslant \sum_{t\in T} p_t x_t^* \tag{2}$$

即篡改后的电费较原来更低。根据窃电用户的具体行为,通常将窃电方式分为8类:欠压法、欠流法、移相法、扩差法、无表法、反向电流法、强磁窃电法和改变电能表机械参数窃电法,如图3所示。

1) 欠压法窃电通常指窃电用户通过各类手段更改线路、接线盒和表计端子等,从而使电能表的电压输入回路失压或计量电压减少,进而减少电能计量[15];

2) 欠流法窃电通常指窃电用户通过各类方法更改线路、接线盒和表计端子等,使电能表的电流计量回路失流,进而缩小计量负荷;

3) 移相法窃电通常指窃电用户通过不同方法使得电能表接线方式错误或增加窃电装置,改变计量表计的电压和电流相位关系,致使电能表错误计量用户实际的电量;

4) 扩差法窃电通常指窃电用户通过私拆电表等各类方法致使表计结构性能变化,导致电能表自身误差增大;

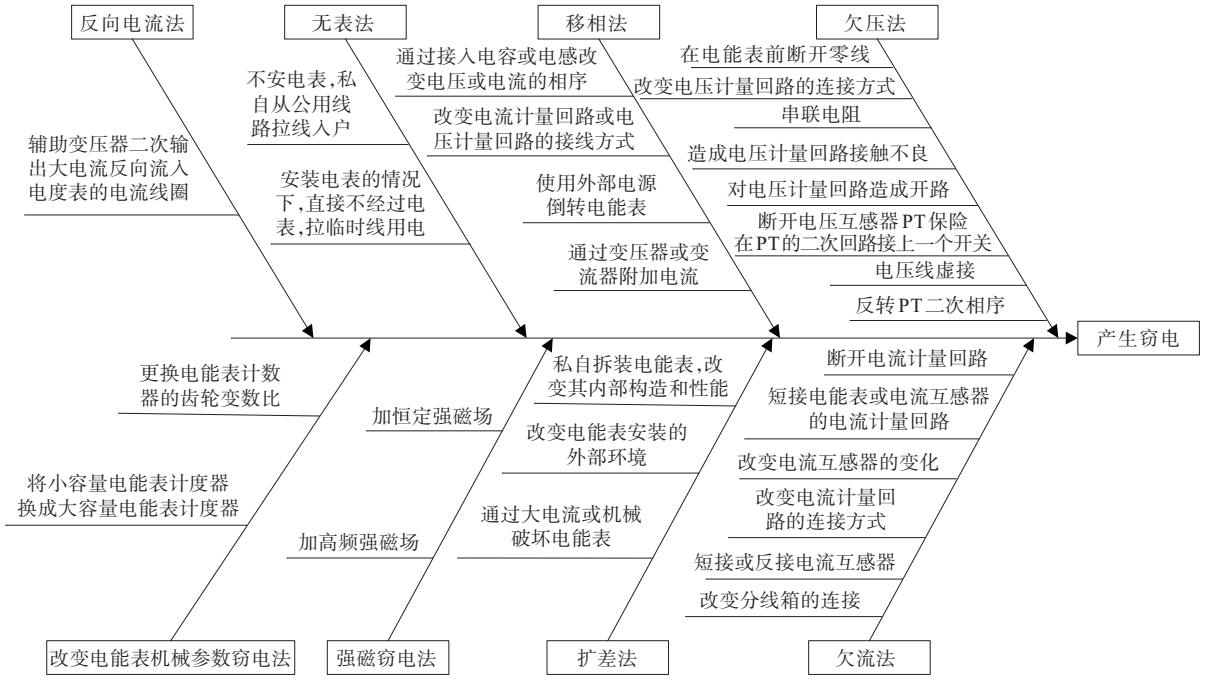

图3　8种窃电方法鱼骨图

Figure 3　Fishbone diagram of the eight ways of electricity theft

5）无表法窃电是指窃电用户没有通过正常的安装电表入户手续，擅自从公用线路拉线入户的非法行为，或用户在安装了电表的情况下，私拉临时线用电且直接不经过电表，使得该部分电量无法经电能表计量[16]；

6）反向电流法指的是窃电用户用辅助变压器二次输出大电流反向流入电度表的电流线圈，从式(1)可知，当电流反向时$P'=-UI\cos\theta$，电能表则反转；

7）强磁窃电法是通过外加强磁场强行干扰电表的磁场，影响电能表内部的变压器正常工作，进而达到窃电目的[17]；

8）改变电能表机械参数窃电法通常是通过更换电能表计数器的齿轮变数比，使电能表的计量负荷成倍缩减。

1.2 评价指标

窃电行为检测本质上为二元分类问题，当算法完成对用户的分类后，需对检测方法进行准确性评估，通常采用混淆矩阵作为依据，如表1所示。

表1 窃电行为检测中的混淆矩阵

Table 1 Confusion matrix in the detection of electricity theft behavior

用户	检测为窃电	检测为正常
实际窃电	T_P(true positive)	F_N(false negative)
实际正常	F_P(false positive)	T_N(true negative)

根据表1的混淆矩阵，定义准确率(accuracy，ACC)和召回率(recall)以及F_1值为

$$A_{CC}=\frac{T_P+T_N}{T_P+T_N+F_P+F_N} \tag{3}$$

$$R_{ec}=\frac{T_P}{T_P+F_N} \tag{4}$$

$$F_1=\frac{2T_P}{2T_P+F_N+F_P} \tag{5}$$

在机器学习领域，接收者操作特征曲线(receiver operating characteristic curve，ROC曲线)用于表示混淆矩阵中伪阳性率(false positive rate，FPR)和真阳性率(true positive rate，TPR)增长率间的相对关系，由表1的混淆矩阵可以得出$T_{PR}=T_P/(T_P+F_N)$、$F_{PR}=F_P/(T_N+F_P)$，FPR描述的是错误归类为正样本的负面事件数量与实际负面事件总数之间的比率，TPR描述的是实际为正样本判断也为正样本的比例。Precision表示当前划分到正样本类别中被正确分类的比例，其计算式为

$$P_{re}=T_P/(T_P+F_P) \tag{6}$$

贝叶斯检出率(bayesian detection rate，BDR)为评价窃电行为的重要指标，BDR是对FPR和TPR的调和，其综合考虑窃电发生概率及窃电稽查成本，计算式为

$$B_{DR}=\frac{P(I)\cdot T_{PR}}{P(I)\cdot T_{PR}+(1-P(I))\cdot F_{PR}} \tag{7}$$

式中，$P(I)$为窃电发生概率。

ROC曲线下面积(area under curve，AUC)是机器学习领域的一种模型评价指标。对于比较各分类器的分类性能，AUC值越大越好，当AUC为1时为理想分类器。AUC的计算式为

$$A_{UC}=\frac{\sum_{i\in 正例}R_{ank_i}-\frac{M(1+M)}{2}}{M\cdot N} \tag{8}$$

式中，R_{ank_i}为第i个样本的排序值；M为正样本的个数；N为负样本的个数。

平均精度均值(mean average precision，MAP)在机器学习领域常用于评估模型检测性能。MAP@N定义为在前N个嫌疑度最高的用户中，检测模型正确识别为窃电用户的平均精度均值，即

$$M_{AP}@N=\frac{\sum_{i=1}^{r}P@k_i}{r} \tag{9}$$

其中，r表示前N个嫌疑度最高的用户中窃电用户的数量，$P@k_i$定义为

$$P@k_i=Y_{ki}/k_i \tag{10}$$

其中，Y_{ki}表示前k个嫌疑度最高的用户中正确识别窃电用户的数量，$k_i(i=1,2,\cdots,r)$表示k的位置。

1.3 窃电检测中使用的数据集

当前，窃电检测领域研究受制于各研究机构或电网企业，无法提供开放的包含窃电用户和正常用户用电行为数据集。文献[18-23]使用某单位提供的未公开数据集，文献[24-25]利用公开的智能电表数据集和通过某种方式自我定义的窃电函数，产生包含窃电用户用电行为的某种数据集，通过8种篡改公式针对正常数据集进行篡改，以模拟窃电行为[26]，如表1所示，其中，$\tilde{x}_t$为窃电后实际计量电量；x_t为正常用电量；$\bar{X}$为用电量均值。其他高质量数

据集包括:爱尔兰智能电表数据集[27]、伦敦低碳项目数据集[28]、澳大利亚居民负荷数据集[29]、中国国家电网(state grid corporation of China,SGCC)公开数据集[30]和美国国家能源局EERE数据库[31]。

表 2　8种篡改模式

Table 2　Eight types of tampering modes

攻击类型	攻击方式
1	$\tilde{x}_t=\alpha x_t, 0.2<\alpha<0.8$
2	$\tilde{x}_t=\alpha_t x_t, 0.2<\alpha_t<0.8$
3	$\tilde{x}_t=\beta x_t, \beta=\begin{cases}1, 若 t_1<t<t_2\\0, \quad 其他情况\end{cases}$
4	$\tilde{x}_t=\alpha_t \bar{X}, 0.2<\alpha_t<0.8$
5	$\tilde{x}_t=\bar{X}$
6	$\tilde{x}_t=x_{48-t}$
7	$\tilde{x}_t=f(t)x_t, 其中\begin{cases}0<f(t)<1, 若 t_1<t<t_2\\f(t)=1, \quad 其他情况\end{cases}$
8	$\tilde{x}_t=0_t$, 全时段持续为零电量

2　基于电网状态分析的窃电检测方法

在基于电网状态分析的研究中,状态估计为首选的检测方法。通过计算电力用户数据中的异常和错误,或分析配电网中的功率平衡来判断是否存在异常[32]。除智能电表所记录的数据外,现有研究还引入传感器等作为辅助设备以获取配电网中的其他电气参数[33]。文献[13]提出基于状态估计的电力变压器负载估计方法,其根据注入在馈线中的伪量测值和估计值的拟合程度判断用电是否异常,其次使用方差分析列出可疑的窃电用户;文献[34]提出了基于卡尔曼滤波和紧耦合滤波器的窃电用户检测方法,通过估算线电流与量测值的偏差判定用户是否为窃电用户;文献[35]提出了一种基于多元控制图的异常用电检测方法,通过实时比较电压和电流量测值,结合状态估计方法计算的数值判断可疑区域,其次使用A-Star算法缩小可疑区域,并重复上述步骤直至找到窃电用户;文献[36]提出使用电力用户的有功和无功功率的归一化残差来检测和定位配电网中的异常用电。

引入信号处理技术进行分析。Krishna等在文献[37-39]中分别基于主成分分析、Kullback-Leibler散度和差分自回归移动平均法进行异常用电数据分析,并在不同数据集下分别验证各方法的准确性和有效性。

3　基于机器学习的窃电检测方法

随着机器学习和大数据技术的发展,涌现了许多利用机器学习算法对用户用电数据信息进行分析,以判断用户异常用电情况。本文将研究基于数据驱动方法分为基于分类方法、回归方法及聚类的方法。基于分类和回归方法属于有监督学习(supervised learning)的方法,而基于聚类则属于无监督学习(unsupervised learning)的方法。尽管上述方法的思路和理论具有较大差异,但它们都依据窃电用户的行为模式与正常用户用电模型存在不同,此外,对于半监督学习方法,其非常适用于解决实际电网情况下窃电标签难以获取的难题。

3.1　基于分类的方法

基于分类的方法根据输入的(x,y)示例中学习统计规律,进而对于新的x得出对应的y。针对窃电检测,根据用户的特征量将正常和异常用户从用户集辨别出来是分类的目标。一般地,基于分类的方法需提供大量含正、负样本标签数据,通过不断的学习训练更新模型参数,以获得最优的训练模型,从而对用户进行分类。基于分类用电异常的检测流程如图4所示。

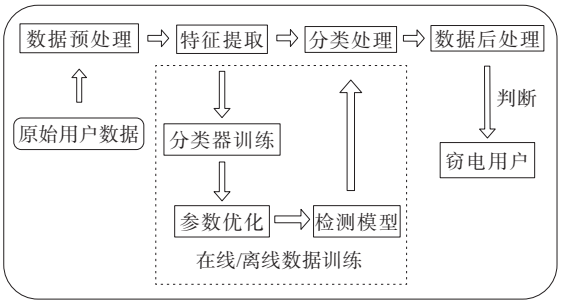

图 4　基于分类方法的窃电检测流程

Figure 4　Electricity theft detection process based on classification method

该流程的主要思想是基于正常和异常测试数据集,将异常的用电模式与所有用电模式区分开。在基于分类的方法中,当前最常使用的算法包括支持向量机和人工神经网络等。文献[40-41]提出了

一种基于支持向量机的非技术性损失检测方法，将用户负载曲线等信息作为输入判断用户嫌疑程度，该方法帮助马来西亚Tenaga Nasional Berhad公司的检测率从3%提升至60%；文献[42]提出了一种基于自组织映射神经网络和分类回归树的非技术性损失检测框架，除用电量外，作者还使用地理位置、合同电量和经济活动等信息作为特征进行判断，帮助西班牙能源公司Endesa将检测成功率从5%提升到14.75%；文献[43]使用决策树预测用户用电量，配合家庭户数、地区温度和季节等特征输入到SVM进行训练，在检测美国能源公司所有TMY3住宅的用电量数据中准确率和误检率分别达到92.50%和5.12%；文献[44]提出一种混合模型检测窃电用户，使用卷积神经网络提取特征，并将所提取特征输入至随机森林进行分类；文献[45]分别使用XGBoost、CatBoost和LightGBM测试在ISET数据集中的性能，结果显示梯度提升模型要优于文献[24]中基于SVM的窃电检测系统；文献[46]对比了SVM、XGBoost、线性回归和K-NN算法在检测窃电用户数据的性能，结果显示XGBoost要优于其他3个算法；文献[47]采用支持向量机针对电网中的非技术性损失进行检测；为解决传统窃电检测模型中单一分类方法的局限，文献[48-49]分别提出了基于AdaBoost集成学习方法和基于Bagging异质集成学习方法对窃电行为进行检测，2种集成学习方法均在爱尔兰智能电表数据集下完成验证。

针对网络攻击侵入智能电网进行窃电，文献[50]通过网络攻击领域的智能电表数据，定义了2个层次的数据偏差，以此提出隐蔽的窃电检测策略，在改进深度学习方法下实现有效检测。文献[35]提出一种利用多元控制图来检测用户窃电的策略，该控制图建立了一个可靠的区域来监测测量方差，在检测到窃电损失后，基于a-star算法的寻路过程可以定位到具有非技术损失的消耗点，此外，地理信息系统应用程序还可显示网络攻击目标。

为检测比特币挖矿用户的海量窃电问题，文献[51]基于功率数据分析技术研究窃电行为，利用用电数据采集系统对用户的电压、功率等数据对用电量行为进行监控，并分析计算各用户用电量与电站线损统计之间的Pearson相关系数，通过现场稽查证明该方法的准确性；文献[52]提出一种基于网络流量的挖矿行为检测识别模型，该模型通过对Stratum、Getwork等矿池协议的指令特征提取分析，可实现对挖矿行为的自动检测识别，并由此可检测用电异常，为现场排查疑似窃电提供依据。

工程上应用同期线损系统进行窃电检测是当下较为普及的方法，文献[53]利用线损变化率和三相电压及电流不平衡率作为输入，并基于BP神经网络对窃电用户进行检测；文献[54]建立台区窃电用户用电量与线损电量间的关系，通过高损台区实际数据，提出基于边缘计算的窃电检测方法；文献[55]利用格兰杰归因分析对高损台区进行窃电检测，均取得较高的检测准确率。

3.2 基于回归的方法

回归分析是另一类监督学习方法，通过统计学分析方法，拟合因变量和自变量的关系进而对因变量未来的变化趋势做出预测。窃电检测中回归分析常用于短期负荷预测，通过预测负荷和实际负荷曲线之间的偏差判定用户用电情况是否异常。

文献[42]提出了一个框架：第1个模块基于文本挖掘和互补人工神经网络的客户筛选；第2个模块是通过数据挖掘过程开发的，包含一个分类和回归树以及一个自组织映射神经网络，使用这些模块，检测的成功率将是原来的3倍，在西班牙Endesa电力公司的实际应用中得到了非常好的效果。文献[56]开发了基于物理的用于窃电检测数据驱动算法；文献[57]提出了一种异常数据检测模型，利用支持向量回归法对负荷进行预测，再根据电网潮流计算网络负荷，对比支持向量回归预测值和潮流计算值的偏差，将偏差较大的情况认定为异常情况。

3.3 基于聚类的方法

基于无监督学习的模型，根据样本的相似属性将其划分为不同的组别和子集。聚类是典型的无监督学习方法，进一步又可分为基于密度、划分、层次和网格的聚类等，窃电行为检测领域主要采用基

于密度和划分的聚类方法。基于划分的聚类方法原理是根据样本点的特性和数据相似性划分为不同的类别。通常基于点与点之间的距离进行衡量,即相同类别的样本点尽可能近,而不同类别间的样本点尽可能远,其中最常使用的算法为k-means聚类方法。基于密度的聚类方法特点是根据样本点的密度将稀疏的样本点进行分割。文献[58]为准确检测窃电用户而提出一种基于深度学习的检测方法,该方法克服了难以从大量高维数据提取数据特征的缺点,基于TensorFlow架构建立了特征提取模块和多层特征匹配网络;文献[59]、[60]分别采用基于实值深度置信网络的用户侧窃电行为检测模型和基于堆叠去相关自编码器和支持向量机的检修模型,均能实现有效的异常检测。

文献[61]提出在高斯核函数上改进的样本数据离群点检测方法;文献[62]提出了一种基于相关性分析的窃电用户检测方法,通过分析集中器数据和单个用户用电量数据的相关性,判断用户的窃电嫌疑程度;文献[63]结合最大互信息系数和基于密度聚类的算法,提出一种基于数据驱动的窃电用户检测方法;文献[64]利用向量自回归模型对高损台区进行窃电检测,该方法的假设前提是窃电用户用电量与线损存在正相关关系,并通过实际数据验证了方法的准确率。

基于无监督学习的模型并不依赖于通过带标签样本训练分类器,而是根据样本的潜在属性进行划分,对于尚处于初期未构建窃电数据集时的区域检测更符合要求。

3.4　基于半监督学习的方法

在窃电用户检测领域,无标签的用户数据较容易获取,而有标签的用户数据需要电网工作人员现场稽查,经济成本高,收集起来通常非常困难。因此,半监督学习可有效地用于窃电用户检测中,该方法只需少量有标签样本和大量无标签样本。半监督学习的思想是先利用少量有标签数据集训练出一个初始学习器,再使用该学习器对大量未标记的样本进行检测,从检测结果中筛选出分类置信度高的样本,将其加入训练集中再次进行训练,直至将所有样本划分至最优类别。

文献[65]最先提出将半监督学习用于非技术损失的检测中,分析了一种基于半监督的窃电用户检测方法的性能,该方法从一组有标签的数据开始,将标签扩展到无标签的数据,然后检测新的窃电,验证了半监督学习的可行性;文献[66]提出一种基于深度学习的半监督自动编码器的非技术性损失检测模型;文献[67]为了处理高维输入用户负荷数据并从中提取出有效特征,使用半监督的训练方式进行模型的训练,有效利用有标签和没有标签的数据中包含的知识信息,降低了建立模型的数据需求;文献[68]为解决传统NTL问题中输入数据维度高并且数据不平衡的问题,提出使用相关去噪自编码器和注意力引导的三项对抗生成网络;文献[69]提出一种半监督学习的窃电检测方法,利用隐马尔可夫模型,通过迭代学习方法建立隐马尔可夫拓扑结构的窃电检测模型。

4　基于博弈论的窃电检测方法

基于博弈论的研究假设窃电用户的决策为最大化非法利润的同时尽可能降低被检测的概率,供电企业的决策为最大限度降低检测窃电用户所付出的成本。文献[70]将窃电用户检测问题描述为供电企业和窃电用户之间的博弈,作者由窃电用户组成的独立集合建立了与供电企业之间的非零和Stackelberg博弈,并建立了相应的纳什均衡模型;文献[71]针对供电企业和窃电用户之间的对抗本质建立了博弈论框架,模型考虑了存在窃电用户情况下供电企业的电费定价和稽查力度;文献[72]根据智能家居能源调度对电力市场的影响,提出使用博弈论解决新型智能家居环境下的电力市场模型构建问题;文献[73]运用基于Benford's law建立的Stackelberg博弈论模型,分析最优窃电检测策略。该类研究采用经济学模型分析窃电治理的效益,注重分析供电企业和用户存在窃电时的决策行为建模,为窃电用户检测研究提供了新的视角;不足之处是现有研究很少讨论具体的窃电检测策略,仅提供似然比验证的模型。基于博弈论的研究依然处于理论推演和仿真实验上,目前无法提供实际验证。

5 基于硬件的窃电检测方法

基于硬件的解决方案分为3个子类:反窃电装置研发、邻域网窃电用户搜索算法和窃电检测装置的部署策略。针对反窃电装置的研发,包括新式智能电表、馈线终端装置(feeder remote terminal unit,FRTU)和远程稽查装置。文献[4]设计了一款基于Arduino和Rasberry Pi的智能电表,可通过发现用户负载曲线骤降等异常数据对窃电用户准确定位;文献[74]开发了一款现场窃电用户检测装置,包含一个用于测量电流的表计、一个将量测电流发送到主站的传输单元和一个用于接收主站量测结果的接收单元,装置通过比较现场的量测数据和主站量测数据的差异分析是否存在用电异常。邻域网窃电用户搜索算法的研究专注于在智能电网邻域网场景下快速检测出所有窃电用户[75]。文献[76]提出了基于二进制编码的邻域网窃电用户快速定位方法;文献[77]中提出了一种基于二叉树的邻域网窃电用户检测算法;文献[78]提出一种窃电用户自适应二分查找算法,根据要检查的用户数量在二分法和顺序查找法之间切换;文献[79]提出了一种基于分组测试的混合检测算法;针对窃电检测装置部署测试的混合检测算法,文献[80]提出一种数字保护继电器(digital protective relays,DPR)部署策略,将DPR部署在多租户数据中心,通过最小协方差行列式进行边缘计算,以检测区域内的异常用电。

基于电网状态分析、机器学习、博弈论和硬件的窃电检测方法的优缺点如表3所示。由于各类窃电检测方法参考文献繁多,而其中包含的算法和模型差异较大,因此,本文只给出各方法的整体定性对比。

表3 各窃电用户检测方法的优点和缺点

Table 3 Advantages and disadvantages of each method for electricity theft user detection

窃电检测方法		优点	缺点
基于电网状态分析		通过分析配电网中用户数据的计算值和量测值,结合网络潮流计算、系统状态等理论可以有效地定位窃电用户所在的台区	现实中难以获取完整的网络拓扑和参数信息,此外现实中电网结构和装置类型多,数据庞杂,计算难度大
基于机器学习	分类	具有更好的准确性和可靠性	模型需要带标签的样本,而在实际中这些样本往往难以获取
	回归	对窃电量小的用户识别率高	需要电价、天气等多源数据
	聚类	不需要带标签的数据集	模型的准确性和可靠性较低,同时算法复杂度高
	半监督学习	在实际电网中,难以获取大量有标签数据下,可同时利用电网中少量带标签数据和大量未带标签数据进行模型训练,模型具有较高检测准确率精度和较强泛化能力	该方法受关注程度低,缺乏有效验证,模型准确率等指标相比有监督学习方法较低
基于博弈论		从经济学的角度为供电企业稽查部门提供了决策和建议,关注供电企业和用户在存在窃电情况下双方行为决策的分析,为研究窃电检测问题提供了新思路	现实中难以获取完整的网络拓扑和参数信息,这些数据也常常是变化的。此外现实中电网结构和设备种类多、数据复杂、计算难度大
基于硬件	窃电检测装置	有效稽查台区窃电用户,为收集窃电的证据提供有效帮助	面对高科技手段窃电时常规检测装置难以发现
	邻域网窃电用户搜索算法	能够快速定位智能电网邻域网场景下的窃电用户	需要假设一种能随时切换与电能表连接的检测器,该设备仅停留在理论层面
	检测装置的部署策略	通过优化窃电检测装置在网络中的部署策略,能有效降低供电企业成本	仅能缩小范围至采集馈线,无法定位到用户

6 窃电行为检测总结与展望

通过上述的讨论和分析可知,目前窃电行为检测方法众多,虽然检测的准确度在不断提高,但在实时性、通用性以及泛化性方面离工程实际还存在一定差距,未来的研究可从如下方面展开。

6.1　合理的数据预处理方法

根据分析结果和数据特性发现,原始数据中存在一定数量的异常值和缺失值,且数据存在严重不平衡。如果对不平衡数据、异常值和缺失值不进行处理,会降低数据样本的表现力,引起参数估计的偏差,影响机器学习模型的学习分析能力,最终导致预测结果产生错误。窃电检测领域最常遇到的问题是数据不平衡,即在实际电网中窃电用户的数量远少于正常用户。如果对类别不平衡的数据不进行预处理,直接使用原始数据训练模型,模型会倾向于给样本数量较多的类别更多的权重,因此会对少数类样本产生较差的预测精度,导致属于少数类的测试数据样本被误分类为多数类,即无法检测出窃电用户。因此,对不平衡原始数据的预处理是窃电行为检测领域不可或缺的重要一环。此外,由于智能电表等装置或用电信息采集系统的故障,电表采集回来的数据不可避免的会存在异常值和缺失值,甚至于有可能出现大量连续的缺失值情况,根据具体情况研究数据补齐方法,能有效降低包含缺失值数据集带来的不确定性影响,提高模型预测的准确性。针对窃电行为的特点,选取最优的模型后还需保证算法的实时性和准确度,以供供电企业在线检测,并及时给稽查人员提供可靠位置和依据。为降低模型整体运算时间,通常会采用最大期望算法、随机梯度下降法等最优化或变量估计算法;针对深度学习的检测方法,通常会选择采用自适应注意力机制对模型进行优化以提高模型的检测效率,降低模型训练时间,为在线稽查提供时间保障。

6.2　低误检率的检测方法

目前,大多数用电异常诊断的研究采用正确率衡量用电异常分类器的性能。然而,用来评估模型性能的数据集往往是极端不平衡的,而在不均衡样本中以准确率高为目标进行异常检测,本身就是一种误导。一般认为电力用户中用电异常用户占比不高,是典型的不平衡样本。当用电异常用户占比为 1% 时,用电异常诊断只需要将所有样本判定为正,检测准确率就可达 99%,但此指标实际上不具备参考价值。实际上,采用检出率和误检率 2 个指标最能反映用电异常诊断器的性能。

从供电企业角度来看,杜绝用电异常现象并不需要查处全部用电异常用户,准确检测部分用电异常用户进而震慑其他用户,同样可以达到目的。电网公司用户体量庞大,其中相当比例为用电异常用户。从实际工作出发,漏报部分用电异常用户对于开展用电稽查影响不大,但出现误报将使用电稽查失去靶向性,进而导致稽查人员放弃使用数据驱动用电异常诊断方法。综上,工程应用对于用电异常诊断的要求是可容忍一定程度的漏报率,并尽可能降低 FPR。目前,降低 FPR 可采用随机欠采样技术、基于合成少数类过采样技术以及优化分类算法的分类阈值等方法。

6.3　高质量数据生成方法

在实际电网中,窃电用户数量占全部用户的比例较小,电力计量自动化系统采集的用户侧数据集存在数据不平衡问题,这样会严重影响检测模型的准确度,尽管部分算法采用不平衡数据处理方法,但准确度有待进一步提高。另一方面,电网公司面临的主要挑战是获取有标签的数据成本极高,而实际采集到的数据包含大量未标记的数据,为此,通过某种算法生成与原始数据相似的大量高质量用户侧数据,以平衡数据达到窃电行为的准确检测是未来研究的重要思路。无论是无监督、有监督或半监督学习,生成对抗网络(generative adversarial network, GAN)提供了一个处理问题的崭新思路,即将博弈论引入至机器学习中,如图 5 所示。

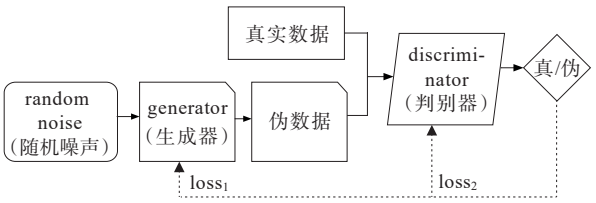

图 5　生成对抗网络结构

Figure 5　The structure diagram of GAN

该方法通过生成器生成服从真实样本分布的标记样本和与真实样本分布不同的未标记样本,其中生成的标记样本扩充了监督信息,生成的未标记样本减少了密度间隙中邻近节点的影响,从而提高检测效果。

6.4　不同反窃电技术发展前景

现有的反窃电技术主要有基于电网状态分析、

机器学习、博弈论以及硬件的异常用电检测方法。

基于电网状态分析的方法引入信号处理技术进行分析;基于机器学习的方法,因无标签数据较易获取,而有标签用户数据需人工现场稽查,经济成本高且获取困难,因此半监督学习将成为机器学习的主流方向;基于博弈论的方法注重分析供电企业和用户存在窃电时的决策行为建模,可为窃电用户检测研究提供新的视角;软硬件结合是该未来的研究方向,利用机器学习的软件优势,有效融合硬件技术,将半监督机器学习算法嵌入硬件技术中,最终实现反窃电的实时检测。

现有技术中机器学习算法嵌入硬件实现难度较大是限制该类应用的主要瓶颈。综合考虑之下,结合线损进行异常用电检测仍是工程实际主流研究方向,而利用线损的方法需以台区为载体来获取用户用电信息。事实上,因线损的计算受到线路状态的角度影响,未来台区线损的检测方式将逐渐被机器学习融合测量设备的方式所取代。

6.5 多种检测技术手段融合

智能电表数据分析是一个跨学科领域,涉及电气工程和计算机科学,尤其是机器学习。标签数据的缺乏是智能电表数据分析的主要挑战之一。如何使用迁移学习将其他对象学到的知识应用到研究窃电检测中,是未来研究的可行方向。将深度学习和迁移学习这2种新兴机器学习技术的结合在该领域具有广泛的应用价值。此外,由于智能电表数据本质上是实时流数据,在线学习和增量学习适用于处理这些实时流数据。

在实际过程中,尽管电网公司持续更新已构建的专家样本库,以此尽可能覆盖各类型窃电用户的检测,但窃电技术也朝着高科技、多场景和隐蔽性发展,这对电网公司的检测带来新的挑战,为此,需要将上述新型方法综合在一起,构建一个更为系统的异常用电行为检测框架,实现全场景下的异常用电行为检测。

7 结语

随着智能电表的普及,在AMI下,用电企业收集的海量用户用电数据信息为实现窃电用户检测研究提供了坚实的基础,为电网公司发现异常用电行为、稽查窃电用户提供有效的参考依据,提高现场检测的命中率,降低企业运营成本。本文首先介绍了窃电检测的基本原理,找出多种常见的窃电手段,并通过篡改公式,对正常用户进行窃电以模型窃电行为找出窃电规律。随后,对窃电检测领域的相关文献进行了深入的调研和分析,将窃电检测的方法归纳为基于电网状态分析、机器学习、博弈论和硬件4种类型的检测方法,并对不同方法的机理进行了阐述,从建模复杂度、数据依赖程度以及检测准确率等方面深入对比,总结了不同方法的优劣。最后,从实时性、通用性以及泛化性角度归纳当前窃电检测领域的局限,并进一步展望未来的研究工作。

随着泛在电力物联网的深入开展和电力市场化进程的加速,电力计量自动化系统的用户侧数据将更加丰富。因此,未来的工作应专注于分析电网公司海量的数据集,分析窃电检测模型的普适性,尤其是在实际情况下,考虑减少电力公司现场稽查成本,通过少量标签数据进行半监督学习方法的研究,以增加现场稽查效率,减少电网运营成本。

参考文献:

[1] 张衡,张沈习,程浩忠,等.Stackelberg博弈在电力市场中的应用研究综述[J].电工技术学报,2022,37(13):3250-3262.
ZHANG Heng,ZHANG Shenxi,CHENG Haozhong,et al.A state-of-the-art review on Stackelberg game and its applications in power market[J]. Transactions of China Electrotechnical Society,2022,37(13):3250-3262.

[2] 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 consumption behaviors: review and prospect[J]. Automation of Electric Power Systems,2018,42(17):189-199.

[3] IBRAHEM M I,MAHMOUD M M E A,ALSOLAMI F,et al. Electricity-theft detection for change-and-transmit advanced metering infrastructure[J]. IEEE Internet of Things Journal,2022,9(24):25565-25580.

[4] PATIL N V,KANASE R S,BONDAR D R,et al.Intelligent energy meter with advanced billing system and electricity

theft detection[C]// International Conference on Data Management, Analytics and Innovation (ICDMAI), Pune, India,2017.

[5] 南方+.茂名破获20年来最大团伙窃电案,案值超两百万! [EB/OL].https://www.sohu.com/a/348239613_810830, 2019-10-20.
South+.Maoming cracked the largest gang electricity theft case in 20 years, worth more than 2 million yuan![EB/OL]. https://www.sohu.com/a/348239613_810830,2019-10-20.

[6] 福建日报.全国首例智能电表高科技特大窃电案告破[EB/OL].https://news.bjx.com.cn/html/20131209/478446.shtml,2013-12-09.
Fujian Daily. The country's first intelligent meter high-tech electricity theft case was solved[EB/OL].https://news. bjx. com. cn/html/20131209/478446. shtml, 2013-12-09.

[7] 新华社.江苏破获特大盗电"挖"比特币案件案值近 2 000 万元[EB/OL].https://www.163.com/tech/article/EJSLMB6B00097U7R.html,2019-07-12.
Xinhua News Agency. The case of "digging" bitcoin in Jiangsu Province is worth nearly 20 million yuan[EB/OL]. https://www. 163. com/tech/article/EJSLMB6B00097U7R. html,2019-07-12.

[8] CUI X, LIU S, LIN Z, et al. Two-step electricity theft detection strategy considering economic return based on convolutional autoencoder and improved regression algorithm[J].IEEE Transactions on Power Systems,2022,37(3):2346-2359.

[9] NABIL M,ISMAIL M,MAHMOUD M M E A,et al.PPETD: privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks[J]. IEEE Access,2019,7:96334-96348.

[10] VIEGAS J L,ESTEVES P R,MELÍCIO R,et al.Solutions for detection of non-technical losses in the electricity grid: A review[J].Renewable and Sustainable Energy Reviews, 2017,80:1256-1268.

[11] PEREIRA J, SARAIVA F. A comparative analysis of unbalanced data handling techniques for machine learning algorithms to electricity theft detection[C]//IEEE Congress on Evolutionary Computation (CEC), Glasgow, United Kingdom,2020.

[12] HUANG S H, LO Y L, LU C N. Non-technical loss detection using state estimation and analysis of variance [J]. IEEE Transactions on Power Systems, 2013, 28(3): 2959-2966.

[13] HAN W L, XIAO Y. FNFD: a fast scheme to detect and verify non-technical loss fraud in smart grid[C]// Proceedings of the 2016 ACM International Workshop on Traffic Measurements for Cybersecurity,Xi'an,China,2016.

[14] 孔晶.配电网窃电技术与反窃电措施的研究[D].济南:山东大学,2018.
KONG Jing. Research on power stealing technology and anti-stealing measures in distribution network[D]. Jinan: Shandong University,2018.

[15] 丛干胜.低压配电用户防窃电问题及解决措施[D].济南:山东大学,2018.
CONG Gansheng. Anti-stealing power problems and solutions of low voltage distribution users[D]. Jinan: Shandong University,2018.

[16] 匡红刚,易鹏飞,邹平,等.常见窃电手段分析及反窃电装置设计[J].电工技术,2020(4):64-65.
KUANG Honggang,YI Pengfei,ZOU Ping,et al.Analysis of common electricity stealing methods and design of anti-stealing electricity device[J]. Electric Engineering, 2020(4):64-65.

[17] 徐为,霍晓艳,严璐,等.供电企业窃电方式分析及反窃电案例研究[J].自动化应用,2020(8):90-92.
XU Wei, HUO Xiaoyan, YAN Lu, et al. Analysis of electricity stealing methods of power supply companies and case study of anti-electricity stealing[J]. Automation Application,2020(8):90-92.

[18] 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. Anomaly detection for power consumption patterns based on unsupervised learning[J]. Proceedings of the CSEE, 2016, 36(2):379-387.

[19] GLAUNER P, MEIRA J A, DOLBERG L, et al. Neighborhood features help detecting non-technical losses in big data sets[C]. Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing Applications and Technologies (BDCAT),Shanghai,China, 2016.

[20] ZHENG Z, YANG Y, NIU X, et al. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids[J]. IEEE Transactions on Industrial Informatics,2018,14(4):1606-1615.

[21] YAO D, WEN M, LIANG X, et al. Energy theft detection with energy privacy preservation in the smart grid[J]. IEEE Internet of Things Journal, 2019, 6(5): 7659-7669.

[22] NIZAR A H, DONG Z Y, WANG Y. Power utility nontechnical loss analysis with extreme learning machine method[J]. IEEE Transactions on Power Systems, 2008, 23(3): 946-955.

[23] BUZAU M, TEJEDOR-AGUILERA J, CRUZ-ROMERO P, et al. Hybrid deep neural networks for detection of non-technical losses in electricity smart meters[J]. IEEE Transactions on Power Systems, 2020, 35(2): 1254-1263.

[24] JOKAR P, ARIANPOO N, LEUNG V C M. Electricity theft detection in AMI using Customers' consumption patterns [J]. IEEE Transactions on Smart Grid, 2016, 7(1): 216-226.

[25] ZANETTI M, JAMHOUR E, PELLENZ M, et al. A Tunable fraud detection system for advanced metering infrastructure using short-lived patterns[J]. IEEE Transactions on Smart Grid, 2019, 10(1): 830-840.

[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 on data-drive based electricity theft detection method and research prospect for low false positive rate[J]. Automation of Electric Power Systems, 2022, 46(1): 3-14.

[27] BUZAU M, TEJEDOR-AGUILERA J, CRUZ-ROMERO P, et al. Hybrid deep neural networks for detection of non-technical losses in electricity smart meters[J]. IEEE Transactions on Power Systems, 2020, 35(2): 1254-1263.

[28] NIZAR A H, DONG Z Y, WANG Y. Power utility nontechnical loss analysis with extreme learning machine method[J]. IEEE Transactions on Power Systems, 2008, 23(3): 946-955.

[29] ISSDA. Data from the commission for energy regulation (CER)-smart metering project[EB/OL]. http://www.ucd.ie/issda/data/commissionforenergyregulationcer, 2018-06-15.

[30] PRIYANKA M C, KUMAR M A, SHEKAR E C, et al. GSM based electricity theft identification in distribution system [J]. International Journal of Research in Engineering, Science and Management (IJRESM), 2019, 2(4): 27-29.

[31] MUJEEB S, JAVAID N, AHMED A, et al. Electricity theft detection with automatic labeling and enhanced RUSBoost classification using differential evolution and jaya algorithm[J]. IEEE Access, 2021, 9: 128521-128539.

[32] 唐秋杭, 李涛, 陈华东. 基于载波通信的电力终端数据采集检测技术研究[J]. 电网与清洁能源, 2022, 38(3): 74-79.
TANG Qiuhang, LI Tao, CHEN Huadong. Research on data acquisition and detection technology of power terminal based on carrier communication[J]. Power System and Clean Energy, 2022, 38(3): 74-79.

[33] BIN-HALABI A, NOUH A, ABOUELELA M. Remote detection and identification of illegal consumers in power grids[J]. IEEE Access, 2019, 7: 71529-71540.

[34] SALINAS S A, LI P. Privacy-preserving energy theft detection in microgrids: a state estimation approach[J]. IEEE Transactions on Power Systems, 2016, 31(2): 883-894.

[35] LEITE J B, MANTOVANI J R S. Detecting and locating non-technical losses in modern distribution networks[J]. IEEE Transactions on Smart Grid, 2018, 9(2): 1023-1032.

[36] RAGGI L, TRINDADE F, CARNELOSSI DA CUNHA V, et al. Non-technical loss identification by using data analytics and customer smart meters[J]. IEEE Transactions on Power Delivery, 2020, 35(6): 2700-2710.

[37] KRISHNA V B, WEAVER G A, SANDERS W H. PCA-based method for detecting integrity attacks on advanced metering infrastructure[J]. Quantitative Evaluation of Systems, 2015, 9259: 70-85.

[38] KRISHNA V B, GUNTER C A, SANDERS W H. Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud[J]. IEEE Journal of Selected Topics in Signal Processing, 2018, 12(4): 790-805.

[39] KRISHNA V B, LEE K, WEAVER G A, et al. F-DETA: a framework for detecting electricity theft attacks in smart grids[C]//46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, France, 2016.

[40] NAGI J, KEEM SIAH Y, SIEH KIONG T, et al. Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system[J]. IEEE Transactions on Power Delivery, 2011, 26(2): 1284-1285.

[41] NAGI J, YAP K S, TIONG S K, et al. Nontechnical loss detection for metered customers in power utility using support vector machines[J]. IEEE Transactions on Power Delivery, 2010, 25(2): 1162-1171.

[42] 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, 2018, 33(2): 1209-1218.

[43] 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.

[44] LI S,HAN Y H,YAO X,et al.Electricity theft detection in power grids with deep learning and random forests[J]. Journal of Electrical And Computer Engineering, 2019, 2019:4136874.

[45] 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.

[46] 陈钢,李德英,陈希祥.基于改进XGBoost模型的低误报率窃电检测方法[J].电力系统保护与控制,2021,49(23):178-186.
CHEN Gang,LI Deying,CHEN Xixiang.Detection method of electricity theft with low false alarm rate based on an XGBoost model[J]. Power System Protection and Control, 2021,49(23):178-186.

[47] MESSINIS G M,RIGAS A E,HATZIARGYRIOU N D.A hybrid method for non-technical loss detection in smart distribution grids[J]. IEEE Transactions on Smart Grid, 2019,10(6):6080-6091.

[48] 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 Systems Protection and Control,2020,48 (19):151-159.

[49] 游文霞,申坤,杨楠,等.基于Bagging异质集成学习的窃电检测[J].电力系统自动化,2021,45(2):105-113.
YOU Wenxia, SHEN Kun, YANG Nan, et al. Electricity theft detection based on Bagging heterogeneous ensemble learning[J].Power Systems Protection and Control,2021,45 (2):105-113.

[50] CUI L, GUO L, GAO L X, et al. A covert electricity-theft cyberattack against machine learning-based detection models[J]. IEEE Transactions on Industrial Informatics, 2022,18(11):7824-7833.

[51] KANG L Y,SHANG Y,ZHANG M X,et al.Research on monitoring technology of power stealing behavior in bitcoin mining based on analyzing electric energy data[C]// International Conference on New Energy and Power Engineering (ICNEPE),Sanya,China,2021.

[52] 史博轩,林绅文,毛洪亮.基于网络流量的挖矿行为检测识别技术研究[J].计算机应用研究,2022,39(7):1956-1960.
SHI Boxuan,LIN Shenwen,MAO Hongliang.Research on mining behavior detection and identification technology based on network traffic[J]. Application Research of Computers,2022,39(7):1956-1960.

[53] 邓鹏,刘敏.基于改进聚类和RBF神经网络的台区电网线损计算研究[J].智慧电力,2021,49(2):107-113.
DENG Peng,LIU Min.Power line loss calculation in low voltage region based on improved clustering algorithm and RBF neural network[J]. Smart Power, 2021, 49(2): 107-113.

[54] 郑应俊,杨艺宁,舒一飞,等.基于边缘计算的低压用户窃电检测[J].电力系统自动化,2022,46(11):111-120.
ZHENG Yingjun, YANG Yining, SHU Yifei, et al. Electricity theft detection for low-voltage users based on edge computing[J].Automation of Electric Power Systems, 2022,46(11):111-120.

[55] 刘永光,谭煌,李志鹏.一种基于电能表误差和窃电分析的线损分层定位方法[J].电测与仪表,2022,59(9):188-194.
LIU Yongguang, TAN Huang, LI Zhipeng. A hierarchical line loss location method based on the analysis of electricitymeter error and electricity stealing[J].Electrical Measurement & Instrumentation,2022,59(9):188-194.

[56] GAO Y, FOGGO B, YU N. A physically inspired data-driven model for electricity theft detection with smart meter data[J].IEEE Transactions on Industrial Informatics, 2019,15(9):5076-5088.

[57] DENG Y Y,ZHU K,WANG R,et al.Real-time detection of false data injection attacks based on load forecasting in smart grid[C]//IEEE International Conference on Communications,Control,and Computing Technologies for Smart Grids,Beijing,China,2019.

[58] 赵文清,沈哲吉,李刚.基于深度学习的用户异常用电模式检测[J].电力自动化设备,2018,38(9):34-38.
ZHAO Wenqing,SHEN Zheji,LI Gang.Anomaly detection for power consumption pattern based on deep learning[J]. Electric Power Automation Equipment,2018,38(9):34-38.

[59] 张承智,肖先勇,郑子萱.基于实值深度置信网络的用户侧窃电行为检测[J].电网技术,2019,43(3):1083-1091.
ZHANG Chengzhi, XIAO Xianyong, ZHENG Zixuan. Electricity Theft detection for customers in power utility based on real-valued deep belief network[J].Power System Technology,2019,43(3):1083-1091.

[60] 滕伟,黄乙珂,吴仕明,等.基于XGBoost与LSTM的风力发电机绕组温度预测[J].中国电力,2021,54(6):95-103.
TENG Wei,HUANG Yike,WU Shiming,et al.Wind turbine generator winding temperature prediction based on XGBoost and LSTM[J].Electric Power,2021,54(6):95-103.

[61] 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. Improved outlier detection method of power consumer data based on Gaussian kernel function[J]. Power System Technology, 2018,42(5):1595-1606.

[62] BISWAS P P, CAI H, ZHOU B, et al. Electricity theft pinpointing through correlation analysis of master and individual meter readings[J]. IEEE Transactions on Smart Grid,2020,11(4):3031-3042.

[63] 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.

[64] 殷涛,薛阳,杨艺宁,等.基于向量自回归模型的高损线路窃电检测[J].中国电机工程学报,2022,42(3):1015-1024.
YIN Tao, XUE Yang, YANG Yining, et al. Electricity theft detection of high-loss line with vector autoregression[J]. Proceedings of the CSEE,2022,42(3):1015-1024.

[65] TACÓN J, MELGAREJO D, RODRÍGUEZ F, et al. Semisupervised approach to non-technical losses detection [J].Springer Berlin Heidelberg,2014,8827:698-705.

[66] LU X, ZHOU Y, WANG Z, et al. Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid[J].Energies,2019,12(18):3452.

[67] HU T, GUO Q, SHEN X, et al. Utilizing Unlabeled data to detect electricity fraud in AMI: a semisupervised deep learning approach[J]. IEEE Transactions on Neural Networks and Learning Systems,2019,30(11):3287-3299.

[68] ASLAM Z, AHMED F, ALMOGREN A, et al. An attention guided semi-supervised learning mechanism to detect electricity frauds in the distribution systems[J]. IEEE Access,2020,8:221767-221782.

[69] 李和平,胡占义,吴毅红,等.基于半监督学习的行为建模与异常检测[J].软件学报,2007(3):527-537.
LI Heping, HU Zhanyi, WU Yihong, et al. Behavior modeling and abnormality detection based on semi-supervised learning method[J]. Journal of Software, 2007(3):527-537.

[70] CARDENAS A A, AMIN S, SCHWARTZ G, et al. A game theory model for electricity theft detection and privacy-aware control in AMI systems[C]//50th Annual Allerton Conference on Communication, Control, and Computing (Allerton),UIUC,Illinois,USA,2012.

[71] AMIN S, SCHWARTZ G A, CARDENAS A A, et al. Game-theoretic models of electricity theft detection in smart utility networks providing new capabilities with advanced metering infrastructure[J]. IEEE Control Systems Magazine,2015,35(1):66-81.

[72] LIU Y, HU S, HUANG H, et al. Game-theoretic market-driven smart home scheduling considering energy balancing[J].IEEE Systems Journal,2017,11(2):910-921.

[73] WEI L, SUNDARARAJAN A, SARWAT A I, et al. A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game[C]// Resilience Week (RWS),Wilmington,Delaware,USA,2017.

[74] HENRIQUES H O,BARBERO A P L,RIBEIRO R M,et al. Development of adapted ammeter for fraud detection in low-voltage installations[J].Measurement,2014,56:1-7.

[75] XIAO Z, XIAO Y, DU D H C. Exploring malicious meter inspection in neighborhood area smart grids[J]. IEEE Transactions on Smart Grid,2013,4(1):214-226.

[76] XIA X, LIANG W, XIAO Y, et al. BCGI: afast approach to detect malicious meters in neighborhood area smart grid [C]//IEEE International Conference on Communications (ICC),London,UK,2015.

[77] XIA X, LIANG W, XIAO Y, et al. A difference-comparison-based approach for malicious meter inspection in neighborhood area smart grids[C]//IEEE International Conference on Communications (ICC),London,UK,2015.

[78] XIA X, XIAO Y, LIANG W. ABSI: an adaptive binary splitting algorithm for malicious meter inspection in smart grid[J]. IEEE Transactions on Information Forensics and Security,2019,14(2):445-458.

[79] XIA X, XIAO Y, LIANG W, et al. GTHI: a heuristic algorithm to detect malicious users in smart grids[J].IEEE Transactions on Network Science and Engineering,2018,7 (2):805-816.

[80] ZHOU Y, LIU Y, HU S. Energy theft detection in multi-tenant data centers with digital protective relay deployment[J]. IEEE Transactions on Sustainable Computing,2018,3(1):16-29.