DOI:10.19651/j.cnki.emt.2518301

基于 CNN-BiLSTM 模型的多场景窃电检测与类型判别研究*

韦江衡[1] 韦杏秋[1] 杨 舟[1] 唐宇靖[2] 苗 强[2]
(1.广西电网有限责任公司 南宁 530022;2.四川大学电气工程学院 成都 610065)

摘 要:为了避免因窃电行为造成的安全隐患与经济损失,同时为了高效精准的找出窃电用户并且对其窃电模式准确类型判别,提出了一种基于 CNN 和 BiLSTM 相结合的窃电检测与类型判别方法。首先,采用包含 16 种用电用户类型的基于开放能源数据倡议数据集,针对六种不同的窃电模式对数据进行篡改,同时对数据进行了 Min-Max 归一化处理;接下来,模型通过卷积层提取多尺度局部特征,利用膨胀卷积进一步扩展感受野,有效捕捉环境干扰下的细微变化;随后,采用 BiLSTM 对时序数据进行正反向建模,从而全面捕捉长距离依赖关系和上下文信息。为提高模型的鲁棒性和泛化能力,本文还引入了 Dropout 和动态学习率调整机制。最后,通过在二分类、六分类和七分类任务下进行实验,对比不同训练集比例的结果,实验表明所提方法在准确率、AUC 和 F1-score 等指标上均显著优于传统方法,验证了模型在复杂场景下的检测和类型判别能力。

关键词:窃电检测;类型判别;CNN;BiLSTM
中图分类号:TN98;TP206+.3 **文献标识码**:A **国家标准学科分类代码**:510.4030

Multi-scenario electricity theft detection and type discrimination study based on a CNN-BiLSTM model

Wei Jiangheng[1] Wei Xingqiu[1] Yang Zhou[1] Tang Yujing[2] Miao Qiang[2]
(1. Guangxi Power Grid Co., Ltd., Nanning 530022, China; 2. College of Electrical Engineering, Sichuan University, Chengdu 610065, China)

Abstract: In order to mitigate the security risks and economic losses caused by electricity theft, and to efficiently and accurately identify theft users while discriminating their theft patterns, propose an electricity theft detection and type discrimination method that integrates a convolutional neural network (CNN) with a bidirectional long short-term memory (BiLSTM) network. Initially, an open energy data initiative (OEDI) dataset comprising 16 types of electricity users is employed. The dataset is modified according to six distinct theft patterns and subjected to Min-Max normalization to eliminate the influence of differing feature scales. Subsequently, the model extracts multi-scale local features via convolutional layers and further expands the receptive field using dilated convolution, thereby effectively capturing subtle variations amid environmental interference. Thereafter, BiLSTM is utilized to model the sequential data in both forward and backward directions, comprehensively capturing long-range dependencies and contextual information. To enhance the model's robustness and generalization capability, dropout and dynamic learning rate adjustment mechanisms are incorporated. Finally, experiments are conducted under binary, six-class, and seven-class classification tasks with varying training set ratios. The experimental results demonstrate that the proposed method significantly outperforms traditional approaches in terms of accuracy, AUC, and F1-score, thereby validating its effectiveness in electricity theft detection and type discrimination under complex scenarios.

Keywords: electricity theft detection; type discrimination; CNN; BiLSTM

0 引 言

自近现代以来,电能在推动社会进步与技术革新中扮演着关键角色。然而,随着电力需求不断攀升,电网在传输和分配过程中不可避免地面临各种损耗问题。通常,这些损耗可分为技术性损耗和非技术性损耗,其中后者不仅涉及计量误差,还包括人为因素引发的非法用电行为。非法用电不仅给电力企业带来巨大的经济压力[1],而且可能危

收稿日期:2025-03-10
*基金项目:四川省科技计划项目(2025YFHZ0157)资助

及电网的安全稳定运行[2]。因此,如何迅速、准确地识别并制止这一行为,成为电力系统管理领域亟待解决的重大课题。

以往,电力部门主要依靠定期现场巡查、电表核查及用户举报等传统手段进行检测,但这些方法存在周期长、覆盖面窄、效率低及难以精确定位异常点等不足[3]。部分早期研究尝试借助高精度传感器监控关键参数,但由于设备成本高昂及安装维护复杂,该方案在大规模应用中受到了限制。

随着互联网发展,智能电网和先进计量系统的规模也不断推广[4]。大规模实时数据采集和处理已成为可能,为非法用电检测提供了新的技术路径[5]。目前,主要的检测方法可以概括为以下 3 类:

基于电网运行状态分析的方法依托于对电压、电流、功率等核心参数的实时监控,利用状态估计模型对比理论计算值与实际测量值。当两者之间的偏差超过设定阈值时,即可判定存在异常用电现象[6-7]。尽管此方法在整体电网监控中具有较高准确性,但对数据采集设备和通信系统的要求较高,且在用户侧检测中应用受限。

基于博弈论策略的方法将电力企业与非法用电者视作追求自身利益最大化的理性主体,通过构建对抗性博弈模型,分析双方的决策行为,并据此设计出优化的检测与惩处方案[8]。然而,由于实际情况中各方可能存在非理性行为,加上效用函数难以精确定量,该方法在实践中仍面临较大挑战。

近年来,大数据与人工智能技术的发展为非法用电检测提供了全新思路,基于数据挖掘与机器学习的方法随之出现。无监督学习方法(例如聚类和 PCA 降维技术[9])则在缺乏充分标注数据的情况下,能够挖掘出隐藏的异常模式。部分研究还结合了半监督和深度学习方法,以进一步提升对隐蔽非法用电行为的识别能力。但对于大型复杂数据集,准确推断出数据集中实际的聚类数量非常困难。这种不确定性可能导致分类的准确性下降。并且由于缺乏实际类别标签的知识,无监督聚类方法仅基于聚类空间中的数据结构进行标记。这种方法容易出现标记错误,从而降低了窃电检测的可靠性。

利用监督学习算法(如决策树(decision trees, DT)[10]、支持向量机[11]和随机森林(random forest, RF)[12])对历史用电数据进行建模,可以较为精准地分辨正常与异常用电行为;许智等[13]提出选择了支持向量机、随机森林和迭代决策树 3 种机器学习中较常用的大数据算法进行分析,对比分析结果发现,随机森林算法运行时间与准确率表现最好。Hasan 等[14]提出将卷积神经网络(convolutional neural network, CNN)和长短期记忆网络(long short-term memory network, LSTM)结合,CNN 提取数据深度高维特征,LSTM 提取用户用电时间关联特征,卷积神经网络作为神经网络的一种独特形式,将神经网络的隐藏层由矩阵相乘替换为卷积运算,可训练更少参数、减少计算成本。Zheng 等[15]提出了宽度和深度 CNN 模型,宽度部分利用线性模型强记忆能力挖掘提取特征间的相关性,深度部分从二维的用电数据中提取周期性特征,再将两部分模型进行联合训练得出最终分类结果。Finardi 等[16]提出在 CNN 基础上引入自注意力机制,提高 CNN 特征提取的效率和最终检测精度。并且考虑到电力数据中存在大量缺失值,巧妙地设计二进制掩码来识别缺失值的位置,使网络能够学习如何处理这些值。Zhu 等[17]提出以局部到全局的方式捕获多尺度特征。同时,提出了一个自依赖建模模块,从自相关矩阵中学习二阶表示,最后将二阶表示与一阶表示结合,预测电力消费者的异常得分。Liao 等[18]提出了一种基于图注意网络的模型,从图域的新视角提高了检测精度。

虽然这些机器学习/深度学习方法均取得了不错的效果,但仍存在着一些不足。一是所有的方法都是针对特殊数据集或特殊应用场景量身定制,严重依赖于特定场景的领域知识或辅助数据;二是在面对多场景数据,这些方法并不适用甚至无法使用;三是之前的工作并没有对各种窃电模式进行识别,对于特殊窃电模式分析不足。

针对上述问题,现提出一种基于 CNN 和双向长短期记忆网络(bidirectional long short-term memory, BiLSTM)的混合模型,该模型不仅提高了时间序列数据的特征提取能力,还增强了模型对不同时间尺度的特征学习能力。首先,通过引入膨胀卷积层消除用电数据中环境因素的干扰,有效地提取用户用电的模式信息。其次,模型采用 BiLSTM 网络,进一步增强了对序列数据的建模能力,从而提升了异常检测的准确性和鲁棒性。这一混合模型的创新之处在于,通过膨胀卷积层和 BiLSTM 层的结合,不仅优化了特征提取流程,还提升了对时间序列中复杂依赖关系的建模能力,有效提高了窃电检测系统的准确度与稳定性。最后采用开放能源数据倡议(open energy data initiative, OEDI)数据集[19]对模型进行验证该模型的准确性和创新性。

1　相关理论介绍

1.1　一维卷积神经网络

CNN 是一类深度学习算法,广泛应用于图像处理、语音识别、自然语言处理等领域[20]。CNN 的核心思想是通过局部感受野、共享权重及池化操作,自动从输入数据中提取特征,并将这些特征用于分类或回归任务。CNN 的结构通常包括输入层、卷积层、激活层、池化层、全连接层等部分。

一维 CNN 的基本结构如图 1 所示,其通常由卷积层、激活函数和池化层交替堆叠而成,这些层依次对输入数据进行特征提取和降维操作。

膨胀卷积是一种扩展卷积操作的方法,最早应用于语音信号处理领域[17]。与标准卷积不同,膨胀卷积在卷积核

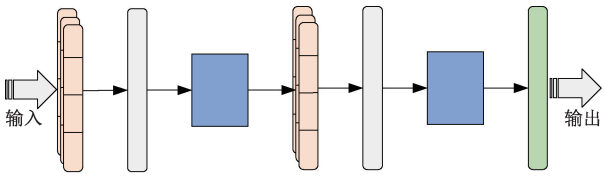

图 1　一维 CNN 结构

Fig. 1　1-D CNN structure

的每个元素之间引入间隔(膨胀因子),这样可以在保持卷积核大小不变的情况下,增加其感受野。其表达式为:

$$F(i)=\sum_{k=1}^{K} f(i+(k-1)\cdot d)\cdot \omega(k) \tag{1}$$

其中,$f(i)$ 是输入序列,$F(i)$ 是输出序列,K 是卷积核的大小,$f(i+(k-1)\cdot d)$ 表示输入序列中经过膨胀卷积核作用的第 $i+(k-1)\cdot d$ 个位置的输入数据,k 是卷积核的位置索引,$\omega(k)$ 是卷积核的第 k 个权重,d 为膨胀因子。

1.2　双向长短时记忆神经网络

LSTM 是一种特殊的递归神经网络,被设计用于解决传统循环神经网络(recurrent neural network, RNN)在处理长序列数据时出现的梯度消失和梯度爆炸问题[21]。LSTM 的结构在标准 RNN 的基础上进行了改进,引入了记忆单元和门控机制,使得它能够有效地捕捉长期依赖关系。

BiLSTM[22]则是在 LSTM 的基础上引入了双向结构,旨在更加全面地捕捉序列数据中的上下文信息。与传统的单向 LSTM 不同,BiLSTM 包含两个相互独立、相向传播的 LSTM 网络,即:BiLSTM 的隐藏状态是由正向 LSTM 和反向 LSTM 的隐藏状态拼接而成,其基本结构如图 2 所示,其中每个时间步的表示同时包含了该时间点之前和之后的上下文信息,更好地理解了长时间下的依赖关系。

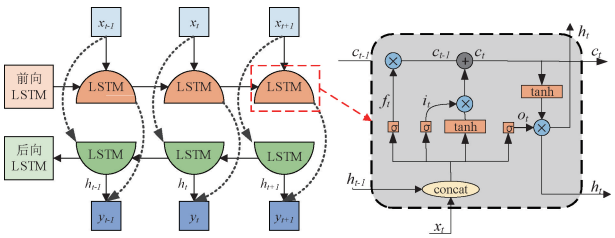

图 2　BiLSTM 结构

Fig. 2　BiLSTM structure

以单向 LSTM 为例,其计算公式为:

$$f_t=\sigma(\boldsymbol{W}_f\cdot[h_{t-1},x_t]+b_f) \tag{2}$$

$$i_t=\sigma(\boldsymbol{W}_i\cdot[h_{t-1},x_t]+b_i) \tag{3}$$

$$\tilde{c}_t=\tanh(\boldsymbol{W}_c\cdot[h_{t-1},x_t]+b_c) \tag{4}$$

$$c_t=f_t\cdot c_{t-1}+i_t\cdot\tilde{c}_t \tag{5}$$

$$o_t=\sigma(\boldsymbol{W}_o\cdot[h_{t-1},x_t]+b_o) \tag{6}$$

$$h_t=o_t\cdot\tanh(c_t) \tag{7}$$

其中,σ 是 Sigmoid 激活函数,用于将值压缩到 0～1;$\boldsymbol{W}_f$、$\boldsymbol{W}_i$、$\boldsymbol{W}_c$、$\boldsymbol{W}_o$ 是权重矩阵;b_f、b_i、b_c、b_o 是偏置项;tanh 是双曲正切激活函数,输出范围为−1～1。

2　多分类窃电检测模型

2.1　数据集介绍

OEDI 数据集源自一个集中存储美国的高价值能源研究数据集的数据库。原始数据涵盖了 16 种不同类型消费者的能源消耗数据,涉及公寓、医院、饭店等多种实际用电场景。该数据集记录了若干客户在连续 12 个月期间的能耗情况,并采用全天候实时监测的方式,每小时采集一次数据,共计 24 个时段的测量值[19]。具体的数据信息及相关统计指标如表 1 和 2 所示。

表 1　数据详细信息

Table 1　Data details

指标	数量
实例总数	560 640
特征数量	11
客户类型	12
每个客户类型实例数	35 040

表 2　用户类型表

Table 2　Users type

编号	客户类型	编号	客户类型
1	全服务餐厅	9	仓库
2	医院	10	中学
3	大型酒店	11	小型酒店
4	大型办公室	12	小型办公室
5	中型办公室	13	独立零售店
6	中层公寓	14	购物中心
7	小学	15	超市
8	门诊医院	16	快餐店

数据集中包含了例如风扇、燃气、照明等不同的用电量,但考虑到实际运用中很难获取到此类特征,故仅选用总用电量作为研究对象。

2.2　窃电模式分析

OEDI 数据集用户每一个小时记录一次用电量,向量 $\boldsymbol{X}=[x_1,x_2,\cdots,x_{24}]$ 表示着每个用户一天的用电量。对总电量分析,窃电用户总是通过降低总用电量或根据电价实时波动的性质篡改电表从而降低自己所需支付的电费[23]。

文献[24-25]提出了 6 种不同类型的窃电行为。它们由一些用户可能造成的不同类型的盗窃组成。第 1 类盗窃包括在白天大量减少电力消耗,通过将用电量乘以 0.1 和 0.8 之间随机选择的值来计算这种盗窃。在第 2 种类型的

盗窃中，电力消耗随机地在任意时间段内降至零。第 3 种类型的盗窃类似于第一种类型，将用电量（每小时）乘以一个随机数。第 5 种类型取当日用电量的平均值。第 4 种类型的盗窃类似于第 5 种类型，在平均值的基础上乘以 0.1～0.8 的随机值。第 6 种类型颠倒了用电量读数的顺序。具体篡改公式如表 3 所示。

表 3　OEDI 数据 6 种篡改公式

Table 3　Six formulas for tampering with OEDI data

篡改类型	篡改公式
类型 1	$\hat{x}_t = \alpha x_t, 0.2 < \alpha < 0.8$
类型 2	$\hat{x}_t = \alpha_t x_t, 0.2 < \alpha_t < 0.8$
类型 3	$\hat{x}_t = \beta x_t, \beta = \begin{cases} 1, t_1 < t < t_2 \\ 0, \text{其他} \end{cases}$
类型 4	$\hat{x}_t = \alpha_t \bar{X}, 0.2 < \alpha_t < 0.8$
类型 5	$\hat{x}_t = \bar{X}$
类型 6	$\hat{x}_t = x_{24-t}$

由于不同客户类型不同，用电模式也不同，为了提高模型训练的效率与准确性，并确保不同特征之间的数值尺度统一，对 OEDI 数据集中的各项能源消耗数据进行了 Min-Max 归一化处理。其计算式为：

$$f(x_i) = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{8}$$

其中，$\min(x)$ 和 $\max(x)$ 分别是数据集中的最小值和最大值。故经过公式篡改与归一化之后的数据用户标签统计如表 4 所示。

表 4　数据用户标签统计表

Table 4　Statistical table of data user labels

用户标签	数量	占总数比例/%
正常用户	13 864	59.35
类型 1 窃电用户	2 137	9.15
类型 2 窃电用户	926	3.96
类型 3 窃电用户	1 851	7.92
类型 4 窃电用户	1 716	7.35
类型 5 窃电用户	1 396	5.98
类型 6 窃电用户	1 470	6.29
总数	23 360	
窃电用户占总数比例/%	40.65	

2.3　基于 CNN-BiLSTM 的窃电检测模型

由于 CNN 与 BiLSTM 均能够在多层次、多尺度上提取和建模时序数据的特征，并能够捕捉到长时间跨度和复杂依赖关系。为了充分发挥这两种网络的优势，本文设计了基于 CNN-BiLSTM 的窃电检测模型。整体模型框架如图 3 所示。

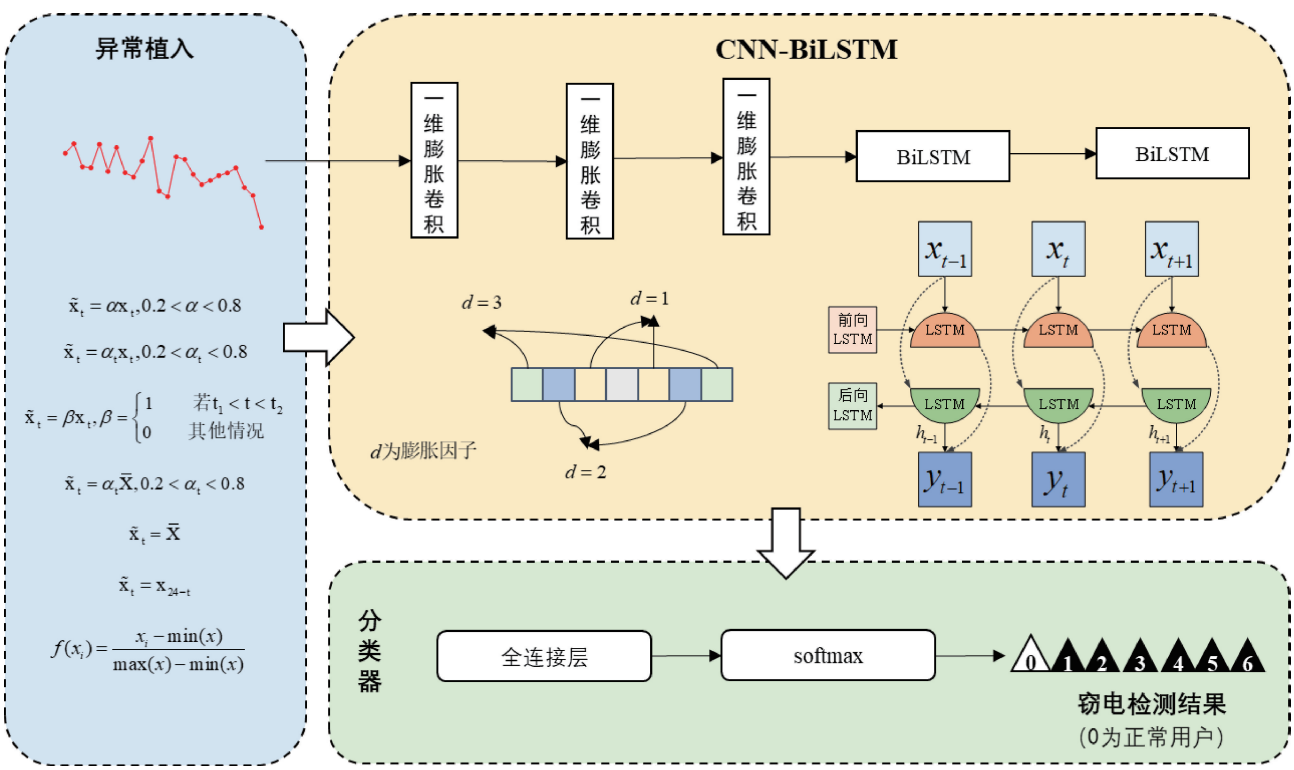

图 3　基于 CNN-BiLSTM 的窃电检测模型框架

Fig. 3　CNN-BiLSTM based modeling framework for electricity theft detection

用户用电数据可以视为用电行为与环境因素的结合,环境因素包括客户类型、地区等,这些因素通常较为稳定。为了减少环境因素带来的干扰,本文提出采用膨胀卷积的方法。通过设置差分滤波卷积核(如 [−0.5, 1, −0.5]),可以有效捕捉微小波动,消除由环境因素(如地区和客户类型)引起的干扰,进而提高模型在复杂环境下的鲁棒性。而双向 LSTM 通过同时利用过去和未来的信息建模长期依赖关系,二者的结合能够显著提升模型对复杂时序数据的预测精度和鲁棒性,充分满足实际任务中复杂环境下窃电检测的需求。

膨胀卷积模块由一维卷积层、激活层和 dropout 层组成,BiLSTM 模块由两个 BiLSTM 层和批归一化层组成,同时利用正向和反向的信息,有效提升模型对复杂序列数据的学习能力,做出更加准确的分类。最后的窃电检测分类器采用 Softmax 激活函数,它将模型的输出转换为一个概率分布。同时为了提高模型的训练效率和稳定性,采用了 ReduceLROnPlateau 回调函数来动态调整学习率。该方法会根据验证集的表现自动调整学习率,避免训练过程中学习率过高导致的模型不稳定,或过低导致的训练速度过慢。模型具体配置如表 5 所示。

表 5　模型配置

Table 5　Model configuration

模块名称	层名称	参数
CNN * 3	一维卷积层	卷积核数量:128 卷积核大小:3 膨胀因子:[1,2,3] 卷积核:(−0.5,1,−0.5)
	激活层	$\mathrm{prelu}(\mu)=\begin{cases}\mu, & \mu\geqslant 0\\ 0.25\mu, & \mu<0\end{cases}$
	Dropout 层	灭活比例:0.5
BiLSTM	双向 LSTM 层	单元数:128
	批归一化层	—
	双向 LSTM 层	单元数:128
	批归一化层	—
分类器	展平层	—
	全连接层	激活函数:Softmax

3　实验分析

3.1　评价指标

为了验证所提方法在窃电检测中的准确性,本文采用了准确率(accuracy,Acc)、曲线下面积(area under ROC curve,AUC)和 F1 分数(F1 score,F1)作为评估指标。这些指标能够全面反映模型的性能,并帮助更好地分析模型在不同场景下的表现。

由于本文涉及二分类与多分类任务,对于二分类任务,模型的预测结果通常分为两类:正类和负类,如本研究中窃电行为和非窃电行为。对于多分类任务,虽然类的数量增加了,但每一类依然可以根据真正例(true positive,TP)、真反例(true negative,TN)、假正例(false positive,FP)和假反例(false negative,FN)来计算得分。TP 表示模型正确预测为正类(即窃电行为)且实际为正类的样本数量。TN 表示模型正确预测为负类(即非窃电行为)且实际为负类的样本数量。FP 表示模型错误地将负类预测为正类的样本数量,也称为假阳性。FN 表示模型错误地将正类预测为负类的样本数量,也称为假阴性。具体方法是基于每个类别进行单独评估,最后通过加权平均等方式得到整体评估结果。具体计算公式如下:

$$Acc=\frac{TP+TN}{TP+TN+FP+FN} \tag{9}$$

$$AUC=\int_0^1 \frac{TP}{TP+FN}\mathrm{d}\left(\frac{FP}{FP+TN}\right) \tag{10}$$

$$P=\frac{TP}{TP+FP} \tag{11}$$

$$R=\frac{TP}{TP+FN} \tag{12}$$

$$F1=2\times\frac{P\times R}{P+R} \tag{13}$$

$$F1_{weighted}=\frac{\sum_{i=1}^{n}(\omega_i\times F1_i)}{\sum_{i=1}^{n}\omega_i} \tag{14}$$

其中,$F1_i$ 是第 i 类的 F1-score;ω_i 是第 i 类的样本数量占总样本数量的比例,计算公式为:

$$\omega_i=\frac{\text{第 } i \text{ 类样本数}}{\text{总样本数}} \tag{15}$$

通过权重 F1 的计算,类别数量较多或者样本数较多的类别对最终的 F1 影响较大,而样本较少的类别对最终结果的影响较小。

3.2　实验结果与分析

1)实验设置

本文所有实验在 CentOS7 系统下开展,其中 CPU 为 GeForce RTX 4090,采用 Python 作为开发语言,Tensorflow 作为深度学习框架。

实验使用第 2 节经过公式篡改与归一化之后的数据,并按 8∶2 的比例划分为训练集和测试集。首先,将重点进行正常用户与窃电用户的二分类任务,这是本研究的主要任务,记为任务一;接下来,将考虑正常用户与前五种类型窃电用户的多分类任务,记为任务二;最后,将扩展到正常用户与六种类型窃电用户的多分类任务,记为任务三。在确保能够准确识别窃电用户的基础上,进一步精确分类不同的窃电模式,这对于实际应用具有重要的意义。

2)对比实验分析

为了验证本文模型窃电检测的准确性,与当前广泛使

用的 RF、DT、CNN、LSTM 四种方法进行对比，为了进行公平的比较，采用控制变量法，通过多次不同规模的实验来选择合适的参数值。每种方法分别独立运行 20 次，得到测试集的平均 Acc、AUC 和 F1 score，实验结果如表 6 所示。

表 6　不同任务的实验结果对比

Table 6　Comparison of experimental results for different tasks

方法	任务一(二分类)		
	Acc	AUC	F1
RF	0.875 1	0.884 9	0.882 0
DT	0.858 0	0.856 1	0.865 4
CNN	0.895 1	0.899 1	0.881 6
LSTM	0.898 6	0.891 0	0.892 4
本文模型	**0.925 2**	**0.938 0**	**0.918 4**
方法	任务二(六分类)		
	Acc	AUC	F1
RF	0.910 6	0.955 5	0.892 0
DT	0.901 9	0.922 9	0.865 5
CNN	0.912 5	0.975 0	0.902 1
LSTM	0.910 1	0.982 5	0.900 1
本文模型	**0.942 5**	**0.991 5**	**0.934 7**
方法	任务三(七分类)		
	Acc	AUC	F1
RF	0.838 9	0.925 4	0.810 1
DT	0.824 8	0.840 5	0.802 6
CNN	0.835 4	0.930 5	0.812 8
LSTM	0.841 1	0.931 6	0.801 1
本文模型	**0.875 8**	**0.972 1**	**0.855 4**

实验结果表明，本文提出的模型得到了最佳的总体结果。本文所提出的模型在不同任务下均显著优于传统方法。在二分类任务中，本文模型的 Acc 达到了 0.925 2，相较于 RF(0.875 1)、DT(0.858 0)、CNN(0.895 1)和 LSTM(0.898 6)，分别提高了约 5.9%、6.7%、3.0%和 2.9%；同时，其 AUC 为 0.938 0，比 RF(0.884 9)和 LSTM(0.891 0)分别提高了约 5.9%和 5.3%；F1-score 达到了 0.918 4，相较于 RF(0.882 0)和 LSTM(0.892 4)分别提升了约 4.1%和 3.0%。

在六分类任务中，本文模型的 Acc 为 0.942 5，高于 RF(0.910 6)、决策树(0.901 9)、CNN(0.912 5)和 LSTM(0.910 1)，与最佳对比方法(CNN)的 Acc 相比，提升约 3.3%；其 AUC 值为 0.991 5，相比于 CNN(0.975 0)和 LSTM(0.982 5)分别提升了约 1.7%和 0.9%；F1-score 为 0.934 7，则相对于 CNN 的 0.902 1，提升约 3.6%。

在七分类任务中，本文模型的表现同样优异，其 Acc 达到 0.875 8，相较于 RF(0.838 9)、决策树(0.824 8)、CNN(0.835 4)和 LSTM(0.841 1)均有明显提升，最高提升幅度约 3.5%；AUC 和 F1-score 分别为 0.972 1 和 0.855 4，也较对比方法分别提高了约 4.0%和 4.3%。

在训练过程中，采用交叉熵损失函数进行优化。如图 4 所示，训练集的 loss 从 0.659 6 逐步下降至 0.360 2，而验证集的 loss 也呈现下降趋势，最终稳定在 0.360 2 左右。这表明模型能够有效学习数据分布，并且在测试集上具有良好的泛化能力。

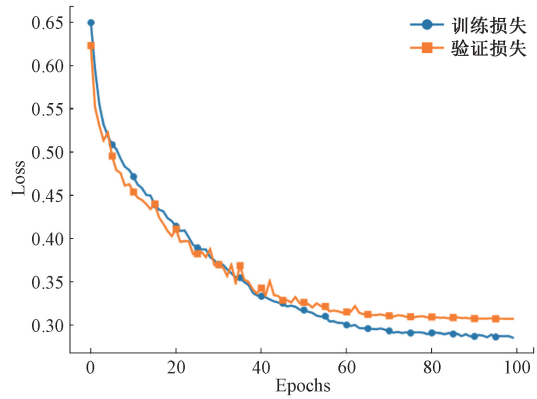

图 4　训练与验证集损失变化曲线

Fig. 4　Training loss and validation loss curve

以任务一为例，训练时间通常取决于模型的复杂度、数据规模和计算资源。本实验共进行 100 轮(epochs)训练，在 584 个 batch 训练的情况下，单次 epoch 约需 5 s，总训练时间约为 500 s 左右，与 CNN 总时间 300 s 相比，虽然模型训练时间有所增加，但窃电检测精度显著提升。而对于 4 672 个测试样本，模型推理时间为 1.1 s，表明该模型不仅具有高精度，还能在短时间内完成大批量推理，可适用于需要高效预测的实际应用场景。

综上所述，无论是在二分类还是多分类任务中，本文模型均展现出更高的预测精度和更优的分类性能，验证了所提方法在窃电检测中的有效性与鲁棒性，为实际复杂环境下的窃电行为检测提供了有力的技术支持。因此，可以说明本文模型不仅能精准的区分窃电用户与正常用户，还能对用户的窃电模式进行准确的细分。图 5、6、7 分别是 3 个任务的混淆矩阵。

通过任务二与任务三的对比，发现任务二的各项指标明显优于任务三，三项指标分别提高了 6.67%、1.94%和 7.93%。这是因为类型六的窃电模式难以检测，图 6、7 分别给出的任务二和任务三的混淆矩阵也证实了这一点。类型六的窃电模式的检测难度较大，这显著影响了任务三模型的整体检测性能。混淆矩阵表明，正常用户与类型六用户之间存在严重的误判问题。在实际的 286 个类型六窃电用户样本中，只有 41 个被正确识别，然而有多达 184 个被误判为“正常”类，另有 61 个被误判为前五种类型窃

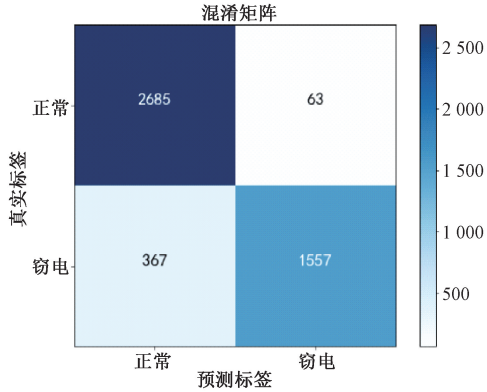

图 5　任务一混淆矩阵

Fig. 5　Task 1 confusion matrix

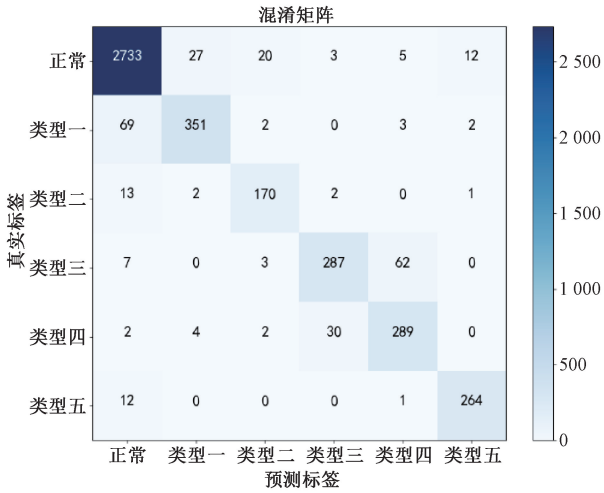

图 6　任务二混淆矩阵

Fig. 6　Task 2 confusion matrix

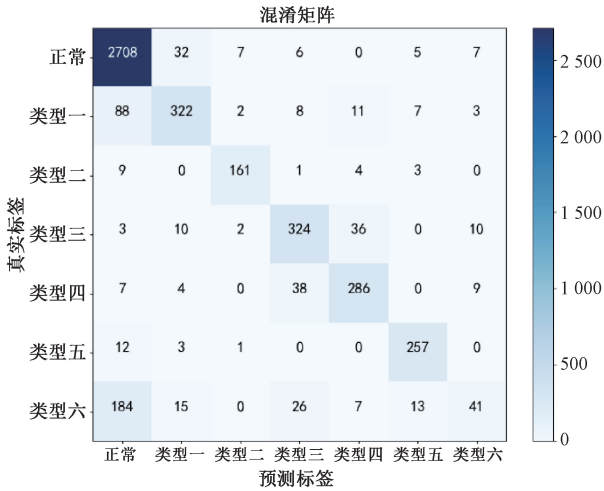

图 7　任务三混淆矩阵

Fig. 7　Task 3 confusion matrix

电用户。

这种误判现象可以通过类型六的篡改公式特征来解释:该类型的欺诈行为主要表现为时间跨度很小的用电异常,即先前时间戳中的欺诈性消费取代了真实的消费记录。因此,模型难以有效区分正常用户和类型六窃电用户的样本。

3)消融实验分析

此外,为了评估模型中每个模块的影响,将进行消融实验。具体而言,将分别使用仅包含膨胀 CNN 模块和仅包含 BiLSTM 模块的模型,并与整体模型进行对比,观察各个模块的组合对整体性能提升的作用。训练集与测试集比例仍为 8∶2,实验结果如表 7 所示。

表 7　消融实验结果对比

Table 7　Comparison of ablation experiment results

方法	任务一(二分类)		
	Acc	AUC	F1
仅膨胀 CNN	0.905 6	0.918 1	0.894 4
仅 BiLSTM	0.901 2	0.918 9	0.901 1
本文模型	**0.925 2**	**0.938 0**	**0.918 4**
方法	任务二(六分类)		
	Acc	AUC	F1
仅膨胀 CNN	0.920 6	0.985 5	0.901 6
仅 BiLSTM	0.921 9	0.982 9	0.902 5
本文模型	**0.942 5**	**0.991 5**	**0.934 7**
方法	任务三(七分类)		
	Acc	AUC	F1
仅膨胀 CNN	0.849 8	0.957 9	0.823 6
仅 BiLSTM	0.851 2	0.958 1	0.821 5
本文模型	**0.875 8**	**0.972 1**	**0.855 4**

表 7 展示了在基于 CNN-BiLSTM 的窃电检测模型中各个模块对模型性能的影响。与表 6 相比,可以看出引入膨胀卷积后,3 个指标得到了一定的增长,这是因为膨胀卷积通过扩大感受野捕捉局部特征,并且消除用户用电数据中的环境干扰;同时,BiLSTM 获得的双向特征表示相比 LSTM 通常更加丰富和鲁棒,这有助于提高模型在多分类和二分类任务中的整体性能。特别是在窃电检测场景下,利用 BiLSTM 可以更好地识别细微的异常变化,从而提升检测精度。将本文模型与仅膨胀 CNN、仅 BiLSTM 的模型对比,3 个指标均得到了较大的提升,这说明本文模型将 CNN 与 BiLSTM 巧妙的融合在一起,大幅提高了窃电检测的精度与鲁棒性。

4　结　　论

本论文提出了一种基于 CNN-BiLSTM 的窃电检测模型。该模型将 CNN 与 BiLSTM 很好的融合在一起,利用膨胀卷积层在不增加计算复杂度的情况下扩展感受野,有效捕捉不同时间尺度的局部特征,并且剔除用电环境的干

扰；同时，采用 BiLSTM 对输入时序数据进行正向与反向建模，从而充分提取长距离依赖信息，提高异常模式判别的精度与鲁棒性。本文首先实验部分采用 OEDI 数据集，针对六种不同的窃电模式对数据进行篡改，同时对数据进行了 Min-Max 归一化处理；然后采用 CNN-BiLSTM 进行窃电检测，充分挖掘不同尺度的特征，同时关注历史与未来的依赖信息，提升检测精度，为防止模型过拟合，本文引入了自适应激活函数、Dropout 策略以及动态学习率调整机制；最后在二分类、六分类和七分类任务下设置开展对比实验，利用准确率、AUC 和 F1-score 等指标全面评估模型性能。实验结果表明，本模型在识别窃电行为及其细分模式方面均表现出较高的准确性和稳定性，明显优于传统方法；消融实验进一步验证了膨胀卷积与 BiLSTM 模块在整体模型中的关键作用。综上所述，本文研究成果为窃电检测提供了一种高效、准确的技术方案，并为智能电网异常监测任务的深入开展奠定了理论与实践基础。未来工作将进一步优化模型结构，聚焦第 6 种类型的窃电模式，并在更大规模的实际数据中验证其推广应用价值。

参考文献

[1] 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.

[2] 刘东涛. 电力计量中的反窃电措施分析[J]. 集成电路应用，2020，37(4)：92-93.
LIU D T. Analysis of anti stealing measures in electric power measurement[J]. Application of IC, 2020, 37(4): 92-93.

[3] 肖宇，叶志，黄瑞，等. 窃电行为检测方法研究综述[J]. 电力科学与技术学报，2023，38(4)：1-14.
XIAO Y, YE ZH, HUANG R, et al. Summary of research on electricity theft behavior detection methods[J]. Journal of Electric Power Science and Technology, 2023, 38(4): 1-14.

[4] 舒珏淋，张力，胡建. 基于高斯混合模型的智能电表误差数据挖掘与分析方法[J]. 电子测量技术，2021，44(15)：56-61.
SHU Y L, ZHANG L, HU J. Data mining and analysis method for smart meter error data based on Gaussian mixture model[J]. Electronic Measurement Technology, 2021, 44(15): 56-61.

[5] 林振智，崔雪原，金伟超，等. 用户侧窃电检测关键技术[J]. 电力系统自动化，2022，46(5)：188-199.
LIN ZH ZH, CUI X Y, JIN W CH, et al. Key technology for detecting power theft on the customer side [J]. Automation of Electric Power Systems, 2022, 46(5): 188-199.

[6] 李先怀，李君，许健. 基于暂态电流突变特性的窃电检测研究[J]. 大众用电，2020，35(5)：30-32.
LI X H, LI J, XU J. Research on electricity theft detection based on transient current mutation characteristics[J]. Popular Utilization of Electricity, 2020, 35(5): 30-32.

[7] PEI CH, XIAO Y, LIANG W, et al. Detecting false data injection attacks using canonical variate analysis in power grid [J]. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 971-983.

[8] 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]. 2017 Resilience Week(RWS), IEEE, 2017: 5-11.

[9] HUSSAIN S, MUSTAFA M W, JUMANI T A, et al. A novel unsupervised feature-based approach for electricity theft detection using robust PCA and outlier removal clustering algorithm [J]. International Transactions on Electrical Energy Systems, 2020, 30(11): e12572.

[10] LEPOLESA L J, ACHARI S, CHENG L. Electricity theft detection in smart grids based on deep neural network[J]. IEEE Access, 2022, 10: 39638-39655.

[11] 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.

[12] GUNTURI S K, SARKAR D. Ensemble machine learning models for the detection of energy theft[J]. Electric Power Systems Research, 2021, 192: 106904.

[13] 许智，李红娇，陈晶晶. 基于机器学习的用户窃电行为预测[J]. 上海电力学院学报，2017，33(4)：389-393.
XU ZH, LI H J, CHEN J J. Prediction of user stealing behavior based on machine learning [J]. Journal of Shanghai University of Electric Power, 2017, 33(4): 389-393.

[14] HASAN M N, TOMA R N, NAHID A A, et al. Electricity theft detection in smart grid systems: A CNN-LSTM based approach [J]. Energies, 2019, 12(17): 3310.

[15] ZHENG Z B, YANG Y T, NIU X D, et al. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids[J]. IEEE Transactions on Industrial Informatics, 2017, 14(4): 1606-1615.

[16] FINARDI P, CAMPIOTTI I, PLENSACK G, et al. Electricity theft detection with self-attention [J].

ArXiv preprint arXiv:2002.06219, 2020.

[17] ZHU Y Y, ZHANG Y, LIU L B, et al. Hybrid-order representation learning for electricity theft detection[J]. IEEE Transactions on Industrial Informatics, 2022, 19(2): 1248-1259.

[18] LIAO W L, ZHU R J, YANG ZH, et al. Electricity theft detection using dynamic graph construction and graph attention network[J]. IEEE Transactions on Industrial Informatics, 2023, 20(4): 5074-5086.

[19] ZIDI S, MIHOUB A, QAISAR S M, et al. Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment [J]. Journal of King Saud University-Computer and Information Sciences, 2023, 35(1): 13-25.

[20] LI Z W, LIU F, YANG W J, et al. A survey of convolutional neural networks: Analysis, applications, and prospects [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(12): 6999-7019.

[21] 刘少卿, 李帅, 苗建国, 等. 基于 TCN-BiGRU 的锂离子电池健康状态评估[J]. 电子测量技术, 2023, 46(23): 68-76.
LIU SH Q, LI SH, MIAO J G, et al. Lithium-ion battery state of health estimation based on TCN-BiGRU [J]. Electronic Measurement Technology, 2023, 46(23): 68-76.

[22] 陈晓, 杨瑶. 融合注意力机制的 BiLSTM 网络实现无创血压测量[J]. 电子测量技术, 2022, 45(23): 59-65.
CHEN X, YANG Y. Noninvasive blood pressure measurement based on BiLSTM network with attention mechanism [J]. Electronic Measurement Technology, 2022, 45(23): 59-65.

[23] 程俊文, 李慧娟, 曹志强. 基于 K-means 算法和用电信息采集系统的防窃电研究[J]. 供用电, 2019, 36(1): 75-80.
CHENG J W, LI H J, CAO ZH Q. Research on anti-stealing based on K-means clustering algorithm and electricity information collection system [J]. Distribution & Utilization, 2019, 36(1): 75-80.

[24] 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 SH, SU SH, XUE Y, et al. A review of data-driven electricity theft detection methods and research outlook on low false alarm rate[J]. Automation of Electric Power Systems, 2022, 46(1): 3-14.

[25] AHUJA R, CHUG A, GUPTA S, et al. Classification and clustering algorithms of machine learning with their applications[J]. Nature-Inspired Computation in Data Mining and Machine Learning, 2020: 225-248.

作者简介

苗强(通信作者),教授,主要研究方向为重大装备故障诊断、健康评估以及可靠性研究。

E-mail: mqiang@scu.edu.cn