Electricity theft Detection with Borderline-SMOTE and WDCBL in the Smart Grid

Tao Liu[1], Honghao Liang[1], Xiaowei Chen[1], Jiahao Qi[2], Yihong Guo[2], and Yueming Lu[2*]

[1]Shenzhen Power Supply Co., Ltd, Shenzhen, China
[2]Beijing University of Posts and Telecommunications Beijing, China

Received: April 1, 2022; Accepted: June 24, 2022; Published: July 15, 2022

Abstract

The non-technical loss caused by electricity theft on the user side not only increases the operation cost of the smart grid but also causes some harm to the electricity system. At present, the existing electricity theft detection model ignores the time-series correlation of user power consumption data, and the distribution of positive and negative samples in the relevant data sets is uneven. Aiming at the existing problems, we propose an electricity theft detection model based on Borderline-SMOTE and WDCBL(wide and deep CBL) networks. The WDCBL model consists of wide components and deep CBL components. The wide part uses a fully connected layer to extract one-dimensional features in user electricity consumption data. The model introduces the hybrid network model of a one-dimensional convolutional neural network(CNN) and bidirectional long-term and short-term memory network(BiLSTM) into the deep part, which can learn both spatial and temporal features in user electricity consumption data. Finally, we conducted a comparative experiment on the user electricity consumption data published by SGCC. The results show that our model is superior to others in the comprehensive performance.

Keywords: CNN, BiLSTM, Neural Network, Electricity theft Detection, Smart Grids

1 Introduction

With the maturity and wide application of technologies related to the Internet of Things and Big Data, the degree of informatization of power system equipment has been continuously improved, and smart grids have gradually become popular. The power distribution data has good measurement and monitoring conditions, and the data volume and types are growing rapidly, but at the same time, a new terminal power theft carrier has been introduced [1]. Electricity theft has also gradually turned into high-tech electricity theft, showing the characteristics of diversification and concealment [2]. How to detect the user's electricity consumption status in real-time, accurately identify and locate electricity stealing behaviors, and maintain electricity order and grid security have become crucial issues.

In recent years, algorithms such as data mining and machine learning have achieved remarkable results in target classification and identification, abnormal behavior detection, and rich research and applications have also been born in electricity theft detection. Hasan MN et al. [3] proposed a power theft detection system based on a convolutional neural network (CNN) and long short-term memory (LSTM) architecture. This method combined LSTM to optimize the feature extraction of power consumption time series data, and designed a new data preprocessing method to solve the problem of the imbalanced

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 8, Article No. 5 (July 15, 2022)
DOI:*10.22667/ReBiCTE.2022.07.15.005*

[*]Corresponding author: Beijing University of Posts and Telecommunications Beijing, 100876, China, Email: ymlu@bupt.edu.cn

dataset; Chen Z et al. [4] proposed a new deep bidirectional recurrent neural network. Network (ETD-DBRNN) electricity theft detection method, which can extract internal features and external correlations by learning power consumption records and influencing factor representations. The comparison analysis of actual data proves that this scheme has higher recognition. Hu W et al. [5] proposed to identify electricity theft behavior through multi-source data. In addition to user electricity consumption, the scheme also combined equipment regional and climate factors to analyze user behavior. They built a hierarchical electricity theft identification model. This work has been applied in practical enterprises; CHAO Z et al. [6] proposed a scheme of electricity theft detection based on SMOTE and XGBoost. By using the SMOTE algorithm oversampling, the problem of data imbalance has been solved. XGBoost data feature extraction and classification. Experiments show that the model has good performance in solving the problem of unbalanced data classification; Cai J et al. [7] used a dense convolutional neural network (DenseNet) to automatically extract features from large-scale smart meter data sets, combined with random forest (RF) to train classifiers and used grid search algorithm to determine the optimal parameters. To detect whether the user steals electricity, the experiment proves that the model has higher recognition accuracy and generalization characteristics. Liu Y et al. [8] improved the RNN network into a parallelized network, fragmented the input feature vectors of long-term sequences, and overcome the shortcomings of information loss in the RNN network when processing long sequences. Simulation experiments show that, under the same time complexity, the comprehensive performance of this method is significantly improved compared with the traditional RNN; Xiao D et al. [9] proposed a power theft detection model based on multiple heads' attention mechanism. The model is based on a bi-directional gated recurrent neural network, which extracts data temporal features, introduces a multi-head attention mechanism, increases the depth of the model, and optimizes the extraction ability of common features. It performs well on the customer electricity consumption data set.

In summary, the current machine learning algorithm research on electricity stealing has a rich research foundation, but problems such as time series feature extraction and data imbalance still affect the accuracy of the model. We propose a new electricity theft detection model, which combines Borderline-SMOTE and WDCBL (wide and deep CBL) to further optimize the above problems and improve the comprehensive performance of the model.

2 Electric theft detection model based on Wide and Deep CBL network

2.1 CNN and BiLSTM

The good learning ability of convolutional neural networks and long-term and short-term neural networks makes them widely used in image recognition, machine translation, automatic driving, and other fields. Some researchers [10] have introduced them into the field of electricity theft detection and achieved good results.

CNN is usually composed of a convolution layer, pooling layer, and full connection layer, which has the characteristics of local connection and weight sharing. The function of the convolution layer is to extract features, and the pooling layer is used to further filter features to reduce the number of parameters. The traditional convolutional network uses a two-dimensional convolution kernel, which can effectively extract two-dimensional image features, but it is not ideal for serialized data processing. Given this, literature [11] pointed out that one-dimensional CNN is used to process serialized temporal data, so this paper uses a one-dimensional convolutional neural network to extract spatial features in the data.

The traditional recurrent neural network often uses the logistic nonlinear activation function for cyclic learning. Since the derivative value of the logistic function is between 0 and 1, when the time interval is large, it is easy to make the gradient tend to 0 or become very large, resulting in a Vanishing gradient or exploding gradient problem. The Long Short-Term Memory Neural Network (LSTM) [12] is proposed to solve the gradient vanishing problem of the traditional Recurrent Neural Network (RNN). Its basic unit is a structure containing multiple groups of neurons, called cells, as shown in Fig. 1 shown. The three control gates f , i , and o are respectively called the forgetting gate, the input gate, and the

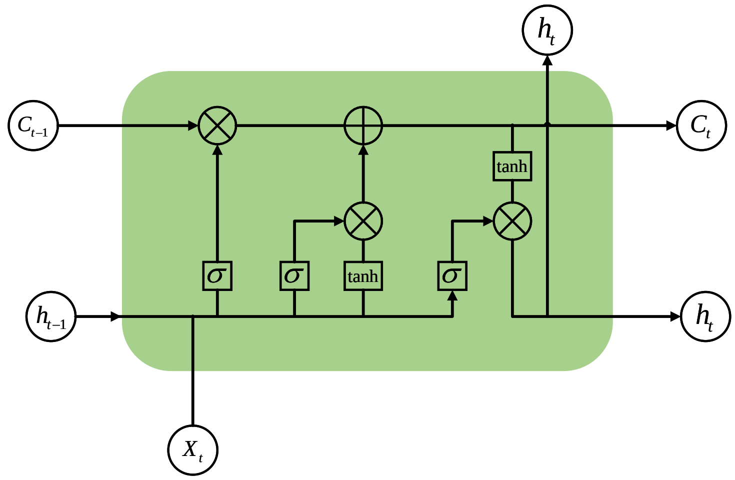

Figure 1: The basic unit of LSTM

output gate. By setting the parameters of the three control gates reasonably, the memory function of LSTM can be realized. The core calculation formula is as follows.

$$f_t = (W_f \cdot [h_{t-1}, x_t] + b_f) \tag{1}$$

$$i_t = \tanh(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{2}$$

$$c_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \tag{3}$$

$$c_t = f_t * c_{t-1} + i_t * c_t o_t = W_o(h_{t-1}, x_t) + b_o \tag{4}$$

$$h_t = o_t * \tanh(c_t) \tag{5}$$

Among them, f, i, t, o, h, c, W, b represent forgetting, input, time step, output layer, hidden layer, unit state, weight matrix, and bias, respectively. LSTM extracts timing information from one direction, but for timing prediction, the current state of the network may be related to both past and future states. To improve the prediction effect, a bidirectional long and short-term memory network (BiLSTM) is introduced to better extract the hidden time series features from the data.

The output of BiLSTM is jointly determined by two LSTM layers. The forward LSTM layer can be regarded as a forward calculation from the start time to the last time, and the reverse LSTM layer can be regarded as a reverse calculation from the last time to the start time. The calculation process is handled in the same way. Finally, the outputs of the forward layer and the reverse layer at each moment are combined to obtain the output at that moment.

2.2 Wide and Deep CBL Framework

The Wide and Deep CBL framework mainly consists of two major components: the wide component and the deep CBL component. As shown in Fig. 2, We then explain them in detail as follows.

The wide component is mainly composed of a fully connected layer with 1034 hidden units, which can learn global knowledge from 1-D electricity consumption data. Motivated by the previous study [13], We use wide components to process one-dimensional time series power consumption data, and extract common features that frequently appear in time series data.

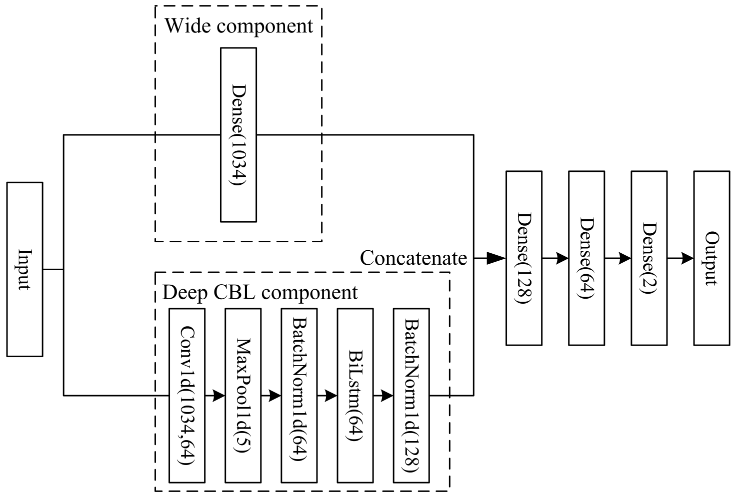

Figure 2: wide and deep CBL framework

The deep CBL component is mainly composed of a one-dimensional convolutional neural network and a bidirectional long and short-term neural network. CNN and BiLSTM have excellent characteristics in data feature extraction, so this paper adopts a hybrid model composed of a one-dimensional convolutional neural network and bidirectional long-term and short-term neural network, referred to as the deep CBL model. Deep CBL Component can not only extract the spatial features of the user's electricity data sequence through a one-dimensional convolutional neural network but also learn the forward and backward time series data through the BiLSTM layer. The MaxPool layer can amplify the features extracted by the model and discretize the parameters, thereby reducing training time and preventing overfitting. The BatchNorm layer after the MaxPool layer can normalize the parameters of the middle layer to speed up the training speed for the subsequent calculations.

Finally, the features extracted from WDCBL components are combined by cascading and used as the input of the final full connection layer to calculate the overall model output.

3 Dataset selection and processing

The selection and preprocessing part of the dataset is mainly divided into three parts, the first part is the selection of the dataset, the second part is the data preprocessing stage, and the third part is the imbalance processing of the dataset. The specific processing flow and algorithm are shown in Fig. 3.

3.1 Data selection

In this paper, we experiment on an electricity consumption dataset, which was publicly released by SGCC (the State Grid Corporation of China). This dataset contains electricity consumption data of 42,372 electricity customers in 1035 days (from January 1, 2014, to October 31, 2016). The data contains a label for whether the user has been stealing electricity. A total of 42 372 valid records were obtained after data preprocessing. Each valid record contains the following fields: customer number, electricity stealing (1 electricity stealing, 0 non-stealing electricity), and electricity consumption data for 1 034 d (in kWh). Table 1 lists the details of the preprocessed datasets used to train the model.

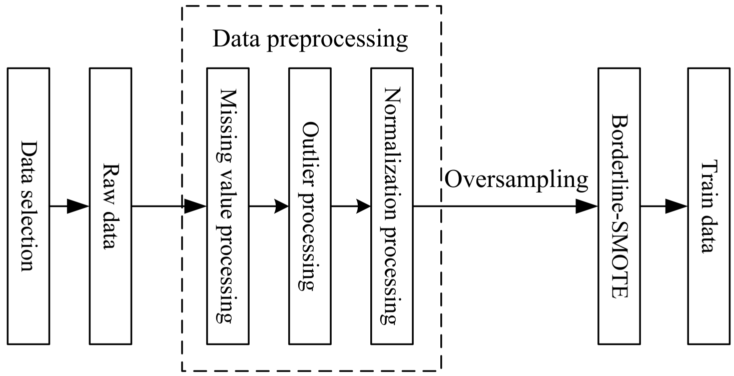

Figure 3: Dataset selection and processing

Table 1: Dataset details

	SGCC
Number of samples	42372
Number of normal samples	38757
Number of abnormal samples	3615

3.2 Data Preprocessing

Due to the failure of smart meters and unreliable transmission of measurement data, users' electricity consumption data often contain missing or erroneous values. The basic steps of preprocessing include missing value processing, outlier processing, and normalization processing.

1) Missing value processing: we use the interpolation method to recover the missing values according to the following equation [14]:

$$f(x_t) = \begin{cases} \frac{x_{t-1}+x_{t+1}}{2}, & \text{if } x_t \in NAN, x_{t-1} \text{ and } x_{t+1} \notin NAN \\ 0, & \text{if } x_t \in NAN, x_{t-1} \text{ or } x_{t+1} \in NAN \\ x_t, & \text{if } x_t \notin NAN \end{cases} \tag{6}$$

If the first value of the sequence and the last value are NAN, we set this value to 0.

2) Outlier processing: In the process of processing the data, we found that there are outliers in the user's electricity consumption data. In particular, we restore the value by the following equation according to the "Three-sigma rule of thumb" [15].

$$f(x_i) = \begin{cases} \operatorname{avg}(\mathbf{x}) + 2 \cdot \operatorname{std}(\mathbf{x}) & \text{if } x_i > \operatorname{avg}(\mathbf{x}) + 2 \cdot \operatorname{std}(\mathbf{x}) \\ x_i & \text{otherwise} \end{cases} \tag{7}$$

where, avg() and std() are used to calculate the mean and standard deviation of the series x, respectively.

3) Normalization: to reduce the influence of different attribute value ranges in the data on the calculation, we use formula (8) to process the data.

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

where min(x) is the minimum value in x, and max(x) is the maximum value in x.

3.3 Imbalance handling

As can be seen from Table 1, only 3,615 (8.5%) users were identified as electricity theft by professionals. The samples in the dataset have a serious imbalance problem, which may lead to a low detection rate of the classifier for the minority class samples. In this paper, we decided to introduce the Borderline-SMOTE algorithm [16] to oversample the data, which is proposed based on the SMOTE algorithm [17]. The Borderline-SMOTE algorithm takes into account the importance of boundary data points. First, it determines the boundary samples of the minority class according to the rules and then uses the SMOTE algorithm to generate new samples for the boundary samples.

Suppose S is the sample set, $S_{\min}$ is the minority sample set, $S_{\max j}$ is the adjacent majority sample set, m is the number of adjacent samples, x_i is all the attributes of the sample, x_{ij} is all the attributes of the adjacent samples, x_n is the adjacent samples, R_{ij} takes 0.5 or 1, the synthesis algorithm steps are as follows[16]:

1) Assuming that each $x_i \in S_{\min}$, determine the sample set closest to it, its data set is S_{NN}, and $S_{\mathrm{NN}} \in S$.

2) For each sample x_i, determine the number of nearest neighbors belonging to the majority sample set, namely $|S_{\mathrm{NN}} \cap S_{\max}|$.

3) The selection conforms to: $x_i : x_i {:} \frac{m}{2} < \left| S_{\mathrm{NN}} \cap S_{\mathrm{maxj}} \right| < m$; Synthesize the samples of the minority class. That is, the difference between x_i and the adjacent attribute j corresponding to x_n is recorded as $d_{ij} = x_i - x_{ij}$. Obtain a synthetic new minority class sample $h_{ij} = x_i + d_{ij} \times \operatorname{rand}(0, R_{ij})$.

Table 2: Dataset details after Borderline-SMOTE oversampling

	SGCC
Number of samples	77514
Number of normal samples	38757
Number of abnormal samples	38757

Table 2 shows the result of the number of samples in the dataset after Borderline-SMOTE oversampling.Through the Borderline-SMOTE algorithm, the distribution of the original data can be approximately learned, so that the synthetic data can be as close as possible to the characteristics of the real data. As shown in Table 2, after using SMTOE smoothing, the distribution of the two categories is uniform, and the number of ordinary users and electricity stealing users is equal. The problem of data imbalance is solved, and the bias of classification detection will not appear in the subsequent model training.

4 Experimental Results

4.1 Experimental Settings

To evaluate the proposed model, we conduct the simulations on a 64-bit computer with an Intel Core i7-6700 3.40-GHz CPU and 16-GB RAM. We use the Pytorch deep learning framework and use the scikit-learn machine learning framework for programming and experimentation. The specific model parameter settings are shown in Table 3.

Table 3: Model parameter settings

Hyperparameters	Value
BatchSize	128
Epoches	40
LearningRate	0.001
KernelSize	1034
LstmHiddenSize	64
DropoutValue	0.5
Optimizer	Adam
LossFunction	CrossEntropyLoss

4.2 Performance Metrics

As a way to evaluate the performance of the model, the confusion matrix is often used to evaluate many binary classification problems including electricity stealing detection. The confusion matrix in Table 4 includes all possible classification results in the binary classification problem, where the columns represent the actual category, and the row represents the predicted category. In this paper, to evaluate the performance of the model, we use accuracy, precision, recall, and F1-Score as performance evaluation metrics. The definitions of various indicators are as follows. In the mid-term, TP represents the correctly classified positive samples, FP represents the wrongly classified negative samples, TN represents the correctly classified negative samples, and FN represents the wrongly classified negative samples.

Accuracy: indicating the proportion of correctly classified samples in the total sample

Table 4: Confusion matrix

	Classification result	
Label Attributes	Normal	Abnormal
Normal	TN	FP
Abnormal	FN	TP

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

Precision: indicating the proportion of correctly classified positive samples to all positive samples

$$\text{P} = \frac{TP}{TP+FP} \tag{10}$$

Recall: Indicates the proportion of correctly classified positive samples in all positive samples

$$\text{R} = \frac{\text{TP}}{\text{TP}+FN} \tag{11}$$

F1-Score: A harmonic mean for precision and recall

$$F1 = \frac{2PR}{P+R} \tag{12}$$

Table 5: Model performance on the raw and transformed datasets

Parameters		Before applying Borderline-SMOTE	After applying Borderline-SMOTE
Precision	Normal user	0.925	0.937
	Theft user	0.389	0.958
Recall	Normal user	0.967	0.96
	Theft user	0.209	0.935
F1-Score	Normal user	0.946	0.948
	Theft user	0.272	0.946
Overall Accuracy		0.902	96.23

4.3 Borderline-SMOTE effect analysis

In the experiment, we set the maximum number of epochs to 40, make statistics on the accuracy of the classification results of the model after each training epoch, and use a control experiment to test the accuracy of data recognition by the system before and after processing with the Borderline-SMOTE algorithm. The classification results after 40 epochs are counted, as shown in Fig. 4.

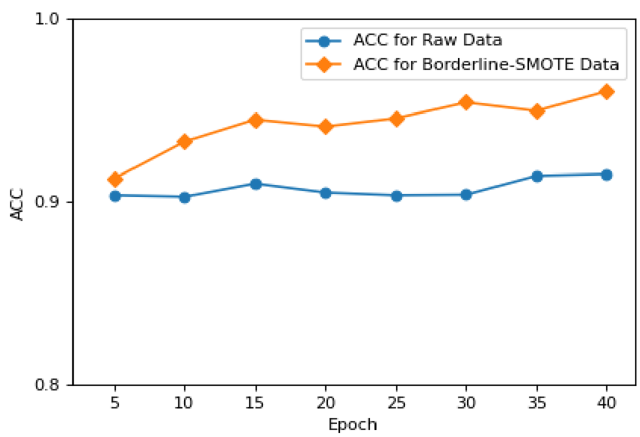

Figure 4: Comparison of model recognition rates before and after oversampling

As can be seen from Fig. 4, as the training continues, the performance of models trained with different data is gradually improving, and the classification accuracy of the model trained with Borderline-SMOTE oversampled data is significantly higher than that of the original dataset training. We can intuitively see that the data after introducing the imbalance processing algorithm has a great effect on the training and performance of the model. Table 5 summarizes the performance parameters in the raw dataset and the transformed dataset after applying Borderline-SMOTE.

4.4 Model Performance Comparison

To further verify the effectiveness of the model proposed in this paper, we compare the model of this scheme with random forest, support vector machine, and traditional logistic regression, and show the results from multiple indicators.

Combining Table 6 and Fig. 5-6, it can be seen that the WDCBL model proposed in this paper

Table 6: Performance comparison of each model

Parameters		WD-CBL	RF	SVM	LR
Precision	Normal user	0.937	0.883	0.911	0.688
	Theft user	0.958	0.899	0.879	0.734
Recall	Normal user	0.96	0.901	0.895	0.764
	Theft user	0.935	0.88	0.924	0.652
F1-Score	Normal user	0.948	0.892	0.917	0.724
	Theft user	0.946	0.889	0.921	0.691
Overall Accuracy		0.962	0.8911	0.919	0.721

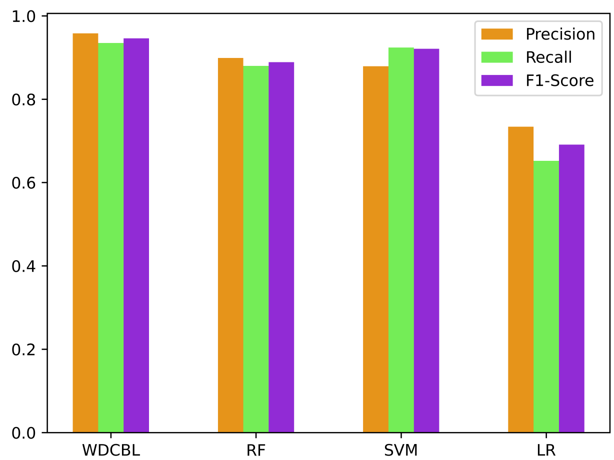

Figure 5: Comparison of model performance with different models among normal users

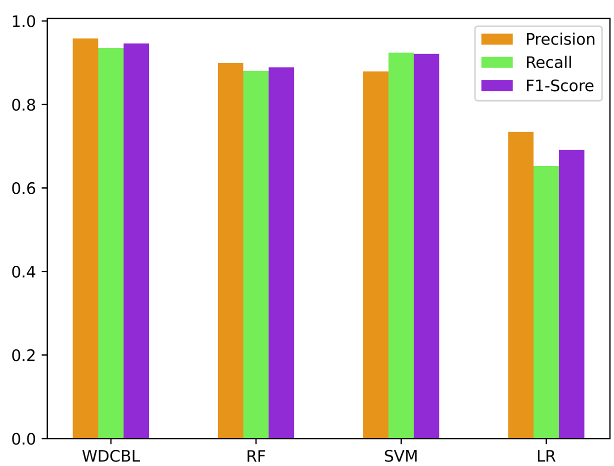

Figure 6: Comparison of model performance with different models among electricity theft users

has a significant detection effect on the user power consumption data set released by SGCC. The three evaluation indicators are higher than other models.

Comprehensive analysis of the above experimental results, we can see that the electricity stealing detection model based on Borderline-SMOTE and WDCBL proposed in this paper can well solve the electricity stealing problem in smart grid systems.

5 Conclusion

This paper proposes an electricity theft detection model based on Borderline-SMOTE and WDCBL. The model is based on the time series data of smart meters and judges whether users have electricity theft behavior by learning the characteristics of users' electricity consumption. To solve the problem of data class imbalance in SGCC dataset, this paper uses Borderline-SMOTE oversampling method to synthesize new data, to solve the problem of data set imbalance. WDCBL model is mainly composed of wide components and deep CBL components. WDCBL model can combine the features extracted by wide component and deep CBL component. The model proposed in this paper has been verified on the user power consumption data set released by SGCC. The simulation results show that WDCBL model has better performance than RF, SVM, and logistic regression.

Acknowledgments

This research is supported by the National Key R&D Program of China under Grant (No. 2019YFB2102400)

References

[1] Z. Li, C. Li, and Y. Li. Reduced dimension of power consumption characteristics and detection of electricity larceny by extreme learning machine. *Computer Applications and Software*, 35(12):179–186, December 2018.

[2] P. Jokar, N. Arianpoo, and V. C. M. Leung. Electricity theft detection in ami using customers' consumption patterns. *IEEE Transactions on Smart Grid*, 7(1):216–226, January 2016.

[3] M. N. Hasan, R. N. Toma, A. A. Nahid, Mmm Islam, and J. M. Kim. Electricity theft detection in smart grid systems: A cnn-lstm based approach. *Energies*, 12(3310):1–18, August 2019.

[4] Z. Chen, D. Meng, Y. Zhang, T. Xin, and D. Xiao. Electricity theft detection using deep bidirectional recurrent neural network. In *Proc. of 2020 22nd International Conference on Advanced Communication Technology (ICACT'20), Phoenix Park, South Korea*, pages 401–406. IEEE, February 2020.

[5] W. Hu, Y. Yang, J. Wang, X. Huang, and Z. Cheng. Understanding electricity-theft behavior via multi-source data. In *Proc. of the 2020 Web Conference 2020 (WWW'20), Taipei*. ACM, April 2020.

[6] Z. Chao and M. Wen. Scheme for electricity theft detection based on smote and xgboost. *Power Grid Analysis and Study*, 11(48):97–102, July 2020.

[7] J. CAI, K. Wang, K. Dong, Y. Yao, and Y. Zhang. Power user stealing detection based on densenet and random forest. *Journal of Computer Applications*, 41(S1):75–80, June 2021.

[8] Y. Liu, S. Zheng, X. Yang, W. Li, and T. Wei. Research on detection method of stealing electricity based on improved recurrent neural network. *Journal of Electronic Design Engineering*, 29(2):103–107, January 2021.

[9] D. Xiao, Y. Zhang, and H. Ji. Electricity theft detection based in multi-head attention. *Journal of Computer Science*, 49(1):140–145, January 2022.

[10] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang. Energy theft detection with energy privacy preservation in the smart grid. *IEEE Internet of Things Journal*, 6(5):7659–7669, January 2019.

[11] M. Azizjon, A. Jumabek, and W. Kim. 1d cnn based network intrusion detection with normalization on imbalanced data. In *Proc. of the 2nd International Conference on Artificial Intelligence in Information and Communication (ICAIIC'20), Fukuoka, Japan*, pages 218–224. IEEE, February 2020.

[12] Kocaman, Behet, and T Vedat. Detection of electricity theft using data processing and lstm method in distribution systems. *Sadhana*, 45(286):1–10, 2020.

[13] H. T. Cheng, L. Koc, J. Harmsen, T. Shaked, T. Chandra, H. Aradhye, G. Anderson, G. Corrado, W. Chai, and M. Ispir. Wide deep learning for recommender systems. In *Proc. of the 1st Workshop on Deep Learning for Recommender Systems, New York, USA*, pages 7–10. ACM, September 2016.

[14] Z. Zheng, Y. Yang, X. Niu, H. N. Dai, and Y. Zhou. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. *IEEE Transactions on Industrial Informatics*, 14(4):1606–1615, April 2018.

[15] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. *ACM Computing Surveys*, 41(3):1–58, July 2009.

[16] H. Hui, W.Y. Wang, and B.H. Mao. Borderline-smote: a new over-sampling method in imbalanced data sets learning. In *Advances in Intelligent Computing. International conference on intelligent computing (ICIC'05), Hefei, China*, volume 3644 of *Lecture Notes in Computer Science*, pages 878–887. Springer-Verlag, August 2005.

[17] N.V. Chawla, K.W. Bowyer, L.O. Hall, and W.P. Kegelmeyer. Smote: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16(1):321–357, January 2002.

Author Biography

Tao Liu received a Ph.D. in computer science from Xi'an Jiao Tong University, China, in 2008. He is currently a senior engineer with the Shenzhen Power Supply Bureau, China Southern Power Grid. His research interests include electric energy measurement, electrical energy measurement automation systems, electricity information acquisition systems.

Honghao Liang received the degree postgraduate majoring in engineering from Shanghai Jiao Tong University, China, in 2008. He is currently a senior engineer with the Shenzhen Power Supply Bureau, China Southern Power Grid. His research interests include electric energy measurement, electrical energy measurement automation systems, electricity information acquisition systems, and Software Engineering.

Xiaowei Chen received the bachelor's degree in computer science and technology from Shenzhen University in 2013. He is an engineer and technician of the Shenzhen Power Supply Bureau, China Southern Power Grid. His research interests include electric energy measurement, electrical energy measurement automation systems, electricity information acquisition systems, and Application of electric energy data

Jiahao Qi was born in Huhhot, China, in 1999. He received the B.S. degree in Computer Science and Technology from Inner Mongolia University of Technology, Huhhot, China, in 2021. He is currently pursuing the M.S. degree in Cyberspace Security with BUPT. He current research interest include computer vision and deep learning.

Yihong Guo was born in ShanXi, China, in 1999. He received the B.S. degree in Computer Science and Technology from Nanjing University of Science and Technology, Nanjing, China, in 2021. He is currently pursuing the M.S. degree in Cyberspace Security with BUPT. He current research interest include cyberspace security and privacy prevention.

Yueming Lu received the B.S. and M.S. degrees in computer science from the Xi'an University of Architecture and Technology, Xi'an, China in 1994 and 1997, respectively, and the Ph.D. degree in computer architecture from Xi'an Jiaotong University, Xi'an, China, in 2000. He is currently a Professor with the Beijing University of Posts and Telecommunications. His current research interests include cyberspace security and blockchain.