

电力自动化系统在用电检查中的 智能化反窃电技术研究

徐申未

(国网常熟市供电公司)

【摘要】电力行业发展过程中存在违规窃电行为,给国家电力系统带来经济损失。为遏制窃电行为、保障国家电网安全稳定运行,文章对电力自动化系统用电检查中的智能化反窃电技术应用展开分析。通过梳理窃电类型与特征,本文构建了融合机器学习与神经网络的智能化反窃电技术模型。依托该模型实现对窃电行为的精准分析与识别,为电力企业反窃电工作提供支撑。本文还设计了反窃电系统架构,深入剖析窃电检测数据,为反窃电技术优化提供理论支撑。

【关键词】用电检查;智能化反窃电技术;电力自动化系统

中图分类号: TM73

DOI: 10.13655/j.cnki.ibci.2025.S2.143

Research on Intelligent Anti-electricity Theft Technology in Power Automation System in Electricity Consumption Inspection

XU Shen-wei

(State Grid Changshu Power Supply Company)

【Abstract】During the development of the power industry, there exist acts of illegal electricity theft, which cause significant economic losses to the national power system. To curb illegal electricity theft and ensure the safe and stable operation of the national power grid, this paper analyzes the application of intelligent anti-electricity-theft technologies in electricity inspection of power automation systems. By sorting out the types and characteristics of electricity theft, this paper constructs an intelligent anti-electricity-theft technology model integrating machine learning and neural networks. Relying on this model, the accurate analysis and identification of electricity theft behaviors are realized, providing support for the anti-electricity-theft work of power enterprises. This paper also designs an anti-electricity-theft system architecture, conducts in-depth analysis of electricity theft detection data, and provides theoretical support for the optimization of anti-electricity-theft technologies.

【Keywords】electricity consumption inspection; intelligent anti-electricity theft technology; power automation system

1 引言

随着电力市场发展与智能电网普及,窃电问题对电力系统稳定运行的影响日益凸显。传统用电检查多以人工巡检、定期审计为核心,但随着窃电手段日趋复杂,传统方式在识别隐蔽性窃电行为上存在明显局限,给电力企业造成经济损失^[1]。

近年来,电力自动化系统与人工智能技术的协同发展,为遏制窃电行为提供了新路径。通过大数据分析、机器学习与智能监测设备的融合应用,可显著提升反窃电技术的精准性与落地性,进一步强化电网运行的安全性与经济性。

本研究围绕电力自动化系统在智能化反窃电技术中的应用展开分析,旨在构建数据驱动的窃电监测模型,提升窃电行为识别率,并对模型有效性开展验证分析。

2 窃电行为分类与特征分析

2.1 窃电行为分类

1) 物理窃电

物理窃电指直接绕过电表接入负载,如非法并联、短接电表,或拆除电表元件、改变电表计量回路,以实现非法用电目的。物理窃电操作原理虽相对直接,但窃电者手段往往隐蔽难查。此类行为既非法占用电力资源、损害电力企业经济利益,又威胁电力系统稳定运行,甚至引发安全事故,影响用户用电安全与电网设备安全^[2],因此需加强物理窃电行为的监测与预防。实际运行中,可通过智能监测设备与大数据技术及时精准识别并预警窃电行为,为电力企业提供技术支撑,保障电网安全稳定运行。

2) 计量窃电

计量窃电以破坏或篡改电能表数据为主要途

径,如通过磁场干扰、修改计量芯片参数,或安装非法设备伪造电能表计量数据,实现窃电目的^[3]。计量窃电方式隐蔽性强,难以直观识别,给监管工作带来挑战。此类行为不仅损害电力企业合法权益,还扰乱正常电力市场秩序。随着科技发展,计量窃电方式持续升级,从传统机械篡改向高科技手段演进,甚至实现远程操控窃电,进一步提升了识别难度。因此,电力自动化系统需开展智能化升级,依托自动化反窃电技术防范计量窃电行为,维护电力市场稳定与公平。

3) 控制信号窃电

控制信号窃电借助无线信号干扰、远程操控技术非法篡改电表读数,或通过黑客技术攻击电力系统、操控电表数据以实现窃电。该方式技术含量高、隐蔽性强,反窃电工作面临较大挑战。此类行为不仅损害电力企业经济利益,更威胁电网运行安全,若未能及时发现并管控,可能损坏电网设备、引发停电事故,甚至造成社会影响与经济损失^[4]。因此需加强对控制信号窃电行为的监测,电力自动化系统需优化智能化反窃电技术,依托加密通信、入侵检测系统、智能识别算法等提升电表数据准确性与安全性,遏制窃电行为;同时电力企业需加大技术研发与创新投入,提升智能化反窃电技术水平,确保适配新型窃电手段。

4) 负荷异常窃电

负荷异常窃电指用户在用电设备上私自接入额外高耗能设备,或采用绕过电表直接用电的方式窃电,导致电表无法准确计量实际用电量^[5]。此类窃电行为会引发用户负荷异常波动,表现出与正常负荷模式的显著差异。为有效检测并预防该类窃电行为,电力自动化系统需引入新型智能化技术,对用户负荷数据进行监测与分析,识别异常负荷并及时采取有效反窃电措施。

2.2 窃电行为特征提取

1) 电能计量异常

主要表现为用户计量电量与负荷模型不匹配,即用户实际用电量与负荷模型预测电量存在较大偏差。例如,某用户负荷模型显示用电量应在特定范围波动,但电表实际记录电量远低于该范围。其原因可能是用户私自篡改电表计量部件,或采用技术手段干扰电表正常工作。因此,通过对比分析用户计量电量与负荷模型的匹配度,可有效识别窃电

行为。

2) 负荷曲线异常

负荷曲线异常分为异常突变与异常平稳两类。异常突变表现为用户负荷在短时间内出现大幅波动,异常平稳则是负荷水平长时间保持稳定,与正常用电负荷曲线存在明显差异。此类异常源于用户非法调整用电设备,或通过技术手段篡改负荷数据导致负荷数据失真。通过分析用户负荷曲线的变化趋势与特征,可精准识别负荷异常类窃电行为,为电力自动化系统反窃电工作提供重要参考。

3) 电压/电流波动异常

窃电行为可能导致电流、电压波动偏离正常范围,具体特征表现为电流、电压突发性增大或骤降,波动模式异常。通过对电力系统中电流、电压进行实时监测,结合异常波动规律可判断是否存在窃电行为。例如,监测到某用户电流波动频繁且幅度大,但用电负荷无显著变化,则可能存在窃电行为。电压、电流波动特征可为电力自动化系统反窃电提供有效参考依据。

4) 功率因数异常

功率因数用于反映电网中有功功率与视在功率的比例关系,其数值与用户负载特性直接相关。窃电行为会引发功率因数异常变化,如突发性下降或偏离正常范围。功率因数与正常负载特性不匹配,可能表现为功率因数持续偏低或频繁波动,与用户实际用电负荷不匹配。对用户功率因数数据进行分析,结合用电负荷特征可识别功率因数异常,进而判断窃电行为。例如,监测到用户功率因数长时间降低,但用电负荷无显著增加,则提示可能存在窃电行为。通过功率因数异常分析,可及时发现并查处窃电行为。

5) 设备运行异常

借助SCADA系统检测功能可识别电表运行模式异常,例如电表在无故障状态下出现停转、反转或转速异常减缓,均为窃电相关的直接异常表现。此外,SCADA系统可监测电表箱门异常开启记录,若电表箱门在非维护时段频繁被开启,则可能存在非法操作行为。设备运行异常分析不仅可及时发现窃电迹象,还能为窃电行为取证提供线索。因此,结合SCADA系统的设备异常监测功能开展反窃电工作,通过智能电表、配电自动化系统及用户数据管理系统采集的数据,为后续智能监测提供支撑。

3 智能化反窃电技术模型

3.1 基于机器学习的窃电模式识别

通过构建机器学习模型实现窃电检测的分类与异常识别。假设用户正常用电数据服从特定统计分布,窃电行为数据分布偏离正常模式,因此可通过分类算法识别。设用户的用电特征向量为:

$$X = \{x_1, x_2, \dots, x_n\}$$
 (1)

式(1)中: x_i 代表某时刻用电特征数据。利用监督学习方法可构建窃电检测模型,定义窃电概率为:

$$P(Y = 1 | X) = f(X)$$
 (2)

式(2)中: Y 为二分类变量, $Y = 1$ 代表窃电, $Y = 0$ 代表正常用电行为, $f(X)$ 为分类模型的输出函数。

常用的窃电检测模型包括:①支持向量机(SVM),适用于小样本、高维数据的窃电检测;②随机森林(RF),适用于特征复杂的窃电模式识别;③长短时记忆网络(LSTM),适用于时序数据的异常检测,能够发现长期窃电行为。

3.2 基于神经网络的智能检测算法

针对大规模用户数据,采用深度学习方法可自动提取窃电特征。先利用卷积神经网络提取窃电特征,再通过LSTM对时序特征建模,构建高效的窃电识别模型。神经网络的窃电识别过程可表示为:

$$\hat{Y} = \sigma(W_2 \cdot ReLU(W_1 \cdot X + b_1) + b_2)$$
 (3)

式(3)中: W_1 、 W_2 为神经网络权重矩阵; b_1 、 b_2 为偏置项; $ReLU(x) = \max(0, x)$ 为激活函数; $\sigma(x)$ 为Sigmoid函数,用于二分类任务。

以大量历史用电数据训练模型,使其学习正常与异常用户的差异,进而提升窃电识别的准确性。

4 反窃电系统架构与数据分析

4.1 反窃电系统架构

智能化反窃电系统通常由数据采集层、数据处理层、窃电检测层、报警与响应层四个核心部分组成。其中数据采集层包括智能电表、负荷传感器、远程监测设备;数据处理层包括大数据平台,负责数据清洗、特征提取;窃电检测层包括基于机器学习和深度学习的窃电识别模型;报警与响应层包括实时告警系统,联动执法机构进行现场核查。

整个系统的工作流程如下。

数据采集:实时获取用户用电数据、环境数据

数据分析:采用机器学习模型进行窃电识别
异常告警:对于高风险用户发送告警信号
现场核查:工作人员对可疑用户进行调查

4.2 窃电检测数据分析

利用某城市电网的用户数据进行窃电检测实验,样本数据包括10000名用户的历史用电信息。实验采用SVM、随机森林和LSTM三种算法进行对比,结果如表1。

表1 三种窃电检测算法性能对比实验数据

模型	准确率(Accuracy)/%	召回率(Recall)/%	F1值/%
SVM	87.2	85.1	86.1
随机森林	91.4	89.5	90.4
LSTM	95.8	93.2	94.5

从实验结果可知,LSTM应用于窃电模型学习可提升窃电行为识别准确率,适合在大数据智能反窃电系统应用。

5 结论与展望

依托电力自动化系统数据采集能力,可对用户用电行为实时监测,为智能化反窃电提供数据支持。机器学习和深度学习方法可有效识别窃电模式,有助于提高检测的准确率。构建基于大数据分析的智能窃电检测系统,可实现窃电行为的精准识别与预警,提高电网安全性和经济效益。未来需进一步优化深度学习模型,提升复杂窃电行为识别能力。结合边缘计算技术,提升窃电监测实时性,增强数据安全性。

参考文献

[1] 杜旭昕, 林锐涛, 黄朝凯, 等. 用电检查与反窃电在线智能分析系统设计[J]. 中国科技期刊数据库 工业 A, 2021 (9): 96-97.
[2] 申苗苗, 王琛莹. 浅析用电信息采集系统在反窃电技术中的应用[J]. 电子乐园, 2021 (1): 383.
[3] 徐峰. 大数据技术在智能反窃电和线损监控中的应用[J]. 数码设计, 2023 (15): 80-82.
[4] 仲景. 大数据技术在智能反窃电和线损监控中的应用分析[J]. 光源与照明, 2022 (6): 211-213.
[5] 范文, 宋萍, 黄阳. 浅谈反窃电检查中电力营销大数据的应用[J]. 电子乐园, 2021 (5): 39.