YIDDISHVol 9 Issue 1April 2018
ISSN NO: 0364-4308

Artificial Intelligence Based Smart Electricity Theft Detection in Power Grids Using Deep Learning Models

S.LAVANYA, N.MAMATHA

[1]Asst.Professor [M.Tech], Department of CSE, DVR &DR.HS MIC College of Technology, Kanchikacherla, Krishna(DT).

ABSTRACT: As one of the major factors of the nontechnical losses (NTLs) in distribution networks, the electricity theft causes significant harm to power grids, which influences power supply quality and reduces operating profits. In order to help utility companies solve the problems of inefficient electricity inspection and irregular power consumption, a novel hybrid convolutional neural network-random forest (CNN-RF) model for automatic electricity theft detection is presented in this paper. In this model, a convolutional neural network (CNN) firstly is designed to learn the features between different hours of the day and different days from massive and varying smart meter data by the operations of convolution and down sampling. In addition, a dropout layer is added to retard the risk of over fitting, and the back propagation algorithm is applied to update network parameters in the training phase. And then, the random forest (RF) is trained based on the obtained features to detect whether the consumer steals electricity. To build the RF in the hybrid model, the grid search algorithm is adopted to determine optimal parameters. Finally, experiments are conducted based on real energy consumption data, and the results show that the proposed detection model outperforms other methods in terms of accuracy and efficiency.

KEY WORDS: Deep neural network, electricity theft, machine learning, minimum redundancy maximum relevance, smart grids.

1. INTRODUCTION

The loss of energy in electricity transmission and distribution is an important problem faced by power companies all over the world. The energy losses are usually classified into technical losses (TLs) and nontechnical losses (NTLs) [1]. The TL is inherent to the transportation of electricity, which is caused by internal actions in the power system components such as the transmission liner and transformers [2]; the NTL is defined as the difference between total losses and TLs, which is primarily caused by electricity theft. Actually, the electricity theft occurs mostly through physical attacks like line tapping, meter breaking, or meter reading tampering [3].These electricity fraud behaviours may bringabout the revenue loss of power companies. As an example, the losses caused by electricity theft are estimated as about $4.5 billion every year in the United States (US) [4]. And it is estimated that utility companies worldwide lose more than 20 billion every year in the form of electricity theft [5]. In addition, electricity theft behaviours can also affect the power system safety. For instance, the heavy load of electrical systems caused by electricity theft may lead to fires, which threaten the public safety. Therefore, accurate electricity theft detection is crucial for power grid safety andstableness.

With the implementation of the advanced metering infrastructure (AMI) in smart grids, power utilities obtained massive amounts of electricity consumption data at a high frequency from smart meters, which is helpful for us to detect electricity theft[6, 7]. However, every coin has two sides; the AMI network opens the door for some new electricity theft attacks. These attacks inthe AMI can be launched by various means such as digital tools and cyber attacks. The primary means of electricity theft detection include humanly examining unauthorized line diversions, comparing malicious meter records with the benign ones, and checking problematic equipment or hardware. However, these methods are extremely time- consuming and costly during full verification of all meters in a system. Besides, these manual approaches cannot avoid cyber attacks. In order to solve theproblems mentioned above, many approaches have been put forward in the past years. These methods are mainly categorized into state-based, game-theory- based, and artificial-intelligence-based models the performance of the detectors is investigated using synthetic data, which does not allow a reliable assessment of the detector's performance compared with shallow architectures. Moreover, the authors in [19] proposed a deep neural network- (DNN-) based customer-specific detector that can efficiently thwart such cyber attacks. In recent years, the CNN has been applied to generate useful and discriminative

features from raw data and has wide applications in different areas [20–22]. These applications motivate the CNN applied for feature extraction from high- resolution smart meter data in electricity theft detection. In [23], a wide and deep convolutional neural network (CNN) model was developed and applied to analyse theelectricity theft in smart grids.

2. LITERATURE SURVEY

In this paper author is using combination of CNN (Convolution Neural Networks) andRandom Forest to detect theft fromelectricity power grid as this theft will cause huge financial loss and disturbance in powersupply. To efficiently detect theft frompower grid author combining CNN and Random Forest Algorithms and after combining we are getting better prediction accuracy compare to normal algorithms. In power consumption if there is huge consumption in certain period then in datasetwe will get value as 1 which indicates energy theft else we will have 0 as class label which means normal energy usage.

3. EXISTING SYSTEM

Research on electricity theft detection in smart grids has attracted many researchers to devise methods that mitigate against electricity theft. Methods used in the literature can be broadly categorized into the following three categories: hardware-based, combined hardware and data-baseddetection methods and data-driven methods. Hardware-based methods [13]–[19]generally require hardware devices such as specialized microcontrollers, sensors andcircuits to be installed on power distribution lines. These methods are generally designed to detect electricity theft done by physically tampering with distribution components such as distribution lines and electricity meters. They can not detect cyber attacks. Electricity cyber attack is a form of electricity theft whereby energy consumption data is modified by hacking theelectricity meters [7].

DISADVANTAGES

- Accuracy is Low.
- Only using Data Mining algorithms.

4. PROPOSED SYSTEM

In this paper author is using combination of CNN (Convolution Neural Networks) andRandom Forest to detect theft fromelectricity power grid as this theft will cause huge financial loss and disturbance in powersupply. To efficiently detect theft frompower grid author combining CNN and Random Forest Algorithms and after combining we are getting better prediction accuracy compare to normal algorithms. In power consumption if there is huge consumption in certain period then in datasetwe will get value as 1 which indicates energy theft else we will have 0 as class label which means normal energy usage.

5. ARCHITECTURE

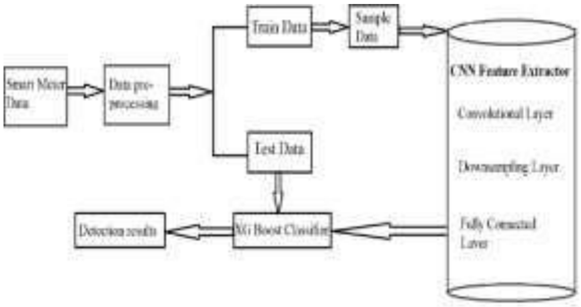

Fig: 1. Architecture

MODULES

1) Reading dataset: using this module reading power consumption dataset
2) Pre process dataset: using this module we will normalize and clean dataset by removing missing dataset
3) Train CNN Model: using this module we will train CNN with dataset and then will extract trained features from CNN and then inputthis trained features to random forest algorithm to build theft prediction model. To remove irrelevant featureswe have added DROPOUT layer.
4) Train CNN with Random Forest: using this module will train random forest with CNN features and thencalculate precision, recall, FSCORE and accuracy
5) Train CNN with SVM: using this module will train SVM with CNNfeatures and then calculate precision,recall, FSCORE and accuracy
6) Train Random Forest without CNN: Here we trained random forest on normal dataset without using CNNfeatures and then calculate precision,recall, FSCORE and accuracy
7) Train SVM without CNN: Here we trained SVM on normal dataset without using CNN features and thencalculate precision, recall, FSCORE and accuracy
8) Comparison Graph: using this we will display comparison graph between all algorithms
9) Predict Electricity Theft: Using this module we will upload test data and

then CNN-RF will predict whethertest records contains ENERGY THEFT or not.

6.1 FEATURE EXTRACTION

Electricity consumption data used in this project is univariate time-series data. A univariate measurement is a single measurement frequently taken over time [11]. For solving classification problems, data can be represented by its features (properties), which can then be fed as input to the classifier, as is the case in [29], [34] and [48]. Data is classified based on the similarity between features [17] given a dataset of different samples. In this work, time-domain and frequency-domain features were extracted and used as input to a deep neural network for classification. Classification performance comparison between time-domain, frequencydomain andcombined features from both domains was carried out.

6. RESULT

Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph

Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph

CONCLUSION

In this paper, a novel CNN-RF model is presented to detect electricity theft. In this model, the CNN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Because a large number of parameters must be optimized that increase the risk of over fitting, a fully connected layer with a dropout rate of 0.4 is designed during the training phase. In addition, the SMOT algorithm is adopted to overcome the problem of data imbalance. Some machine learning and deep learning methods such as SVM, RF, and all those methods have been conducted on SEAI and LCL datasets. The results indicate that the proposed CNN-RF model is quite a promising classification method in the electricity theft detection field because of two properties: The first is that features can be automatically extracted by the hybrid model, while the success of most other traditional classifiers relies largely on the retrieval of good hand-designed features which is a laborious and time-consuming task. The second lies in that the hybrid model combines the advantages of the RF and CNN, as both are the most popular and successful classifiers in the electricity theft detection field

FUTURE SCOPE

In comparison with other data-drivenmethods evaluated on the same dataset, The method used here utilizes consumption data patterns. Apart from its application in power distribution networks, it can be used in anomaly detection applications in any field. Our work brings a small contribution towards accurately detecting energy theft as

we detect theft that only took place overtime. We wish to extend our method to detect real-time electricity theft in the future.

REFERENCE

[1] S. Foster. (Nov. 2, 2021). Non-TechnicalLosses: A $96 Billion Global Opportunity for Electrical Utilities.

[2] Q. Louw and P. Bokoro, ‘‘An alternative technique for the detection and mitigation of electricity theft in South Africa,’’ SAIEE Afr. Res. J., vol. 110, no. 4, pp. 209–216, Dec. 2019.

[3] M. Anwar, N. Javaid, A. Khalid, M.Imran, and M. Shoaib, ‘‘Electricity theft detection using pipeline in machine learning,’’ in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020, pp. 2138–2142.

[4] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, ‘‘Wide and deep convolutionalneural networks for electricity-theftdetection to secure smart grids,’’ IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[5] P. Pickering. (Nov. 1, 2021). E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering. [Online]. Available: https://www.electronicdesign.com/technologies/meters

[6] X. Fang, S. Misra, G. Xue, and D. Yang,‘‘Smart grid—The new and improved powergrid: A survey,’’ IEEE Commun. Surveys Tuts., vol. 14,no. 4, pp. 944–980, 4th Quart.,2012.

[7] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin, and K. Qaraqe,‘‘Efficientdetection of electricity theft cyber attacks in AMI networks,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018,pp. 1–6.

[8] A. Maamar and K. Benahmed,‘‘Machinelearning techniques for energy theft detection in AMI,’’ in Proc. Int. Conf. Softw. Eng. Inf. Manage. (ICSIM), 2018,pp. 57–62.

[9] A. Jindal, A. Schaeffer-Filho, A. K. Marnerides, P. Smith, A. Mauthe, and L.Granville, ‘‘Tackling energy theft in smart grids through data-driven analysis,’’ in Proc.Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2020, pp. 410–414.

[10] I. Diahovchenko, M. Kolcun, Z. Čonka,
V. Savkiv, and R. Mykhailyshyn, ‘‘Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads,’’ Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 44, no. 4, pp. 1319–1333, Dec. 2020.

[11] M. Jaganmohan. (Mar. 3, 2022). GlobalSmart Grid Market Size by Region 2017–2023. [Online]. Available