International Conference on Applied Energy 2019
Aug 12-15, 2019, Västerås, Sweden
Paper ID: 0145

STUDY ON ENERGY THEFT DETECTION BASED ON CUSTOMERS' CONSUMPTION PATTERN

Wen Xiong[1], Ying Cai[1], Li Wang[1], Yufan Zhang[2*], Qian Ai[2], Zhaoyu Li[2], Yue Wang[2], Shuangrui Yin[2]
1 Guangzhou Power Supply Bureau Co., Ltd., Guangzhou, Guangdong Province, 510620, People's Republic of China
2 Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai, 200240, People's Republic of China

ABSTRACT

With the development of industrial Internet of Things (IoT) for smart grid, the amount of data in end user side increases sharply. However, the digitizing also brings great possibility for energy theft. Inspired by the good performance of deep learning models and the computation efficiency of the convolutional neural network (CNN), in this work, we present a deep CNN-based energy theft detector. By learning the statistical pattern in the customers' consumption pattern, the detector is supposed to make correct classification. In reality, the whole dataset tends to have a small portion of energy theft data. To overcome such data imbalance, data of malicious consumption behavior is synthesized according to the predicted energy theft patterns. The experiment is conducted on the open source dataset. The proposed method is compared with the support vector classifier (SVC)-based method. The results show that the proposed method is more robust against the changes of non-malicious consumption behavior and can achieve better classification performance. Moreover, accelerated by GPU, the proposed method is more suitable for real time detection.

Keywords: energy theft detection, CNN, consumption pattern, SVC, IoT

1. INTRODUCTION

Benefiting from the latest information technologies, recent years have witnessed the emerging and fast development of industrial IoT for smart energy [1]. Smart meters, as end devices in IoT, shoulder the responsibility for reporting the energy consumption faithfully. However, the application of digital smart meters introduces the new vectors for energy theft [2]. Methods coping with it can be classified into three categories, namely, state estimation [3], game theory [4] and data-mining method [5]. Data mining-based detection method utilizes machine learning techniques to extract statistical pattern of the energy consumption data. Benefiting from the recent development in machine learning, such method is promising to achieve high performance.

SVC was reported in [5] for detecting the energy theft. It achieved high classification performance and was robust against non-malicious consumption patterns. However, deep learning-based methods were proved to be more powerful than SVC in computer science area. In this work, deep CNN is utilized for energy theft detection. The reasons for using CNN are as followed:

1) High granularity of data and numerous distributed smart meters call for methods coping with big data. Compared with other methods [6], the input of the CNN is matrix, which is effective to consume big data. Moreover, accelerated by GPU, CNN-based detection method is more time-saving than traditional machine learning models, especially under the big data era.

2) Benefiting from the deep structure and convolution kernels, CNN is supposed to be able to understand correlation existing in energy consumption data and thus achieves better performance than the traditional machine learning models.

2. CNN MODEL

2.1 Model Structure

CNN classifier aims to take the inputs of customers' electricity consumption curves and then distinguishes the malicious consumption patterns from the normal ones.

The proposed CNN structure is shown in the Fig 1. It is formed by a stack of convolutional layers and pooling layers, and finally through the fully-connected layer, the

Selection and peer-review under responsibility of the scientific committee of the 11th Int. Conf. on Applied Energy (ICAE2019).

classifier makes the judgment. The convolutional layers, which are composed of learnable filters, extend the depth of features' volume. During forward propagation, the convolution kernels make the convolution computation with the part of the inputs' volume. Then, the convolution kernels shift over the inputs according to the predefined strides. The convolutional layers can help preserve the local features of input data and extract more abstract features through consecutively extending the kernel's depth. The pooling layers implement down-sampling to reduce the dimensionality of each map but the important information is retained. At the end of the CNN structure, neurons are reshaped and form the inputs of the last fully-connected layer. And the outputs are processed by the softmax function to obtain the probability of the inputs to be normal consumption behavior or the malicious one.

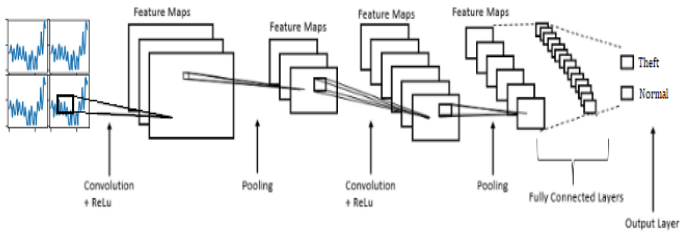

Fig.1 Model Structure of deep CNN

2.2 Loss function

The aim of the CNN based classifier is to output a probability distribution that matches the target distribution which is a discrete distribution and has the only one spike. Hence, the cross-entropy is used as the loss function:

$$\begin{aligned} \mathrm{H}(p,q) &= -E_p[\log q] \\ &= H(p) + D_{\mathrm{KL}}(p \| q) \end{aligned}$$

where $H(p)$ is a constant and $D_{\mathrm{KL}}(p \| q)$ is the Kullback–Leibler divergence between two distributions. Therefore, minimizing the cross-entropy is equivalent to minimizing the Kullback–Leibler divergence which is a measure of how one probability distribution is different from a second.

3. THE PROPOSED METHOD

3.1 Energy theft data synthesis

One of big challenges facing energy theft detection is that the malicious data only occupies a small portion of the whole dataset. The imbalance of the data can result in the high false positive rate. To cope with it, thanks to the predictability of energy theft, malicious data are generated according to energy theft types. The detailed information can be found in [5]. For each normal sample $\boldsymbol{x} = \{x_1, x_2, ..., x_{24}\}$, six types of malicious behaviors are generated:

1) $h_1(\boldsymbol{x}) = \alpha \boldsymbol{x}, \alpha = \mathrm{random}(0.1, 0.8)$

2) $h_2(\boldsymbol{x}) = \boldsymbol{\beta} \cdot \boldsymbol{x}$

$$\beta_t = \begin{cases} 0 & \mathrm{StartTime} < t < \mathrm{EndTime} \\ 1 & \mathrm{Else} \end{cases}$$

3) $h_3(\boldsymbol{x}) = \boldsymbol{\gamma} \cdot \boldsymbol{x}, \gamma_t = \mathrm{random}(0.1, 0.8)$

4) $h_4(\boldsymbol{x}) = \boldsymbol{\gamma} \cdot \mathrm{mean}(\boldsymbol{x}), \gamma_t = \mathrm{random}(0.1, 0.8)$

5) $h_5(\boldsymbol{x}) = \mathrm{mean}(\boldsymbol{x})$

6) $h_6(x_t) = x_{24-t}$

3.2 Evaluation metrics

The classification quality can be first represented by a confusion matrix, depicted in Table 1, where TP, TN, FP, and FN denote the numbers of malicious consumption behavior correctly predicted as energy theft, normal behavior correctly predicted as normal, malicious behavior incorrectly predicted as normal, and normal behavior incorrectly predicted as energy theft.

Table 1 Confusion matrix

	Expected energy theft	Expected normal
Predicted energy theft	TP	FN
Predicted normal	FP	TN

Based on the confusion matrix, the five metrics, namely precision, recall, specificity, F1-score, and accuracy, are used in this work.

1) Precision (PRE): The precision is defined as the proportion of the correctly predicted energy theft cases in all the actual energy theft cases.

$$precision = TP / (TP + FP)$$

2) Recall (REC): The precision is defined as the proportion of the correctly predicted energy theft cases in all the predicted energy theft cases.

$$recall = TP / (TP + FN)$$

3) Specificity (SPE): The specificity is defined as the proportion of the correctly predicted normal energy usage cases in all the predicted normal energy usage cases.

$$specificity = TN / (TN + FP)$$

4) F1-score: The F1-score conveys the balance between the precision and recall and reaches its best value at 1.

$$F_1 = 2 \times PRE \times REC / (PRE + REC)$$

5) Accuracy (ACC): The accuracy is defined by the proportion of correct classification

$$accuracy = (TP + TN) / (TP + FN + FP + TN)$$

3.3 The proposed detection flow

The proposed CNN-based energy theft detection flow chart is shown in Fig 2. The main step is summarized as followed:

1) Synthesize energy theft data according to the predicted energy theft types. Implement data preprocessing and divide the whole dataset into the training set and the test set;

2) Train the deep CNN until convergence;

3) Evaluate the model according to the aforementioned metrics.

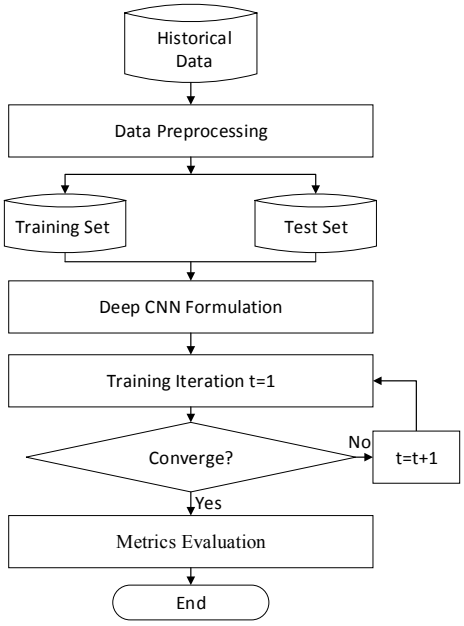

Fig.2 The flowchart of the proposed method

4. IMPLEMENTATION

4.1 Data description

The open source dataset — the GEFCom2012 dataset is used in this work. The dataset includes 20 regional levels and one system level hourly electrical load information, corresponding temperature record, and holiday information. We use the energy consumption data of 20 regions from 2004 to 2005 provided by the competition.

The data normalization is performed to transfer generated malicious consumption behaviors together with the normal ones into the range of $(0,1)$. And the normalized samples are split into the training and test set.

4.2 Model architecture and details of training

Considered the autocorrelation of the energy consumption sequences, the consecutive six days load with the resolution of one hour is used as the inputs and reshaped into the shape of 12×12. The energy theft detector includes two convolutional layers and two maxpooling layers to down-sample the input consumption sequences. Details of the detector's model parameters are listed in Table 2. The program is implemented on the Tensorflow platform with a unit of Intel Core i7-7700 CPU and NVDIA GTX 1080 Ti GPU.

Table 2 Detector model structure

Input	12*12
Layer 1	Conv, 32
Layer 2	Maxpooling
Layer 3	Conv, 64
Layer 4	Maxpooling
Layer 5	FC, 144

The model is trained using AdamProp optimizer with learning rate 1e-3 and mini-batch size 128. For both convolutional layers and fully connected layer, RELU activation is used. Dropout technique is used in the last fully connected layer to prevent overfitting. Once the loss remains stable on the training set, the detector is able to make the judgment of energy theft.

5. RESULTS ANALYSIS

5.1 Synthetic energy theft data

The synthetic energy theft data along with the corresponding normal energy consumption is shown in Fig 3. The energy consumption of energy theft type one, three, and four is always below the expected energy consumption during the day. The type two keeps normal most of the time in the day but suddenly drops to the zero when the electricity tariff is high. The type six reverses the ordering of the reading tries to vary against the different electricity pricing.

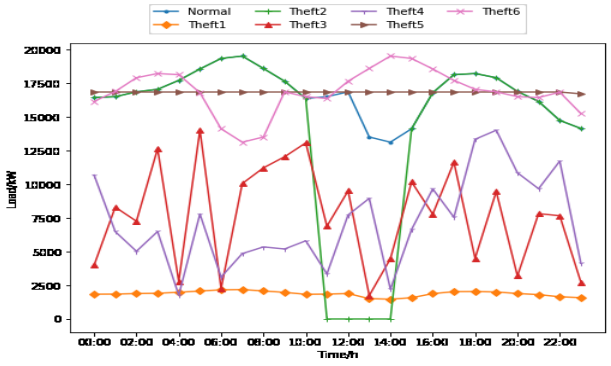

Fig.3 Example of attack patterns

5.2 Energy theft detection results

The dynamic training process is depicted by the loss curve and the accuracy curve in the Fig 4. It is seen that the model converges quickly and remains almost stable in 2000 training iterations. Therefore, it is proved that the model has good convergence performance.

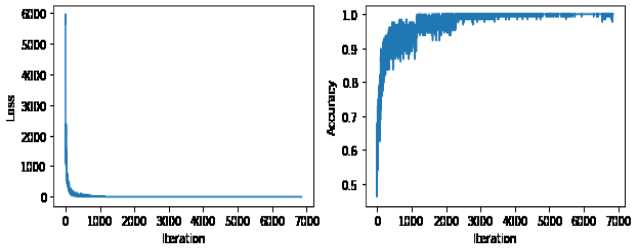

Fig 4 Dynamic training process

The detection results of the proposed method are compared with that of the SVC model in Table 3. Note that the time referred in Table 3 includes both the training and test time. It can be seen that the proposed method can achieve high accuracy on both training and test set. Thus, the proposed method doesn't suffer from the over-fitting problem. Also, in terms of the accuracy on the test set, compared with the SVC method, the relative improvement is around 20.1%. Moreover, Through GPU acceleration, the time for training and testing CNN-based detector is much shorter than the SVC-based method. Therefore, the proposed method is suitable for real time detection.

Table 3 Classification accuracy and time

	Accuracy (Training Set)	Accuracy (Test Set)	Time
SVC	83.41%	83.16%	1h39min51s
The proposed method	100%	99.88%	5min11s

The hotmap of the confusion matrixes on the test set are depicted in Fig 5. And the evaluation metrics results are shown in Table 4. The SVC-based method tends to classify relatively the large number of normal behavior into the energy theft and thus is not robust to the non-malicious consumption behavior changes. Moreover, almost all metrics show that the proposed CNN-based detector outperforms the SVC-based one.

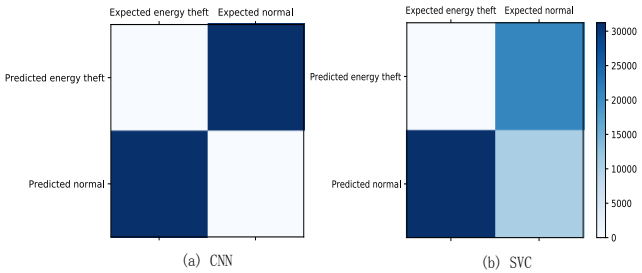

Fig 5 Hotmap of confusion matrixes

Table 4 Classification evaluation metrics

	PRE	REC	SPE	F1
SVC	100%	74.75%	100%	0.8555
The proposed method	99.83%	99.92%	99.83%	0.9988

6. CONCLUSIONS

The results obtained from the work shows that the CNN-based energy theft detector had good generalization performance, and can improve the accuracy on the test set by 20.1% compared with SVC. Also, thanks to the GPU, the proposed method was suitable for real time detection. The confusion matrix analysis proved that the proposed method was more robust against the changes of non-malicious consumption pattern.

ACKNOWLEDGEMENT

The work was supported by the National Key Research and Development Program of China under Grant No. 2016YFB0901300.

REFERENCE

[1] Bedi G, Venayagamoorthy G K, Singh R, et al. Review of Internet of Things (IoT) in electric power and energy systems[J]. IEEE Internet of Things Journal, 2018, 5(2): 847-870.

[2] Ozay M, Esnaola I, Vural F T Y, et al. Machine learning methods for attack detection in the smart grid[J]. IEEE transactions on neural networks and learning systems, 2016, 27(8): 1773-1786.

[3] Lo C H, Ansari N. CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid[J]. IEEE Transactions on Emerging Topics in Computing, 2013, 1(1): 33-44.

[4] Cárdenas A A, Amin S, Schwartz G, et al. A game theory model for electricity theft detection and privacy-aware control in AMI systems[C]//2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton). IEEE, 2012: 1830-1837.

[5] Jokar P, Arianpoo N, Leung V C M. Electricity theft detection in AMI using customers' consumption patterns[J]. IEEE Transactions on Smart Grid, 2016, 7(1): 216-226.

[6] He Y, Mendis G J, Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2505-2516.