Detect the electricity theft event using text CNN

Chenjin Xu¹, Kai Zhang¹,³ and Jianhua Li²
¹ Economy and Technology Research Institute of State Grid Zhejiang Electric Power Co., Ltd;
² State Grid Zhejiang Taizhou Power Supply Company
³ Email:1421997054@qq.com

Abstract. The big data technology has been widely used in power consumption behavior analysis and power user portrait. In this paper, the electricity data is constructed as two-dimensional time-series. Based on the designed data structure, a special kind of Artificial Neural Networks (ANNs) named as text convolutional neural networks (TCNN) is proposed for electricity theft detection. Moreover, considering the imbalance of electricity theft data in realistic datasets, a data augmentation method is proposed. Numerical results obtained on realistic datasets validate the proposed model.

1. Introduction
Electricity theft severely obstructs the normal usage of electricity, it also leads to nonnegligible income losses for power supply enterprises. Moreover, the unauthorized reconnection of lines or meters is prone to cause security accidents, power failure, and fires [1,2]. It is necessary to develop effective technique to timely detect the electricity theft events and thus maintain the reliable operation of the power distribution system.

At present, the support vector machines (SVMs) and Artificial Neural Networks (ANNs) are two typical kinds of data-driven electricity theft detection methods. In [3], a method of data mining based on SVM is proposed to extract features from historical customer consumption data to detect electricity theft. In [4], regions or districts with relatively higher electricity theft probabilities are listed first. Then, for each electricity user, a multi-class cascaded SVM is trained based on historical real measurements and an artificial imitated theft dataset. In [5], an integrated model combining the SVM with an adaptive boosting algorithm is developed for imbalanced datasets. However, most of the approaches based on SVM have limitations on accuracy [6,7]. Currently, more researches utilize neural networks to detect electricity theft. In [8,9], since the electricity consumption signature is a kind of time-series data, the Long Short-Term Memory (LSTM) models are invented to detect the electricity theft events. In [10], a peer to peer hybrid ANN is proposed, which is composed of a short-term memory network and a multi-layer perception machine.

The above methods mainly focus on the correlation between electricity consumption information among different days, which are not capable to characterize the intraday electricity usage patterns. Consequently, if such methods are applied to hourly or more frequent electricity measurements, the accuracy may be relatively inadequate. Actually, those theft users who have considerable electricity demand (mainly industrial or commercial users) prefer to commit the crime during some specific hours due to Time of Use (TOU) tariffs. Meanwhile, some emerging kinds of thefts such as communication interception and deliberate injection of false, invalid data [11,12] make it easier to
implement the thefts during some specific time of the day compared with traditional thefts. Therefore, it is of necessity to develop a detection approach of electricity thefts which is capable to characterize the intraday power usage features.

In this paper, a two-dimensional grid structure for the raw smart meter measurements is utilized. As shown in Figure 1, based on the designed data structure, a special kind of ANNs named as text convolutional neural networks (TCNNs) is proposed for electricity theft detection, whose accuracy is validated by numerical results obtained on realistic smart meter datasets. This work provides a feasible solution for data-driven analytic of electricity theft as well as other abnormal power usage events.

2. Data processing method
To reduce the adverse effect of missing, duplicated, and fault data on the electricity theft detection accuracy, an electricity data processing method is proposed in [7] to repair the missing and erroneous elements in the dataset. Eq.(1) represents a mission data repair technique based on the interpolation.

\[ x^* (d, t) = \begin{cases} 
\frac{x(d, t-1) + x(d, t+1)}{2} & \text{if } x(d, t-1) \neq \text{NaN}, x(d, t+1) \neq \text{NaN} \\
0 & \text{if } x(d, t) \in \text{NaN}, x(d, t-1) \in \text{NaN} \\
x(d, t) & \text{if } x(d, t) \neq \text{NaN} \end{cases} \]  (1)

where \( x(d,t) \) is the power consumption data during time period \( t \) on the \( d \)-th day. And NaN represents the corresponding data is missing or null.

Moreover, the following *Three-Sigma Rule of Thumb* are utilized to repair the abnormal data [13]:

\[ x^* (d, t) = \begin{cases} 
\text{avg}(x(d)) + 2 \cdot \text{std}(x(d)) & \text{if } x_{d,t} > \text{avg}(x(d)) + 2 \cdot \text{std}(x(d)) \\
x(d, t) & \text{otherwise} \end{cases} \]  (2)

where \( x(d) \) is the vector format of \( x(d,t) \), \( \text{avg}(x(d)) \) and \( \text{std}(x(d)) \) are the mean and standard deviation of vector \( x \), respectively.

3. The proposed TCNN for electricity theft detection
As shown in Figure 2, the proposed TCNN structure is mainly consists of convolutional, pooling, and fully-connected layers. The characteristics of the layers are illustrated in the following part.

3.1. Convolutional layer
There are \( H \) different sizes of convolutional kernels in a convolutional layer. In order to maintain the efficiency and accuracy of the classification, the height of kernels is assigned as the number of one
day’s measurements. For convolution kernels with size $H_i$, $D^i = (F, T)$ denotes as the $u$-th data measurement. The corresponding kernel weights $w^u_j \in \mathbb{R}^{F \times K}$ is adopted to characterize the input, where $K$ is the kernel length. For instance, the feature map $o^u_{i,j}$ can be calculated as [12]:

$$o^u_{i,j} = f_u(w^u_j \ast D^u + b^u_j)$$  \hfill (3)

Here, $\ast$ denotes the convolutional operator. $b^u_j \in \mathbb{R}$ is a bias and $f_u(\cdot)$ is a nonlinear activation function. It is relatively not difficult to demonstrate that no matter how many convolutional layers are configured, the output can be expressed as a linear combination of the inputs, which indicates the network is of no hidden layers.

Figure 2. Proposed TCNN structure for electricity theft detection.

There are $C$ kernel weights of size $H_i$ denoted as $\{w^u_1, w^u_2, \ldots, w^u_i, \ldots, w^u_C\}$, which produce $C$ feature maps as follow:

$$o^u_t = [o^u_{i_1,j_1}, o^u_{i_2,j_2}, \ldots, o^u_{i_K,j_K}]^T$$  \hfill (4)

After the first convolution operation, the feature maps of kernel size $1, 2, \ldots, K$ can be expressed as $D_{i_1}^1(N, C, T - K + 1)$.

In order to extract the temporal features and compress the data meanwhile, there are multiple convolutional layers in the proposed network. It is worth mentioning that the kernel size of the cascaded two layers are not necessarily the same [13]. After passing through these convolutional layers, the feature maps of kernel size $\{H_{i_1}, H_{i_2}, \ldots, H_{i_M}\}$ are represented by:

$$D_{i_1}(N, C, T - K_1 - K_2 - \cdots - K_M + M)$$  \hfill (5)

The above $K_{i_1}$ denotes the kernel length of the $M$-th convolutional layer.

3.2. Fully-connected layer

In the fully-connected layer, the input is the output of the pooling layer. A two-class Softmax classifier is adopted. If the calculated probability of committing electricity theft crime is greater than the calculated probability of being normal, the input measurement is classified as an electricity theft event. The final output of the whole network is as follows [13]:

$$f_{\text{Softmax}}\left[ D(N, \sum_i C_{i,1}) \right] = D(N, 2, 1)$$  \hfill (6)
4. Case study

4.1. CNN Parameters
For the TCNN model, the height of kernels is set as the number of one day’s measurements and its width is 2, 3, 5 and 7. Kernels with 2 or 3 width is capable to characterize features from adjacent days. Kernels with 5 or 7 width characterizes features with the weekday and week periodicities, respectively. Moreover, to avoid overfitting, the dropout rate is set at 0.4.

4.2. Data
Real datasets (1) and (2) are obtained from a certain province of China, containing both electricity theft and normal users. Open source dataset (3) is derived from Northern Ireland. The electricity theft data in dataset (3) is deliberately man-made. The details of the datasets are shown in Table 1.

| Datasets | (1) | (2) | (3) |
|----------|-----|-----|-----|
| Total users | 4637 | 8136 | 6000 |
| Normal users | 3364 | 7022 | 6000 |
| Theft users | 1073 | 1114 | 0 |

In dataset (1), the ratio of normal to theft users is about 3.14:1. In dataset (2), the ratio is 6.3:1. In dataset (3), 1500 electricity theft samples are deliberately generated, and the ratio is 4:1.

4.3. Metrics
Table 2 illustrates the confusion matrix of the two-class classification problem.

| Confusion Matrix | Actual |
|------------------|--------|
| Classified       | Negative (normal) | Positive (theft) |
| Positive (normal) | True Negative (TN) | False Positive (FP) |
| True Positive (TP) | False Negative (FN) | True Positive (TP) |

Based on the confusion matrix, several metrics are defined as follows:

\[
AR = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%
\] (7)

Precision rate (PR):

\[
PR = \frac{TP}{TP + FP} \times 100\%
\] (8)

Recall rate (RR):

\[
RR = \frac{TP}{TP + FN} \times 100\%
\] (9)

F1:

\[
F1 = \frac{2 \times PR \times RR}{PR + RR} \times 100\%
\] (10)

The above four indicators can comprehensively measure the accuracy of the proposed classifier.

4.4. Results
Three benchmark methods are adopted including the Logistic Regression (LR), SVM, and the one-dimensional CNN (1D-CNN). The 1D-CNN is similar to the proposed model except for its 1-D power consumption data. The dimension of 1D-CNN input is D(N,1,T). In the previous sections, we have stated that the 2-D data is suitable for characterizing intraday and daily features of electricity, while the data value densities obtained by the benchmark 1-D networks are obviously less. To illustrate the advantage of the 2-D TextCNN, the performance of the proposed and the other three models in three datasets are demonstrated in Table 3.
Table 3. Results on different datasets of different methods

| Model       | Training = 50% | Dataset (1) | Dataset (2) | Dataset (3) |
|-------------|----------------|-------------|-------------|-------------|
|             | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  |
| LR          | 0.851 | 0.623 | 0.488 | 0.547 | 0.614 | 0.636 | 0.488 | 0.553 | 0.706 | 0.827 | 0.762 |
| SVM         | 0.762 | 0.715 | 0.503 | 0.438 | 0.523 | 1.000 | 0.023 | 0.045 | 0.793 | 0.886 | 0.223 | 0.356 |
| 1D-CNN      | 0.871 | 0.689 | 0.439 | 0.536 | 0.714 | 0.913 | 0.488 | 0.636 | 0.843 | 0.682 | 0.677 | 0.787 |
| Proposed CNN | 0.887 | 0.752 | 0.558 | 0.640 | 0.795 | 0.945 | 0.634 | 0.759 | 0.870 | 0.719 | 0.803 | 0.835 |

| Model       | Training = 60% | Dataset (1) | Dataset (2) | Dataset (3) |
|-------------|----------------|-------------|-------------|-------------|
|             | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  |
| LR          | 0.851 | 0.614 | 0.519 | 0.562 | 0.714 | 0.769 | 0.625 | 0.690 | 0.748 | 0.888 | 0.812 |
| SVM         | 0.762 | 0.715 | 0.503 | 0.438 | 0.524 | 1.000 | 0.060 | 0.117 | 0.810 | 0.838 | 0.290 | 0.431 |
| 1D-CNN      | 0.890 | 0.730 | 0.500 | 0.594 | 0.719 | 0.944 | 0.531 | 0.680 | 0.812 | 0.610 | 0.615 | 0.744 |
| Proposed CNN | 0.889 | 0.674 | 0.602 | 0.636 | 0.834 | 0.952 | 0.720 | 0.819 | 0.919 | 0.825 | 0.876 | 0.897 |

| Model       | Training = 70% | Dataset (1) | Dataset (2) | Dataset (3) |
|-------------|----------------|-------------|-------------|-------------|
|             | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  |
| LR          | 0.852 | 0.633 | 0.496 | 0.556 | 0.519 | 0.470 | 0.320 | 0.381 | 0.907 | 0.725 | 0.930 | 0.815 |
| SVM         | 0.762 | 0.715 | 0.503 | 0.438 | 0.555 | 1.000 | 0.040 | 0.0769 | 0.833 | 0.793 | 0.324 | 0.46 |
| 1D-CNN      | 0.875 | 0.778 | 0.398 | 0.527 | 0.776 | 0.85 | 0.680 | 0.756 | 0.840 | 0.750 | 0.500 | 0.750 |
| Proposed CNN | 0.893 | 0.766 | 0.584 | 0.663 | 0.844 | 0.952 | 0.720 | 0.819 | 0.920 | 0.785 | 0.966 | 0.904 |

| Model       | Training = 80% | Dataset (1) | Dataset (2) | Dataset (3) |
|-------------|----------------|-------------|-------------|-------------|
|             | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  | AR  | PR  | RR  | F1  |
| LR          | 0.837 | 0.610 | 0.472 | 0.532 | 0.667 | 0.666 | 0.588 | 0.625 | 0.917 | 0.712 | 0.977 | 0.824 |
| SVM         | 0.762 | 0.715 | 0.503 | 0.438 | 0.555 | 1.000 | 0.058 | 0.111 | 0.833 | 0.684 | 0.302 | 0.419 |
| 1D-CNN      | 0.899 | 0.800 | 0.359 | 0.496 | 0.714 | 0.909 | 0.588 | 0.741 | 0.833 | 0.705 | 0.574 | 0.762 |
| Proposed CNN | 0.891 | 0.681 | 0.618 | 0.648 | 0.901 | 0.958 | 0.841 | 0.896 | 0.958 | 0.857 | 1.000 | 0.947 |

As shown in Table 3, the proposed model generally provides better results than benchmark methods in terms of different training ratios. For training ratio 70%, the proposed model achieves the highest AR and RR in all the three datasets. But other benchmark models are of better PR in some datasets. For instance, the PR of 1D-CNN is the best in dataset (1), which is 1.2% higher than that of the proposed model. However, the proposed model reaches the highest 0.663, 0.819 and 0.897 F1 values in dataset (1), (2) and (3), which is 10.7%, 43.8% and 8.9% higher than the second-best model respectively. Meanwhile, the proposed model operates better with the growing training ratio. For instance, in dataset (3), the F1 value increases from 84.5% to 95.7% as the training ratio grows from 50% to 80%.

It is also worth noted that the proposed model provides better performance in realistic datasets. Comparing the results obtained from dataset (3) with those of dataset (1) and (2), when training ratio is 80%, the proposed model reaches 95% F1 in dataset (3), but only 64.8% and 89.6% F1 values in dataset (1) and (2) respectively. This may be due to the fact that the electricity theft data in dataset (3) is artificial, whose data features can be characterized easily by data-driven machines. However, real electricity theft data is more complicated which may be of no regularity. However, the performance of the proposed model is still the better than other models in the real datasets.
Through the above comparisons, it can be seen that the proposed TCNN model achieves higher accuracy than some state-of-the art data-driven electricity theft detection methods.

5. Conclusions
In this paper, a TCNN method is proposed based on the grid-like data structure for electricity theft detection. Case studies on different datasets are provided to demonstrate the feasibility of the proposed scheme. Numerical results show that the proposed method performs obviously better other benchmark methods, including LR, SVM and 1-D CNN.

References
[1] Depuru S.S.S.R, Wang L, Devabhaktuni, V 2011 Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft Energy Policy 39 1007-1015 doi:10.1016/j.enpol.2010.11.037
[2] Kumar V S, Prasad J, Samikannu R 2017 Overview, issues and prevention of energy theft in smart grids and virtual power plants in Indian context Energy Policy 110 365-374
[3] Nagi J; Yap K S; Tiong S K, Ahmed S K, Mohamad M 2010 Nontchnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines IEEE Trans. Power Delivery 25 1162-1171 doi:10.1109/TPWDR.2009.2030890
[4] Jokar P, Arianpoo N, Leung V C M 2016 Electricity Theft Detection in AMI Using Customers’ Consumption Patterns IEEE Trans. Smart Grid 7 216-226 doi:10.1109/TSG.2015.2425222
[5] Wu R, Wang L, Hu T 2018 AdaBoost-SVM for Electrical Theft Detection and GRNN for Stealing Time Periods Identification. In Proceedings of the IEEE 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society; IEEE: Washington, DC, 3073-3078
[6] Chen Q, Zheng K, Kang C, Huangfu F 2018 Detection Methods of Abnormal Electricity Consumption Behaviors: Review and Prospect Automation of Electric Power Systems 2018 42 189-199, doi:10.7500/AEPS20171128013
[7] Zheng Z, Yang Y, Niu X, Dai H N, Zhou Y 2018 Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids IEEE Trans. Ind. Inf. 14 1606-1615 doi:10.1109/TII.2017.2785963
[8] Hasan Md N; Toma R N, Nahid A A, Islam M M M, Kim J M 2019 Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach Energies 12 3310 doi:10.3390/en12173310
[9] Adil M, Javid N, Qasim U, Ullah I, Shafiq M, Choi J G 2020 LSTM and Bat-Based RUSBoost Approach for Electricity Theft Detection Applied Sciences 10 4378 doi:10.3390/app10124378
[10] Kim T T, Poor H V 2011 Strategic Protection Against Data Injection Attacks on Power Grids IEEE Transactions on Smart Grid 2 326-333 doi:10.1109/TSG.2011.2119336
[11] Zanetti M, Jamhour E, Pellenz M, Penna M, Zambenedetti V, Chueiri I 2019 A Tunable Fraud Detection System for Advanced Metering Infrastructure Using Short-Lived Patterns. IEEE Transactions on Smart Grid 10 830-840, doi:10.1109/TSG.2017.2753738
[12] Kim Y 2014 Convolutional Neural Networks for Sentence Classification. In Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP) Association for Computational Linguistics: Doha, Qatar 1746-1751
[13] Feng X, Hui H, Liang Z, Guo W, Que H, Feng H, Yao Y, Ye C, Ding Y 2020 A Novel Electricity Theft Detection Scheme Based on Text Convolutional Neural Networks Energies 13 5758