

# 基于智能电表与大数据的电力企业反窃电策略

杜豫喆, 胡家玮, 朱军

国网江苏省电力有限公司句容市供电分公司, 江苏 镇江 212400

**摘要:** 随着窃电手段日趋智能化和隐蔽化, 传统反窃电技术面临严峻挑战。本研究基于智能电表高频数据采集与大数据分析技术, 提出了一套多层次的反窃电技术体系。通过构建毫秒级电力数据感知网络, 融合多源异构数据, 并采用深度学习和图神经网络等先进算法, 实现了对复杂窃电行为的高精度检测与快速响应。同时, 结合边缘-云协同计算和区块链存证技术, 形成了从数据采集到证据保全的完整解决方案, 为电力企业应对新型窃电威胁提供了有效的技术支撑。

**关键词:** 反窃电; 大数据分析; 深度学习

## Anti-Power Theft Strategy of Power Enterprises Based on Smart Meters and Big Data

Du Yuzhe, Hu Jiawei, Zhu Jun

State Grid Jiangsu Electric Power Co., Ltd. Zhenjiang City Power Supply Branch, Zhenjiang, Jiangsu 212400

**Abstract:** With the increasingly intelligent and hidden means of power theft, the traditional anti-power theft technology is facing severe challenges. Based on the high-frequency data collection and big data analysis technology of smart meters, this paper proposes a multi-level anti-power theft technology system. By constructing millisecond power data sensing network, integrating multi-source heterogeneous data, and using advanced algorithms such as deep learning and graph neural network, high-precision detection and rapid response to complex power theft behavior are realized. At the same time, combined with edge-cloud collaborative computing and blockchain storage technology, a complete solution from data collection to evidence preservation has been formed, which provides effective technical support for power enterprises to deal with the new threat of power theft.

**Keywords:** anti-power theft; big data analysis; deep learning

## 引言

电力资源的安全稳定供应关系到国民经济和社会发展, 然而近年来窃电行为呈现出技术化、团伙化的新趋势, 给电力企业造成了巨大经济损失。传统基于人工巡检和机械电表的反窃电手段已难以应对日益复杂的窃电技术。随着智能电表的普及和大数据技术的发展, 基于高频数据采集和智能分析的精准反窃电成为可能。本研究旨在探索智能电表与大数据技术相结合的反窃电新方法, 通过构建多层次的技术体系, 提升窃电行为识别的准确性和时效性, 为电力企业提供更加智能化的反窃电解决方案。

## 一、电力企业窃电行为现状

据相关资料显示, 近年来窃电行为呈现出智能化、隐蔽化、产业化的新趋势。例如, 一些地区利用高科技手段进行窃电, 如破解智能电表、无线干扰电表计量、远程控制窃电等, 这些手段使得窃电行为更加难以被发现。此外, 窃电行为还逐渐形成了团伙化、产业化的趋势。常见窃电手段包括居民用户端的零火线反接、强磁干扰电表运转, 工商业场景中的电容柜无功补偿参数篡改、电流互感器短接等传统方式, 以及伴随新能源普及衍生的分

布式光伏系统私接并网、储能设备违规充放电等新型技术手段。同时, 窃电导致的电费分摊失衡严重破坏市场公平。据相关研究估算, 我国每年因窃电造成的经济损失高达200亿元人民币。

## 二、反窃电技术策略

### (一) 数据采集与融合

#### 1. 高频数据实时采集

高频数据实时采集是实现反窃电精准监测的核心技术基础,

### 作者简介:

杜豫喆(1994.12.17-), 男, 民族: 汉, 籍贯: 江苏句容, 学历: 本科, 现任职称: 工程师, 研究方向: 电气工程及其自动化;

胡家玮(1994.03.06-), 男, 民族: 汉, 籍贯: 江苏句容, 学历: 本科, 现任职称: 工程师, 研究方向: 电力系统及其自动化;

朱军(1976.06.16-), 男, 民族: 汉, 籍贯: 江苏句容, 学历: 本科, 研究方向: 电力系统及其自动化。

其核心在于构建毫秒级精度的电力数据全息感知网络<sup>[1]</sup>。在通信传输层面，采用 LoRa+NB-IoT 双模异构组网技术，设计基于动态时间规整（DTW）的自适应压缩算法，实现原始波形数据的无损压缩传输。该算法通过小波包分解提取特征子带，其压缩效率可量化如式（1）：

$$\eta = 1 - \frac{\sum_{k=1}^N |W_k^c|}{\sum_{k=1}^N |W_k^o|} \quad (1)$$

其中， $\eta$  为压缩效率， $N$  为子带总数， $W_k^c$  和  $W_k^o$  分别为原始信号与压缩后信号在第  $k$  个子带的能量范数。边缘侧部署具备 FPGA 加速的数据预处理单元，运用滑动窗口机制实现实时数据流处理，在确保 <20ms 端到端时延的同时，构建包含 256 维时频域特征的特征矩阵。为应对复杂电磁环境下的信号干扰，系统集成改进型卡尔曼滤波算法，通过噪声协方差矩阵的在线估计实现动态降噪，使得信号信噪比（SNR）稳定维持在 45dB 以上。

## 2. 多源数据融合方法

多源数据融合的核心在于解决智能电表高频电气量测、电网拓扑关系、用户历史行为等多模态数据的时空对齐与特征耦合问题。从技术实现层面，需构建统一的时空基准框架：基于 GPS/北斗授时模块实现毫秒级时间同步，利用图结构编码器将电表物理位置映射为拓扑坐标，解决因配电网络动态重构导致的空间关联漂移<sup>[2]</sup>。针对电气量测数据、非电气数据及业务数据的异构性，设计分层特征提取网络，底层采用 1D CNN 提取量测数据局部时序特征，中层通过 GAT（图注意力网络）建模电表节点间的电气关联强度，顶层引入交叉注意力机制实现跨模态特征交互，其权重分配可表示如式（2）：

$$\alpha_{ij} = \frac{\exp(Q_i K_j / \sqrt{d})}{\sum_k \exp(Q_i K_k / \sqrt{d})} \quad (2)$$

其中， $\alpha_{ij}$  为注意力权重， $Q_i$  和  $K_j$  分别代表第  $i$  个模态查询向量与第  $j$  个模态键向量， $d$  为特征维度。为抑制噪声干扰，可采用信息熵加权策略动态评估数据源可靠性，熵值低于阈值的低质量数据自动降权。在计算架构上，依托边缘计算节点实现原始数据轻量化融合，仅上传融合后的高维特征至云端，降低网络带宽压力。

## （二）检测算法设计

### 1. LSTM-Transformer 时序检测

基于电力负荷时序数据的长程依赖性与突变特征耦合特性，可使用 LSTM-Transformer 混合架构，其核心在于融合局部时序特征提取与全局注意力建模能力。系统输入端采用滑动窗口机制将原始高频电流、电压序列分割为多尺度片段，通过双向 LSTM 层捕获局部负荷波动规律<sup>[3]</sup>。针对窃电行为中常见的波形畸变特征，在 LSTM 后端引入时域卷积注意力模块（TCA），通过学习卷积核生成时变权重矩阵，增强对非平稳信号的敏感度。Transformer 编码层采用改进的谱注意力机制，将传统点积注意力扩展至频域空间，定义频域注意力得分计算如式（3）：

$$A_f(Q, K) = F^{-1} \left( \frac{F(Q) \cdot F(K)^*}{\sqrt{d}} \right) \quad (3)$$

其中， $Q, K$  为查询矩阵和键矩阵， $A_f(Q, K)$  为频域注意力得分矩阵， $F$  为傅里叶变换， $d$  为特征维度。系统采用渐进式训练策略，先冻结 LSTM 层参数预训练 Transformer 编码器，再通过端到端微调实现特征表示对齐。为适配边缘设备部署需求，设计通道剪枝算法自动剔除冗余注意力头，同时保持对窃电暂态特征的毫秒级响应能力。

### 2. 图神经网络拓扑分析

配电网的物理拓扑与用户用电行为隐含的关联网络，为窃电检测提供了空间维度的特征补充。基于图神经网络（GNN）的拓扑分析通过建模电表节点间的电气耦合关系与异常传播路径，有效识别传统时序分析难以捕捉的分布式协同窃电模式<sup>[4]</sup>。图神经网络拓扑分析关键参数与性能指标如表 1 所示：

表 1：图神经网络拓扑分析关键参数与性能指标

参数 / 指标	说明	设定值 / 性能表现
节点定义	以智能电表为网络节点	每节点包含电压、电流等 12 维特征
边权重计算	基于电气距离、功率交互强度、用户行为相似度	多维度加权融合公式
聚合函数	GraphSAGE 框架下的层次化信息聚合	3 层神经网络结构
异常检测灵敏度	拓扑梯度损失函数触发的异常响应阈值	0.73（归一化值）
训练效率	在线增量训练所需时间	子图更新平均耗时 28ms

模型需支持在线增量训练，当配电网络重构时，仅需局部更新受影响子图的嵌入表示，同时可扩展至含分布式电源的主动配电网场景，为窃电行为的空间定位提供高分辨率特征基底。

### 3. 边缘-云协同机制

边缘-云协同机制通过分层计算框架实现反窃电检测的实时响应与全局优化，其核心在于动态分配模型推理、特征提取及决策生成等任务的计算负载。在边缘侧部署轻量化异常检测模型，采用量化感知训练技术将 LSTM-Transformer 时序检测模型的参数量压缩至 2MB 以内，利用 TensorRT 引擎优化实现 5ms 级单窗口推理速度。

协同调度层面设计基于强化学习的动态卸载策略，定义状态空间为边缘节点计算负载、网络带宽及云端资源利用率，动作空间为任务卸载比例及数据压缩等级，奖励函数综合考量端到端时延与检测精度，如式（4）：

$$R = \omega \cdot \frac{1}{\log(T)} + (1 - \omega) \cdot A \quad (4)$$

其中， $R$  为奖励函数， $\omega$  为时延-精度权衡系数， $T$  为端到端时延， $A$  为检测精度，通过双延迟深度确定性策略梯度（TD3）算法在线优化<sup>[5]</sup>。数据管道采用流式处理架构，边缘侧通过时间戳对齐与事件窗口管理模块实现数据块的原子化传输，云端利用 Apache Flink 进行多流关联分析，检测到疑似窃电事件时触发反向控制指令，经 MQTT 协议下发至边缘执行单元，完成电表重校或电路隔离等操作。

### (三) 动态响应策略

#### 1. 强化学习阈值调整

基于深度强化学习的动态阈值调控系统，通过构建“感知-决策-反馈”闭环，实现窃电检测灵敏度的自主优化。强化学习阈值调控系统核心架构如表2所示：

表2: 强化学习阈值调控系统核心架构

组件	关键技术	配置参数	功能优势
状态编码器	多模态特征融合 (时序+拓扑+环境)	128维压缩特征	全面感知电网状态
策略网络	边缘MLP+云端 Dueling DQN	边缘2.1MB/云端23MB	分层智能决策
双阈值机制	主阈值(检测)+辅助阈值(数据回传)	±15%动态范围	优化灵敏度与带宽平衡
奖励函数	时延-精度加权优化	$\omega=0.6$ (自适应调节)	多目标协同
抗干扰设计	TCC损失函数抑制震荡	$\lambda=0.85$ 平滑系数	阈值稳定性提升62%
验证系统	数字孪生自动验证	1.2s平均响应	降低误报率

此外，模型训练采用联邦强化学习框架，各区域电力公司的本地数据在加密空间内共享策略梯度，既保障数据隐私又提升模型泛化能力。部署阶段通过 TensorRT 加速引擎优化推理速度，在 Jetson AGX Xavier 设备上实现 8ms 级实时响应。该架构通过模块化设计支持策略组件的热插拔，可快速适配不同区域电网的差异化运行规范，为动态环境下的自适应检测提供标准化技术范式<sup>[6-8]</sup>。

#### 2. 区块链存证技术

针对反窃电业务中的电子证据可信存储需求，可设计基于联盟链的多级存证体系。该体系采用 Hyperledger Fabric 框架构建电力行业专用联盟链网络，包含计量设备层、边缘计算层和云端存证层三级节点架构。智能电表内置轻量级 TEE 可信执行环境，对异常用电数据生成带时间戳的原始哈希值，通过国密 SM2 算法签名后写入边缘节点本地账本。

存证过程采用改进的 Merkle-Patricia 树结构组织数据，将电表计量数据、检测日志和处置记录等异构信息统一编码为标准化合证单元。每个存证单元包含数据指纹、设备数字身份和电网拓扑位置三元组，通过跨链协议与省级电力监管平台实现双向锚定。关键创新在于设计了动态分片共识机制，根据业务负载自动调整 PBFT 共识组的节点数量，在保证数据不可篡改性的同时将交易吞吐量提升至 1500TPS 以上。

### 三、效果验证

通过构建多层次的仿真实验平台，研究全面验证了所提反窃电技术策略的有效性。结果如图1所示：



>图1 反窃电技术策略综合评估

在数据采集层，基于 RT-LAB 实时数字仿真系统和 4 台 4kHz 采样频率的智能电表节点，模拟了 6 类典型窃电场景。实验表明，采用 LoRa+NB-IoT 双模传输和 DTW 压缩算法后，网络带宽占用降低 62.3%，信噪比稳定在 47.2dB 以上；结合 1D CNN-GAT 分层特征提取的多源数据融合方法，使窃电检测准确率达到 93.7%，较传统方法提升 28.5%。

在算法验证层面，针对 200 户居民和 10 个工商业用户构建的配电网数字孪生模型显示：LSTM-Transformer 混合架构对波形畸变的检测响应时间为 18ms，DRR 指标超过阈值 1.8 倍；GraphSAGE 拓扑分析模块成功识别 3 个协同窃电团伙，空间定位误差小于 2 个电表节点，联合算法的 F1-score 达 89.4%，误报率降至 3.2%。

边缘-云协同机制测试中，由 5 个边缘节点和云端中心组成的测试网络实现了 4.8ms 的边缘推理时延，通过 TD3 算法优化的任务卸载策略将端到端时延控制在 56ms 以内。动态阈值系统在 30 天运行周期内，查全率从 82.1% 自主提升至 91.6%，误报次数减少 44%。

区块链存证技术验证方面，模拟 1000 次异常数据上链操作显示：动态分片 PBFT 共识机制使存证吞吐量达 1582TPS，存证单元锚定平均时延 1.4 秒，在确保数据隐私的同时完全满足监管要求<sup>[9-10]</sup>。

### 四、结论

本研究构建的基于智能电表与大数据的反窃电技术体系，通过多层次的技术创新，实现了对新型窃电行为的有效识别与防范。该体系不仅提升了窃电检测的精度和效率，还通过区块链等技术确保了电子证据的可信性，为电力企业的反窃电工作提供了新的技术路径。

### 参考文献

- [1] 许小卉, 许妙琦, 唐冬来, 等. 基于配电网的反窃电预警系统研究及应用 [J]. 计算技术与自动化, 2020, 39(2): 5.
- [2] 石忻, 福建, 永泰. 基于“互联网+”反窃电管理模式的探讨 [J]. 电气技术与经济, 2023(8): 189-191.
- [3] 许明前, 黄晓, 陈富燕. 基于大数据分析的反窃电实践 [J]. 中国电力企业管理, 2021(8): 1.
- [4] 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.
- [5] 谢连芳. 大数据架构下的用电评价与反窃电技术探讨 [J]. 集成电路与嵌入式系统, 2022, 22(2): 22-26.
- [6] 侯力媛. 大数据技术在智能反窃电和线损监控方面的应用 [J]. 当代化工研究, 2021, 000(010): P.172-173.
- [7] 邓丽娟. 基于大数据技术的反窃电分析与仿真研究 [J]. 电工材料, 2022(6): 36-41.
- [8] 王培丰. 如何利用大数据模式提高供电企业反窃电效率 [J]. 前卫, 2020(30): 154-156.
- [9] 陈晓瑜. 电力营销大数据在反窃电检查中的应用 [J]. 电子技术, 2023(11): 124-126.
- [10] 张峰. 反窃电检查中电力营销大数据的应用 [J]. 工程建设(维泽科技), 2022, 5(9): 168-170.