IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908020 |

Electricity Theft Detection Using Machine Learning

Prof.Bharathi kale, Abhishek V Yakkundi, Abhishek M Talekar, Ashish S Kalasannavar, Sanjana Patil

Dept. of Computer Science and Engineering, Visvesvaraya Technological University Belagavi, Angadi Institute of Technology and Management Belagavi, India

ABSTRACT: The focuses on detecting electricity theft cyber-attacks in the consumption domain, this paper investigates electricity thefts at the distributed generation (DG) domain. In this attack, customers hack into the smart meters monitoring their renewable-based DG units and manipulate their readings to claim higher supplied energy to the grid and hence falsely overcharge the utility company. Deep machine learning is investigated to detect such a malicious behavior. A set of cyber-attack functions were introduced to manipulate the integrity of the readings of the injected power from the DG units in order to falsely overcharge the electric utility company. Electricity theft can be harmful to power grid suppliers and cause economic losses. Integrating information flows with energy flows, smart grids can help to solve the problem of electricity theft owning to the availability of massive data generated from smart grids. The data analysis on the data of smart grids is helpful in detecting electricity theft because of the abnormal electricity consumption pattern of energy thieves. However, the existing methods have poor detection accuracy of electricity-theft since most of them were conducted on one dimensional (1-D) electricity consumption data and failed to capture the periodicity of electricity consumption. Deep convolutional Neural Network is performed and analyse the cyber-theft on electrical data. The machine learning and Convolutional Neural Network is applied and find the electricity theft. As a result, Wide & Deep CNN model can achieve the excellent performance in electricity-theft detection. The predicted result in the form of accuracy, precision, recall, f1-measure, sensitivity and specificity.

KEYWORDS: Electricity Theft Detection, Smart Grids, ConvolutionalNeural Networks, Machine Learning, Deep Learning

I. INTRODUCTION

Electrical theft is one of the most prominent issues pertaining to conventional power grids and have been a major concern to the utility providers for quite a long time. The losses incurred by the providers due to these thefts are enormous and undesirable. Electricity theft represents a pressing problem that has brought enormous financial losses to electric utility companies worldwide. This section describes how realistic benign and malicious datasets are developed. Since this data is not publicly available, realistic synthetic data is created. Real load profiles and solar irradiance data are utilized to obtain the benign data, then a set of cyber-attack functions are applied on the benign dataset to obtain the malicious dataset. The benign and malicious datasets will then be used to train the classifier. One of the goals of this work is to investigate the integration of different data sources in the training process of the deep learning-based detector. These various data sources include the readings from DG smart meters, meteorological data (solar irradiance), and SCADA metering points. In order to develop a deep learning-based electricity theft detection system, we have investigated the application of deep feed forward, and deep artificial neural networks. The detector is trained using benign and malicious datasets. Hyper parameter optimization is applied to define the optimal architecture for the detector. The detector developed herein is a general detector trained using datasets obtained from all the DGs in the system, and hence, the detector can be used to detect the presence of electricity theft cyber-attack for any DG unit in the system. Our investigations revealed that a hybrid C-RNN deep learning architecture offers the best detection performance among different deep learning-based models. Optimal selection of hyper-parameters is investigated using a random grid search approach. Our studies also demonstrated that the detection performance can be significantly enhanced if multiple data sources are integrated while training the detector. In specific, the integration of the PV generation profile, irradiance data, and SCADA meter readings. Electrical theft leads to enormous losses to the utilities in the power sector. The major cause of these thefts is the illegal use of electricity by the consumers through tapping. To detect the malicious consumers that intentionally purloin the electricity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908020 |

II. RELATED WORK

We roughly categorize the studies on electricity-theft detection into two types: hardware-based solutions and data-driven solutions. In particular, hardware-based solutions concentrate on designing specific metering devices and infrastructures so that electricity theft can be easily detected. Typical electricity theft detection equipment's include smart meters with ant tampering sensors, radio-frequency identification (RFID) tags and sensors [14], [15], [16]. The main limitations of hardware based solutions include 1) the cost of deploying smart metering devices, 2) the vulnerability of hardware devices (e.g., failure due to severe weather condition), 3) the difficulty in maintaining devices (e.g., replacing batteries of devices). Data driven electricity-theft detection has drawn considerable attentions recently. For example, the work in [2] is based on the data fusion from sensors and advanced metering infrastructure (AMI). Many recent studies [17], [18], [19] are based on support vector-machines (SVM). The main idea of SVM methods is to classify the normal users and the electricity thieves. In addition to SVM, artificial neural networks can also be used to electricity-theft detection [10], [11]. However, most of these studies are less accurate in electricity-theft detection and require artificial feature extraction according to domain knowledge.

B. Anomaly Detection in Smart Grids

Anomaly detection in smart grids represents a substantial body of works related to data driven electricity-theft detection. In particular, anomaly detection (a.k.a. outlier detection) is the procedure of detecting abnormal patterns that do not conform the expected behaviour [20]. Anomaly detection has been widely used in many research areas, such as intrusion detection [21], fraud detection [22] and industrial control systems [23]. Recently, anomaly detection has received extensive attention from the smart grid community since it can help in improving operational safety, enhancing the control reliability and detecting faults in smart metering infrastructure [24], [25], [26]. The typical approaches used in anomaly detection in smart grids mainly include SVM (Support Vector Machine), clustering and classification [27]. Besides, Decision Tree and Rough Sets can also be used in fraud detection in power systems [28]. Moreover, [29] presents a rule-based model to detect the NTLs.

However, most of related studies in either electricity-theft detection or anomaly detection are based on the analysis on 1-D electricity consumption data and fail to capture the periodicity of electricity consumption. Therefore, it is the purpose of this study to propose a novel analytical model to overcome the limitations of the above existing works.

III. PROPOSED SYSTEM

The proposed model is introduced to overcome all the disadvantages that arises in the existing system. We are applying data mining techniques to identify suitable process for electrical theft in smart grid. And, thus the prediction process is less time consuming. It will help to find the electricity theft from smart grid electricity dataset. This system will increase the accuracy of the supervised classification results by classifying the data based electricity theft and using classification algorithm. It enhances the performance of the overall classification results. The machine learning and Convolutional Neural Network is used to predict the electrical theft from the smart grid dataset.

IV. PSEUDO CODE

```
#Feature Scaling
from sklearn. preprocessing import StandardScaler
sc_X = StandardScaler()
X_train =sc_X.fit_transform(X_train)
X_test = sc_X.transform(X_test)

#Fitting Logistic Regression to dataset
from sklearn.linear_model import LogisticRegression
classifier = LogisticRegression()
classifier.fit(X_train, y_train)

#Predicting the test set result
y_pred = classifier.predict(X_test)

#Making the confusion matrix
```

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908020 |

```
from sklearn.metrics import confusion_matrix
cm = confusion_matrix(y_test, y_pred)
```

V. SIMULATION RESULTS

In our Wide & Deep CNN method, the epoch is a parametercontrolling the train round. An epoch is defined by one forwardpass and one backward pass of all training samples. We choosethe similar settings like parameter study to investigate theimpact of the epoch. In particular, we vary the epoch valuesfrom 10 to 100 with the step value of 1 and we fix= 60= 120. Similarly, we also conduct two groups of experiments with different training ratio (60% or 80%).when the epochvalue increases, both AUC and MAP increase at first. But after a certain threshold on the epoch, both AUC and MAPdrop while they increase again later. This phenomenon can be explained as follows. When we choose a smaller epoch value,it may be not enough to let our Wide & Deep CNN system learn from both 1-D and 2-D data. However, it may causeoverfitting when we choose a larger epoch value. Therefore, there also exists a threshold on the epoch value to optimize thetraining procedure in our Wide & Deep CNN. For example, the best performance was achieved when the number of epochsreaches 30 when the training ratio is 60%.

VI. CONCLUSION AND FUTURE WORK

In this process, we present the predictive models by using machine learning methods including Logistic Regression, and deep neural network algorithm of Convolutional Neural Network is to predict Electricity theft. The predictive data model is implemented by using different data mining techniques by paying attention to most unpopular data mining algorithms. As per to the literature surveys conducts in this study, it clearly represents that the most researchers use popular data mining algorithms like Logistic Regression, and Convolutional Neural Network as the classification techniques.

In future, it is possible to provide extensions or modifications to the proposed clustering and classification algorithms using intelligent agents to achieve further increased performance. Apart from the experimented combination of data mining techniques, further combinations such as artificial intelligence, soft computing and other clustering algorithms can be used to improve the accuracy.

REFERENCES

[1] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, “Energy-theft detection issues for advanced metering infrastructure in smart grid,” Tsinghua Science and Technology, vol. 19, no. 2, pp. 105–120, 2014.

[2] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A multi-sensor energy theft detection framework for advanced metering infrastructures,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1319–1330, 2013.

[3] “Smart meters help reduce electricity theft, increase safety,” https://www.bchydro.com/news/conservation/2011/smart meters energy theft.html, BC Hydro Inc., Tech. Rep., March 2011.

[4] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, “Energy big data: A survey,” IEEE Access, vol. 4, pp. 3844–3861, 2016.

[5] X. Yu and Y. Xue, “Smart grids: A cyber–physical systems perspective,” Proceedings of the IEEE, vol. 104, no. 5, pp. 1058–1070, 2016.

[6] Y. Liu, C. Yuen, R. Yu, Y. Zhang, and S. Xie, “Queuing-based energy consumption management for heterogeneous residential demands in smart grid,” IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1650–1659, 2016.

[7] K. Wang, C. Xu, Y. Zhang, S. Guo, and A. Zomaya, “Robust big data analytics for electricity price forecasting in the smart grid,” IEEE Transactions on Big Data, 2017.

[8] Y. Wu, X. Tan, L. Qian, D. H. Tsang, W.-Z. Song, and L. Yu, “Optimal pricing and energy scheduling for hybrid energy trading market in future smart grid,” IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1585–1596, 2015.

[9] M. H. Yaghmaee, M. Moghaddassian, and A. Leon-Garcia, “Autonomous two-tier cloud-based demand side management approach with microgrid,” IEEE Transactions on Industrial Informatics, vol. 13, no. 3, pp. 1109–1120, 2017.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908020 |

[10] B. C. Costa, B. L. A. Alberto, A. M. Portela, W. Maduro, and E. O. Eler, "Fraud detection in electric power distribution networks using an annbased knowledge-discovery process," International Journal of Artificial Intelligence & Applications, vol. 4, no. 6, pp. 17–21, 2013.

[11] J. I. Guerrero, C. Leon, I. Monedero, F. Biscarri, and J. Biscarri, Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection." KnowledgeBased Systems, vol. 71, pp. 376–388, 2014.

[12] C. C. Ramos, A. N. Souza, G. Chiachia, A. X. Falcao, and J. P. Papa, "A novel algorithm for feature selection using harmony search and its application for non-technical losses detection," Computers & Electrical Engineering, vol. 37, no. 6, pp. 886–894, 2011.

[13] L. A. P. Junior, C. C. O. Ramos, D. Rodrigues, D. R. Pereira, A. N. de Souza, K. A. P. da Costa, and J. P. Papa, "Unsupervised nontechnical losses identification through optimum-path forest," Electric Power Systems Research, vol. 140, pp. 413–423, 2016.

[14] B. Khoo and Y. Cheng, "Using rfid for anti-theft in a chinese electrical supply company: A cost-benefit analysis," in 2011 IEEE Conference on Wireless Telecommunications Symposium (WTS). IEEE, 2011, pp. 1–6.

[15] S. Ngamchuen and C. Pirak, "Smart anti-tampering algorithm design for single phase smart meter applied to ami systems," in 2013 IEEE Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). IEEE, 2013, pp. 1–6.

[16] K. Dineshkumar, P. Ramanathan, and S. Ramasamy, "Development of arm processor based electricity theft control system using gsm network," in 2015 IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2015, pp. 1–6.

[17] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," IEEE transactions on Power Delivery, vol. 25, no. 2, pp. 1162–1171, 2010.

[18] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in Power Systems Conference and Exposition (PSCE). IEEE, 2011, pp. 1–8.

[19] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and F. Nagi, "Improving svm-based nontechnical loss detection in power utility using the fuzzy inference system," IEEE Transactions on power delivery, vol. 26, no. 2, pp. 1284–1285, 2011.

[20] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, pp. 15:1–15:58, Jul. 2009.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details