J. COMBIN. MATH. COMBIN. COMPUT. 127b (2025) 1679--1693

Journal of Combinatorial Mathematics and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Study on abnormal power usage detection of grid users based on improved neural network

Wei Zhang[1,✉], Qiong Cao[1], Shuai Yang[1], Yinlong Zhu[1]

[1] *State Grid Shanxi Electric Power Company Marketing Service Center, Taiyuan, Shanxi, 030000, China*

ABSTRACT

This paper presents an AdaBoost-DNN (Adaptive Boosting-Deep Neural Network) model for the detection of anomalous electricity consumption in power grid users. Initially, the k-means SMOTE (Synthetic Minority Oversampling Technique) technique is employed to enhance the sample set of the original anomalous consumption data to address the issue of data imbalance. Subsequently, an ensemble learning model based on AdaBoost-DNN is designed for the detection of anomalous consumption. To validate the effectiveness and superiority of the proposed AdaBoost-DNN model, comparative experiments are conducted with three traditional algorithms.

Keywords: AdaBoost model; deep neural networks; abnormal power consumption; k-means SMOTE

1. Introduction

In the process of power transmission and distribution, various kinds of losses and quality problems will occur, among which the non-technical losses are caused by users' malicious power theft, meter failures, communication system failures and grid billing system failures [1-2]. And the abnormal power usage of malicious power theft is the most important cause of non-technical losses in the power grid. Illegal power usage has existed for a long time and has caused serious negative impacts on the power system and related parties. Illegal power consumption has caused huge economic losses and social impacts on power grid companies, and power theft may also lead to overloading of generating units and transformers [3-4], and power grid companies do not have real statistics on the loads of normal users and power theft users, so it can affect the power supply quality of the power system, and bring about the problem of three-phase imbalance, etc. [5-6]. However, abnormal power usage by grid users can be leakage, standby power consumption of equipment, equalizers, miswiring of meters, seasonal appliance use, short circuit of aging wires, electrical safety hazards, and errors in metering, in addition to power theft [7-8].

In addition, overloaded circuits can also lead to abnormal electricity consumption, and overloaded circuits may lead to overvoltage, which affects the performance of the user's equipment, reduces the

✉ Corresponding author.
E-mail address: 18733974318@163.com (W. Zhang).

Received 30 May 2024; Revised 15 August 2024; Accepted 10 January 2025; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-093

service life of the equipment, and may lead to high temperature of the wiring and equipment, which may lead to fires [9-11]. Users' unauthorized wiring and private meter alterations present safety hazards, such as electrocution, and even lead to operator death. Therefore, there is an urgent need for a method that can effectively detect abnormal power usage detection by power users. Line loss rate is the ratio of the difference between the amount of power input and meter reading to the amount of power input, when the line loss rate of a station area exceeds a given threshold, there may be power theft in the area, which is used as an important assessment criterion to find power thieves [12-13]. However, one of the limitations of this method is that it can only locate in those areas with high line loss where power theft may occur, and cannot precisely locate to the specific power theft users, to realize the abnormal detection of power users' electricity consumption, and the current urgent problem is to accurately audit the power theft users [14-15].

Nowadays, intelligent technology is developing vigorously, and combining the collected user data with abnormal power consumption detection of power users is the latest research direction. Starting from a large number of measured user big data, using neural networks and other algorithms or technologies, mining from the power user data to find out the different characteristics of normal users and abnormal users, and then establish a power user abnormal power detection model, in order to get the power user whether there is theft of electricity and other abnormal power use, targeted to solve the abnormality [16-19].

Power theft as a form of abnormal power consumption, need to be identified and detected to distinguish whether it is power theft, the literature [20] uses the chi-square fitting superiority test and user behavioral feature matching method to analyze and identify the user's psychology, which effectively distinguishes whether a user is a power theft user. However, the method is slow and there is deceptive behavior. Literature [21] constructed a three-stage multi-view superposition integration (TMSE) machine learning model to detect power anomalies as accidental losses or power theft. Literature [22] proposes a fast search and discovery density peak clustering technique that is able to detect electricity theft of arbitrary shape and is fast. There are many methods for abnormal electricity usage detection for electricity theft, such as deep reinforcement learning [23], supervised learning techniques [24], deep neural networks [25], density clustering methods [26], methods combining deep learning and random forests [27], and methods combining k -nearest neighbors and support vector machines [28]. In addition, the literature [29] designed a data-driven power theft detector that can screen out power thieves in real time. This detector is also applied to an advanced metering infrastructure which provides new detection methods for falsified meter readings and electricity theft [30]. This also provides the possibility to reduce the abnormal electricity usage in case of metering errors. In different weather conditions, customers use electricity differently, which leads to confusion in identifying whether or not the electricity usage is abnormal. For this reason, literature [31] constructed a regression model for obtaining the sensitivity data of weather characteristics, and then detected the abnormal electricity usage by a typical outlier identification algorithm, which can be detected without the interference of the quality of raw weather data. And the literature [32] detected the abnormal electricity usage for seasonal monthly electricity consumption, which was mainly recognized by using the long and short-term memory neural network, and the experimental results found the long-term anomalies. This provides a suitable abnormal power usage detection method for users who are not sensitive to power usage. In addition, literature [33] designed a sample-efficient home electricity anomaly detection method consisting of an appliance pattern matching classifier, a semi-supervised learning method that requires only a small number of samples for high accuracy, and an energy consumption habit classifier, which performs anomaly detection under the Hidden Markov Model (HMM). In addition to efficient anomaly detection, literature [34] mentions a visualization technique for scatter representation of micro-moment classes to help users better understand the anomalous power consumption and target anomaly elimination.

This study aims to explore improved neural network algorithm models by analyzing the characteristics of user consumption data within the smart grid environment, resulting in optimized user anomaly detection strategies and solutions. Through these methods, the study seeks to significantly enhance the efficiency and accuracy of user anomaly detection, reduce the associated losses for power companies, and improve the operational safety and economic benefits of power systems, providing scientific and technical support for the operational management of power companies.

2. Method Introduction

2.1. Electrical load sample data augmentation techniques

This study employs k-means SMOTE (Synthetic Minority Oversampling Technique) to address the issue of class imbalance in the electrical load sample set **Error! Reference source not found.**. SMOTE generates synthetic samples by interpolating between samples of the minority class, thereby augmenting the number of samples in the rare electrical usage category and balancing the class distribution. In the application of K-means SMOTE, the k-means algorithm is first used to cluster the data, and then SMOTE synthetic samples are generated only for each cluster within the minority class. The schematic of this principle is illustrated in Figure 1.

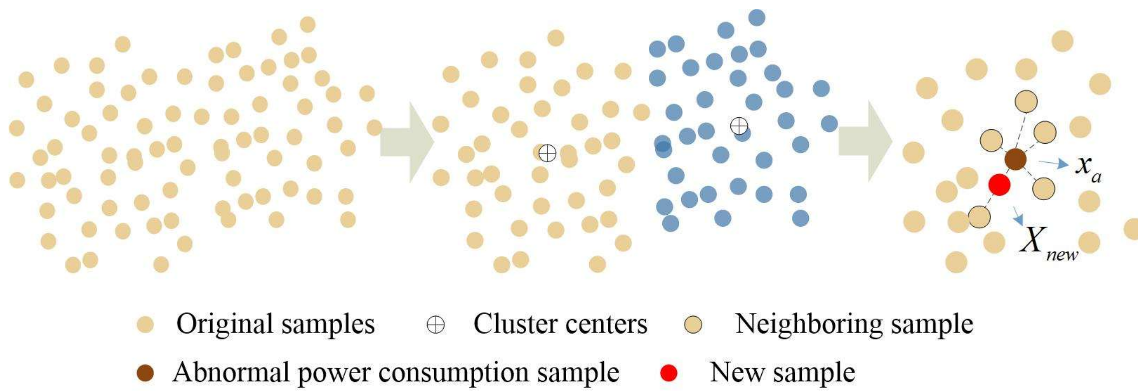

Fig. 1. Principles of the k-means SMOTE Technique

1) For a sample set with m samples, select k clusters. Compute the Euclidean distance of each sample x_i to the centroid C_j of the j-th cluster. Assign each sample to the cluster with the nearest centroid.

$$d_{ij} = \sqrt{\sum_{i=1}^{m}\sum_{i=1}^{k}(x_i - C_j)^2} \tag{1}$$

2) Compute the centroids of the clusters μ_j and update the cluster centers accordingly. The i-th sample of the j-th cluster is denoted as x_{ij}, and the sample size is represented by m_j.

$$\mu_j = \frac{1}{|m_j|}\sum_{x_i \in C_i} x_{ji} \tag{2}$$

3) Compute the ratio IR_j of the number of normal user samples to the number of anomalous user samples within each cluster. Let m_l represent the number of normal user samples, and m_s denote the number of anomalous user samples.

$$IR_j = \frac{m_l + 1}{m_s + 1} \tag{3}$$

4) The quantity g_j of new samples required to be generated for each cluster is calculated as follows.

$$G = m_l - m_s \tag{4}$$

$$g_j = G \cdot c \cdot \frac{average\_distance_j^m}{m_{sj}} \tag{5}$$

where, G denotes the difference in the number of normal and anomalous user samples; c represents the weight for generating new synthetic samples, $c \in [0,1]$; $average\_distance_j^m$ indicates the average distance between each sample in the j-th cluster and the cluster centroid; m signifies the number of features; and m_{sj} denotes the number of anomalous electricity consumption samples in the j-th cluster.

5) Employ the SMOTE algorithm for the synthesis of new samples.

$$X_{new} = x_c + rand(0,1) \times (x_a - x_e) \tag{6}$$

where, X_{new} denotes a newly generated sample, x_e signifies an anomalous electrical sample randomly selected from the cluster; x_a represents a sample chosen from the neighbors of x_e; and $rand(0,1)$ denotes a randomly selected number within the interval (0,1).

6) Continue to expand the sample size until the number of newly generated samples within each cluster reaches g_j 。

2.2. Deep Neural Network Model

Neural networks are a machine learning approach that emulates the signal transmission mechanisms of biological neural systems, comprising multiple neurons connected through summation nodes and activation functions. A Deep Neural Network (DNN) is a robust learning model that captures intricate features of data through multiple layers of nonlinear transformations **Error! Reference source not found.**. DNNs have the capability to automatically extract features and patterns, making them well-suited for handling high-dimensional and complex datasets.

The fundamental principles of deep neural networks are illustrated in Figure 2. As depicted, the input vector $X = (x_1, x_2, x_3, \ldots, x_n)$ serves as the entry point into the network. w_i, b_i denote the weights and biases of the i-th hidden layer respectively. Each hidden layer receives the input vector from the previous layer, performs a linear transformation through weighted summation and bias addition, and then applies a nonlinear activation function to produce the activation values for the current layer. These activation values are subsequently transmitted as inputs to the next layer, progressing through each layer until the final prediction output of the network is achieved.

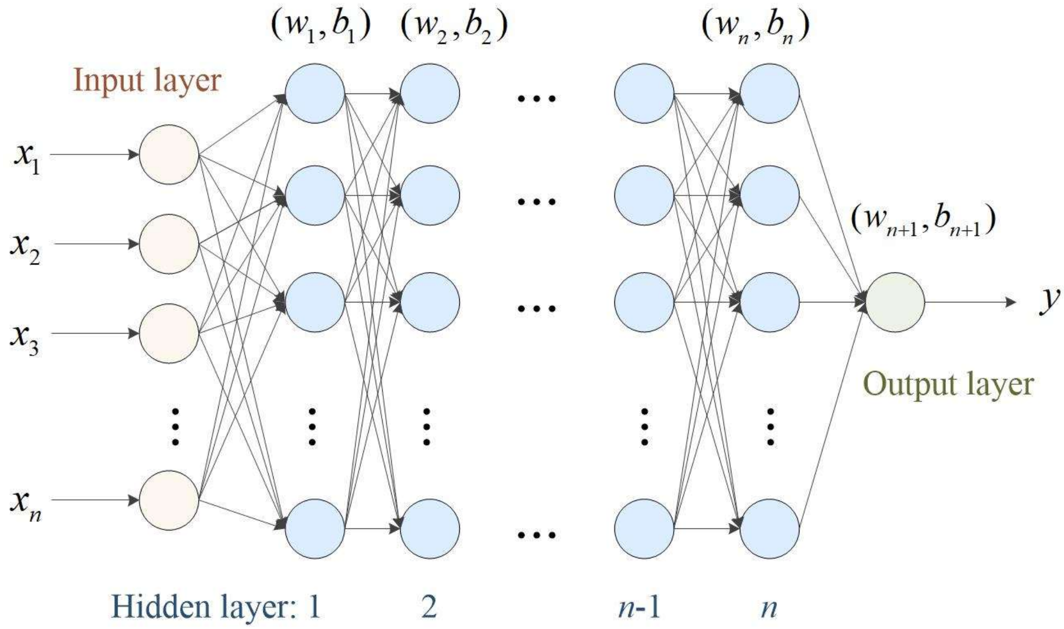

Fig. 2. Basic Principles of Deep Neural Networks

In a fully connected layer, the input vector $a^{(l-1)}$ of the hidden layer is transformed into an output vector $a^{(l)}$ through an activation function f, as represented below.

$$a^{(l-1)} = (a_1^{(l-1)}, a_2^{(l-1)}, \cdots a_i^{(l-1)}, \cdots a_x^{(l-1)})^T \tag{7}$$

$$a^{(l)} = f(\sum_{i=1}^{a} W_{l-1} a_i^{l-1} + b_{i-1}) \tag{8}$$

Propagate the output vector $a^{(l)}$ of the current layer as the input to the subsequent layer, continuing this process layer by layer until reaching the final output layer, thereby producing the ultimate output vector y. β represents the number of neurons in the $n+1$-th hidden layer.

$$y = f^{n+1}(\sum_{i+1}^{\beta} W_{n+1} f^n + b_{n+1}) \tag{9}$$

2.3. AdaBoost Ensemble Learning Method

The fundamental concept behind Boosting algorithms is to enhance the overall model's predictive accuracy by aggregating multiple weak classifiers **Error! Reference source not found.**. While each of these weak classifiers may have limited predictive accuracy on its own, combining them allows Boosting to significantly improve prediction precision and create a robust classifier with superior performance.

AdaBoost (Adaptive Boosting) is a widely used ensemble learning technique extensively applied across various machine learning tasks, as illustrated in Figure 3. AdaBoost iteratively trains multiple weak classifiers, assigning higher weights to misclassified samples with each training cycle, thereby progressively refining classification performance. Its remarkable adaptability enables AdaBoost to excel in handling diverse predictive challenges, automatically adjusting classifier weights and effectively augmenting the overall performance of the model.

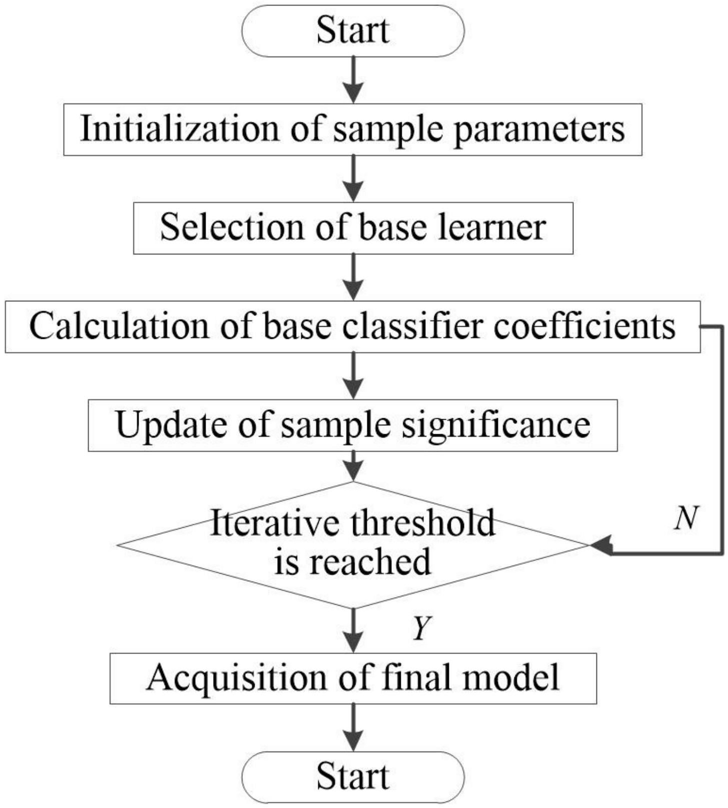

Fig. 3. Workflow Diagram of AdaBoost Ensemble Learning

2.4. AdaBoost-DNN Anomaly Detection Model

AdaBoost enhances the overall accuracy of a model by integrating multiple classifiers. This paper selects Deep Neural Networks (DNN) as the base learners for the AdaBoost model for anomaly detection in electricity consumption, with the fundamental framework illustrated in Figure 4. The AdaBoost-DNN (AdaBoost-Deep Neural Network) anomaly detection model amalgamates the advantages of the AdaBoost algorithm and deep neural networks (DNN) to improve the efficacy of anomaly detection. This integrated approach leverages AdaBoost's weighting mechanism and the powerful feature learning capabilities of DNNs, resulting in superior performance in handling anomaly detection tasks.

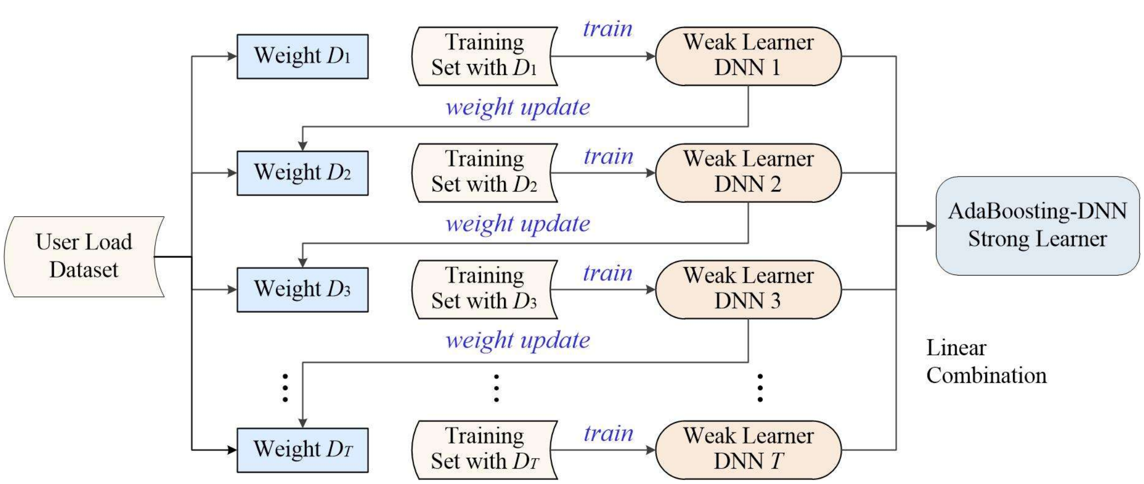

Fig. 4. Framework of the AdaBoost-DNN Model

The fundamental steps are as follows:

1) Initialize weights: The first step of AdaBoost involves assigning initial weights to each sample in the training dataset.

$$D_1 = (w_{11}, \dots, w_{1i}, \dots, w_{1N}) \tag{10}$$

$$w_{1i} = \frac{1}{T}, i = 1, 2, \dots T \tag{11}$$

where, w_{1i} denotes the weight of the i-th sample in the first iteration, while T represents the number of samples.

2) Training the DNN: In the m-th iteration, a deep neural network is trained using the training dataset with

$$y_{mk}(x) : X \to \{-1, 1\}, k = 1, 2, \dots, j \tag{12}$$

3) Compute Classification Error: Determine the classification error e_{mk} of the k-th classifier on the training data, with a particular emphasis on those samples that were misclassified.

$$e_{mk} = P(y_{mk}(X_i) \neq y_i) = \sum_{i=1}^{N} w_{mi}(y_{mk}(X_i) \neq y_k) \tag{13}$$

where, w_{mi} denotes the weight of the i-th sample during the m-th iteration; X_i represents the data for the i-th row.

4) Update the weights: Adjust the sample weights based on the classification error of the DNN, thereby generating the weight α_m for the weak classifier $y_m(x)$.

$$\alpha_m = \frac{\lg \frac{1-e_m}{e_m}}{\sum_{i=1}^{m} \lg \frac{1-e_i}{e_i}} \tag{14}$$

5) Iterative Training: Retrain the DNN with the updated weights, resulting in a new classifier. This process is repeated multiple times, with adjustments made to the sample weights each iteration.

6) Weighted Ensemble: Compile a formidable ensemble classifier by combining all DNN models trained, with each model contributing to the overall classification outcome based on a predetermined weighting scheme.

$$y(x) = sign(\sum_{m=1}^{M} \alpha_m y_m(x)) \tag{15}$$

where, M represents the total number of iterations.

7) Anomaly Detection: The final ensemble classifier is employed to identify anomalous samples. The model determines whether a sample is anomalous based on the aggregated classification results.

2.5. Genetic Algorithms for Hyperparameter Optimization

Genetic algorithms possess remarkable optimization capabilities, with their primary advantage being the ability to perform comprehensive and multi-faceted searches without relying on initial conditions.

The learning rate of deep neural networks is a crucial hyperparameter that determines the magnitude of each weight update step. A diagram illustrating the optimization of learning rate using genetic algorithms is shown in Figure 5.

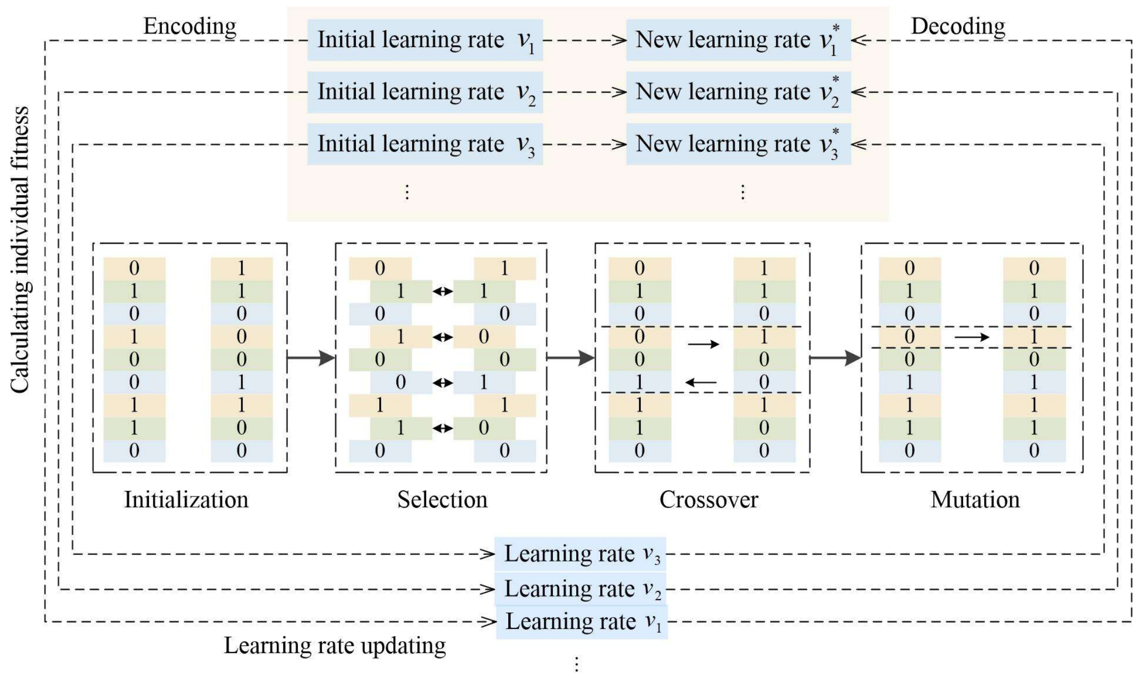

Fig. 5. Optimization of Learning Rate Based on Genetic Algorithms

1) Encoding Learning Rates: Encode the learning rates, such as, to represent various values of learning rates.

2) Fitness Calculation: Compute the fitness for each set of learning rates.

3) Selection Operation: Select the learning rate combinations with higher fitness values.

4) Crossover Operation: Perform crossover on the selected learning rates to generate new learning rate combinations. The operation a_{mj} and a_{lj} at position j of chromosome a_m and chromosome a_l in the m -th and i -th positions, respectively, is represented by Formula (16), where b is a random number in the interval [0,1].

$$\begin{cases} a_{mj} = a_{mj}(1-b) + a_{lj}b \\ a_{lj} = a_{lj}(1-b) + a_{mj}b \end{cases} \tag{16}$$

5) Mutation Operation: Introduce a mutation to the learning rate post-crossover to incorporate novel characteristics.

$$a_{ij} = \begin{cases} a_{ij} + (a_{ij} - a_{\max})h(g), r > 0.5 \\ a_{ij} + (a_{\min} - a_{ij})h(g), r \le 0.5 \end{cases} \tag{17}$$

$$h(g) = r_2(1 - \frac{g}{G_{\max}})^2 \tag{18}$$

where, $a_{\max}$ and $a_{\min}$ represent the lower and upper bounds of the gene a_{ij}, respectively; r_2 denotes a random number, g signifies the current iteration count, $G_{\max}$ represents the maximum number of iterations, and r is a random number within the interval [0,1].

6) Iterative Optimization: Repeatedly performing selection, crossover, and mutation operations until the learning rate meets the optimization criteria or the predetermined number of iterations is reached.

7) Decoding the New Learning Rate: Translating the optimized learning rate from the genetic algorithm's gene representation into an actual learning rate value for further model training and evaluation.

Through the aforementioned process, the genetic algorithm can effectively search for and optimize the learning rate of deep neural network models, thereby enhancing the model's performance.

3. Experiment and Analysis

3.1. Data set and evaluation index

In this study, we utilized a dataset of actual electricity consumption from a smart meter system in a certain city, covering user electricity records from October 1, 2021, to September 30, 2022, encompassing a total of 15,389 entries. The data includes information such as user IDs, timestamps, electricity usage, and locations. The data underwent preprocessing, which involved the removal of outliers, handling missing values, and normalization, and was labeled with normal and anomalous consumption patterns to support model training.

To address the issue of class imbalance in the electricity load sample set, the study employed the K-mean SMOTE technique, which generates synthetic samples through interpolation among minority class samples, thereby increasing the number of anomalous consumption samples and balancing the class distribution. In the resulting dataset, users with anomalous electricity usage account for approximately 10% of the total users. The dataset was split into training and testing sets in a 4:1 ratio for model training and evaluation. The generated training set was used to train the AdaBoost-DNN algorithm. A genetic algorithm was employed to adjust the learning rate of AdaBoost and determine the number of weak learners, among other parameters. The testing set was then input into the trained AdaBoost-DNN model to obtain and output detection results. This study also compared the proposed model with SVM, BP, and RF algorithms to validate its superiority.

Table 1 presents the confusion matrix for electricity anomaly detection. Based on this, several evaluation metrics were proposed to assess the accuracy and effectiveness of the model. These metrics include accuracy (ACC), sensitivity (TPR), and false positive rate (FPR). Additionally, the receiver operating characteristic (ROC) curve was used to describe the relative changes in FPR and TPR metrics, with the area under the ROC curve (AUC) serving as the measurement criterion.

Table 1. Confusion Matrix for Electricity Anomaly Detection

User Category		Detected Status	
		Abnormal User	Regular User
Actual Status	Abnormal User	TP	FP
	Regular User	FN	TN

$$ACC = \frac{TP + TN}{TP + FN + FP + TN} \tag{19}$$

$$TPR = \frac{TP}{TP + FN} \tag{20}$$

$$FPR = \frac{FP}{FP + TN} \tag{21}$$

3.2. Experiment Results and Parameter Determination

Figure 6 contrasts the accuracy and sensitivity of various algorithms in relation to the proportion of anomalous samples. It is evident that, with the increase in the proportion of anomalous samples, all algorithms except SVM exhibit a declining trend in accuracy. Notably, the accuracy of the AdaBoost-DNN algorithm consistently surpasses that of other algorithms. In terms of sensitivity, both the proposed AdaBoost-DNN and RF algorithms demonstrate high sensitivity, which slightly decreases with an increasing proportion of anomalous samples. Overall, BP and SVM show considerable fluctuation in detecting anomalous samples, while the AdaBoost-DNN proposed herein exhibits superior performance in both detection accuracy and hit rate.

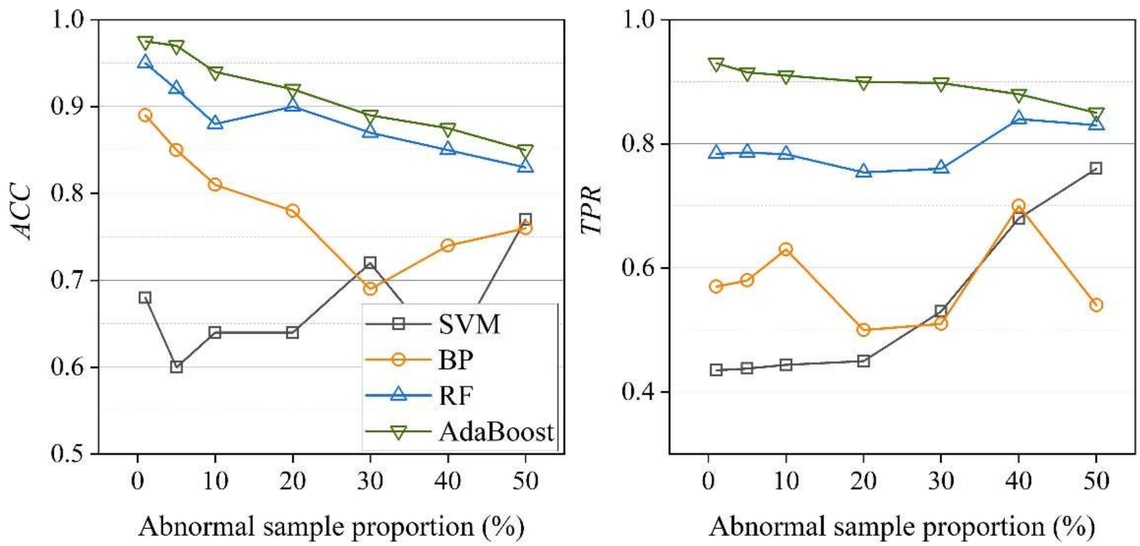

Fig. 6. Comparison of Algorithm Accuracy and Hit Rate at Different Abnormal Power Consumption Sample Proportions

The selection of hyperparameters significantly impacts model performance. By employing genetic algorithms to optimize the hyperparameters of the AdaBoost-DNN ensemble model, particularly the learning rate, one can effectively enhance the model's performance. In this process, the genetic algorithm iteratively seeks the optimal learning rate, thereby refining the training process and overall model performance.

Figure 7 illustrates the iteration process of the AdaBoost-DNN model before and after optimizing the learning rate using genetic algorithms. The figure depicts the dynamic adjustment of the learning rate, showing the transition from an initially random selection to the final convergent optimal value. Without genetic algorithm optimization, the convergence speed was relatively quick, with the learning rate stabilizing at 0.085; however, with optimization, the learning rate was adjusted to 0.051. This indicates that genetic algorithms, through simulating the process of natural selection, can effectively optimize hyperparameters and identify the most suitable learning rate, thereby enhancing the overall performance and accuracy of the AdaBoost-DNN ensemble model.

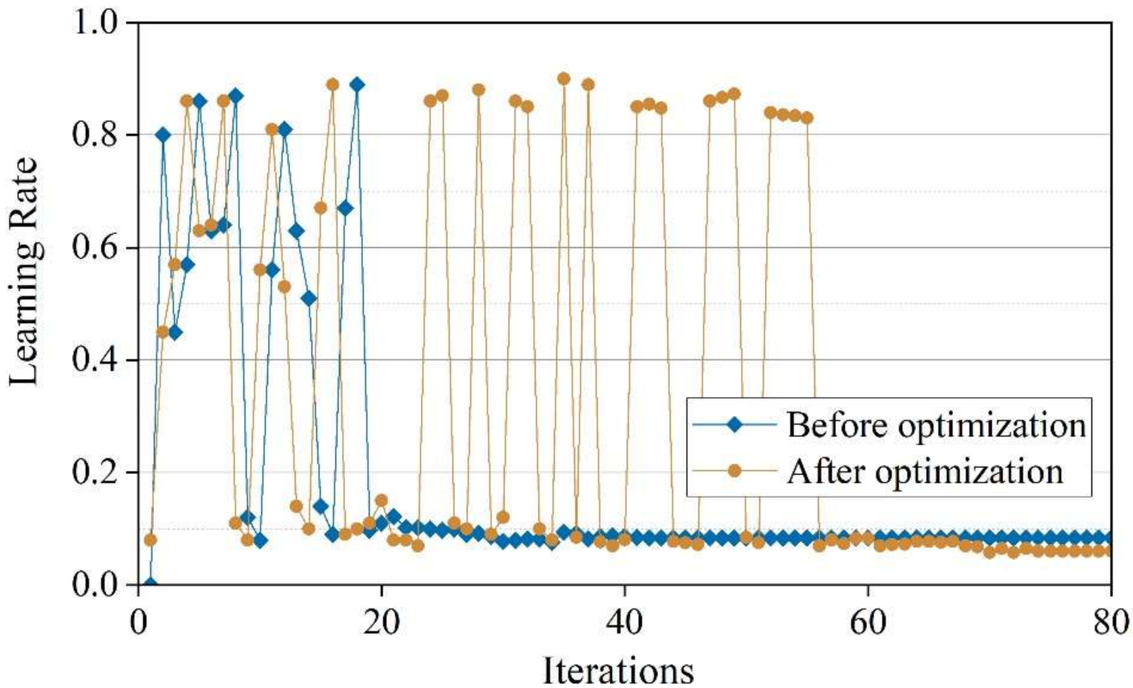

Fig. 7. Optimization Iteration Process of Learning Rate

3.3. Comparative Experiment

To verify the effectiveness and superiority of the AdaBoost-DNN detection model proposed in this paper, a comparative experiment was conducted with three other algorithms (SVM, BP, RF). The evaluation results are presented in Table 2.

The study illustrates the model's performance by plotting the false positive rate (FPR) and true positive rate (TPR). The area under the ROC curve (AUC) provides a comprehensive metric for overall model performance. The comparison of ROC curves for different algorithms is shown in Figure 8. It is evident from the figure that AdaBoost-DNN exhibits the highest AUC value, demonstrating its superior discrimination capability in classification tasks, with the ability to maintain high sensitivity and low false positive rate across various thresholds. Although the ROC curve for BP may be slightly lower, it generally performs better than SVM, as BP excels in capturing non-linear features. The SVM curve is relatively flat, with performance significantly affected by sample complexity. Overall, AdaBoost-DNN and RF offer more stable performance in classification tasks, making them suitable for applications requiring high accuracy, while BP is better suited for data with high non-linearity. SVM may struggle to maintain a balance between high sensitivity and low false positive rate in classification tasks.

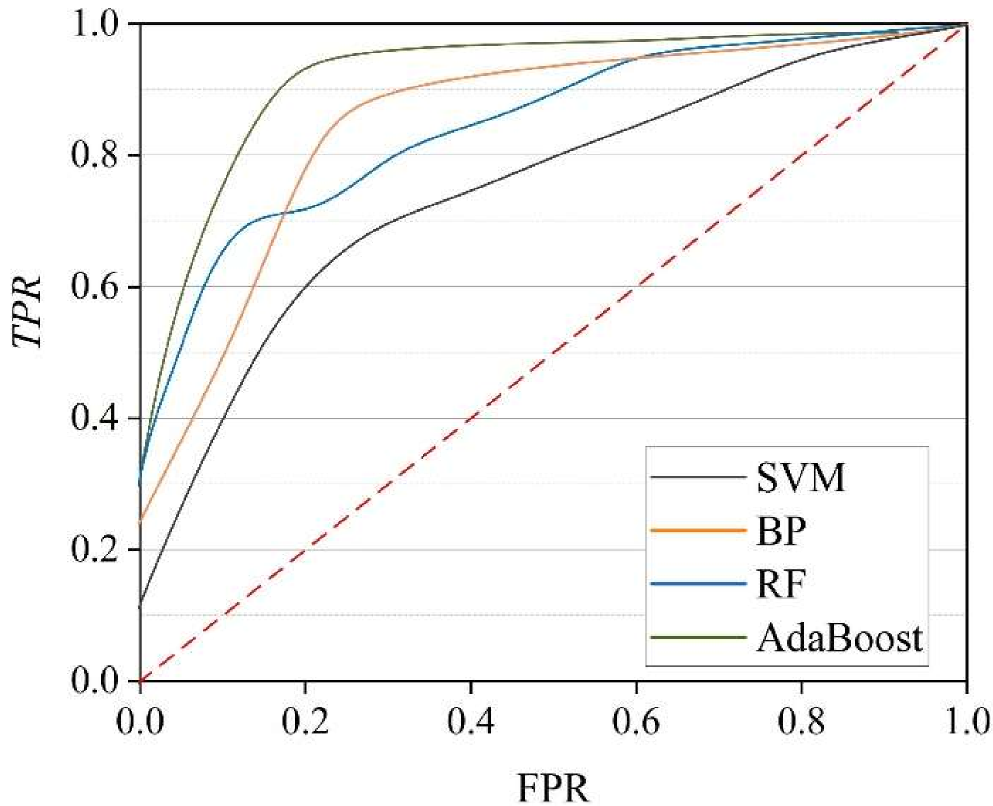

Fig. 8. ROC curves for different algorithms

According to the data in Table 2, there are noticeable differences in performance among the various algorithms for detecting user electricity anomalies. SVM's accuracy is 78.1%, with a true positive rate of 67.8% and an AUC value of 0.74, indicating relatively weak classification performance. The BP neural network shows improvements across all three metrics. Random Forest performs relatively well, suggesting strong data processing capabilities. However, the AdaBoost-DNN model excels in all metrics, with an accuracy of 94.7%, a true positive rate of 94.9%, and an AUC value of 0.94, highlighting its significant advantage in detection tasks.

The accuracy and true positive rate of the AdaBoost-DNN model are significantly higher than those of other algorithms, indicating its exceptional ability to identify anomalies in electricity consumption. Moreover, the AUC value far surpasses that of other models, demonstrating its superior comprehensive performance across various classification thresholds. It is evident that the AdaBoost-DNN model, by effectively integrating AdaBoost with deep neural networks, achieves an enhanced detection efficacy.

Table 2. Comparative Analysis of Detection Results for Various Algorithms

	ACC	TPR	AUC
SVM	78.1	67.8	0.74
BP	83.2	73.4	0.82
RF	86.9	84.0	0.85
AdaBoost-DNN	94.7	94.9	0.94

4. Conclusions

This article presents an ensemble learning model based on AdaBoost-DNN for detecting abnormal electricity consumption among grid users. To substantiate the effectiveness and superiority of the proposed AdaBoost-DNN detection model, a comparative experiment was conducted between this method and three other algorithms (SVM, BP, RF). The comparative results demonstrate that the AdaBoost-DNN model excels across all evaluation metrics, highlighting its distinct advantages in the detection task. This indicates that the refined neural network approach, combined with sample augmentation techniques and ensemble learning strategies, can achieve efficient anomaly detection in electricity consumption. In subsequent research endeavors, consideration might be given to employing diverse user typologies as reference benchmarks. By categorizing electricity users based on their intrinsic attributes, a comprehensive and multi-faceted classification system can be established, thereby enhancing the precision of user identification.

References

[1] Saeed, M. S., Mustafa, M. W., Hamadneh, N. N., Alshammari, N. A., Sheikh, U. U., Jumani, T. A., ... & Khan, I. (2020). Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review. Energies (19961073), 13(18).

[2] Taylor, L., & Short, T. A. (2018). Distribution reliability and power quality. Crc Press.

[3] Nawaz, H., Zohaib, A., Zahra, S. T., Amin, S., Basheer, Y., Ali, Z., ... & Orakzai, M. S. (2023). IoT Based Load Management Control and Theft Protection from DISCO's Side. International Journal of Emerging Engineering and Technology, 2(1), 63-68.

[4] Saini, S. (2017). Social and behavioral aspects of electricity theft: An explorative review. International Journal of Research in Economics and Social Sciences (IJRESS), 7(6), 26-37.

[5] Olaoluwa, O. G. (2017). Electricity theft and power quality in Nigeria. International Journal of Engineering Research & Technology, 6(6), 1180-1184.

[6] Khan, A., & Ali, M. (2023). Three-Phase Load Balancing in Distribution Systems Using Load Sharing Technique. Engineering Proceedings, 46(1), 18.

[7] Xie, Z., Cheng, Y., Chen, A., & Lv, X. (2022, May). Study of abnormal electricity consumption for "coal to electricity" customers. In 2022 IEEE 5th International Electrical and Energy Conference (CIEEC) (pp. 3356-3361). IEEE.

[8] Furse, C. M., Kafal, M., Razzaghi, R., & Shin, Y. J. (2021). Fault Diagnosis for Electrical Systems and Power Networks: A Review. IEEE Sensors Journal, 21(2).

[9] Othman, N. S., Rohani, M. N. K. H., Mustafa, W. A., Wooi, C. L., Rosmi, A. S., Shakur, N. F. M., ... & Shahriman, A. B. (2019, June). An Overview on Overvoltage Phenomena in Power Systems. In IOP Conference Series. Materials Science and Engineering (Vol. 557, No. 1). IOP Publishing.

[10] Jalilian, A., Muttaqi, K. M., & Sutanto, D. (2020, October). A Novel Voltage Clamping based Overvoltage Protection Strategy to Avoid Spurious Trip of Inverter based Resources and Eliminate the Risk of Bushfires following the REFCL Operation. In 2020 IEEE Industry Applications Society Annual Meeting (pp. 1-10). IEEE.

[11] Saini, S. (2018). Malpractice of Electricity Theft: A major cause of distribution losses in Haryana. International Research Journal of Management and Commerce, 5(1), 284-313.

[12] Li, B., & Wang, W. (2024). Knowledge-Graph-Based Integrated Line Loss Evaluation Management System. Applied Sciences (2076-3417), 14(20).

[13] Yan, Z., & Wen, H. (2022). Performance Analysis of Electricity Theft Detection for the Smart Grid: An Overview. IEEE Transactions on Instrumentation Measurement, 71, 3127649.

[14] Biswas, P. P., Cai, H., Zhou, B., Chen, B., Mashima, D., & Zheng, V. W. (2019). Electricity theft pinpointing through correlation analysis of master and individual meter readings. IEEE Transactions on Smart Grid, 11(4), 3031-3042.

[15] Omidvar Tehrani, S., Shahrestani, A., & Yaghmaee, M. H. (2022). Online electricity theft detection framework for large-scale smart grid data. Electric Power Systems Research, 208, 107895.

[16] Buzau, M. M., Tejedor-Aguilera, J., Cruz-Romero, P., & Gomez-Exposito, A. (2020). Hybrid Deep Neural Networks for Detection of Non-Technical Losses in Electricity Smart Meters. IEEE Transactions on Power Systems, 35(2), 1254-1263.

[17] Ahmad, T., Chen, H., Wang, J., & Guo, Y. (2018). Review of various modeling techniques for the detection of electricity theft in smart grid environment. Renewable and Sustainable Energy Reviews, 82(P3), 2916-2933.

[18] Moghaddass, R., & Wang, J. (2018). A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data. IEEE transactions on smart grid, 9(6), 5820-5830.

[19] Ghasemi, A. A., & Gitizadeh, M. (2018). Detection of illegal consumers using pattern classification approach combined with Levenberg-Marquardt method in smart grid. International Journal of Electrical Power and Energy Systems, 99, 363-375.

[20] Xiong, X., Wu, J., Rong, Z., He, P., Dong, N., Jiang, X., ... & Ji, Y. (2022, December). An Abnormal Power Consumption Identification Method Considering User Psychology. In Frontier Academic Forum of Electrical Engineering (pp. 833-842). Singapore: Springer Nature Singapore.

[21] Ouyang, Z., Sun, X., Chen, J., Yue, D., & Zhang, T. (2018). Multi-View Stacking Ensemble for Power Consumption Anomaly Detection in the Context of Industrial Internet of Things. IEEE Access, 6, 9623-9631.

[22] Zheng, K., Chen, Q., Wang, Y., Kang, C., & Xia, Q. (2019). A Novel Combined Data-Driven Approach for Electricity Theft Detection. IEEE Transactions on Industrial Informatics.

[23] El-Toukhy, A. T., Badr, M. M., Mahmoud, M. M., Srivastava, G., Fouda, M. M., & Alsabaan, M. (2023). Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids. IEEE Access, 11, 59558-59574.

[24] Khan, Z. A., Adil, M., Javaid, N., Saqib, M. N., Shafiq, M., & Choi, J. G. (2020). Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data. Sustainability (2071-1050), 12(19).

[25] Lepolesa, L. J., Achari, S., & Cheng, L. (2022). Electricity Theft Detection in Smart Grids Based on Deep Neural Network. IEEE Access, 10, 39638-39655.

[26] Zheng, K., Wang, Y., Chen, Q., & Li, Y. (2018). Electricity theft detecting based on density-clustering method. 2017 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia).

[27] Li, S., Han, Y., Yao, X., Yingchen, S., Wang, J., & Zhao, Q. (2019). Electricity Theft Detection in Power Grids with Deep Learning and Random Forests. Journal of Electrical & Computer Engineering.

[28] Kong, X., Zhao, X., Liu, C., Li, Q., Dong, D., & Li, Y. (2021). Electricity theft detection in low-voltage stations based on similarity measure and DT-KSVM. International Journal of Electrical Power and Energy Systems, 125, 106544.

[29] Xiao, F., & Ai, Q. (2018). Electricity theft detection in smart grid using random matrix theory. IET Generation, Transmission & Distribution (Wiley-Blackwell), 12(2).

[30] Razavi, R., Gharipour, A., Fleury, M., & Akpan, I. J. (2019). A practical feature-engineering framework for electricity theft detection in smart grids. Applied Energy, 238(C), 481-494.

[31] Zhang, Y., Colella, P., Mazza, A., Bompard, E. F., Emiliano, R., & Giuliana, G. (2019). Abnormal Electricity

Consumption Detection from Incomplete Records in Power System. In IEEE ISGT Asia 2019. IEEE.

[32] Wang, X., Zhao, T., Liu, H., & He, R. (2019, April). Power consumption predicting and anomaly detection based on long short-term memory neural network. In 2019 IEEE 4th international conference on cloud computing and big data analysis (ICCCBDA) (pp. 487-491). IEEE.

[33] Wang, X., Yang, I., & Ahn, S. H. (2019). Sample Efficient Home Power Anomaly Detection in Real Time Using Semi-Supervised Learning. IEEE Access, 7, 139712-139725.

[34] Himeur, Y., Alsalemi, A., Bensaali, F., & Amira, A. (2020). A novel approach for detecting anomalous energy consumption based on micro-moments and deep neural networks. Cognitive Computation, 12(6), 1381-1401.