Detecting Energy Theft in Different Regions Based on Convolutional and Joint Distribution Adaptation

Jiangzhao Wang, Yanqing Zhu*, Yunpeng Gao, Ziwen Cai, Yichuang Sun, and Fenghua Peng

***Abstract*—Electricity theft has been a major concern all over the world. There are great differences in electricity consumption among residents from different regions. However, existing supervised methods of machine learning are not in detecting electricity theft from different regions, while the development of transfer learning provides a new view for solving the problem. Hence, an electricity-theft detection method based on Convolutional and Joint Distribution Adaptation(CJDA) is proposed. In particular, the model consists of three components: convolutional component (Conv), Marginal Distribution Adaptation(MDA) and Conditional Distribution Adaptation(CDA). The convolutional component can efficiently extract the customer's electricity characteristics. The Marginal Distribution Adaptation can match marginal probability distributions and solve the discrepancies of residents from different regions while Conditional Distribution Adaptation can reduce the difference of the conditional probability distributions and enhance the discrimination of features between energy thieves and normal residents. As a result, the model can find a matrix to adapt the electricity residents in different regions to achieve electricity theft detection. The experiments are conducted on electricity consumption data from the Irish Smart Energy Trial and State Grid Corporation of China and metrics including ACC, Recall, FPR, AUC and F1Score are used for evaluation. Compared with other methods including some machine learning methods such as DT, RF and XGBoost, some deep learning methods such as RNN, CNN and Wide & Deep CNN and some up-to-date methods such as BDA, WBDA, ROCKET and MiniROCKET, our proposed method has a better effect on identifying electricity theft from different regions.**

***Index Terms*—energy theft; different regions; supervised learning; Irish Smart Energy Trial**

I. Introduction

ENERGY theft has been a major concern for a long time. According to incomplete statistics[1], power companies in different regions suffer huge losses due to energy theft every year. In the United States, power companies lose about $6 billion due to abnormal power consumption, while power utilities in Canada lose $500 million every year as well. In China, the economic loss caused by abnormal power consumption can be about 20 billion RMB. Especially in some Southeast Asian countries, it can bring even more losses. In addition, methods of stealing electricity also harm the stability of the power grid, which can easily lead to electrical accidents such as a large-area blackout. Therefore, a method that can efficiently detect energy theft is urgently needed.

Several existing approaches to electricity theft detection, including hardware and network structure-based detection schemes, require access to a large amount of private information about the user. To prevent the disclosure of this information, we need to analyze the security and reliability of the model, such as the safety assessment[2] of the Belief Rule Base model[3]. To prevent such problems, current methods of detecting energy theft are mainly based on machine learning. These methods mainly realize the abnormal users' detection by analyzing customers' historical power consumption data along with other exterior data.[4] The current detection methods based on machine learning can be divided into supervised learning and unsupervised learning.

Unsupervised learning does not require a training set, a labeled data set. Therefore, unsupervised methods for power theft detection can essentially be explained by searching outliers in high-dimensional space. Zheng *et al.*[5] combined the Maximum Information Coefficient and the Clustering-technique by Fast Search and Find of Density Peaks to detect electricity theft. Biswas *et al.*[6] proposed energy loss coefficient and honest coefficient to evaluate the suspicion level of a consumer's reported energy consumption pattern. Krishna *et al.*[7] extended prior work on the design of approaches to detect electricity theft and presented the study of meter fraud in the context of Distributed Energy Resources. Sun *et al.*[8] proposed an improved outlier detection method based on the Gaussian kernel function. Tian *et al.*[9] proposed a power system power consumption anomaly analysis algorithm based on density clustering technology. Zhuang *et al.*[10] proposed an improved local outlier factor algorithm, which was suitable for the case where there is a lack of training samples in the power customer data. Yuan *et al.*[11] proposed an abnormal power consumption pattern identification method based on an unsupervised combination algorithm. Qi *et al.*[12] proposed a novel unsupervised data-driven method for detecting abnormal users, which incorporates observer meter data, wavelet-based feature extraction, and fuzzy c-means clustering.

On the contrary, supervised algorithms require a labeled data set to build a model and have a better detection effect. Supervised methods mainly include logistic regression[13], Support Vector Machine[14–16], Decision Tree[17, 18], and Neural Network[18–21]. An abnormal power consumption detection algorithm with a secondary screening of the Logistic Regression Algorithm was proposed in [13]. Messinis

This work was supported by Guangdong Provincial Key Laboratory of Intelligent Measurement and Advanced Metering of Power Grid.

Jiangzhao Wang, Yanqing Zhu (Corresponding author) and Yunpeng Gao are with College of Electrical and Information Engineering, Hunan University, Hunan 410012, China (e-mail: wangjiangz6506@hnu.edu.cn; zyq@hnu.edu.cn; gfront@126.com).

Ziwen Cai is with China Southern Power Grid South Electric Power Research Institute (e-mail: caizw@csg.cn).

Yichuang Sun is with School of Engineering and Technology, University of Hertfordshire (e-mail: y.sun@herts.ac.uk).

Fenghua Peng is with State Grid Hunan Electric Power Company Limited, Hunan, China (e-mail: 34585804@qq.com).

et al.[14] selected voltage sensitivity analysis, power system optimization and Support Vector Machine to detect NTL in distribution network under various conditions. Jindal *et al.*[15] proposed a top-down synthesis scheme based on Decision Tree and Support Vector Machine. Jokar *et al.*[16] proposed a new energy theft detector based on consumption mode. Yan *et al.*[17] proposed a metering data-stealing detector based on XGBoost. Guerrero *et al.*[18] presented a framework and methodology, developed as two coordinated modules, that improves this type of inspection. One module is based on text mining for customer filtering and a complementary artificial neural network. The other module is developed from the data mining process and contains a Classification and Regression Tree and a Self-Organizing Map neural network. Zheng *et al.*[19] proposed a wide and deep convolution neural network for power theft detection. Gao *et al.*[20] proposes a convolutional long short-term memory based energy theft detection model to identify electricity theft users. Buzau *et al.*[21] proposed a new end-to-end solution, which used a hybrid depth neural network to learn the anomaly and fraud detection features in smart meters.

Most of these supervised algorithms have two limitations. The one is that they mainly select a single set, which comes from the Irish Smart Energy Trial[14, 16, 17] or State Grid Corporation of China[19]. However, people from different regions have different habits. Hence, these supervised methods[22–24] of machine learning are not effective in detecting electricity theft from different regions. The other is that they primarily select several data from the Irish Smart Energy Trial for their studies and generate malicious customers by using formulas to falsify each data but not considering the periodicity of electricity consumption. It is likely to obtain the power consumption behavior of another normal user, who has fewer appliances but the same electricity habit.

With the development of transfer learning as there are lots of applications of transfer learning in electricity, like non-intrusive load monitoring[25] and load forecasting[26]. Hence, an energy-theft detection framework based on Convolutional and Joint Distribution Adaptation is presented, which could overcome some related problems of existing methods. The main contributions of our paper are as follows.

1) A method based on Convolutional and Joint Distribution Adaptation: We propose a method for electricity theft detection based on Convolutional and Joint Distribution Adaptation. The model consists of three components: convolutional component (Conv), Marginal Distribution Adaptation(MDA) and Conditional Distribution Adaptation(CDA). The convolutional component can efficiently extract the customer's electricity characteristics of the customer. Through the Marginal Distribution Adaptation and Conditional Distribution Adaptation, a transfer matrix can be found to adapt the electricity characteristics of customers to achieve cross-domain electricity theft detection.

2)Comprehensive experiments: To verify the effectiveness of our method, we optimize the existing power theft generation formulas and construct several cross-regional data sets based on data sets from the Irish Smart Energy Trial (ISET) and the State Grid Corporation of China (SGCC) to conduct experiments. The consumption of several weeks is selected for our research, and only a part of the user's weekly data is tampered with by the formulas due to the strong correlation between the electricity consumption data of normal customers and the weak correlation between the electricity consumption of energy thieves[19]. The effectiveness and superiority of our method are validated by experimenting with different types of electricity theft based on cross-regional data sets.

The remaining paper is organized as follows. Proposed method is presented in Section II. The experiments and results are shown in Section III. Section IV finally concludes the paper.

II. PROPOSED METHOD

Traditional supervised learning assumes that the distribution of the training and test data and the learning task are both the same. In many existing works of energy theft detection, training and test data are derived from a data set. The model is trained on the training set and tested on the test set. However, the test set is not controllable. In other words, the distribution of the test set is not the same as that of the training set, so an over-fitting problem can occur. The training results of the model are excellent, but the test results are not ideal. That is because the features of users are not clear, which results in a lower accuracy rate of identification. To address this problem, Convolutional and Joint Distribution Adaptation is proposed, which can find a metric to transfer the training set and test set to obtain two new sets with a similar distribution.

A. The principle of CJDA

An energy-theft detection method based on Convolutional and Joint Distribution Adaptation could identify energy thieves from different regions. The energy theft detection framework based on CJDA is shown in Fig.1. The learning manner of our proposed approach is a supervised domain learning method of transfer learning. The input of the framework is two data sets, the source domain and the target domain. In this paper, the source domain, a training set, is from ISET, while the target domain, a test set, is from SGCC. The convolutional component extracts features, while MDA and CDA are utilized for adapting marginal and conditional distribution, respectively, to adjust and optimize the datasets for training and test. The data sets are then used to train and test a stacking classifier based on Random Forest (RF) and Support Vector Machine (SVM) because they are well-established and widely used classification algorithms and are commonly used for electricity theft detection like [15]. Finally, the target domain with the labels is output by the trained stacking classifier. Therefore, the electricity theft customers in different regions can be identified by our scheme.

1) Convolutional Component: The convolutional component consists of several convolutional units, and the parameters of each unit are given. The purpose of the convolution operation is to extract the different features of consumption. In this paper, the convolutional component can extract a large number of features including edge and line features for marginal distribution adaptation.

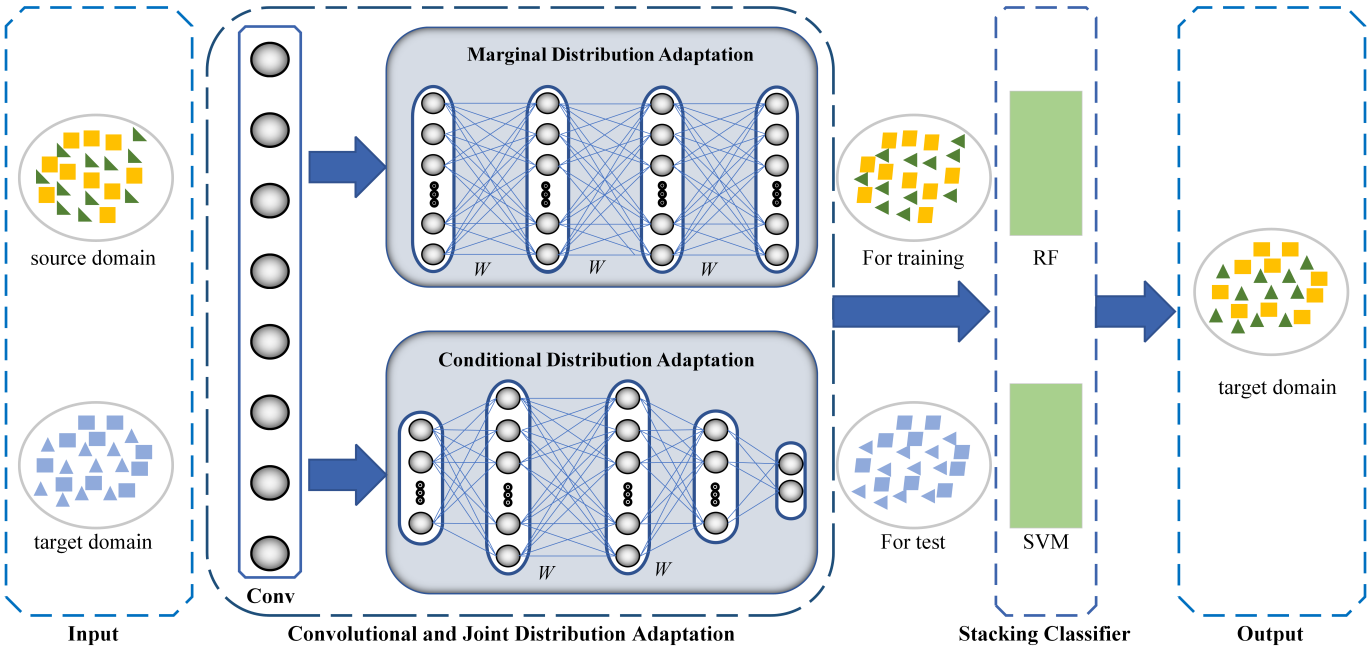

Fig. 1. Energy theft detection framework based on Convolutional and Joint Distribution Adaptation

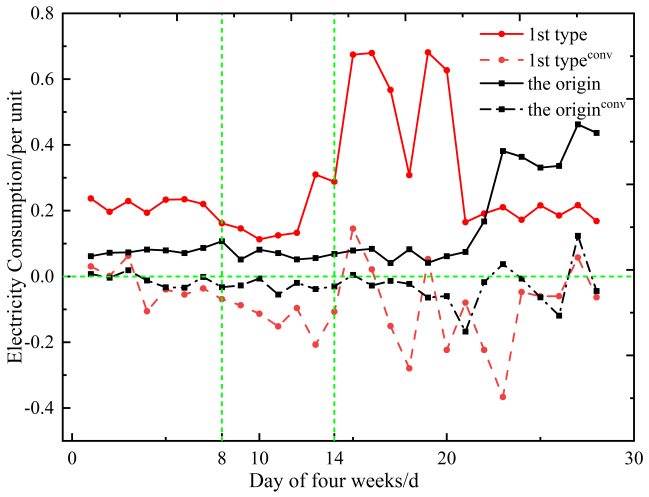

Fig. 2. Electricity consumption of normal and abnormal users with and without the convolutional component

For analysis, Fig.2 shows the electricity consumption characteristics of normal and abnormal users before and after they are filtered by the convolutional component. From that, the fluctuation of power curves with convolutional component becomes smaller. Compared with the curve of abnormal users, the curve of normal users is closer to $ElectricityConsumption = 0$ and less volatile with convolutional component.

2) Marginal Distribution Adaptation: A marginal distribution adaptation network is developed to learn a nonlinear subspace to match the marginal probability distributions. For marginal distribution, the empirical maximum mean dispersion (MMD) is to measure the distance between the marginal distribution of the source domain and target domain $p(x_s)$ and $p(x_t)$. The goal is to minimize the marginal distribution of the source domain and the target domain as much as possible.

MMD of the marginal distribution is computed as follows.

$$\begin{aligned} \mathrm{MMD}\left(x_s, x_t\right) &= \left\| \frac{1}{n}\sum_{i=1}^{n} A^{\mathrm{T}} x_i - \frac{1}{m}\sum_{j=n+1}^{n+m} A^{\mathrm{T}} x_j \right\|^2 \\ &= \mathrm{tr}\left(A^{\mathrm{T}} X M_0 X^{\mathrm{T}} A\right) \end{aligned} \tag{1}$$

where n and m stand for the number of samples in the source domain and the target domain, respectively. A is the transformation matrix to project data into the feature space. X is the combined data of the source domain and target domain. x_s and x_t stand for the data of the source domain and target domain, respectively. M_0 is the MMD matrix by the following equations:

$$\left(M_0\right)_{ij} = \begin{cases} \frac{1}{n^2} & 1 \le i, j \le n \\ \frac{1}{m^2} & n < i, j \le n+m \\ -\frac{1}{mn} & \text{otherwise.} \end{cases} \tag{2}$$

3) Conditional Distribution Adaptation: In classification tasks, minimizing the discrepancies of conditional probability distributions across domains is crucial. Unfortunately, it is impossible to match the conditional distributions based on the same transformation matrix, A with no labeled data in the target domain. To address it, the pseudo labels of the target data are proposed, which can be easily predicted by applying some base classifiers trained on the labeled source data to the unlabeled target data. Hence, there is a transformation matrix A, which can be utilized to minimize the distance between the conditional distribution of the source domain and target domain, $p(y_t|x_t)$ and $p(y_s|x_s)$. The specific steps are as follows.

According to the class-conditional probability, $(x_t|y_t)$ and Bayesian formula, Equation(3) occurs.

$$p\left(y_t \mid x_t\right) = p\left(y_t\right) p\left(x_t \mid y_t\right). \tag{3}$$

The pseudo labels $\widehat{y}_t$ of the target data can be predicted by applying the stacking classifier trained on the source data, (x_s, y_s), to the unlabeled target data, x_t. Conveniently, $p(y_s|x_s)$ is denoted as Q_s, and $p(\widehat{y}_t|x_t)$ is denoted as Q_t. According to the pseudo label, the MMD of the conditional distribution is computed as follows.

$$\begin{aligned} \mathrm{MMD}\left(Q_s, Q_t\right) &= \sum_{c=1}^{C} \left\| \frac{1}{n_c} \sum_{i=1}^{n_c} A^{\mathrm{T}} x_i - \frac{1}{m_c} \sum_{j=n_c+1}^{n_c+m_c} A^{\mathrm{T}} x_i \right\|^2 \\ &= \sum_{c=1}^{C} \mathrm{tr}\left(A^{\mathrm{T}} X M_c X^{\mathrm{T}} A\right) \end{aligned} \tag{4}$$

where $c = 1, ...C$, n_c and m_c are the number of class c samples in the source domain and the target domain, respectively. M_c is as follows.

$$(M_c)_{ij} = \begin{cases} \frac{1}{n_c^2} & 1 \le i, j \le n_c \\ \frac{1}{m_c^2} & n < i, j \le n_c + m_c \\ -\frac{1}{m_c n_c} & \begin{cases} 1 \le i \le n_c < j \le n_c + m_c \\ 1 \le j \le n_c < i \le n_c + m_c \end{cases} \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

4) Convolutional and Joint Distribution Adaptation: Combine Equation(1) and (4), and then the overall optimization objective function is obtained.

$$\min \sum_{c=0}^{C} \mathrm{tr}\left(A^{\mathrm{T}} X M_c X^{\mathrm{T}} A\right) + \lambda \|A\|_F^2 \tag{6}$$

where λ is the regularization parameter, and $\lambda\|A\|_F^2$ is the regularization term, which is applied to guarantee the optimization problem is well-defined.

The variance of data between the source and target domain is the same, so the following equation is obtained.

$$I = A^{\mathrm{T}} X \mathbf{H} X^{\mathrm{T}} A \tag{7}$$

where $\mathbf{H}$ is a central matrix and I is an identity matrix.

Hence, we can get Equation (8).

$$\begin{aligned} \min \textstyle\sum_{c=0}^{C} \mathrm{tr}\left(A^{\mathrm{T}} X M_c X^{\mathrm{T}} A\right) + \lambda \|A\|_F^2 \\ \text{s.t. } A^{\mathrm{T}} X H X^{\mathrm{T}} A = I. \end{aligned} \tag{8}$$

According to the constrained optimization theory, the Lagrange multiplier method is used to solve Equation (8), and a new equation is got.

$$\begin{aligned} L = \mathrm{tr}\left(A^{\mathrm{T}}\left(X \sum_{c=0}^{c} M_c X^{\mathrm{T}} + \lambda I\right) A\right) \\ + \mathrm{tr}\left(\left(I - A^{\mathrm{T}} X H X^{\mathrm{T}} A\right) \Phi\right) \end{aligned} \tag{9}$$

where Φ is $diag(\phi_1, ..., \phi_k) \in R_{k*k}$, which stands for the Lagrange multiplier.

Then, taking the derivative of A with L and making the derivative equal to 0, we can obtain Equation(10).

$$\left(X \sum_{c=0}^{c} M_c X^{\mathrm{T}} + \lambda I\right) A = X H X^{\mathrm{T}} A \Phi. \tag{10}$$

In this equation, the new pseudo labels $\widehat{y}_t$ are obtained by iterative updating, and the transformation matrix A is found again according to the optimization target, further reducing the distribution difference between the source domain and the target domain until the algorithm converges.

B. The Flow of CJDA

For several-week electricity consumption data of all customers, one customer's consumption data $x_f \in X_F$ corresponds to one label $y \in Y$ for each customer. $x_{fs} \in X_{Fs}$ and $x_{ft} \in X_{Ft}$ stand for the customers in the source domain and target domain. $y_s \in Y_s$ and $y_t \in Y_t$ stand for the electricity consumption data in the source domain and target domain.

The purpose of CJDA is to find a transformation matrix A to reduce the marginal and conditional distribution differences between $X_{Fs}$and X_{Ft} after extracting electricity features by applying the convolutional component. Therefore, the flow steps of the CJDA are shown below.

Step 1: Input the customers' electricity consumption matrix, $X_f(X_{Fs}, X_{Ft})$, and labeling matrix in the source domain, Y_s.

Step 2: Extract the electricity consumption features matrix, $X(X_s, X_t)$, by applying the convolutional component to the electricity consumption matrix, $X_F(X_{Fs}, X_{Ft})$.

Step 3: Construct M_0 by Equation (2), and set $M_c = 0$.

Step 4: Train a stacking classifier on (X_s, Y_s) to obtain the pseudo target label $\widehat{Y}_t$ with X_t, and then construct the matrix A by Equation(10).

Step 5: Train a stacking classifier on $(A^{\mathrm{T}}X_s, Y_s)$ to update the pseudo target label $\widehat{Y}_t$ with $A^{\mathrm{T}}X_t$ and the matrix A.

Step 6: If equation(10) convergence or the maximum number of iteration cycles is reached, return an adaptive stacking classifier f trained on $(A^{\mathrm{T}}X_s, Y_s)$, and transformation matrix A. If not, update M_c by Equation (5) and return to Step 5.

Step 7: Calculate $A^{\mathrm{T}}X_t$, import it into the adaptive Stacking classifier, and finally output Y_t.

III. EXPERIMENT AND ANALYSIS

To verify and test the feasibility and detection effect of the proposed framework, the computer (i5-12600k 3.69GHz and 16G RAM) is applied for simulation in Python 3.7. Indexes such as ACC, Recall, FPR, AUC, and F1Score, are used to evaluate the effectiveness in TABLE I.

A. Data preparation

In the literature, most articles primarily select several days for their studies and generate malicious customers by using formulas to falsify each piece of data. However, there is a strong correlation of normal customers' weekly electricity consumption and a weak correlation of malicious customers' weekly electricity consumption[19]. It is likely to obtain the power consumption behavior of another normal user, who has

TABLE I
INDEXES FOR EVALUATION OF ENERGY THEFT DETECTION

Indexes	Introduction
ACC	Ratio of correctly predicted samples to predicted samples
Recall	Ratio of predicted positive samples to real positive samples
FPR	Ratio of predicted as positive samples in real negative samples
AUC	Area under ROC curve
F1Score	Weighted harmonic average of precision and recall

fewer appliances but the same electricity habit. To avoid this, several weeks of the user's data are selected and only part of the user's weekly data is tampered with.

1) Data processing: The experiments are conducted on two data sets, the ISET data set, and the SGCC data set. ISET data set comes from the Irish Smart Energy Trial. It includes half-hourly active energy consumption of about 5000 residential and commercial consumers during 2009 and 2010. SGCC data set was released by the State Grid Corporation of China. It contains the electricity consumption data every day of 42,372 electricity customers within 1035 days (from January 1, 2014 to October 31, 2016).

For conducting our experiments, the load data of ISET is converted to daily load as the following formula.

$$x_{new}(i) = \sum_{j=1}^{48} x(i*48+j-48) \quad for \quad i = 1, \ldots, n \quad (11)$$

where $x(i)$ stands for the value in the electricity consumption data of ISET. $x_{new}(i)$ stands for the value in the daily electricity consumption data of ISET.

2) Malicious sample generating: In [16], six types of malicious samples are generated by six formulas and two of them represent attacks against billing mechanisms in which the price of electricity varies over different hours of the day. However, the minimum unit of power load of State Grid data is the day. Hence, those two of them cannot be regarded as stealing electricity. Then based on the data set of benign samples, we generate four types of malicious samples in TABLE II.

TABLE II
FOUR TYPES OF MODIFYING NOMARL USER LOAD

Attack Types	Modification
Type 1	$f_1(x_t) = \alpha x_t, 0.2 < \alpha < 0.8$
Type 2	$f_2(x_t) = \alpha_t x_t, 0.2 < \alpha_t < 0.8$
Type 3	$f_3(x_t) = \beta x_t, \beta = \begin{cases} 1 & \text{if } t_1 < t < t_2 \\ 0 & \text{otherwise} \end{cases}$
Type 4	$f_4(x_t) = \alpha_t \overline{x}, 0.2 < \alpha_t < 0.8$

In TABLE II, tampering methods can be explained as follows.

1) $f_1(*)$ multiplies all the samples by the same randomly chosen value α;
2) $f_2(*)$ multiplies each meter reading by a different random number;
3) $f_3(*)$ means the smart meter does not send its measurements or sends zero for a random duration;
4) $f_4(*)$ multiplies the value of the average of each meter reading over the week by a different random number.

Several weeks of the data are selected and only part of the weekly data is tampered with. Finally, many more reasonable malicious samples are generated.

B. Constructing training set and test set

To deal with different regions with different electricity behavior, different data sets are used for test and training. In other words, ISET is adopted as the training set, and SGCC is adopted as the test set. Hence, 2500 samples of ISET, and 10000 samples of SGCC are selected for conducting the training and test set respectively, and some of them are tampered with. Hence, four-week consumption is selected for research, and the second-week data are tampered with by formulas. An example of one-week consumption of a customer of two regions is shown in Fig 3 and 4. Five data sets are obtained for experiments based on four types of attacks, including the first attack data set, the second attack data set, the third attack data set, the fourth attack data set, and the mix of four attack data set. These five data sets are constructed as shown in TABLE III.

TABLE III
RATIO BETWEEN ABNORMAL AND NORMAL CUSTOMERS OF FIVE TYPES OF ATTACK DATA SETS

Data sets	Training (built by ISET)	Test (built by SGCC)
1st type attack data set	1 : 1	1 : 1
2nd type attack data set	1 : 1	1 : 1
3rd type attack data set	1 : 1	1 : 1
4th type attack data set	1 : 1	1 : 1
Mixed-type attack data set	$4(1:1:1:1):1$	$4(1:1:1:1):1$

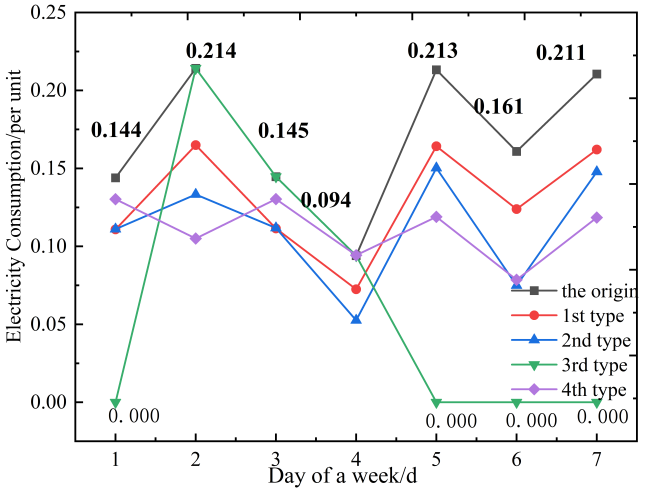

Fig. 3. Example of one-week consumption and attack patterns of ISET

C. Indexes evaluation based on our method

To identify energy theft in different regions, an electricity-theft detection framework based on Convolutional and Joint

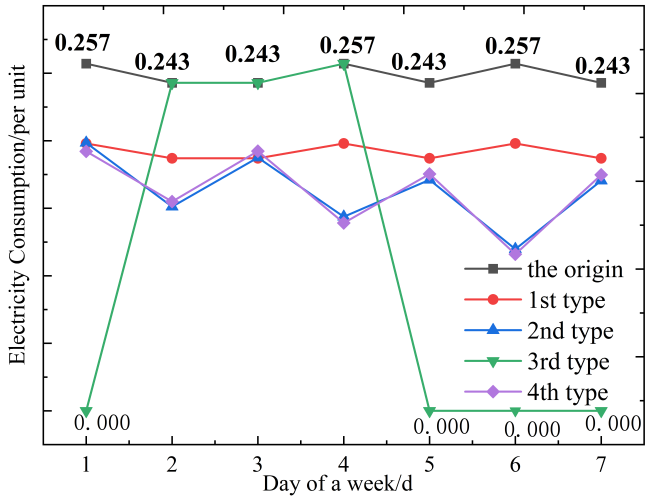

Fig. 4. Example of one-week consumption and attack patterns of SGCC

Distribution Adaptation is proposed. We organize relative experiments to examine the performance of our framework. Five data sets in TABLE III are used to perform experiments. Results are shown in TABLE IV.

TABLE IV
DETECTION RESULTS FOR THE FIVE DATA SETS

Type of Attack	ACC (%)	Recall (%)	FPR (%)	AUC(%))	F1Score (%)
1st type attack	82.41	80.16	15.34	90.15	82.01
2nd type attack	93.15	93.10	6.80	97.54	93.15
3rd type attack	99.32	99.00	0.36	99.95	99.32
4th type attack	95.52	95.68	4.64	98.75	95.53
Mixed-type attack	91.77	96.86	28.60	95.30	94.96

From TABLE IV, the results of five experiments show that our method has high ACC, high Recall, low FPR, high AUC, and high F1Score, in identifying electricity theft from different areas. High ACC means that our method can identify normal and abnormal customers. Identifying customers who steal electricity is important. Hence, a high recall value brings a high probability of predicting the actual energy theft. FPR is the ratio of electricity theft customers mistaken as normal customers to all electricity theft customers. In other words, the lower the FPR, the more effective the model is in detecting electricity theft customers. AUC is the area under the ROC curve. The closer the AUC is to 1.0, the higher the authenticity of the test method. F1Score is an important index of a model. A high F1Score means the model is of high quality.

From the results, we can find that our framework can easily identify different types of attacks on customers from different areas correctly. After convolution processing, We find a transformation matrix A to adapt both Marginal Distribution Adaptation and Conditional Distribution Adaptation based on ISET and SGCC. MDA can match marginal probability distributions and solve the dimensional discrepancies of residents from different regions and CDA can reduce the difference in the conditional probability distributions and enhance the discrimination of features between energy thieves and normal residents. As the results suggest, our framework can detect energy theft from different regions.

D. *Indexes comparisons of different methods*

In this subsection, we conduct several comparative experiments with some existing methods.

1) Existing Methods for Comparison: In this part, we choose some machine learning methods, some deep learning methods and some other up-to-date methods for comparison.

Joint distribution adaptation is the origin of our method, which aims to jointly adapt both the marginal distribution and conditional distribution in a principled dimensionality reduction procedure, and construct new feature representation[30].

Machine learning methods include Decision Tree (DT), Random Forest (RF) and Extreme Gradient Boosting (XGBoost)[17]. RF is an ensemble method that consists of many decision trees. XGBoost is one of the best algorithms for fitting the true distribution among supervised machine learning algorithms. Its core idea is to select an additive mode to reduce the residuals generated for classification and regression during the training process.

Deep learning methods include Recurrent Neural Network (RNN) and Wide & Deep CNN Network (WCNN)[19]. Convolutional Neural Network (CNN) is a deep learning method that is commonly used for classification. A recurrent neural network is a deep learning network structure that is typically used to process time series. The wide and deep CNN model consists of two components: the wide component and the deep CNN component. The combination of two components can accurately identify the non-periodicity of electricity theft.

Some other up-to-date methods include Balanced Distribution Adaptation (BDA), Weighted and Balanced Distribution Adaptation (WBDA)[27], Random Convolutional Kernel Transform (ROCKET)[28], Minimally Random Convolutional Kernel Transform (MiniROCKET)[29]. BDA and WBDA are derivatives of the algorithm proposed in the article, while ROCKET and MiniROCKET can achieve state-of-the-art time series classification accuracy by transforming the input time series with a random convolutional kernel and using the transformed features to train a linear classifier.

2) Performance Metrics: Mean Average Precision (MAP) is often used to judge the performance of the target detection algorithm. In this paper, this metric is used for comparisons, which is obtained by a combined weighted average of the average correct rate for all categories of tests.[19]

3) Performance comparisons: TABLE V presents the performance comparison of the CJDA scheme and other schemes. We conduct five groups of experiments with five data sets in TABLE III. During the experiment, the parameter settings of other algorithms follow the rules. For some traditional methods such as DT, RF, and CNN, we use the default parameters according to the general guidelines. For other methods, including XGBoost [17], WCNN [19],WBDA [27], ROCKET [28] and MiniROCKET [29], we set the relevant parameters according to their original papers for electricity theft detection. In each group of experiments, we evaluate performance metrics (ACC, MAP@100, and MAP@200) for these schemes. It is shown in TABLE V that our proposed scheme performs better than these

TABLE V
PERFORMANCE COMPARISON OF OUR PROPOSED CJDA MODEL AND OTHER CONVENTIONAL SCHEMES

Methods	1st type attack			2nd type attack			3rd type attack			4th type attack			Mixed-type attack		
	ACC (%))	MAP@ 100(%)	MAP@ 200(%)	ACC (%))	MAP@ 100(%)	MAP@ 200(%)	ACC (%))	MAP@ 100(%)	MAP@ 200(%)	ACC (%))	MAP@ 100(%)	MAP@ 200(%)	ACC (%))	MAP@ 100(%)	MAP@ 200(%)
DT	54.77	79.70	53.46	61.71	77.64	77.02	89.63	**99.64**	99.15	66.24	68.70	71.51	54.77	79.70	53.46
RF	50.07	58.82	55.26	54.26	62.66	60.25	91.33	90.54	91.69	54.82	63.56	61.30	81.41	54.42	54.48
XGBoost[17]	50.39	56.93	55.58	53.73	49.64	50.64	91.79	89.86	91.22	54.94	59.53	58.39	56.42	56.67	55.41
RNN	55.21	79.19	80.45	49.94	80.69	78.62	81.27	92.79	93.73	45.95	14.10	14.29	79.99	69.10	69.99
CNN	49.98	73.44	79.06	49.68	73.21	72.64	50.06	78.51	76.91	50.10	82.52	81.53	79.90	52.89	51.58
WCNN[19]	81.55	81.21	81.59	91.69	92.65	92.34	96.47	92.49	93.84	88.26	88.21	88.34	80.55	51.52	51.42
BDA	75.61	75.98	75.94	90.10	89.62	90.30	99.11	99.45	99.22	92.05	90.20	91.22	91.72	89.30	89.03
WBDA [27]	79.70	81.21	81.59	90.61	89.62	90.11	99.12	97.30	97.97	91.70	91.12	91.85	91.61	**89.30**	**89.09**
ROCKET[28]	59.20	30.45	30.52	60.78	42.34	42.98	79.37	94.78	95.28	60.08	84.50	84.04	57.50	47.89	48.77
MiniROCKET[29]	50.09	69.78	72.30	50.11	72.89	74.31	53.96	76.28	76.28	50.37	92.45	94.61	80.22	82.76	83.65
JDA[30]	79.64	75.41	78.43	91.99	90.98	91.75	99.24	99.45	**99.22**	92.39	91.12	91.85	90.23	76.37	77.79
CJDA	**82.41**	**83.82**	**83.10**	**93.15**	**94.12**	**93.91**	**99.32**	98.99	98.96	**95.52**	**94.86**	**95.30**	**91.77**	86.11	85.66

machine learning including DT, RF and XGBoost[17] and deep learning methods such as CNN, RNN and WCNN[19]. For example, the CJDA scheme can achieve the maximum MAP@200 value of 95.30 compared with other schemes in the 4th type attack data set. This implies that our method has the best identification of energy theft among these methods.

Although electricity thieves in different regions steal electricity with the same methods, the electricity consumption behavior of customers in different regions can seriously affect the judgment of models, such as RF, XGBoost and WCNN. In domain learning, the electricity consumption behavior of customers in different regions can be regarded as different distributions. As we all know, the real set of electricity consumption data is not controllable, it tends to have a different distribution than the training set. Hence, training samples and test samples have different distributions. Although RF, XGBoost and WCNN are the best algorithms for fitting the true distribution among supervised machine learning algorithms, their identification effect of electricity theft from different distributions is very poor.

E. Parameter study of the convolutional component

We then investigate the impacts of various parameters on the performance of the Convolutional component of our scheme.

1) Effect of numbers of the convolutional layers M: We choose M to control the number of convolutional layers in CJDA. To investigate the impact of M on prediction results, we vary the value of M from 0 to 5 with the step value of 1 considering the absence of the convolutional component. The experiment results are shown in Table VI. Overall, the convolutional component in CJDA can extract a large number of features including edge and line features for marginal distribution adaptation, but the increased number of layers can diminish the performance.

2) Effect of strides value of the convolutional layers S: We choose S to control the strides value of convolutional layers in CJDA. To investigate the impact of S on prediction results, we vary the value of S from 1 to 9 with the step value of 2. The experiment result is shown in Table VII. Overall, the increased strides value make more data lost, hence the prediction performance is poor.

TABLE VI
IMPACT OF M ON THE EFFECT OF OUR SCHEME

Numbers of Conv layers M	Mixed-type attack		
	ACC(%)	MAP@100(%)	MAP@200(%)
0	90.23	76.37	77.79
1	**91.77**	**86.11**	**85.66**
2	91.27	79.82	82.93
3	91.42	82.42	83.21
4	91.57	81.82	83.05
5	91.24	80.40	81.60

TABLE VII
IMPACT OF S ON THE EFFECT OF OUR SCHEME

Steps value of Conv layers S	Mixed-type attack		
	ACC(%)	MAP@100(%)	MAP@200(%)
1	**91.77**	**86.11**	**85.66**
3	89.14	78.27	78.93
5	81.47	57.47	57.38
7	81.34	58.94	60.02
9	79.88	53.01	52.18

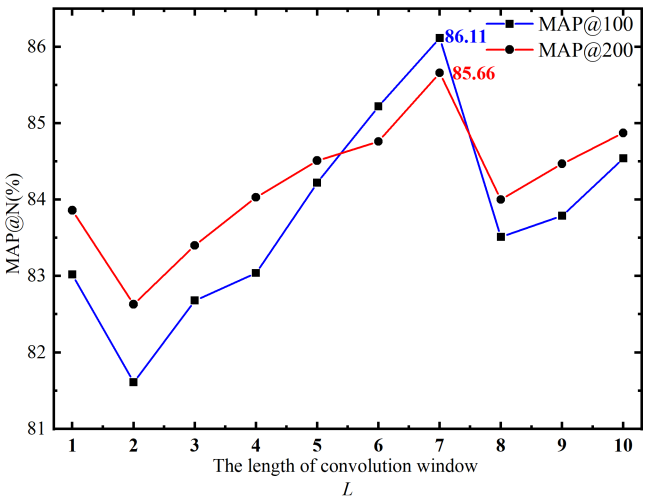

Fig. 5. Impact of L on the Effect of our scheme

3) Effect of the length of convolution window L: We choose L to control the length of the convolution window in CJDA. To analyze the impact of the window length on detection results, we conduct a comprehensive parameter study. It is worth noting that there is a strong correlation of normal customers' weekly electricity consumption according to [19]. The maximum length for the convolution window is set to 1.5 times the length of the cycle. Therefore, we systematically vary its value L from 1 to 10, incrementing by a step value of 1. The experiment result is shown in Fig. 5. From that, the increased length of the convolution window enhances and then weakens the prediction performance. The best performance is got when $L = 7$ due to the strong correlation of the user's weekly data.

IV. CONCLUSION

In this paper, a method for energy theft detection based on Convolutional and Joint Distribution Adaptation is proposed, which is composed of Convolutional Component, Marginal Distribution Adaptation and Conditional Distribution Adaptation. The convolutional component can efficiently extract the customer's electricity characteristics. Through the Marginal Distribution Adaptation and Conditional Distribution Adaptation, a transfer matrix can be found to adapt the electricity characteristics of customers to achieve cross-domain electricity theft detection while other supervised methods cannot. To demonstrate the effectiveness, we conduct extensive experiments on real electricity consumption data released by the Irish Smart Energy Trial and State Grid of China Corporation. With ISET for training and SGCC for the test, several experiments are conducted on different types of electricity theft. The experimental results show that our method outperforms other supervised algorithms.

Although our method can detect energy theft in different regions, it is difficult to obtain enough theft data to train our model in engineering practice. In the follow-up study, we will explore how to train a good model with small samples and incorporate it into our model for better application in engineering practice.

REFERENCES

[1] R. Czechowski and A. M. Kosek, "The most frequent energy theft techniques and hazards in present power energy consumption," in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pp. 1–7, 2016.

[2] Z. Feng, W. He, Z. Zhou, X. Ban, C. Hu, and X. Han, "A New Safety Assessment Method Based on Belief Rule Base With Attribute Reliability," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, pp. 1774–1785, November 2021.

[3] Z. Feng, Z.-J. Zhou, C. Hu, L. Chang, G. Hu, and F. Zhao, "A New Belief Rule Base Model With Attribute Reliability," *IEEE Transactions on Fuzzy Systems*, vol. 27, pp. 903–916, May 2019.

[4] Z. Yan and H. Wen, "Performance Analysis of Electricity Theft Detection for the Smart Grid: An Overview," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–28, 2022.

[5] K. Zheng, Q. Chen, Y. Wang, C. Kang, and Q. Xia, "A Novel Combined Data-Driven Approach for Electricity Theft Detection," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1809–1819, 2019.

[6] P. P. Biswas, H. Cai, B. Zhou, B. Chen, D. Mashima, and V. W. Zheng, "Electricity Theft Pinpointing Through Correlation Analysis of Master and Individual Meter Readings," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3031–3042, 2020.

[7] V. B. Krishna, C. A. Gunter, and W. H. Sanders, "Evaluating Detectors on Optimal Attack Vectors That Enable Electricity Theft and DER Fraud," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 790–805, 2018.

[8] S. Yi, L. Shihao, C. Can, L. Bin, C. Song, and C. Gaoying, "Improved Outlier Detection Method of Power Consumer Data Based on Gaussian Kernel Function," *Power System Technology*, vol. 42, no. 5, pp. 1595–1604, 2018.

[9] T. Li and X. min, "Abnormal Power Consumption Analysis Based on Density-based Spatial Clustering of Applications with Noise in Power Systems," *Automation of Electric Power Systems*, vol. 41, no. 5, pp. 64–70, 2017.

[10] Z. Chijie, Z. Bin, H. Jun, L. qiushuo, and Z. Rong, "Anomaly Detection for Power Consumption Patterns Based on Unsupervised Learning," *Proceedings of the CSEE*, vol. 36, no. 2, pp. 379–387, 2016.

[11] Y. Xiangyu, Z. penghe, X. Suqin, Z. Bo, and C. Da, "Research on identification method of abnormal power consumption based on logistic regression algorithm," *Electrical Measurement and Instrumentation*, vol. 58, no. 12, pp. 81–87, 2021.

[12] R. Qi, J. Zheng, Z. Luo, and Q. Li, "A Novel Unsupervised Data-Driven Method for Electricity Theft Detection in AMI Using Observer Meters," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–10, 2022.

[13] Y. Xiangyu, Z. penghe, X. Suqin, Z. Bo, and L. Qiuyang, "Identification of abnormal power consumption mode based on combination algorithm," *Electrical Measurement and Instrumentation*, vol. 55, no. 8, pp. 1–7, 2021.

[14] G. M. Messinis, A. E. Rigas, and N. D. Hatziargyriou, "A Hybrid Method for Non-Technical Loss Detection in Smart Distribution Grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6080–6091, 2019.

[15] 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 Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1005–1016, 2016.

[16] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016.

[17] Z. Yan and H. Wen, "Electricity Theft Detection Base on Extreme Gradient Boosting in AMI," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–9,

2021.

[18] J. I. Guerrero, I. Monedero, F. Biscarri, J. Biscarri, R. Millán, and C. León, "Non-Technical Losses Reduction by Improving the Inspections Accuracy in a Power Utility," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1209–1218, 2018.

[19] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, 2018.

[20] H.-X. Gao, S. Kuenzel, and X.-Y. Zhang, "A Hybrid ConvLSTM-Based Anomaly Detection Approach for Combating Energy Theft," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, no. 1, pp. 1–10, 2022.

[21] M.-M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Hybrid Deep Neural Networks for Detection of Non-Technical Losses in Electricity Smart Meters," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1254–1263, 2020.

[22] K. Zheng, Q. Chen, Y. Wang, C. Kang, and Q. Xia, "A Novel Combined Data-Driven Approach for Electricity Theft Detection," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1809–1819, 2019.

[23] T. Hu, Q. Guo, X. Shen, H. Sun, R. Wu, and H. Xi, "Utilizing Unlabeled Data to Detect Electricity Fraud in AMI: A Semisupervised Deep Learning Approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 11, pp. 3287–3299, 2019.

[24] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Robust Electricity Theft Detection Against Data Poisoning Attacks in Smart Grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2675–2684, 2021.

[25] R. Punmiya and S. Choe, "Energy Theft Detection Using Gradient Boosting Theft Detector With Feature Engineering-Based Preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2326–2329, 2019.

[26] E. Lee and W. Rhee, "Individualized short-term electric load forecasting with deep neural network based transfer learning and meta learning," *IEEE Access*, vol. 9, no. 2, pp. 15413–15425, 2021.

[27] J. Wang, Y. Chen, S. Hao, W. Feng, and Z. Shenk, "Balanced distribution adaptation for transfer learning," *arXiv*, pp. 1129–1134, 2018.

[28] A. Dempster, F. Petitjean, and G. Webb, I, "ROCKET: exceptionally fast and accurate time series classification using random convolutional kernels," *DATA MINING AND KNOWLEDGE DISCOVERY*, vol. 34, pp. 1454–1495, SEP 2020.

[29] A. Dempster, D. F. Schmidt, and G. I. Webb, "MiniRocket: A Very Fast (Almost) Deterministic Transform for Time Series Classification," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 248 – 257, 2021.

[30] M. Long, J. Wang, G. Ding, J. Sun, and P. S. Yu, "Transfer feature learning with joint distribution adaptation," in *2013 IEEE International Conference on Computer Vision*, pp. 2200–2207, 2013.