DOI: 10.19783/j.cnki.pspc.211653

一种基于 CAEs-LSTM 融合模型的窃电检测方法

董立红[1]，肖纯朗[1]，叶 鸥[1]，于振华[1]

（西安科技大学计算机科学与技术学院，陕西 西安 710000）

摘要：为解决现有的智能电网电力盗窃行为检测方法中准确性不足、检测效率低下等问题，提出了一种由卷积自编码器网络(convolutional auto-encoders, CAEs)和长短期记忆网络(long short term memory, LSTM)相结合的 CAEs-LSTM 检测模型。该模型通过分析数据集的特点对电力数据进行二维转换，设计卷积自编码器结构，采用池化、下采样和上采样重构电力数据的二维空间特征，加入高斯噪声提高模型鲁棒性，并构建长短期记忆网络以学习全局时序特征。最后，对提取的时空特征进行融合从而检测能源窃贼，并进行了参数调优。在由国家电网公布的真实数据集上，通过将 CAEs-LSTM 模型与支持向量机、LSTM 以及宽深度卷积神经网络进行对比，CAEs-LSTM 模型的平均精度均值和曲线下面积值均最优。仿真实验表明，基于 CAEs-LSTM 模型的窃电检测方法具有更高的窃电检测效率和精度。

关键词：窃电检测；长短期记忆网络；卷积自编码器；深度学习；缺失值填补

Electricity theft detection method based on a CAEs-LSTM fusion model

DONG Lihong[1], XIAO Chunlang[1], YE Ou[1], YU Zhenhua[1]

(School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710000, China)

Abstract: To solve the problems of insufficient accuracy and low detection efficiency in existing detection methods of electricity theft in smart grids, a CAEs-LSTM detection model combining convolutional auto-encoders (CAEs) with long short-term memory networks (LSTM) is proposed. The model conducts two-dimensional conversion to power data, designs the encoder structure by analyzing the characteristics of data set, and reconstructs the two-dimensional space characteristics of the electricity data using pooling layers, down and up sampling layers. It adds Gaussian noise to improve its robustness, and builds long short-term memory networks to learn the global characteristics. Finally, spatial-temporal characteristics are fused to detect energy thieves, and parameter tuning is performed. Based on the public available real data set of the State Grid, the CAEs-LSTM model is optimal in the value of mean average prediction and area under curve, by comparing the CAEs-LSTM model with support vector machines, the LSTM model, and wide and deep convolutional neural networks. Simulation experiments show that the theft detection method based on the CAEs-LSTM model has higher detection efficiency and accuracy.

This work is supported by the National Natural Science Foundation of China (No. 61873277).

Key words: electricity theft detection; long short-term memory network; convolutional auto-encoders; deep learning; missing value imputation

0 引言

近年来，随着智能电网的发展，用电居民在享受其带来的便利的同时，供电企业的线路损失率居高不下，这导致了供电运营成本的提升。在电力系统中，电力损耗有两种类型：技术性损失(technical losses, TLs)和非技术性损失(non-technical losses, NTLs)[1]。技术性损失是电能在传输过程中无法避免的固有损耗，主要由电力系统中组件自身的功率损耗组成。导致非技术性损失的原因有很多种[2]，主要包括：篡改仪表、从电源上安装线路绕过仪表、贿赂抄表员、仪表故障或损坏[3]、数据处理以及计费中的技术和人为错误。在实际场景中，非法篡改

基金项目：国家自然科学基金项目资助(61873277)；中国博士后科学基金项目资助(2020M673446)

导致的损耗是非技术性损失的主要原因，也被称为电力盗窃。

电力盗窃正在不断削弱世界各地的公用事业供应商，它不仅影响了电力系统的稳定运行，甚至产生危及生命的公共安全问题。根据东北集团的数据显示，NTLs 每年在全球造成 960 亿美元的损失[4]，中国福建省的年窃电损失高达 1 亿美元[5]。据报告，在东南亚国家联盟的大多数发展中国家中，NTLs 活动的发生率很高。世界银行还报告说，由电力盗窃而产生的损失是发展中国家近一半的发电量[6]。

对于电力盗窃问题，执行定期检查的费用非常高，因此很难计算或衡量实际损失[7]。随着智能电网技术的不断发展，用电信息采集异常几率逐渐增大，累计的终端用户异常用电数据也越来越多，异常的用电模式蕴藏着电网的重要信息。因此，对用电数据进行深层次挖掘，通过其隐藏的规律可以有效检测出异常的用电模式。

用电异常检测是指利用电力系统中的历史数据和实时数据，检测电力系统中存在的异常用电用户或异常用电行为[8]。聚类[9]和支持向量机(support vector machines, SVM)等在电力盗窃检测中应用广泛[10-14]，文献[15]利用历史消费数据，使用数据挖掘方法和 SVM 分类器检测异常行为，利用能源消费的长期趋势来检测欺诈客户。然而，基于 SVM 的电力窃取检测通常需要大量的训练数据并且依赖从历史数据中提取的特征，不适用于处理高维数据中的类别不平衡问题。集成学习也被用于电力盗窃检测，文献[16]通过改进 XGBoost 模型，通过实际电力用户数据实现了低误报率的检测。

近年来，深度学习在用电异常检测中的应用越来越广泛。文献[17]通过对数据集进行特殊的缩减，提取数据集中有意义的信息，然后构建长短期记忆网络(long short term memory, LSTM)模型识别异常用户。文献[18]采用归一化和插值方法对电力数据进行预处理，然后将预处理后的数据送入 LSTM 模块进行特征提取，最后将选定的特性传递给提出的 RUSBoost 模块进行分类。混合深度学习技术能结合不同模型的优点，近年来常被用于负荷预测等研究[19]。文献[20]使用 6 个盗窃案例来合成盗窃数据，以模拟真实世界的场景。文献[21]将卷积神经网络(convolutional neural network, CNN)与随机森林算法相结合，在超过 5000 名住宅和商业消费者的真实数据集上验证了模型的有效性。受宽深度推荐系统的启发，文献[22]提出了一种宽深度混合模型，在由国家电网公布的真实数据集上通过监督训练验证了窃电检测的效率。在此基础上，文献[23]通过串行将 CNN 和 LSTM 结合起来，研究电力数据的时间特性，并合成恶意数据进行注入来解决异常检测中的样本失衡问题。然而，混合模型的应用需要考虑到数据集的特性，这些检测方法没有从大量高维度数据中充分提取出数据的特征，检测精度仍有待提升。

本文提出了一种新的深度学习模型，用以解决上述问题。首先对数据集中的缺失值及异常值进行处理，然后构建 LSTM 学习数据的全局时序特征，通过卷积自编码器网络(convolutional auto-encoders, CAEs)学习数据的空间特征，并将两者学习到的特征进行融合，用于训练监督模型。本文考虑了所使用数据集的时空特性，并在卷积自编码器的输入中加入了高斯噪声，提高了模型的鲁棒性。最后，通过 42 373 个用户的日负荷数据来训练和评估提出的模型，验证其优越性。

1　相关技术说明

Keras 是一款用 Python 编写且可兼容 Tensorflow 的神经网络高级包，支持快速实验。本文通过 Keras 建立基于 CAEs-LSTM 的电力盗窃行为检测模型，实现电力盗窃用户的检测。

1.1　卷积自编码器

作为深度学习的流行算法之一，自动编码器已经被广泛应用于医学、图像、生物工程、信息物理融合系统等各个领域进行降维或特征学习[24]。自动编码器有一个输入层，一个隐含层和一个输出层。典型的自编码器结构如图 1 所示。

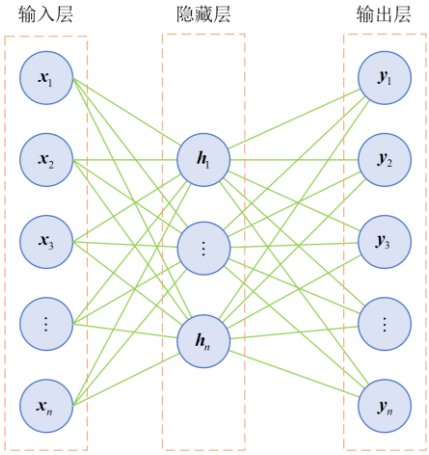


图 1　卷积自编码器结构

Fig. 1 Structure of convolutional auto-encoders

输入层到隐含层的映射关系可以被看作是一个编码过程，通过映射函数 f 把输入向量 $\boldsymbol{x}$ 映射到隐含层输出 $\boldsymbol{y}$。从隐含层到输出层的过程相当于一

个解码过程。对于每一个输入样本 $\boldsymbol{x}$ 而言，经过自动编码器之后都会转化为一个对应的输出向量 $\boldsymbol{z}=g[f(\boldsymbol{x})]$。

对自动编码器结构进行改进，可以得到其他类型的自动编码器，如卷积自编码器。其主要思想就是加入一些卷积操作，将基本的自编码器全连接层替换为卷积层、池化层以及采样层。

卷积层的思想来源于利用人类视觉皮层进行物体识别的工作原理。在卷积阶段，初始化 k 个卷积核，每个卷积核搭配一个偏置 $\boldsymbol{b}$，与输入 $\boldsymbol{x}$ 卷积后生成 k 个特征图 $\boldsymbol{h}$，可表示为

$$\boldsymbol{h}^k=\sigma(\boldsymbol{x}*\boldsymbol{W}^k+\boldsymbol{b}^k) \tag{1}$$

式中：“$*$”为卷积操作；σ 为激活函数，用来加入非线性因素；$\boldsymbol{h}^k$ 为经过一层卷积操作后得到的特征。

池化层作为紧邻卷积层的步骤，是一个下采样过程，通常被置于两个卷积层之间。池化层的作用是进行特征选择，减少特征数量，进而减少网络参数量，实现降维，并在一定程度上达到防止过拟合的效果。

经过多层叠加的卷积及池化过程后得到特征 $\boldsymbol{h}^t$，对 $\boldsymbol{h}^t$ 进行特征重构，即解码阶段，解码阶段对应的卷积层和上采样层的参数与编码阶段一一对应，为对称结构。反卷积层后紧跟着与池化层步长相同的上采样层，目的是将特征图还原到原大小。

每张特征图 $\boldsymbol{h}$ 与其对应的卷积核的转置进行卷积操作，并将结果求和，然后加上偏置 $\boldsymbol{c}$，可以得到

$$\boldsymbol{y}^t=\sigma(\sum\nolimits_t \boldsymbol{h}^t*\boldsymbol{W}^t+\boldsymbol{c}) \tag{2}$$

最终得到对应 $\boldsymbol{x}$ 的重构特征 $\boldsymbol{y}$。两者相似度可以通过定义损失函数 L 来描述。

$$L=\frac{\sum_{i=1}^{n}(\boldsymbol{x}_i-\boldsymbol{y}_i)^2}{n} \tag{3}$$

重构误差可表示为

$$R_{\mathrm{E}}=\sum_{i=1}^{n}(\boldsymbol{x}_i-\boldsymbol{y}_i)^2 \tag{4}$$

1.2 长短期记忆网络

为了解决循环神经网络的短期记忆问题，提出长短期记忆网络。长短期记忆网络具有额外的特征来记忆数据序列，能克服循环神经网络中的消失梯度问题。LSTM 能够从网络的初始阶段到最后阶段记忆和传播重要信息，在处理时序数据的特征提取上有非常显著的效果，因此常被用于时间序列数据预测及分类[25-26]。

每个 LSTM 是一组单元或系统模块，在每个单元中使用了一些门，单元中的数据流可以被捕获并存取，然后处理、过滤或添加到下一个单元中，因此单元可以有选择地让信息通过或者删除，其结构如图 2 所示。

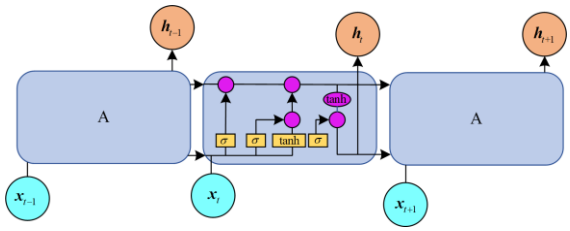


图 2 LSTM 单元结构

Fig. 2 Structure of LSTM unit

它通过 3 个门(称为遗忘门、输入门和输出门)，来控制信息的传递，可以通过以下公式进行概括。

遗忘门：

$$f_t=\sigma(\boldsymbol{W}_f\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_f) \tag{5}$$

输入门：

$$\begin{aligned} i_t&=\sigma(\boldsymbol{W}_i\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_i)\\ \tilde{\boldsymbol{C}}_t&=\tanh(\boldsymbol{W}_C\cdot[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_C)\\ \boldsymbol{C}_t&=f_t*\boldsymbol{C}_{t-1}+i_t*\tilde{\boldsymbol{C}}_t \end{aligned} \tag{6}$$

输出门：

$$\begin{aligned} o_t&=\sigma(\boldsymbol{W}_o[\boldsymbol{h}_{t-1},\boldsymbol{x}_t]+\boldsymbol{b}_o)\\ \boldsymbol{h}_t&=o_t*\tanh(\boldsymbol{C}_t) \end{aligned} \tag{7}$$

式中：$\boldsymbol{x}_t$ 表示时间步 t 的输入；$\boldsymbol{h}_t$ 表示时间步 t 的隐藏状态；$\boldsymbol{h}_{t-1}$、$\boldsymbol{C}_{t-1}$ 分别表示前一个时间步的隐藏状态和单元状态；$\tilde{\boldsymbol{C}}_t$ 表示候选的单元状态；i_t、f_t 和 o_t 分别表示输入门、遗忘门和输出门；$\boldsymbol{W}$、$\boldsymbol{b}$ 分别表示权重和偏差；σ 表示门的非线性激活函数，默认为 sigmoid。

2 异常用电模型

为了更好地完成异常用电模式检测，本文提出一种基于 CAEs-LSTM 的用户异常用电模式检测模型，如图 3 所示。该模型通过混合深度学习模型找出电力数据中潜藏的用电模式，以检测异常用电数据。

2.1 数据集

为了监测消费者的用电行为，配电公司每天定期记录实际日负荷数据。电力盗窃数据属于敏感数据，本文所使用的数据集是来自国家电网(SGCC)发布的数据集，数据的采集频率为 1 天 1 次，这些数据已经由国家电网专业人员处理过，包含标记的正常用户和电力窃贼。数据集包含了 42 372 个用户从 2014 年 1 月 1 日至 2016 年 10 月 31 日共 1036 天每

天的能耗统计数据，其中正常用户数量为 38 767，电力窃贼数量为 3615，表 1 给出了数据的元信息。

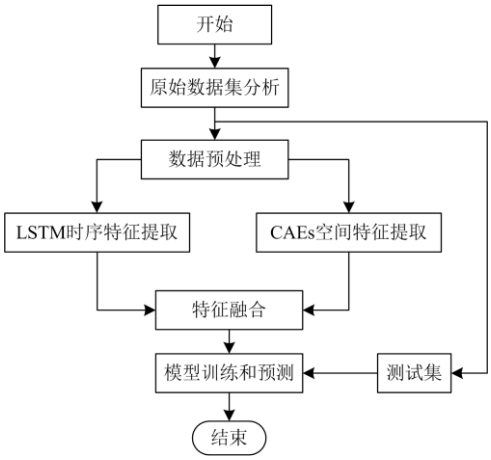


图 3 用户异常用电模式检测流程

Fig. 3 Process of abnormal user power consumption mode detection

表 1 数据集元信息

Table 1 Metadata information

属性	值
数据时间窗	2014 年 1 月 1 日—2016 年 10 月 31 日
消费者总数	42 372
正常用户数量	38 767
电力窃贼数量	3615

通过对数据集进行初步观察，发现正常用户和电力窃贼在日负荷趋势上存在差别，日负荷数据处于不间断的波动中，而正常用户的日负荷数据相对平缓，电力窃贼的日负荷数据波动性比较强，且电力窃贼的能耗值一般比正常用户高出很多，如图 4 所示。

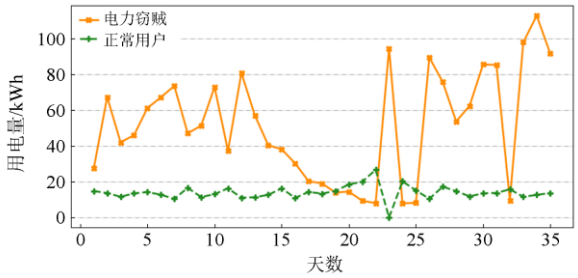


图 4 正常用户和电力窃贼的日负荷数据

Fig. 4 Daily electricity data of normal user and electricity thief

2.2 数据预处理

2.2.1 缺失值处理

由于电表故障、系统不稳定、存储异常及自然因素等原因，数据在采集的过程中往往会丢失，导致数据集中出现大量缺失值。本文所使用的数据中，发现了大量的缺失值以及 0 值，如表 2 所示，缺失率为当前列中所缺失的行数占总行数的比率。经统计，缺失主要集中在列缺失率为 30%~40%，而 0 值主要集中在 0 值占整列行数为 10%~20%的列中。这表明数据缺失程度比较大，因此首先对缺失数据进行处理。

表 2 数据集缺失值和 0 值比例

Table 2 Lack and 0 value ratio in dataset

比率值	缺失列数	0 值列数
≤0.1	304	107
0.1~0.2	0	927
0.2~0.3	146	1
0.3~0.4	421	0
0.4~0.5	161	0
0.5~0.6	1	0

首先考虑缺失值比较多的用户，对于连续缺失天数超过 30 的用户，将其定义为已损坏数据，并删除该用户。对其余的缺失数据，通过基于灰色关联分析的 K 近邻缺失值填补方法进行模型拟合，得到近似的数值进行填补。考虑数据集 $\boldsymbol{D}=\{\boldsymbol{x}_0,\boldsymbol{x}_1,\mathrm{L}\ ,\boldsymbol{x}_n\}$，$\boldsymbol{x}$ 表示某具体用户的日负荷数据实例，每个实例 $\boldsymbol{x}_i$ 有 m 个特征，表示为 $\boldsymbol{x}_i=(\boldsymbol{x}_i(1),\boldsymbol{x}_i(2),\mathrm{L}\ ,\boldsymbol{x}_i(m)), i=0,1,\mathrm{L}\ ,n$，两个特征间的灰色关联系数可表示为

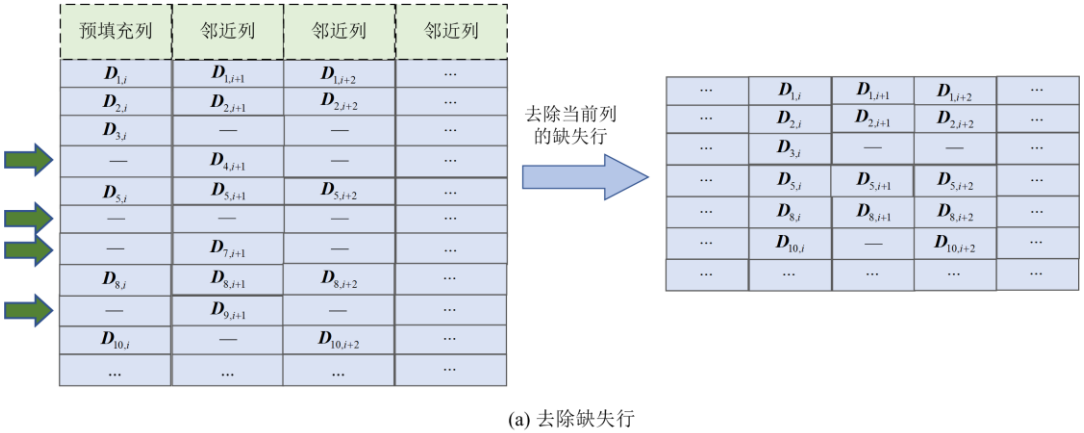
$$GRC(\boldsymbol{x}_0(p),\boldsymbol{x}_i(p))=\frac{\min_{\forall j}\min_{\forall k}|\boldsymbol{x}_0(k)-\boldsymbol{x}_j(k)|+\rho\max_{\forall j}\max_{\forall k}|\boldsymbol{x}_0(k)-\boldsymbol{x}_j(k)|}{|\boldsymbol{x}_0(p)-\boldsymbol{x}_i(p)|+\rho\max_{\forall j}\max_{\forall k}|\boldsymbol{x}_0(k)-\boldsymbol{x}_j(k)|} \tag{8}$$

式中：$i,j=0,1,\mathrm{L}\ ,n$；$k,p=0,1,\mathrm{L}\ ,m$；p 表示具体的一个特征；$x_0(p)$ 表示实例 x_0 中特征 p 处的值。$x_0(p)-x_i(p)$ 项指两个实例 x_0 和 x_i 在特征 p 处取值的差值，其余三项通过求最值过程，遍历所有实例 j 和所有特征 k 并求其和，然后计算这个与参考实例 x_0 间的差值的最小值以及最大值。

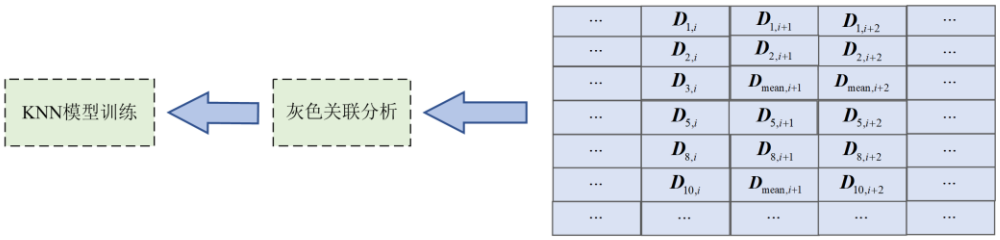
对于要进行填补的某一列，首先去除当前列中带缺失值的行，去掉缺失行后，将剩余行中对应的当前列的列值作为标签，统计当前列相邻前后各 5 列的数据，如果这 5 列数据中仍存在缺失值，则以这些列的列均值取代。实验中存在一种情况：选取的某列全部都为缺失值，此时通过原始未处理数据的列均值来取代这些缺失值。

对提取的 10 列数据进行灰色关联分析，得到灰色关联矩阵，对关联矩阵中的关联系数由大到小排

序，并记录列索引。排序的前 5 列为与填补列相关性最高的特征，将这 5 列作为 K 近邻模型的输入。



(a) 去除缺失行



(b) 灰色关联分析和K近邻模型拟合

图 5 缺失值填补流程

Fig. 5 Process of missing value imputation

2.2.2 异常值处理

对于电力能耗数据，在部分情况下会出现偏离正常趋势的较大或较小值，这些对应于实际生活中的特定假日，比如在春节等节日，用电量会迅速提高，形成远离序列一般水平的极端大值和极端小值，即离群点。离群点会降低模型的泛化性能，对于这类值，本文采用三西格玛经验法则进行调整，可表示为

$$f(x_i)=\begin{cases}\text{avg}(x)+2\cdot\text{std}(x), & x_i>\text{avg}(x)+2\cdot\text{std}(x)\\ x_i, & \text{其他}\end{cases} \tag{9}$$

式中，$\text{avg}(x)$ 和 $\text{std}(x)$ 分别表示当前列中日负荷数据的均值和标准差。

2.2.3 数据归一化

由于神经网络对不同的数据比较敏感，需要对数据进行归一化。常用的归一化方法是最小−最大归一化，可表示为

$$f(x_j)=\frac{x_j-\min(x)}{\max(x)-\min(x)} \tag{10}$$

式中，$\min(x)$ 和 $\max(x)$ 分别表示当前列中日负荷数据的最小值和最大值。

归一化后，随机取部分正常用户和电力窃贼 35 天的数据进行分析，如图 6 所示，可以明显的看到，电力窃贼的负荷数据波动性非常突出。

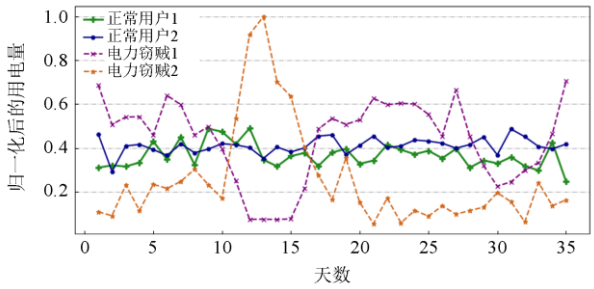


图 6 归一化后正常用户和电力窃贼的用电趋势图

Fig. 6 Daily electricity data of normal users and electricity thieves after normalization

2.3 基于 CAEs-LSTM 的混合模型

在本文中，卷积自编码器和长短期记忆网络被组合起来进行分类检测，模型结构图如图 7 所示。

通过数据分析得知，正常用户的用电量和窃电者的用电量具有波动差异性。客户的用电量在数据集上表现为一维时间序列，本文将数据处理后得到

的一维负荷数据 $\boldsymbol{x}=[x_1,x_2,\mathrm{L}\ ,x_{1036}]$ 共 1036 维，作为 LSTM 网络的输入。本文选择单层的 LSTM 进行特征提取，通过 LSTM 学习全局电力数据中隐含的时间特征，最后得到 $\boldsymbol{y}=[y_1,y_2,\mathrm{L}\ ,y_{64}]$，共 64 维的输出。

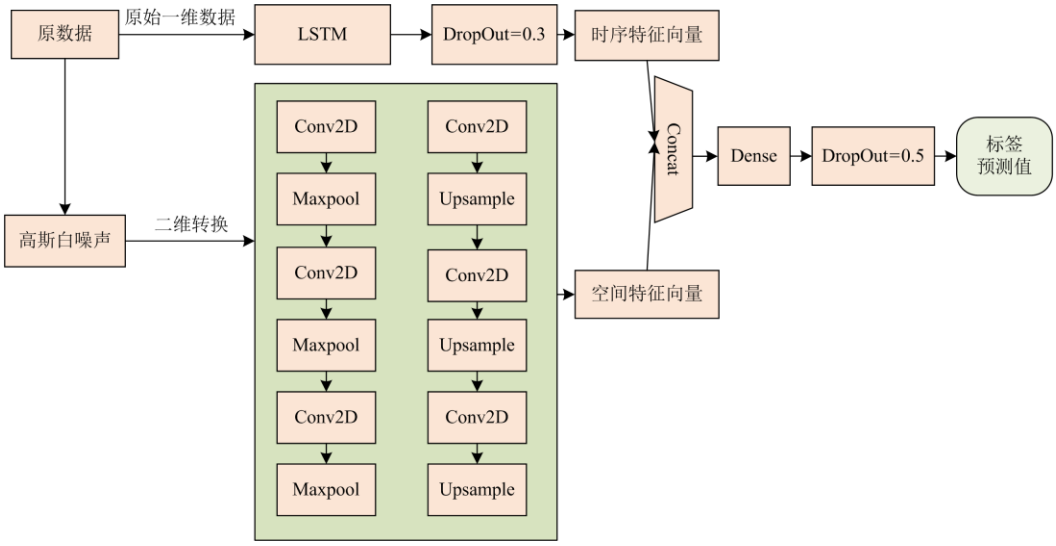


图 7　CAEs-LSTM 混合模型结构

Fig. 7 Hybrid structure of CAEs-LSTM

用户用电数据隐藏着周期性的规律，为了更好地探索和利用用户日负荷数据的周期性和空间特性，本文采用卷积形式的自动编码器。将原始一维电力负荷数据进行二维转换，作为卷积自编码器的输入。为了提高卷积自编码器的泛化性能和鲁棒性，在输入的数据中加入高斯白噪声。

对于用户 t，总计数据为 n 天的用电量，其第 i 天的用电量为 $\boldsymbol{x}_i, i=1,2,\mathrm{L}\ ,n$，对于 $\boldsymbol{x}_i$，有 $\boldsymbol{x}_{\mathrm{inoise}}=\boldsymbol{x}_i+\boldsymbol{x}_{\mathrm{random}}$，其中 $\boldsymbol{x}_{\mathrm{random}}$ 是均值为 0，标准差为 0.3 的高斯白噪声。本文将用电量数据 $\boldsymbol{x}_i$ 转化为维度为 7 的矩阵，作为卷积自编码器层中 2D 卷积层的输入。

在编码阶段，卷积自编码器模型由三层的 2D 卷积层构成，在每个卷积层后面都紧跟着池化层。第一层为一个 16 核，步长 3×3 的卷积层，为了尽量避免降采样中特征丢失，本文选取步长为 2 的池化层，第二层和第三层均为一个 8 核，步长 3×3 的卷积层，衔接一个步长为 2 的池化层。编码部分的卷积池化结构及参数设置如图 8 所示。本文采用 Relu 激活函数，最终将重构的特征平展并连接到 64 个节点的全连接层。

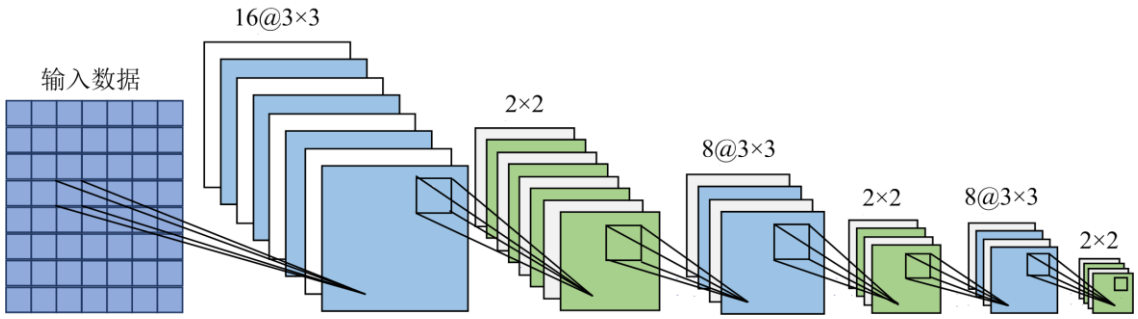


图 8　卷积自编码器编码结构

Fig. 8 Structure of the encoding section of CAEs

在解码阶段，通过与之对称的卷积层和上采样层完成。通过卷积自编码器获取从二维用电数据重构的空间特征。最后，分别将获取的空间和时间特征进行融合。为了均衡融合提取的时序特征和空间特征，本文将卷积自编码器重构的特征连接到一个可变数神经元的全连接层上，神经元的数量和 LSTM 的隐藏单元数保持一致。由此得到数据深层次的隐含特征，用于分类检测。本文使用二进制交叉熵损

失函数计算当前模型的损失偏差程度，可表示为

$$L_{\text{oss}} = -\frac{1}{N}\sum_{i=1}^{N} y_{\text{true}} \cdot \log y_{\text{pre}} + (1-y_{\text{true}}) \cdot \log(1-y_{\text{pre}}) \quad (11)$$

式中：N 表示用户数量；y_{true} 为样本真实标签；y_{pre} 为分类结果。模型参数优化采用随机梯度下降算法进行训练得到最优结果。

2.4 评价指标

2.4.1 AUC

AUC 在机器学习领域中是一种模型评估指标，常用于评价分类的准确性。AUC 被定义为 ROC 曲线下与坐标轴围成的面积，而 ROC 曲线有一个很好的特性：当测试集中的正负样本分布发生变化，ROC 曲线可以保持不变。在实际应用中，经常会出现数据集类别不平衡现象，而 ROC 曲线基本可以保持在类别均衡时绘制的曲线原貌。因此，AUC 非常适用于本实验的性能指标。

AUC 值等于随机选择的阳性样本排名高于随机选择的阴性样本的概率，其值越大表示性能越好。其计算公式为

$$A_{\text{UC}} = \frac{\sum_{ins_i \in \text{positiveclass}} r_{\text{ank}ins_i} - \dfrac{M \times (M+1)}{2}}{M \times N} \quad (12)$$

式中：$r_{\text{ank}ins_i}$ 表示第 i 条样本的序号(概率得分从小到大排，排在第 $rank$ 个位置)；M、N 分别是正样本和负样本的个数；$\sum_{ins_i \in \text{positiveclass}}$ 表示只把正样本的序号加起来。

2.4.2 MAP

本文使用平均精度来衡量信息检索的有效性。它是根据预测得分对测试集的标签进行排序，然后选择从上往下的前 K 个标签来评估性能，可表示为

$$MAP@K = \frac{\sum_{i=1}^{n} r_i}{n} \quad (13)$$

式中：n 表示按照预测得分排序后的前 K 个用户中电力窃贼的数量；$r_i, i = 1,2,\text{L}\ ,n$ 为电力窃贼在排序中的位置信息。

3 实验与结果分析

本节通过实验仿真，验证本文所提出的 CAEs-LSTM 模型的有效性。实验是在小型服务器上使用 Python 3.7 实现的，基于 Keras 实现了卷积自编码器和长短期记忆网络融合的结构。

3.1 性能验证

为了验证本文提出方法的性能，将其与支持向量机、LSTM 和宽深度卷积模型[22]进行比较。

支持向量机：SVM 通过找到最优的分离超平面，将非线性分离问题转化为线性分离问题。它常被作为一个后续处理方案，应用于基于人类知识和专业知识的欺诈行为检测。

LSTM：基于在处理时间序列数据上的优秀能力及其可记忆的特点，LSTM 常被用于作为入侵检测系统的基础架构。

宽深度卷积模型(wide_deep_ CNN)：基于文献[24]所提出的宽深度卷积模型，在处理电力数据集上有非常好的效果。

表 3 为本文仿真实验的参数设置情况。

表 3 对比实验参数设置

Table 3 Comparison of experiment parameter setting

方法	输入数据格式	参数
SVM	原始 1 维数据	内核函数的 GINI 参数 (RBF)：0.0005
LSTM	原始 1 维数据	隐藏层单元：64
wide_deep_ CNN	2 维特征图	卷积层：3×3 最大池化层：3×3 全连接层单元：64

本文划分了不同的训练比来进行实验，表 4 为提出的 CAEs-LSTM 模型与其他检测方案的性能比较。本文分别进行了训练数据比例为 50%、60%、70%和 80%的 4 组实验，并记录了 AUC 以及 MAP@100 和 MAP@200 的值。

表 4 CAEs-LSTM 模型与其他方案的性能比较

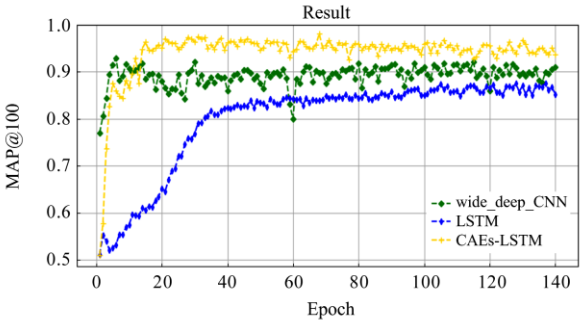
Table 4 Performance comparison of CAEs-LSTM model and other schedules

模型	0.5			0.6			0.7			0.8		
	AUC	MAP@100	MAP@200	AUC	MAP@100	MAP@200	AUC	MAP@100	MAP@200	AUC	MAP@100	MAP@200
SVM	0.6943	0.6562	0.5588	0.7109	0.6877	0.5761	0.6998	0.6911	0.5701	0.7234	0.7191	0.5907
wide_deep_ CNN	0.7626	0.9321	0.9090	0.7723	0.9281	0.8979	0.7764	0.9287	0.8971	0.7813	0.9428	0.9051
LSTM	0.7469	0.9010	0.8701	0.7560	0.8752	0.8501	0.7548	0.8752	0.8501	0.7603	0.8863	0.8633
CAEs-LSTM	0.7728	0.9849	0.9499	0.7829	0.9801	0.9491	0.7899	0.9829	0.9533	0.7911	0.9737	0.9271

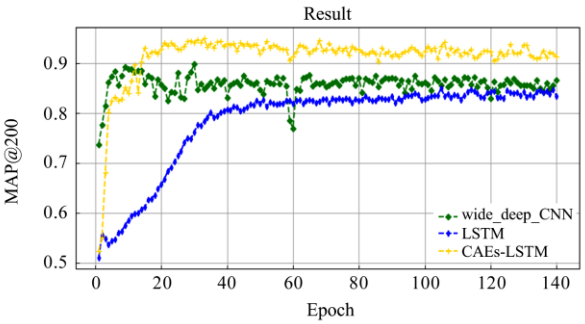
从表 4 可以看出，本文提出的模型在 3 组指标中均优于 SVM、LSTM 以及宽深度卷积模型。特别需要指出，当训练比为 60%时，AUC 指标达到 78%，MAP 指标达到 98%，这表明 CAEs-LSTM 模型的稳

定性更好。

MAP 指标的迭代结果如图 9 所示，结果表明，相比于其他模型，本文提出的模型达到峰值所需要的迭代次数更少。



(a) MAP@100



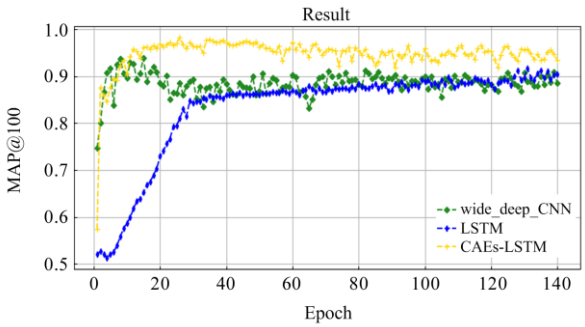
(b) MAP@200

图 9　60%训练比下 MAP 测试结果对比

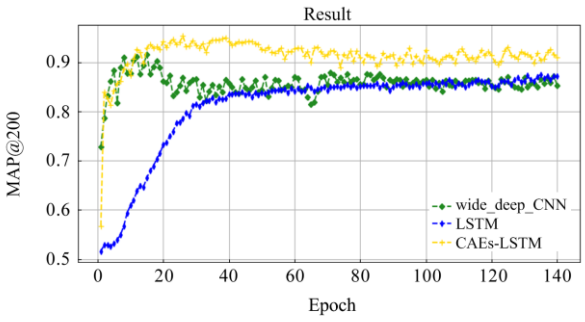
Fig. 9 Comparison of MAP with 60% training ratio

当训练比为 60%时，本文模型相较于 LSTM，AUC 值提高近 2.5%，MAP@100 和 MAP@200 值分别提高将近 11.5%和 10%；相较于宽深度卷积模型，AUC 值提高 1%左右，MAP@100 和 MAP@200 值分别提高将近 6%和 5%。因此，该模型具有更高的检测精度。本文还在多个训练比下进行了实验，如图 10 所示。

结果表明，在不同的训练比下，本文提出的模型都有稳定的结果。



(a) MAP@100



(b) MAP@200

图 10　70%训练比下 MAP 测试结果对比

Fig. 10 Comparison of MAP with 70% training ratio

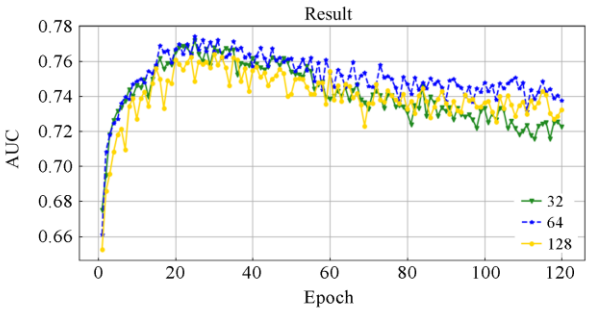
3.2　参数调优

为了使本文提出模型达到更好的效果，对模型中的部分参数进行了优化，并在此节给出了调参的结果。

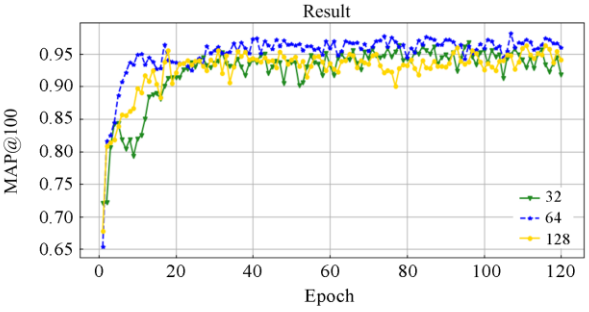
3.2.1 LSTM 节点数

LSTM 的节点数代表隐藏层的神经元个数，也代表输出层的维度，它决定参数量的大小。网格搜索对于大批次数据训练往往会存在训练时间长、延时以及误差等问题，本文应用常规的节点个数设置，分别测试了单元数为 32、64 和 128 的情形，如图 11 所示。

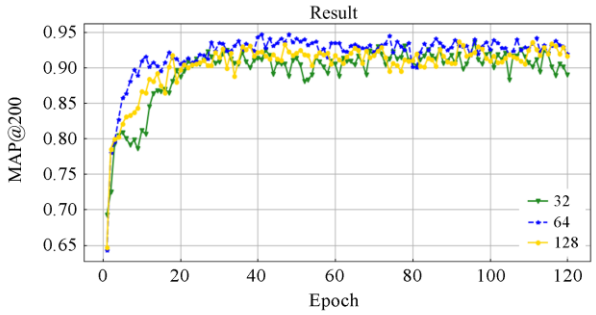
在训练比为 60%的情形下进行实验，结果表明，隐藏层神经元数为 64 时达到较优的结果。



(a) AUC



(b) MAP@100



(c) MAP@200

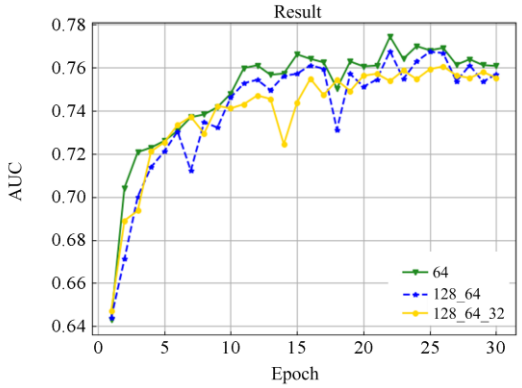
图 11 LSTM 节点数的影响

Fig. 11 Influence of LSTM neuron number

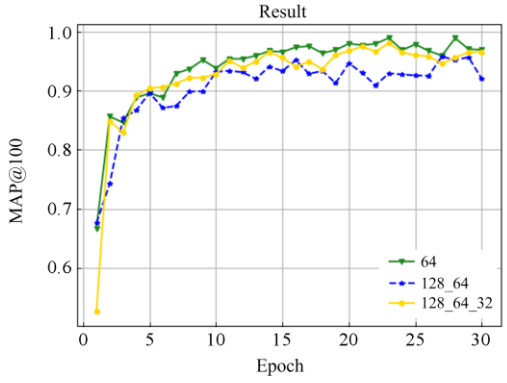
3.2.2 LSTM 层数

LSTM 的层数对实验性能有较大的影响，对时序数据额外的处理是非常耗时的。实验中使用了常用的 LSTM 参数设置，得到结果的如图 12 所示。

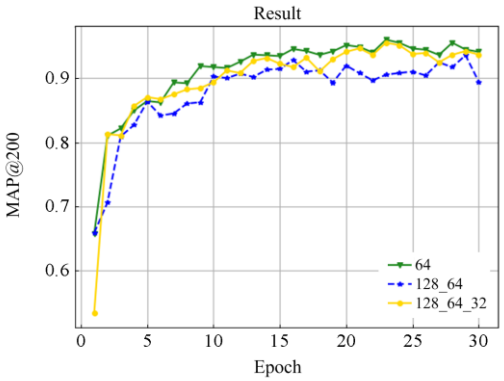
结果表明，过量的叠加层数反而会弱化模型效果，导致拟合性能变差。造成上述结果的原因是层数叠加致使参数冗余，导致过拟合，此时性能也会降低。因此，选择单层的 LSTM 能取得最好的效果。



(a) AUC



(b) MAP@100



(c) MAP@200

图 12 LSTM 层数的影响

Fig. 12 Influence of LSTM layers

4 结语

本文提出了一种 CAEs-LSTM 模型来检测智能电网中的窃电行为，并在国家电网公布的真实数据集上进行了实验。在缺失值处理阶段，本文引入了基于灰色关联分析的 K 近邻模型拟合方法，寻求最优的拟合值作为填补。真实数据集中通常带有一些不可避免的噪声，本文在训练阶段加入了高斯白噪声，以提高模型泛化、抗噪能力以及鲁棒性。所提出的 CAEs-LSTM 模型在窃电检测领域中是一项比较先进的方法，它具有以下两个特性：一是混合模型可以自动提取特征，而其他大多数传统分类器的成功很大程度上依赖于手工设计的特征；二是混合模型结合了 CAEs 和 LSTM 的优点，融合的特征能较好地表征数据集的特点，因此在窃电检测的数据集上能表现出非常好的效果，本文的模型还可用于计算机视觉领域。

参考文献

[1] BISWAL M, DASH P K. Measurement and classification of simultaneous power signal patterns with an S-transform variant and fuzzy decision tree[J]. IEEE Transactions on Industrial Informatics, 2012, 9(4): 1819-1827.

[2] GLAUNER P, MEIRA J A, VALTCHEV P, et al. The challenge of non-technical loss detection using artificial intelligence: a survey[J]. arXiv preprint arXiv: 1606.00626, 2016.

[3] MISHRA S K, TRIPATHY L N. A critical fault detection analysis & fault time in a UPFC transmission line[J]. Protection and Control of Modern Power Systems, 2019, 4(1): 24-33.

[4] ANGELOS E W S, SAAVEDRA O R, CORTÉS O A C, et al. Detection and identification of abnormalities in customer consumptions in power distribution systems[J]. IEEE Transactions on Power Delivery, 2011, 26(4):

2436-2442.
[5] 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.
[6] KOSEK A M. Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model[C] // 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), April 12-13, 2016, Vienna, Austria: 1-6.
[7] JIANG R, LU R, WANG Y, et al. Energy-theft detection issues for advanced metering infrastructure in smart grid[J]. Tsinghua Science and Technology, 2014, 19(2): 105-120.
[8] 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.
[9] 李清. 基于改进 PSO-PFCM 聚类算法的电力大数据异常检测方法[J]. 电力系统保护与控制, 2021, 49(18): 161-166.
LI Qing. Power big data anomaly detection method based on an improved PSO-PFCM clustering algorithm[J]. Power System Protection and Control, 2021, 49(18): 161-166.
[10] 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, 2009, 25(2): 1162-1171.
[11] DEPURU S S S R, WANG L, DEVABHAKTUNI V. Support vector machine based data classification for detection of electricity theft[C] // 2011 IEEE/PES Power Systems Conference and Exposition, March 20-23, 2011, Phoenix, AZ, USA: 1-8.
[12] NAGI J, YAP K S, TIONG S K, 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.
[13] ESMALIFALAK M, LIU L, NGUYEN N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2014, 11(3): 1644-1652.
[14] ALVES H, BRETAS A S, BRETAS N G. Smart grids cyber-attack defense: a solution based on an incremental learning support vector machine[C] // 2019 North American Power Symposium (NAPS), October 13-15, 2019, Wichita, KS, USA.
[15] JOKAR P, ARIANPOO N, LEUNG V C M. Electricity theft detection in AMI using customers' consumption patterns[J]. IEEE Transactions on Smart Grid, 2015, 7(1): 216-226.
[16] 陈刚, 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.
[17] KOCAMAN B, TÜMEN V. Detection of electricity theft using data processing and LSTM method in distribution systems[J]. Sādhanā, 2020, 45(1): 1-10.
[18] ADIL M, JAVAID N, QASIM U, et al. LSTM and bat-based RUSBoost approach for electricity theft detection[J]. Applied Sciences, 2020, 10(12).
[19] TIAN C, MA J, ZHANG C, et al. A deep neural network model for short-term load forecast based on long short-term memory network and convolutional neural network[J]. Energies, 2018, 11(12).
[20] MUNAWAR S, ASIF M, KABIR B, et al. Electricity theft detection in smart meters using a hybrid bi-directional GRU bi-directional LSTM model[C] // Conference on Complex, Intelligent, and Software Intensive Systems, 2021, Springer, Cham: 297-308.
[21] LI S, HAN Y, 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.
[22] 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, 2017, 14(4): 1606-1615.
[23] HASAN M, 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).
[24] COLAK I, SAGIROGLU S, FULLI G, et al. A survey on the critical issues in smart grid technologies[J]. Renewable and Sustainable Energy Reviews, 2016, 54: 396-405.
[25] CHANG Z, ZHANG Y, CHEN W. Electricity price prediction based on hybrid model of Adam optimized LSTM neural network and wavelet transform[J]. Energy, 2019, 187.
[26] LE T, VO M T, VO B, et al. Improving electric energy consumption prediction using CNN and Bi-LSTM[J]. Applied Sciences, 2019, 9(20).

收稿日期：2021-12-04；　修回日期：2022-02-27

作者简介：

董立红(1968—)，女，博士，教授，主要研究方向为智慧矿山建设顶层设计及大数据、工业互联网等新技术在煤矿电力中的应用；E-mail: 1430315357@qq.com

肖纯朗(1997—)，男，通信作者，硕士，主要研究方向为电力系统安全，深度学习和异常检测。E-mail: 2867836467@qq.com

（编辑　许　威）