

Received August 8, 2021, accepted September 2, 2021, date of publication September 6, 2021, date of current version September 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3110510

Electricity Theft Detection Based on Stacked Autoencoder and the Undersampling and Resampling Based Random Forest Algorithm

GUOYING LIN^{1,2}, XIAOFENG FENG², WENCHONG GUO², XUEYUAN CUI¹, SHENGYUAN LIU¹, (Graduate Student Member, IEEE), WEICHAO JIN¹, ZHENZHI LIN¹, (Member, IEEE), AND YI DING¹, (Member, IEEE)

¹College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China

²Metrology Center of Guangdong Power Grid Corporation, Guangzhou 510080, China

Corresponding author: Shengyuan Liu (eelsy@zju.edu.cn)

This work was supported by the Project of Science and Technology Foundation of China Southern Power Grid Company Ltd. under Grant GDKJXM20185800.

ABSTRACT Electricity theft has been a major concern to the secure operation of power systems and the interests of power companies. Due to the different methods and types of electricity theft behaviors, it is difficult to determine the suspicion levels of consumers in the research of electricity theft detection. An electricity theft detection method based on stacked autoencoder (SAE) and the undersampling and re-sampling based random forest (UaRe-RF) algorithm is proposed in this work to formulate appropriate strategies for the practical electricity theft detection requirements of the power company. In the proposed method, the supervised SAE is first trained to extract electricity consumption features that are more adaptable to the classification algorithm for electricity theft detection. Then, the UaRe-RF algorithm is used to establish the class-balanced subsets and determine the suspicion level of each electricity theft user. Finally, two cases of different datasets of electricity consumers are studied for demonstrating the effectiveness of the proposed method, and the results show that higher classification accuracy and more targeted detection strategies can be achieved through the proposed method.


INDEX TERMS Electricity theft, class imbalance, suspicion level, feature extraction, machine learning, random forest.

NOTATIONS AND ABBREVIATIONS

NOTATIONS

L_{AE} Loss function in the reconstruction process.
 N Number of users.
 x_i Electricity vector of user i .
 \tilde{x}_i Output vector of AE reconstructed from x_i .
 L_2 Constant in L_{AE} .
 m Dimension of feature vectors in the hidden layer of AE.
 w Weight vector in the encoding process.
 F Set of feature vectors.
 L_{SAE} The overall loss of SAE.
 N_{tr} Number of users in the training set.
 X_p Normal users in the training set.

X_q Electricity theft users in the training set.
 S Number of combined subsets.
 N_r Number of base classifiers in RF.
 H_i RF classifier.
 X_{or} Combination set.
 X_{re} Resampled set.
 H_f Final classifier integrated from H_i .
 α_i Ensemble weight of RF.
 θ Classification threshold.
 r_j^{ac} Accuracy of RF classifier.
 R_1 Recall rate.
 R_2 Precision rate.
 R_3 ROC.
 N_{TP} Number of TP users in the classification result.
 N_{FN} Number of FN users in the classification result.
 N_{TN} Number of TN users in the classification result.
 N_{FP} Number of FP users in the classification result.

The associate editor coordinating the review of this manuscript and approving it for publication was Taha Selim Ustun .

- E Electricity matrix of input users.
 d Time length of input electricity vector.
 ρ^+ Suspicion level of electricity theft samples.
 ρ^- Possibility of normal samples.

ABBREVIATIONS

AE	Autoencoder.
AMI	Advanced measurement infrastructure.
BRF	Balanced random forest.
CFSFDP	The clustering technique by fast search and find of density peaks.
DS-I	Dataset from the Irish CER Smart Metering Project.
DS-II	Dataset of special transformer users.
ET	Electricity theft users.
FN	False negative.
FP	False positive.
FPR	False positive rate.
GSM	Gateway smart meter.
MIC	Maximum information coefficient.
MIU	Monitoring and inspection unit.
NTL	Non-technical loss.
NU	Normal users.
RF	Random forest.
ROC	Receiver operating characteristic curve.
SAE	Stacked autoencoder.
SVM	Support vector machine.
Target-I	The first detection target.
Target-II	The second detection target.
Target-III	The third detection target.
TN	True negative.
TP	True positive.
TPR	True positive rate.
TSM	Terminal smart meter.
UaRe-RF	Undersampling and re-sampling based random forest.

I. INTRODUCTION

Electricity theft is a type of malicious behavior that electricity consumers pay fewer charges than the normal electricity consumption by illegal means. Electricity theft has become the main part of non-technical loss (NTL) and a major concern to the secure operation of power systems as well as the interests of power companies [1]. In recent years, the loss caused by electricity theft in the world has exceeded 89.3 billion US dollars, including 58.7 billion US dollars in developing countries, where the top three are India (16.2 billion US dollars), Brazil (10.5 billion US dollars), and Russia (5.1 billion US dollars) [2]. According to the World Bank, electricity theft has caused more than 25% of India's power supply losses, 16% in Brazil, 6% in China and the United States, and 5% in Australia [3], respectively. To reduce NTL, power supply companies need to take the necessary measures to detect electricity theft behaviors. However, the traditional means need expensive manpower in

the on-the-spot inspection of electricity meters of consumers, and only a small part of electricity theft cases can be detected successfully [4].

To detect electricity theft more effectively, in the past decades, researchers from various countries have proposed different detection methods, which can be divided into three types: state estimation-based, game theory-based, and machine learning algorithm-based ones [5]. For the state estimation-based method, the operation data in the distribution network collected by advanced measurement infrastructure (AMI) [6], [7], wireless sensor, and other equipment are used to detect the operation status of the system to determine the abnormality in the power systems [8]–[13]. In [8], a detection method of electricity theft is proposed based on illegal branch impedance identification. The terminal smart meter (TSM) sends high-frequency and low-voltage signals to the gateway smart meter (GSM), and the meter value modification and electricity theft behaviors around the meter are detected based on the transmission time. The high frequency and integrity of data acquisition are required to ensure the accuracy of this method. Thus it can only be applied to the areas with perfect smart grid infrastructure construction, and there is a risk of invasion of user privacy. In [12], the electricity theft behaviors are identified by comparing the difference between the power supply load of the distribution transformer and the total load based on a central monitoring and inspection unit (MIU). The relationship between the user load and NTL is judged through the sequential power-off operation to determine the electricity theft users.

For the game theory-based method, the problem of electricity theft can be regarded as a game model of electricity theft users, normal users, and distribution companies [14], [15]. In the game model, the distribution companies need to determine the construction cost of AMIs to improve the accuracy of electricity theft detection, the normal users need to choose the reasonable electricity purchase and consumption mode to achieve the optimal electricity price, and the electricity theft users need to consider the electricity theft benefits and punishment risks. The optimal AMIs deployment scheme is achieved by constructing the benefit function of electricity theft users, normal users, and distribution companies, then the optimal strategy of the game model is solved to combat electricity theft effectively.

The detection technology of electricity theft based on machine learning does not rely on the information about the power grid model and electricity theft means. It only uses the data set of electricity theft samples and historical power consumption data to train the detector to find the electricity theft behaviors and abnormal electricity consumption. The technology makes use of widely collected smart meter data without additional monitoring or control equipment, so the expensive manpower costs can be reduced. The principle of several artificial intelligence methods (such as fuzzy algorithm, neural network, and optimal path forest) used in NTL detection are discussed and the main challenges (such

as class imbalance, evaluation indexes, feature description, data quality, and algorithm portability) of applying artificial intelligence method are proposed in [16], [17].

So far, much research work on machine learning-based electricity theft detection methods has been presented. In [18]–[25], different kinds of combined machine learning algorithms are used to improve the accuracy in the detection of electricity theft. In [18], a combined method based on a two-way flow of information and energy is proposed to determine the suspicion ranks of most types of electricity thefts. The maximum information coefficient (MIC) is used to detect the electricity theft that appears normal in power consumption curves by analyzing the correlation between NTL and a certain electricity consumption behavior of users. The clustering technique by fast search and find of density peaks (CFSFDP) algorithm is suitable for detecting electricity theft with arbitrary shapes of load profiles. Combining the advantages of both methods, the users with higher suspicion degrees are finally determined as the electricity theft users. In [19], a three-stage multi-view stacking ensemble machine learning algorithm is proposed to analyze the electricity theft problem. The power consumption data are divided into different features based on hierarchical time series feature extraction methods. Through the integration of multiple classification algorithms of the meta-model, the accuracy of electricity theft detection is improved and the computing time is reduced. A combined model of the decision tree and support vector machine (SVM) algorithm is proposed in [20]. This model considers different levels of electricity theft behaviors (e.g., transmission, distribution, and user terminals), and takes the data processed by the decision tree as the input for SVM to realize the real-time detection of electricity theft at all levels of power systems. Two-dimensional electricity data are taken as input in [21], and a kind of wide and deep CNN model is trained to identify the non-periodic electricity theft and periodic normal power consumption. In [22], the relational denoising autoencoder is implemented to derive features and their associations in the high-dimensional imbalanced data of users, which helps improve the performance for electricity theft detection by maintaining the presence of features' associations. As a kind of spatiotemporal deep learning approaches, the stacked autoencoder (SAE) outperforms conventional machine learning approaches on electricity theft detection, which is evaluated in an IEEE 123-bus test feeder in [23]. The random forest (RF) algorithm integrates multiple decision trees to obtain higher classification accuracy than a single classifier. The RF model is trained in [24], [25] based on the obtained features to speculate the possible ways of stealing the abnormal data, which provides technical reference for on-site investigation of electricity theft.

In [26]–[30], some new or improved methods are proposed to implement the detection of electricity theft for specific application scenarios. Aiming at detecting malicious consumers that report fake or abnormal electricity consumption in AMI, an electricity theft detection scheme with load

monitoring and billing for AMI networks considering privacy-preserving is proposed in [26]. The convolutional neural network model is trained by masking fine-grained power consumption data to detect electricity theft users. A time-efficient NTL detection algorithm is proposed in [27] by solving the linear system of equations that describe the honesty of energy consumers. In [28], a parallelized method of encoding procedure and rule engine calculation is used to simplify the electricity consumption data without compromising the data quality, which helps improve the efficiency of electricity theft detection. In [29], the influence of noise in the electricity consumption data on the electricity theft detection results is focused on to make a distinction between special power consumption and abnormal power consumption, and the Bayesian detection rate is proposed to evaluate the accuracy in the different scenes of electricity theft detection comprehensively. In [30], a gradient boosting theft detector algorithm based on gradient boosting classifiers is proposed to weight the extracted features according to the importance for the electricity theft detection, and the complexity for classifying the electricity theft users is reduced.

It can be seen from the above literature review that most of the existing studies use different machine learning algorithms to extract time-series features to analyze the possibility of electricity theft behavior. However, there is still a research gap in the current research on electricity theft detection. First, many studies using classification algorithms have not focused on the problem of class imbalance (i.e., the number of electricity theft users is far less than the number of normal users), which could lead to a bad detection result that the electricity theft users are classified as the normal users incorrectly. Second, most of the existing studies only focus on comparing the output results with the actual labels of users, but ignoring the analysis of the suspicion level of each electricity theft user, which makes it difficult to determine the detection priority and the electricity theft users to be inspected in the actual detection process.

To improve the classification accuracy of the normal and electricity theft users, and formulate reasonable detection strategies to determine the detection priority for the electricity theft users, an electricity theft detection method based on SAE and the undersampling and re-sampling based random forest (UaRe-RF) algorithm is proposed in this work. First, the problem of class imbalance is mitigated by establishing subsets containing the normal users and the electricity theft users of similar proportions and integrating the classification result of each subset based on the proposed UaRe-RF algorithm, which not only ensures that the electricity theft users can be correctly detected, but also reduces the misclassification of normal users. Second, the proposed method analyses the suspicion levels of different electricity theft users, which refer to the possibilities of electricity theft (the suspicion level of a consumer is higher, the possibility that this consumer is an electricity theft user is higher). The detection priority can be flexibly adjusted

according to different targets in electricity theft inspection, which improves the flexibility and practicability of the method in practical engineering application. The results of the smart meter datasets from the Irish CER Smart Metering Project [31] and special transformer users in the distribution network of a certain area in China show that the electricity theft detection method proposed in this work can achieve a high accuracy rate in the detection results of different proportions of electricity theft users. Furthermore, the distribution of the suspicion levels is consistent with the actual situation, which helps to improve the detection priority of the electricity theft users with high suspicion levels and to reduce the workload of the actual inspection.

The main contributions of the proposed method are concluded as follows.

- 1) The features of the electricity consumption data are extracted by the supervised SAE, which is trained by stacking each autoencoder (AE) and adopting the supervised classification layer. The time complexity of the proposed algorithm is reduced because the feature adaptability is improved for the classification between the electricity theft users and the normal users.
- 2) A data sampling method for the extracted electricity features is proposed to establish subsets containing the normal users and the electricity theft users of similar proportions, which mitigates the problem of class imbalance and reduces the risk of misclassification in electricity theft detection.
- 3) The RF algorithm is adopted as the sub-classifier for each subset of electricity features, then the final model for electricity theft detection is established by integrating each sub-classifier with the corresponding weight. The accuracy of electricity theft detection is improved by integrating the classification result of each sub-classifier, and the detection priority can be adjusted flexibly based on the suspicion levels of each electricity theft user.

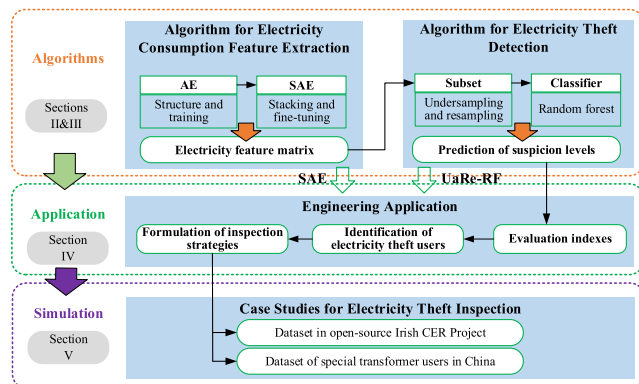


FIGURE 1. Overview of this paper.

The overview of this paper is shown in Fig. 1, and the rest of this work is organized as follows. The stacked autoencoder algorithm to extract electricity consumption features is

introduced in Section II. The classification algorithm for electricity theft detection based on UaRe-RF is presented in Section III. The overall electricity theft detection model is given in Section IV. Two cases are presented in Section V. Conclusions are given in Section VI.

II. STACKED AUTOENCODER BASED ELECTRICITY CONSUMPTION FEATURE EXTRACTION ALGORITHM

Electricity theft behaviors are often different from normal behaviors in electricity consumption features due to abnormal meter measurements. It is important to extract electricity consumption features with good discrimination between the electricity theft users and the normal users, which is guaranteed through the large-scale dataset with high completeness and the feature extraction algorithm with good performance. In the field of machine learning, SAE effectively reduces the difficulty in the parameter training process by adopting layer by layer stacking and parameter fine-tuning means [32], [33], and shows better performance in feature extraction than the traditional neural network.

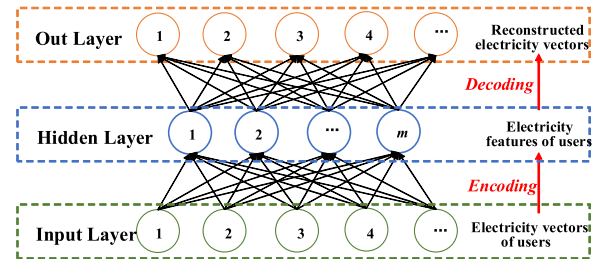


FIGURE 2. Structure of AE with electricity vectors as input.

A. STRUCTURE AND TRAINING PROCESS OF AUTOENCODER

The basic unit of SAE is an autoencoder (AE) which is a three-layer neural network structure (i.e., an input layer, a hidden layer, and an output layer), and the training process of AE is relatively simple [34]. The structure of AE is shown in Fig. 2, and the training process of AE consists of two processes: encoding and decoding. In the encoding process, the input of AE firstly is mapped to the hidden layer $F = \{f_1, f_2, \dots, f_N\}$, which is represented as

$$f_i = s(\omega \cdot x_i + b), \quad f_i \in \mathbf{R}^m \quad (1)$$

where the electricity consumption data acquired from meters of different users are set as $X = \{x_1, x_2, \dots, x_N\}$, $x_i \in \mathbf{R}^d$; N is the number of users and x_i is the electricity vector of user i with dimension d (the time length of the acquired electricity data); ω and b are the weight and deviation vector of the encoding formula respectively; s are the activation functions, such as sigmoid and tanh; m is the dimension of f_i reduced from d .

In the decoding process, F is mapped to the output layer $\tilde{X} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N\}$, which can be represented by

$$\tilde{x}_i = s(\tilde{\omega} \cdot f_i + \tilde{b}), \quad \tilde{x}_i \in \mathbf{R}^d \quad (2)$$

where $\tilde{\omega}$ and \tilde{b} are the weight and deviation vector of the decoding formula respectively, and d is the dimension of \tilde{X} that is reconstructed from F .

On the premise of reconstructing the electricity vector in the input layer as much as possible in the output layer, the dimension reduction data after encoding in the hidden layer are extracted as the features of the input electricity consumption data. The loss function L_{AE} in the reconstruction process is defined as

$$L_{AE} = \frac{1}{N} \sum_{i=1}^N \|x_i - \tilde{x}_i\|^2 + \frac{L_2}{2m} \|\omega\|^2 \quad (3)$$

where N is the number of users; x_i is the electricity vector of user i ; \tilde{x}_i is the output vector reconstructed from x_i ; L_2 is a constant to adjust the weight of the norm term; m is the dimension of feature vectors in the hidden layer; ω is the weight vector in the encoding process. The first term of L_{AE} is the reconstruction error between the input vector and the output vector, and the second term is the L2 norm to reduce the overfitting problem in the reconstruction process.

The training process of AE ends when the loss function L_{AE} in the reconstruction process meets the requirements, and the set of feature vectors $F = \{f_1, f_2, \dots, f_N\}$ is extracted from AE, where f_i is the feature vector compressed from x_i .

B. ELECTRICITY CONSUMPTION FEATURE EXTRACTION BASED ON STACKED AUTOENCODER

The SAE is established by cutting out the output layer of each AE and stacking the hidden layer of the former AE as the input layer of the latter AE. For a large-scale user dataset with high-dimensional electricity consumption data, the features extracted by a single AE are shallow and have low discrimination for electricity theft detection, so the cooperation of multiple AEs should be considered to fully extract the input features.

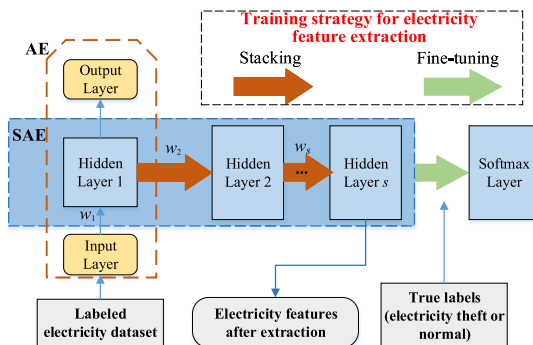


FIGURE 3. The training process of SAE for electricity feature extraction.

The training process of SAE for electricity consumption feature extraction is shown in Fig. 3, which includes layer-by-layer training and overall fine-tuning [35], [36]. The collected electricity vector of each user is taken as the input to train the first AE, then the next AE is stacked until the output of the

hidden layer in the last AE meets the dimension requirement. The overall loss of SAE L_{SAE} is represented as

$$L_{SAE} = 1 - \prod (1 - L_{AE}) \quad (4)$$

After all the trained AEs are stacked layer by layer, it is necessary to fine-tune the parameters of SAE to make the output of electricity consumption features after stacking more adaptable for the task of electricity theft detection. In the fine-tuning process, a training set is established with the original electricity vectors of users and the corresponding label vector (normal users or electricity theft users) as the input, and a softmax classification layer is added after the last AE layer. The output feature vectors of the last AE and the label vector of the training set are taken as the input for the softmax layer to train the overall structure, so the process of feature extraction is combined with the information of user type in the supervised fine-tuning process, which makes the final output of electricity consumption features in SAE more adaptable to classify the electricity theft users and the normal users.

III. UaRe-RF BASED ELECTRICITY THEFT DETECTION ALGORITHM

The electricity theft users can be detected from the abnormal electricity consumption features that are different from normal users. Take the electricity theft users and normal users as two labels, and the electricity theft detection can be regarded as a binary classification problem. For this kind of problem, the random forest algorithm in ensemble learning has shown good practicability by constructing multiple classifiers and integrating the results of each classifier. Furthermore, more attention should be paid to the fact that the number of electricity theft users is generally far less than that of normal users, so it is necessary to deal with the problem of class imbalance before the detection of electricity theft. Based on the above two points, the UaRe-RF based electricity theft detection algorithm is proposed in this work to mitigate the problem of class imbalance and improve the accuracy of electricity theft detection. First, the random undersampling and re-sampling methods are adopted to establish class balanced classification subsets. Then the RF algorithm is used to train each subset. Finally, the voting method is used to ensemble the results of each RF classifier to determine the suspicion levels and detect electricity theft users.

A. CLASS IMBALANCE PROBLEM IN ELECTRICITY THEFT DETECTION

The electricity theft detection is faced with the problem of class imbalance for the reason that the number of electricity theft users is generally far less than the normal users in the actual distribution systems. If the original data set is classified directly, the algorithm tends to classify electricity theft users as normal users. To deal with the problem of class imbalance, methods such as undersampling for majority samples, oversampling for minority samples, and cost sensitivity learning are presented.

For electricity theft detection, the undersampling method can effectively reduce the training time by selecting some normal users to construct a smaller but class balanced dataset. However, many samples of normal users are discarded and only limited features are learned for electricity theft detection. The oversampling method generates electricity theft samples to balance the two classes of samples. However, the training time of the larger dataset is increased and the inappropriate generation methods of electricity theft samples have a negative impact on the detection of electricity theft. The electricity theft users are set greater weights in the cost sensitivity learning. However, the weight setting method tends to be subjective, and the accuracy of electricity theft detection cannot be guaranteed.

To mitigate the problem of class imbalance and fully learn the electricity consumption features, the undersampling method is combined with the ensemble learning algorithm [37]–[40]. In [37], the majority samples are divided into several subsets independently, and the size of each subset is equal to that of the minority samples. On the one hand, the time complexity is greatly improved because of the increased subsets when the proportion of electricity theft users is too low. On the other hand, the same minority samples are used in each classifier, so the diversity of classifiers is relatively low and it is easy to be overfitted in the training process. The undersampling method is combined with the AdaBoost [38] and the RF algorithm in the EasyEnsemble [39] and the balanced random forest (BRF) algorithm [40]. The training time is acceptable in the two proposed algorithms, but the problem of low diversity is still not solved due to the same processing method for minority samples as in [37].

B. ELECTRICITY THEFT DETECTION BASED ON UaRe-RF ALGORITHM

The UaRe-RF based electricity theft detection algorithm is proposed in this work to mitigate the problem of class imbalance. An initial combination set is firstly established in UaRe-RF based on dividing the majority of samples into subsets with the same size as the minority samples. Then, each combination subset is re-sampled and taken as the input of each classifier. Finally, all the trained classifiers are integrated into the electricity theft detection model. The classifier adopted in the proposed algorithm is RF, whose training process for electricity theft detection is shown in Fig. 4. RF integrates multiple decision trees to obtain higher classification accuracy than a single classifier. The classification performance of RF is closely related to the performance of the decision tree and the diversity of input training subsets, which ensure the accuracy and the generalization ability of the ensemble classifier.

The whole training process of UaRe-RF is shown in Fig. 5. The undersampling and re-sampling method is used to establish the class-balanced subsets in the proposed UaRe-RF algorithm. In the undersampling process, each class-balanced subset is established by selecting the samples randomly in the

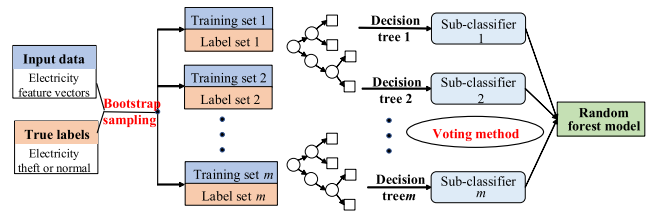


FIGURE 4. The training process of RF for electricity theft detection.

group of normal users, and the number of normal users that are selected is equal to the number of electricity theft users. The undersampling process ends when all the normal users are selected out. In the re-sampling process, the samples in each subset are selected again through the bootstrap method, which helps improve the diversity of feature attributes and achieve a better training effectiveness of the random forest classifier. The training set with N_{tr} users is divided into normal users X_p and electricity theft users X_q ($|X_q| < |X_p|$). There are S combined subsets and N_r base classifiers in the RF classifier H_i ($i = 1, 2, \dots, S$). The training process of UaRe-RF is as follows:

Step 1: Undersample the X_p randomly without replacement to get $X_{p,1}, X_{p,2}, \dots, X_{p,S}$, $|X_{p,i}| = |X_q|$ and $(X_{p,1} + X_{p,2} + \dots + X_{p,S}) = X_p$.

Step 2: Establish the initial combination set $X_{or} = [(X_{p,1} + X_q), (X_{p,2} + X_q), \dots, (X_{p,S} + X_q)]$.

Step 3: Resample each initial subset in X_{or} to get the resampled set X_{re} through the bootstrap method.

Step 4: Take the S resampled subsets in X_{re} as the inputs of each RF classifier, and the training result of H_i can be represented as

$$H_i = \text{sgn}\left(\sum_{j=1}^{N_r} h_{i,j}(x)\right) \quad (5)$$

where $h_{i,j}(x)$ is the training result of the decision tree j in the RF classifier i ; N_r is the number of decision trees in H_i ; $\text{sgn}(x)$ is the signum function, $\text{sgn}(x) = 1$ if $x > 0$ and $\text{sgn}(x) = -1$ if $x < 0$.

The trained RF classifiers are ensemble to get the final classifier H_f as

$$H_f = \text{sgn}\left(\sum_{i=1}^S \alpha_i H_i - \theta\right) \quad (6)$$

where α_i is the ensemble weight of each RF classifier and θ is a classification threshold.

A 10-fold cross-validation method is used to determine the accuracy r_j^{ac} ($j = 1, 2, \dots, 10$) of each RF classifier. The ensemble weight α_i of classifier H_i is determined as follows.

$$\alpha_i = \frac{1}{10} \sum_{j=1}^{10} r_j^{ac} \quad (7)$$

For UaRe-RF based electricity theft detection algorithm, the original training set is divided into S subsets after

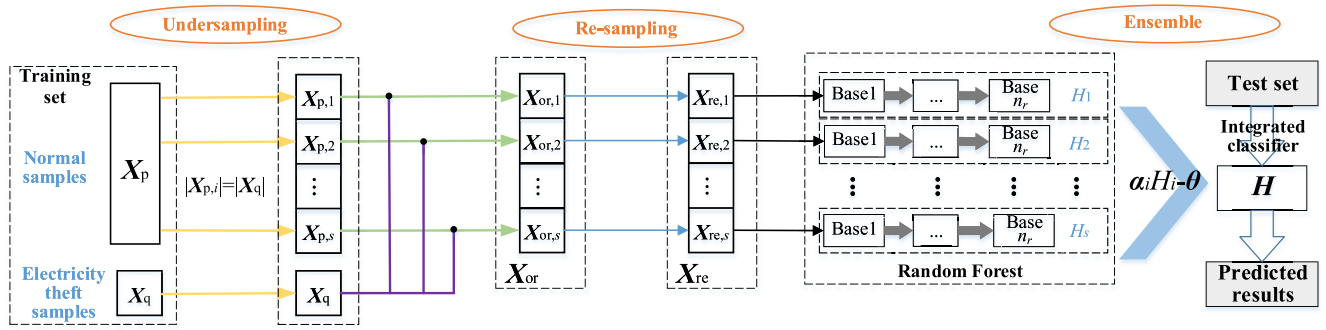


FIGURE 5. The training process of the UaRe-RF algorithm for electricity theft detection.

undersampling and re-sampling, which are used as the inputs to train RF classifiers. Thus, all the electricity consumption features of normal users are trained from the initial combination set X_{or} established by undersampling, and the overfitting problem caused by the same minority samples in each RF classifier is alleviated by the resampling method. The time complexity of UaRe-RF is reduced for the reason that each RF in this method can be trained parallelly, and the training time cost by undersampling and re-sampling can be ignored compared with that of the RF algorithm. Because of the strong adaptability of the RF algorithm, each sub-classifier can achieve high classification accuracy and the diversity of each input subset can be guaranteed by re-sampling. Therefore, after the sub-classifiers are ensemble, the accuracy of electricity theft detection is improved.

C. CLASSIFICATION INDEXES

To evaluate the classification performance of the proposed method in this work, three classification indexes are selected based on the true positive (TP), false positive (FP), true negative (TN), and false negative (FN) in the confusion matrix (taking the electricity theft samples as the positive class).

1) R_1 : R_1 represents the recall rate to evaluate the completeness of electricity theft samples in detection results. A larger R_1 means that more real electricity theft users are correctly detected in the classification result and fewer real electricity theft users are misclassified as normal users.

$$R_1 = \frac{N_{TP}}{N_{TP} + N_{FN}} \tag{8}$$

where N_{TP} and N_{FN} are the numbers of TP and FN, respectively.

2) R_2 : R_2 represents the precision rate to evaluate the influence of the misclassified normal samples (FP) on the detection of electricity theft users. A greater R_2 means that fewer actual normal users are misclassified as electricity theft users in the classification result. Due to the class imbalance between positive and negative classes, the number of TP and FP would be quite different. It cannot accurately express the relative numerical relationship between normal and electricity theft users when the number of TP and FP is

directly calculated. Therefore, the ratio of TP and FP in the positive class and negative class (denoted as r_{TP} and r_{FP}) is respectively used to determine R_2 as follows.

$$R_2 = \frac{r_{TP}}{r_{TP} + r_{FP}} \tag{9}$$

$$\begin{cases} r_{TP} = \frac{N_{TP}}{N_{TP} + N_{FN}} \\ r_{FP} = \frac{N_{FP}}{N_{FP} + N_{TN}} \end{cases}$$

where N_{TN} and N_{FP} are the numbers of TN and FP, respectively.

3) R_3 : R_3 is the area under the receiver operating characteristic curve (ROC), which takes the false positive rate (FPR) as the x-axis and the true positive rate (TPR) as the y-axis. In general, a larger R_3 represents a better overall performance of the classifier for the higher true positive rate and the lower false positive rate.

IV. THE PROPOSED ELECTRICITY THEFT DETECTION METHOD IN ENGINEERING APPLICATION

The flowchart of the proposed electricity theft detection method based on the SAE and UaRe-RF algorithms is presented in Fig. 6, and the key steps in engineering application are described as follows.

1) Take the collected electricity data of users to be detected as the input, and extract the electricity consumption features in the training process of SAE.

Collect the electricity data of N users (the time length is d) and establish the input electricity matrix $E \in \mathbf{R}^{N \times d}$ as

$$E = \begin{bmatrix} E_{1,1} & E_{1,2} & \cdots & E_{1,d} \\ E_{2,1} & E_{2,2} & \cdots & E_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ E_{N,1} & E_{N,2} & \cdots & E_{N,d} \end{bmatrix} \tag{10}$$

where $E_{i,j}$ is the j -th electricity value in the electricity records of the i -th user.

In the training process of SAE, each AE is trained layer by layer and the stacking process is terminated when the last AE meets the requirement of L_{SAE} . The output of compressed electricity features and the user labels are taken as the input

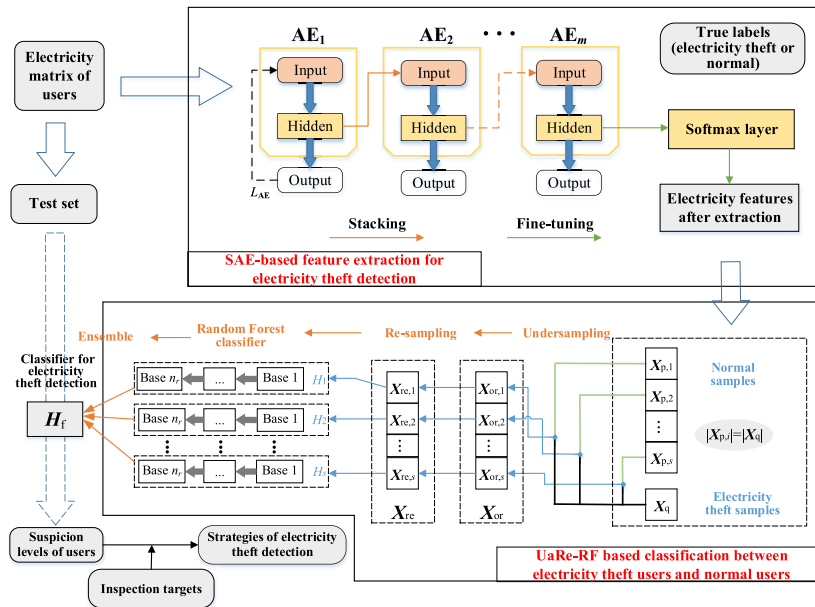


FIGURE 6. Flowchart of the proposed electricity theft detection method.

of the softmax classification layer, and the parameters of SAE are fine-tuned to improve the adaptability of the output electricity features for electricity theft detection. When the accuracy requirement is satisfied, the fine-tuning process is finished, and the output of SAE is taken as the final electricity feature matrix.

2) Establish the class balanced subsets with the extracted electricity features as input, and integrate each trained RF to get the final classifier for electricity theft detection.

A sample reconstruction method based on random under-sampling and re-sampling is adopted for the normal user samples to establish the class balanced subsets (i.e., the number of normal users and electricity theft users are relatively balanced). The sub-classifier RF is trained by the electricity features in each subset, and the classification accuracy of each RF in cross-validation is taken as the ensemble weight to determine the integrated classifier for electricity theft detection.

3) Classify the electricity theft users and the normal users, and formulate the flexible detection strategies for practical requirements based on the suspicion levels of electricity theft users.

In the practical engineering application, the proposed method not only classifies the electricity theft users and the normal users by mitigating the class imbalance problem, but also determines the suspicion level of each potential electricity theft user, which provides a more reasonable reference and basis for the actual electricity theft inspection. The strategies of electricity theft detection can be formulated based on the distribution of suspicion levels according to different inspection targets, which helps reduce the workload and improve the efficiency in the actual electricity

theft inspection. The classification performance for periodic electricity theft detection mainly depends on the difference of the potential electricity consumption features between the normal and the electricity theft users. However, the time of electricity theft and normal electricity consumption of non-periodic electricity theft users is difficult to be distinguished because of its non-periodic electricity theft behavior. A feasible method for non-periodic electricity theft detection is to establish a long-term observation strategy and learn the difference of electricity consumption features between the normal and the electricity theft period of the user by the proposed model.

V. CASE STUDIES

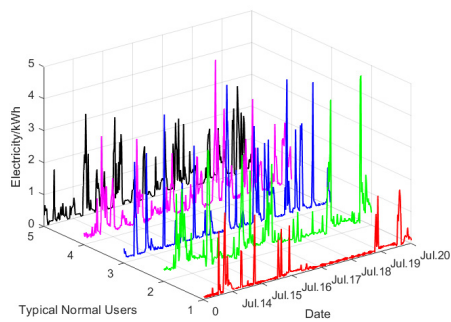
The proposed electricity theft detection model is simulated using the software Spyder, and the programming language is Python (Version 3.7). The simulation results are visualized by Matlab 2019b. The experimental environment is running on Intel (R) Xeon (R) Gold 5117 CPU @ 2.00 GHz, having 64GB RAM and the graphics processing unit (Nvidia GeForce RTX 2080 Ti, 11 GB video memory).

A. ORIGINAL DATASETS

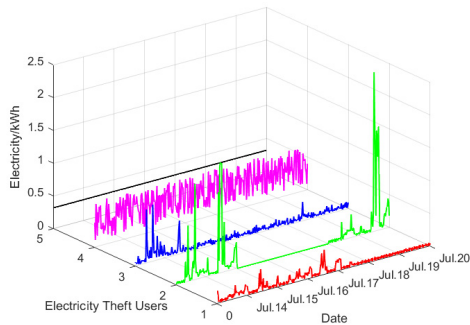
The original datasets include the electricity consumption data in the smart meter dataset from the Irish CER Smart Metering Project [31] (denoted as DS-I) and the actual electricity consumption data of special transformer users in the distribution network of a certain area in China (denoted as DS-II). The DS-I can be used to remodel the proposed method by readers, which helps verify the generality of the proposed model. The DS-II helps verify the accuracy of electricity theft detection and the flexibility in the actual application case. It can be seen that the two datasets are used to analyze and

verify the different application effectiveness of the proposed model, however, it does not mean that the proposed model can only perform well in the two cases.

In DS-I, there are 4225 households, 485 small and medium-sized enterprises, and 1735 users of other types with 535 days of electricity consumption data and the acquisition interval is 30 minutes. To unify the user types and collection periods, this work selects the electricity consumption data of 7 days (i.e., 336 in dimension) with 1800 households to form the original data set. Since all users in DS-I can be considered as normal users, this work uses the principles in [29] to generate samples of electricity theft users, which are represented in the appendix.



(a) Weekly electricity consumption curves of normal users



(b) Weekly electricity consumption curves of electricity theft users

FIGURE 7. Weekly electricity consumption curves of normal and electricity theft users.

The weekly electricity consumption curves of five types of electricity theft users and five typical normal users are shown in Fig. 7 respectively.

DS-II contains 50 electricity theft users who have been checked correctly and about 500 normal special transformer users with about 200 days of electricity consumption data. The acquisition interval is 15 minutes. In this work, the electricity consumption data in 7 days (i.e., 672 in dimension) of 450 normal users and 50 electricity theft users are selected to form the input data set.

To analyze the effectiveness of the proposed model on different levels of class imbalance, four different proportions of electricity theft users are set as 5%, 10%, 15%, and 20%, respectively. The number of electricity theft (denoted as ET)

TABLE 1. Input settings of DS-I and DS-II.

	Proportion	5%		10%		15%		20%	
		Class	ET	NU	ET	NU	ET	NU	ET
DS-I	Total	80	1520	180	1620	180	1020	180	720
	Training set	50	950	120	1080	120	680	120	480
	Test set	30	570	60	540	60	340	60	240
DS-II	Total	20	380	50	450	45	255	50	200
	Training set	10	190	30	270	25	145	25	100
	Test set	10	190	20	180	20	110	25	100

TABLE 2. The main parameters of algorithms.

Algorithms	Main parameters
SAE	Number of layers: 2; Max-epochs: 400; Hidden size of layer 1: 80; Hidden size of layer 2: 16.
UaRe-RF	Max-depth: 6; Max-features: 7; Number of estimators: 100; Classification threshold: 0.5.

and normal users (denoted as NU) in the training set and test set of DS-I and DS-II are shown in Table 1.

The main parameters manually set for SAE and the UaRe-RF algorithm are mainly listed in Table 2.

B. FEATURE EXTRACTION AND CLASSIFICATION FOR ELECTRICITY THEFT DETECTION

1) FEATURE EXTRACTION PROCESS

The training process of SAE mainly includes the training of each AE, layer by layer stacking, and supervised fine-tuning.

The reconstruction loss L_{AE} of each AE and the L_{SAE} of SAE are considered in the training of AE to determine the output dimension of each layer of AE to stack the next layer. In the process of stacking, the total reconstruction loss is not higher than 1%. When DS-I is taken as input, the dimension is reduced to 80 from the first encoder with $L_{AE} = 0.0655$. The dimension of the output of the first AE is reduced to 16 in the second encoder with $L_{AE} = 0.0238$. The L_{SAE} is obtained as 0.0877 and meets the requirement.

After the stacking process of SAE layer by layer, the softmax layer is added to build the whole neural network, and the training set data labels are used as an additional input to conduct the supervised fine-tuning process of SAE.

After the parameters of the whole neural network are fine-tuned, input the training set and test set respectively, and 16-dimensional electricity consumption features can be extracted from both DS-I and DS-II.

2) CLASSIFICATION PROCESS

After undersampling is performed randomly for normal users, the initial combination sets are established and re-sampled respectively to obtain the relatively class balanced subsets.

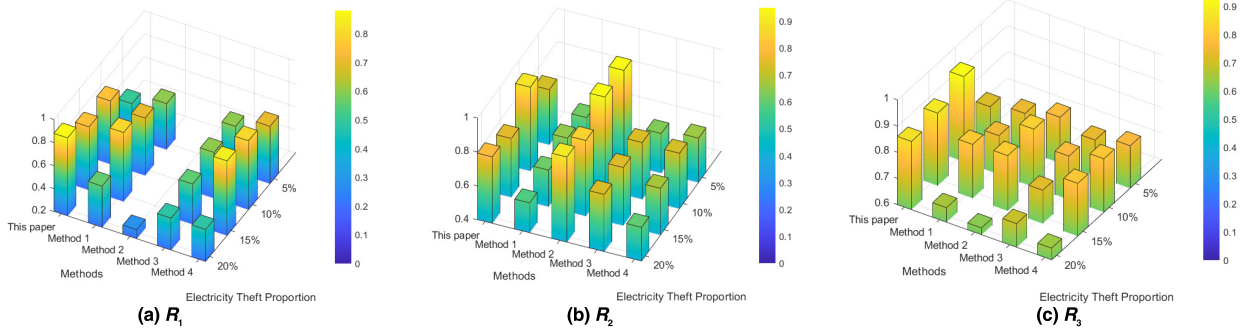


FIGURE 8. Performance of the methods in different electricity theft proportions in DS-I.

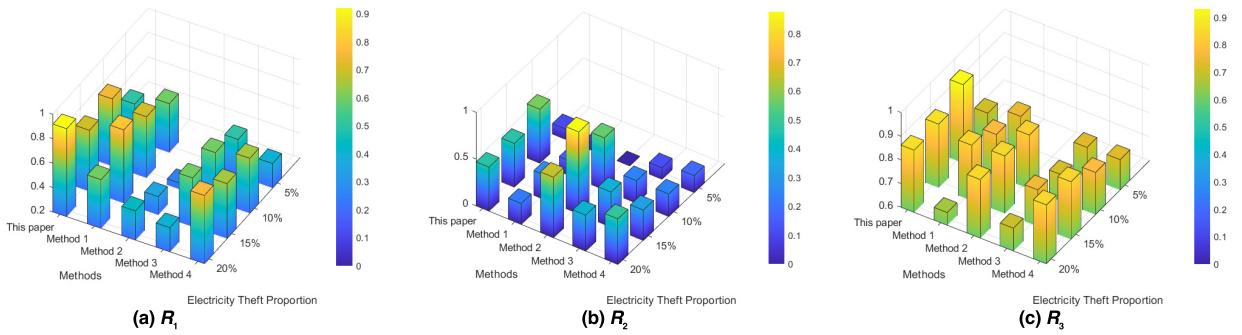


FIGURE 9. Performance of the methods in different electricity theft proportions in DS-II.

Taking DS-I as an example, the proportion of electricity theft users is 10% and s is 9. Finally, the weights of s RFs are $\alpha = [0.112, 0.112, 0.112, 0.112, 0.110, 0.109, 0.109, 0.109, 0.115]$. The principle of RF for binary classification problems is to determine the possibility of each input sample, whose range is from 0 to 1. The proposed UaRe-RF model takes each RF as the sub-classifier, and the suspicion level of each user is determined by the combination of the output classification possibility of each RF. Suppose that the possibilities of electricity theft and normal samples returned in each RF classifier are ρ_i^+ and $\rho_i^- = 1 - \rho_i^+$, so the ensemble possibilities of two classes are defined as $\rho^+ = \sum_{i=1}^s \alpha_i \rho_i^+$ and $\rho^- = \sum_{i=1}^s \alpha_i \rho_i^-$, and the suspicion level of electricity theft users is ρ^+ . The range of suspicion level is from 0 to 1, and the user is more likely to be detected as the electricity theft user if its suspicion level is closer to 1.

C. CLASSIFICATION PERFORMANCE OF THE PROPOSED ELECTRICITY THEFT DETECTION METHOD AND THE COMPARISONS

To verify the effectiveness of the method proposed in this work for the electricity theft detection, the proposed method is compared with other related methods. The feature extraction and classification algorithms adopted in each comparison are shown in Table. 3.

TABLE 3. The related methods for electricity theft detection in comparisons.

Methods	Feature extraction	Classification algorithm
Method 1	Unsupervised SAE	UaRe-RF
Method 2	SAE	RF
Method 3	SAE	Balanced RandomForest [40]
Method 4	SAE	EasyEnsemble [39]

It can be seen in Table 3 that: the supervised SAE proposed in this work is compared with Method 1 to verify the function of the supervised fine-tuning process for feature extraction in SAE; the necessity of mitigating the problem of class imbalance is verified by comparing the proposed method with Method 2; the proposed UaRe-RF algorithm is compared with the existing ensemble learning algorithms that consider the class imbalance problem in Methods 3 and 4 to verify the higher accuracy in electricity theft detection.

The classification threshold θ is set as 0.5, which means a sample will be regarded as an electricity theft user if its suspicion level is greater than 0.5; otherwise, it will be regarded as a normal user. For the different proportions of electricity theft samples, the statistics of classification indexes associated with different methods in DS-I and DS-II are shown in Figs. 8 and 9, respectively.

As can be seen from Figs. 8 and 9, Method 2 performs better than other methods w.r.t. the index R_2 for the reason that RF does not consider the problem of class imbalance,

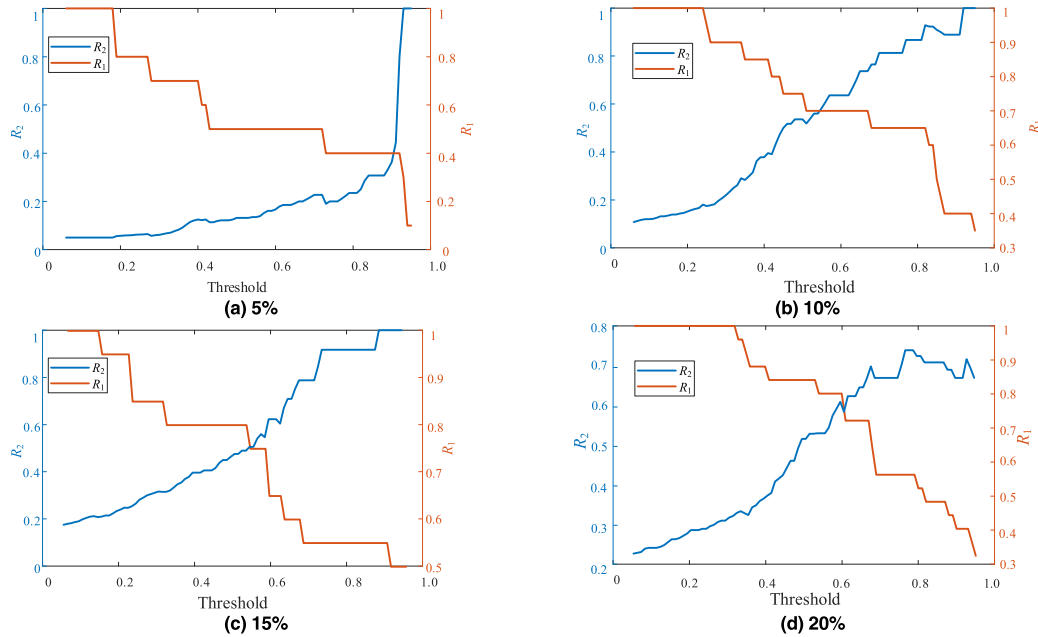


FIGURE 10. Trends of R_1 and R_2 with the increased classification threshold.

so it tends to classify all samples as normal users with few normal users that are classified as electricity users incorrectly.

Other methods (i.e., Methods 1, 3, and 4) that consider the process of class imbalance perform better w.r.t. the index R_1 than Method 2 (i.e., more electricity theft users are detected correctly), but more normal users are mistakenly classified as electricity theft users in them, so Methods 1, 3, and 4 perform worse than the proposed method in this work w.r.t. R_2 .

As R_3 is a comprehensive evaluation index that is related to both R_1 and R_2 , it can be seen that the method proposed in this work has the best performance w.r.t. R_3 for the reason that it performs well w.r.t. R_1 and especially R_2 . Compared with Method 1 (unsupervised SAE), the adaptability of the extracted electricity consumption features to UaRe-RF can be improved by adding a supervised fine-tuning training process to SAE, thus misclassifications of normal users are reduced and more electricity theft users are classified correctly.

D. DISTRIBUTION OF SUSPICION LEVELS AND DETECTION STRATEGY FOR DS-II

This section analyzes the influence of the change in classification threshold w.r.t. R_1 and R_2 , then formulates specific strategies for actual detection work based on the distribution of suspicion levels in DS-II.

1) CLASSIFICATION PERFORMANCE WITH THE CHANGE OF THRESHOLD

As shown in Fig. 10, when the classification threshold increases from 0.1 to 0.9, the R_1 gradually decreases with the decreased number of detected electricity theft users, and

the R_2 gradually increases with the decreased number of normal users detected incorrectly under different electricity theft proportions. When the threshold is lower, R_2 is lower too for the reason that although some electricity theft users are constantly detected, more normal users are incorrectly classified as electricity theft users.

To sum up, it is necessary to increase the threshold appropriately when focusing on the detection of electricity theft users with a high suspicion level. At the same time, the efficiency of electricity theft detection is higher, and the workload is reduced when more attention is paid to users with higher suspicion levels.

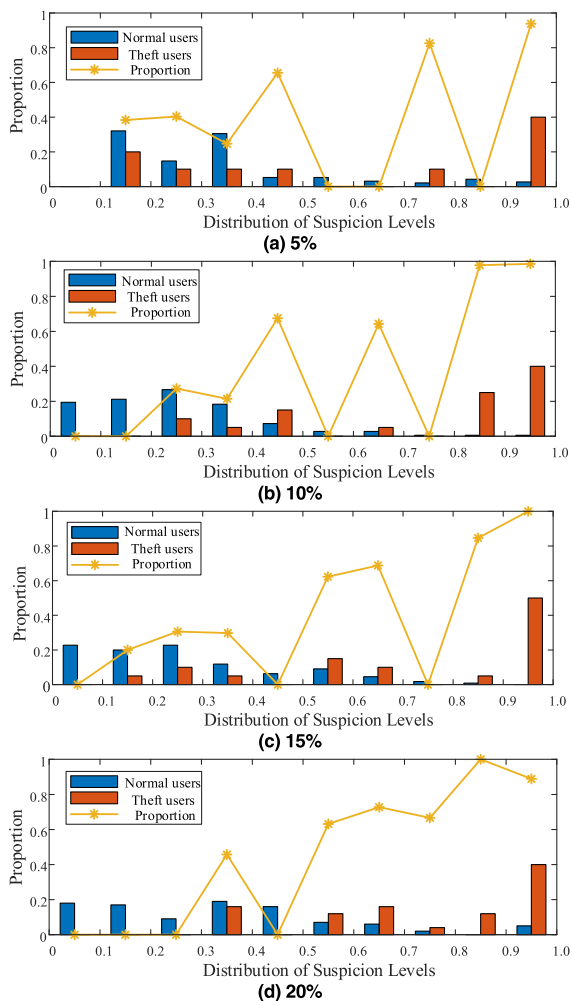
2) FORMULATION OF DETECTION STRATEGIES

It can be seen from the previous section that the trend of R_1 and R_2 varies with the classification threshold. Therefore, in the actual detection work, it is necessary to select a reasonable range of suspicion levels to determine the key electricity theft users considering the specific inspection purposes. The distributions of suspicion levels under different electricity theft proportions are shown in Fig. 11. In the different suspicion intervals, the histograms represent the respective proportions of normal and electricity theft users, and the line graphs represent the proportion of electricity theft users to all users in this interval.

It can be seen from Fig. 11 that the suspicion levels of the most normal users are distributed in $(0.1, 0.5]$, which indicates a low electricity theft possibility. In the distribution of high suspicion levels, the proportion of normal users is small, but it is reasonable to suspect that they are actual electricity theft users.

TABLE 4. Ranges of suspicion levels for target-I and target-II.

The proportion of electricity theft users in DS-II	Target-I		Target-II	
	Range of suspicion levels	The proportion of electricity theft users detected correctly	Range of suspicion levels	The proportion of normal users detected incorrectly
5%	(0.2,1)	80%	(0.7,0.8] (0.9,1)	17.4% 6.2%
10%	(0.4,1)	85%	(0.8,0.9] (0.9,1)	2.2% 1.4%
15%	(0.5,1)	80%	(0.8,0.9] (0.9,1)	15.4% 0
20%	(0.5,1)	84%	(0.8,0.9] (0.9,1)	0 11.1%

**FIGURE 11. Distribution of suspicion levels in different proportions.**

When the proportion of electricity theft is low (e.g., 5% or 10%), the suspicion levels of some electricity theft users are distributed in (0.1,0.4], which makes it difficult to detect in the actual inspection; the others are distributed in (0.7,0.9] and the possibility of electricity theft is high. When the proportion of electricity theft is high (e.g., 15% or 20%), the suspicion levels of electricity theft users are higher overall, which are generally distributed in (0.5,1.0).

For specific detection targets (denoted as Target-I, Target-II, and Target-III) in detection work, the optimal detection strategies are made as follows:

1) Target-I: the actual work pays more attention to the number of electricity theft users correctly detected, and this target sets $R_1 \geq 80\%$, that is, at least 80% of the electricity theft users are detected correctly.

The ranges of suspicion levels to be detected are shown in Table 4 to achieve Target-I, and there are at least 80% of electricity theft users that can be detected correctly.

2) Target-II: the actual work pays more attention to the efficiency of the detection process, and this target sets $R_2 \geq 80\%$, that is, the actual normal users incorrectly detected are not more than 20%.

The ranges of suspicion levels to be detected are shown in Table 4 to achieve Target-II, and there are no more than 20% of normal users that are detected incorrectly.

3) Target-III: the actual work only concerns the suspicion levels of electricity theft behavior in all users. A normal user with a high suspicion level is still regarded as an electricity theft user who has not been detected before.

For this target, the range of suspicion levels is (0.9,1), and there are 5, 1, 0, and 5 normal users that need to be detected whether there is an electricity theft problem in the proportion of 5%, 10%, 15%, and 20%, respectively.

E. SUMMARY OF CASE STUDIES

The summary concluded from the results in Sections V-C and V-D is concluded as follows:

First, as it can be seen from Figs. 8 and 9, the proposed method has the best performance in R_3 and performs well in R_1 and R_2 compared with other methods. The adaptability of the extracted electricity consumption features to UaRe-RF can be improved by adding a supervised fine-tuning training process to SAE, and the proposed data sampling method for the extracted electricity features mitigates the problem of class imbalance and reduces the risk of misclassification in electricity theft detection. Therefore, misclassifications of normal users are reduced and more electricity theft users are classified correctly based on the proposed method.

Second, as it can be seen from Figs. 10 and 11, the R_1 and R_2 change differently when the classification

threshold increases from 0.1 to 0.9. It is necessary to increase the threshold appropriately when focusing on the detection of electricity theft users with a high suspicion level. Furthermore, the strategies of electricity theft detection can be formulated based on the distribution of suspicion levels according to different inspection targets, which helps reduce the workload and improve the efficiency in the actual electricity theft inspection.

VI. CONCLUSION

To improve the accuracy in electricity theft detection and further improve the detection priority of the electricity theft users with high suspicion levels, an electricity theft detection method is proposed in this work based on SAE and UaRe-RF algorithm. The results of two types of data sets show that the proposed method has a higher accuracy rate in different electricity theft proportions compared with other related methods by mitigating the problem of class imbalance and adding the fine-tuning process in SAE. Furthermore, reasonable strategies are formulated for specific detection purposes based on the distribution of suspicion levels, and the key electricity theft users are considered with a higher detection priority, thus the workload is reduced as well.

In further research, the proposed method will take more types of electrical data (e.g., current, voltage, and power factor) as the input to verify the robustness and accuracy. In addition, the proposed model will be used in two-dimensional scenarios to provide an auxiliary reference for the classification of electricity theft users and malfunctioned AMI owners (i.e., the difference of electricity consumption of different users in the same period can be modeled to analyze the features of abnormal power consumption, and the difference of electricity consumption of the same user in different periods can be modeled to locate the start time and duration of the abnormal power consumption).

APPENDIX

The five principles for the generation of the electricity theft samples in DS-I are represented as

$$\left\{ \begin{array}{l} y_1(t) = \alpha \cdot x(t), \\ \alpha = \text{rand}(0.1, 0.8) \\ y_2(t) = \begin{cases} 0, & t \in (t_1, t_2) \\ x(t), & t \in [1, t_1] \cup [t_2, T] \end{cases} \\ y_3(t) = \beta(t) \cdot x(t), \\ \beta(t) = \text{rand}(0.1, 0.8) \\ y_4(t) = \beta(t) \cdot \frac{1}{T} \sum_{t=1}^T x(t) \\ y_5(t) = \frac{1}{T} \sum_{t=1}^T x(t) \end{array} \right. \quad (\text{A1})$$

where $x(t)$ is the electricity value of a normal user at time t ; $y_1(t)$ - $y_5(t)$ are the different kinds of generated electricity value of electricity theft; $\text{rand}(0.1, 0.8)$ is a function that

returns a random number from 0.1 to 0.8; T is the time length of daily electricity series; t_1 and t_2 are the time between the start and end time at a day.

ACKNOWLEDGMENT

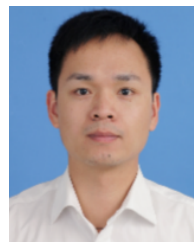
The authors would like to thank Dr. Li Yang for the valuable discussions and advices, and thank Huakun Que and Zetao Jian for their help and cooperation to extract the data.

REFERENCES

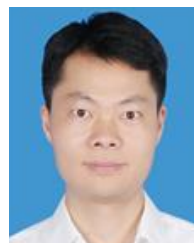
- [1] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gomez-Exposito, "Detection of non-technical losses using smart meter data and supervised learning," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2661–2670, May 2019.
- [2] Northeast Group LLC. (2017). *Electricity Theft and Non-Technical Loss: Global Markets, Solutions, and Vendors*. [Online]. Available: <http://www.northeast-group.com>
- [3] B. Businessweek. (2014). *India Fights to Keep the Lights*. [Online]. Available: <https://www.bloomberg.com/news/articles/2014-06-05/india-fights-electricity-theft-as-modi-pledges-energy-upgrade>
- [4] Y. Song, X. Liu, Z. Li, M. Shahidepour, and Z. Li, "Intelligent data attacks against power systems using incomplete network information: A review," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 4, pp. 14–25, 2018.
- [5] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, Apr. 2014.
- [6] S. Liu, X. Cui, Z. Lin, Z. Lian, Z. Lin, F. Wen, Y. Ding, Q. Wang, L. Yang, R. Jin, and H. Qiu, "Practical method for mitigating three-phase unbalance based on data-driven user phase identification," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1653–1657, Mar. 2020.
- [7] Y. Xu, "A review of cyber security risks of power systems: From static to dynamic false data attacks," *Protection Control Mod. Power Syst.*, vol. 5, no. 1, pp. 8–19, Dec. 2020.
- [8] B. Bat-Erdene, B. Lee, M.-Y. Kim, T. H. Ahn, and D. Kim, "Extended smart meters-based remote detection method for illegal electricity usage," *IET Gener., Transmiss. Distrib.*, vol. 7, no. 11, pp. 1332–1343, Nov. 2013.
- [9] P. Jokar and V. C. M. Leung, "Intrusion detection and prevention for ZigBee-based home area networks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1800–1811, May 2018.
- [10] S. Liu, Z. Lin, Y. Zhao, Y. Liu, Y. Ding, B. Zhang, L. Yang, Q. Wang, and S. E. White, "Robust system separation strategy considering online wide-area coherency identification and uncertainties of renewable energy sources," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 3574–3587, Sep. 2020.
- [11] W. Fan and Y. Liao, "Wide area measurements based fault detection and location method for transmission lines," *Protection Control Mod. Power Syst.*, vol. 4, no. 1, pp. 53–64, Dec. 2019.
- [12] A. Bin-Halabi, A. Nouh, and M. Abouelela, "Remote detection and identification of illegal consumers in power grids," *IEEE Access*, vol. 7, pp. 71529–71540, 2019.
- [13] S. G. Naik, V. Ravi, and R. Arshiya, "Programmable protective device for LV distribution system protection," *Protection Control Mod. Power Syst.*, vol. 3, no. 1, pp. 285–290, Dec. 2018.
- [14] A. A. Cardenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1830–1837.
- [15] C. H. Lin, S. J. Chen, C. L. Kuo, and J. L. Chen, "Non-cooperative game model applied to an advanced metering infrastructure for non-technical loss screening in micro-distribution systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2468–2469, Sep. 2014.
- [16] T. Ahmad, H. Chen, J. Wang, and Y. Guo, "Review of various modeling techniques for the detection of electricity theft in smart grid environment," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 2916–2933, Feb. 2018.
- [17] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," *Int. J. Comput. Intell. Syst.*, vol. 10, no. 1, p. 760, 2017.
- [18] K. Zheng, Q. Chen, Y. Wang, C. Kang, and Q. Xia, "A novel combined data-driven approach for electricity theft detection," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1809–1819, Mar. 2019.

- [19] Z. Ouyang, X. Sun, J. Chen, D. Yue, and T. Zhang, "Multi-view stacking ensemble for power consumption anomaly detection in the context of industrial Internet of Things," *IEEE Access*, vol. 6, pp. 9623–9631, 2018.
- [20] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.
- [21] 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 Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.
- [22] Z. Aslam, F. Ahmed, A. Almogren, M. Shafiq, M. Zuair, and N. Javaid, "An attention guided semi-supervised learning mechanism to detect electricity frauds in the distribution systems," *IEEE Access*, vol. 8, pp. 221767–221782, 2020.
- [23] R. R. Bhat, R. D. Trevizan, R. Sengupta, X. Li, and A. Bretas, "Identifying nontechnical power loss via spatial and temporal deep learning," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Anaheim, CA, USA, Dec. 2016, pp. 272–279.
- [24] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity theft detection in power grids with deep learning and random forests," *J. Electr. Comput. Eng.*, vol. 2019, p. 12, Oct. 2019.
- [25] K. Yan, J. Zhao, and Y. Ren, "Electricity theft identification algorithm based on auto-encoder neural network and random forest," in *Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Mar. 2021, pp. 2641–2645.
- [26] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmay, and E. Serpedin, "PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96334–96348, 2019.
- [27] J. Y. Kim, Y. M. Hwang, Y. G. Sun, I. Sim, D. I. Kim, and X. Wang, "Detection for non-technical loss by smart energy theft with intermediate monitor meter in smart grid," *IEEE Access*, vol. 7, pp. 129043–129053, 2019.
- [28] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and R. C. Green, "High performance computing for detection of electricity theft," *Int. J. Electr. Power Energy Syst.*, vol. 47, pp. 21–30, May 2013.
- [29] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.
- [30] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.
- [31] (Nov. 2020). *Irish Social Science Data Archive*. [Online]. Available: <http://www.ucd.ie/issda/data/commissionforenergyregulationcer>
- [32] S. Liu, S. You, H. Yin, Z. Lin, Y. Liu, W. Yao, and L. Sundaresh, "Model-free data authentication for cyber security in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4565–4568, Sep. 2020.
- [33] E. Hosseini-Asl, J. M. Zurada, and O. Nasraoui, "Deep learning of part-based representation of data using sparse autoencoders with nonnegativity constraints," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 12, pp. 2486–2498, Dec. 2016.
- [34] X. Yuan, B. Huang, Y. Wang, C. Yang, and W. Gui, "Deep learning-based feature representation and its application for soft sensor modeling with variable-wise weighted SAE," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3235–3243, Jul. 2019.
- [35] X. Yuan, C. Ou, Y. Wang, C. Yang, and W. Gui, "A layer-wise data augmentation strategy for deep learning networks and its soft sensor application in an industrial hydrocracking process," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 8, pp. 3296–3305, Aug. 2021, doi: [10.1109/TNNLS.2019.2951708](https://doi.org/10.1109/TNNLS.2019.2951708).
- [36] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, 2006.
- [37] P. K. Chan and S. J. Stolfo, "Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection," in *Proc. 4th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*, New York, NY, USA, 1998, pp. 164–168.
- [38] S. Liu, S. You, Z. Z. Lin, C. Zeng, H. Li, W. Wang, X. Hu, and Y. Liu, "Data-driven event identification in the U.S. power systems based on 2D-OLPP and RUS boosting trees," *IEEE Trans. Power Syst.*, early access, Jun. 24, 2021, doi: [10.1109/TPWRS.2021.3092037](https://doi.org/10.1109/TPWRS.2021.3092037).

- [39] X.-Y. Liu, J. Wu, and Z.-H. Zhou, "Exploratory undersampling for class-imbalance learning," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 39, no. 2, pp. 539–550, Apr. 2009.
- [40] C. Chen, A. Liaw, and L. Breiman, "Using random forest to learn imbalanced data," Dept. Statist., Univ. California, Berkeley, CA, Tech. Rep. 666, 2004.

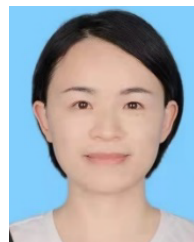


GUOYING LIN received the B.S. degree in electrical engineering and automation from Zhejiang University, Hangzhou, China, in 2005, and the M.S. degree in electrical engineering and automation from Shanghai Jiao Tong University, Shanghai, China, in 2008. He is currently pursuing the Ph.D. degree with the College of Electrical Engineering, Zhejiang University. His research interests include data mining and electricity theft detection.



XIAOFENG FENG received the B.E. degree from Hebei University of Science and Technology, Shijiazhuang, in 2007, the M.S. degree from Guangdong University of Technology, Guangzhou, in 2010, and the Ph.D. degree from the South China University of Technology, Guangzhou, in 2016.

He is currently a Senior Engineer with Metrology Center of Guangdong Power Grid Corporation. His research interests include power marketing and electricity theft detection.



WENCHONG GUO received the B.E. degree from the South China University of Technology, Guangzhou, in 2008.

She is currently a Senior Engineer with Metrology Center of Guangdong Power Grid Corporation. Her research interests include power marketing and electricity theft detection.



XUEYUAN CUI received the B.E. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2019, where he is currently pursuing the M.S. degree with the College of Electrical Engineering.

His research interests include power big data analysis and machine learning in electricity theft detection.



systems, situation awareness of power systems, and data-driven approaches in power systems.

SHENGYUAN LIU (Graduate Student Member, IEEE) received the B.E. degree in electrical engineering from Shandong University, Jinan, China, in 2017. He is currently pursuing the Ph.D. degree with the College of Electrical Engineering, Zhejiang University, Hangzhou, China. He was a Visiting Ph.D. Student with The University of Tennessee, Knoxville, for a period of one year, from 2019 to 2020. His research interests include wide area monitoring and control of power



a Research Associate with the College of Engineering and Computing Sciences, Durham University, from 2013 to 2014. He is currently a Professor with the College of Electrical Engineering, Zhejiang University, Hangzhou, China. His research interests include power system wide-area monitoring and control, controlled islanding and power system restoration, and data mining in power systems.

ZHENZHI LIN (Member, IEEE) received the Ph.D. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 2008.

He was a Research Assistant with the Department of Electrical Engineering, The Hong Kong Polytechnic University, from 2007 to 2008, a Research Scholar with the Department of Electrical Engineering and Computer Science, The University of Tennessee, from 2010 to 2011, and



WEICHAO JIN received the B.E. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2018, where he is currently pursuing the M.S. degree with the College of Electrical Engineering.

His research interests include power big data analysis and data-driven approaches in power systems.



He was an Associate Professor with the Department of Electrical Engineering, Technical University of Denmark (DTU), Denmark. He also held research and teaching positions at the University of Alberta, Canada, and NTU. He is currently a Professor with the College of Electrical Engineering, Zhejiang University (ZJU), China. His research interests include power system planning and reliability evaluation, smart grid, and complex system risk assessment. He is a member of IEC working groups for micro-grid standards. He is an Editorial Board Member of international journals of *Electric Power Systems Research* and *Journal of Modern Power Systems and Clean Energy*. He is a Guest Editor for the Special Section of IEEE TRANSACTIONS ON POWER SYSTEMS.

YI DING (Member, IEEE) received the B.Eng. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2000, and the Ph.D. degree in electrical engineering from Nanyang Technological University (NTU), Singapore, in 2007.

He was an Associate Professor with the Department of Electrical Engineering, Technical University of Denmark (DTU), Denmark. He also held research and teaching positions at the University

...