JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Anomaly Attack Detection Model in Microgrids using Machine Learning

Monika KC
BE, Student
Dept of Computer Science
K S Institute of Technology
Bangalore, Karnataka
kcmonika259@gmail.com

Chaithra R
BE, Student
Dept of Computer Science
K S Institute of Technology
Bangalore, Karnataka
krishnachaithra2000@gmail.com

Fariya N
BE, Student
Dept of Computer Science
K S Institute of Technology
Bangalore, Karnataka
fariya2700@gmail.com

Mr. Kushal Kumar BN
Assistant Professor
Dept of Computer Science
K S Institute of Technology
Bangalore, Karnataka
kushalkumarbn@gmail.com

***Abstract*— In recent years, Microgrids are involved in Communication and Information Technology, and recognized as an important unit of Internet of Things (IoT). A number of CII which is Critical Information Infrastructure systems are relying on these technologies. This dependency of microgrids makes them prone to malicious cyberattacks, which can create major technical, economic, social and control problems in power network systems. Detection of cyber-attacks with high accuracy is a challenge. In microgrids, the Advanced Metering Infrastructure (AMI) is developed to monitor and control the grid for stable and efficient operation. The AMI is vulnerable to cyberattacks. Many research efforts are going on detecting such attacks. This paper performs a survey on various algorithms implemented to detect data integrity attacks and anomaly attacks that happen during transmission in a microgrid.**

Keywords—*Smart grids, Cyberattack, Advanced Metering Infrastructure (AMI), Machine learning, Anomaly attack.*

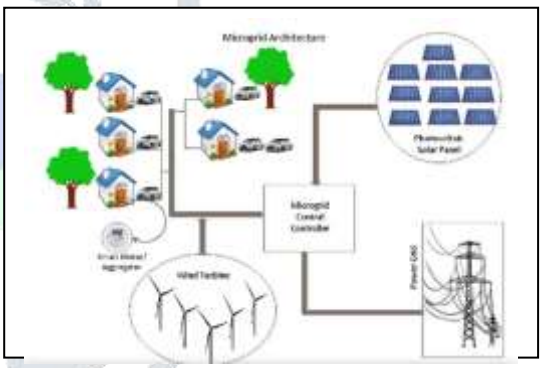

Figure 1: Architecture of Microgrid [15]

I. INTRODUCTION

Microgrid is an evolution of electric grid system that utilizes renewable energy sources such as solar panels and wind turbine. The power grid is a network of power generators, transmission lines, transformers and distribution systems used to deliver power/electricity to the consumers. These grids are connected to homes, industries, Areas, or other buildings to constantly supply power. But if this grid is repaired or happens to blackout, the whole unit stops working and no power is delivered to the consumers, that is when microgrids comes into picture. The microgrid is connected to the grid which consists of generators, renewable sources etc. These microgrids can work with or without the help of main grid i.e., either in grid-connected mode or in island-mode.

Whenever there is a power outage in the power grid, the microgrid acts as a backup for grid in case of emergencies. It disconnects from the traditional grid and operates to continue delivering electricity to the consumers.

The Microgrid consisting of distributed generators, batteries, renewable sources like solar panels are connected to the grid. These microgrids can work with or without the help of main grid i.e., either in grid-connected mode or in island-mode. Whenever there is a power outage in the power grid, the microgrid acts as a backup for grid in case of emergencies. It disconnects from the traditional power grid and operates to continue delivering electricity to the consumers.

The Advanced Metering Infrastructure is the system which is used to collect and analyze the data provided by the smart meters by using two-way communication. Smart meters, Communication Networks etc., are the components of the AMI. These smart meters allow consumers/customers to

control their power consumption and also allows them to manage the power in case of high-power usage. AMI can reduce the cost of traditional utility operations which includes readings of meter, customer and field services, management of theft and other functions. The Communication Network transmits the data from smart meters to utility organization and vice-versa. Overall, AMI is responsible of efficient operation of the microgrid therefore the security of smart meters is very important.

The most common attacks that happen are Data Integrity Attacks and Anomaly Attack. The former where the original true data is replaced with false data acknowledged by the smart meters also where the attackers can encrypt sensitive or important corporation information. Anomaly is an occurrence of a rare event that does not fall with the usual when the attacker targets the network by injecting false data or manipulating the data sharing in the network. Anomaly detection is a process in data mining that checks the points or events that are different from a dataset's usual behavior. It is an important role in detecting any crime or intrusion happening in the network and other rare events.

II LITERATURE SURVEY

Xinyu Yang, Peng Zhoa, et.al [1] In this paper, a Guassian-Mixture based method is implemented in order to detect the attacks like Data Integrity (alters the true data) in the Smart Grid System. This technique is used to obtain a narrowed area of actual data based on lower (i.e., minimum) and upper (i.e., maximum) values to detect false data more precisely.

Jie Duan, Wente Zeng, et.al [2] In this paper the authors have constructed a four-step attack-resilient control process (consisting of information estimation, false information detection, attack identification and attack mitigation) is built along with DC-OPF algorithm to detect the Data Integrity Attacks.

Omar Ali Beg and Taylor T. Johnson [3] have proposed FDIA (False Data Integrity Attack) detection framework where the erroneous data is recognized by differentiating the candidate invariants and the actual invariants so that any mismatch reveals the existence of a cyber-attack.

Qingyu Yang, Donghe Li, et.al [4] A method is proposed to overcome the data integrity attack. Basically, a defensive framework is built where the minimum number of nodes are considered, and counter schemes are applied to that.

Christian Promper, Dominik Engel, et.al [5] In this paper, they have created a system that include developed anomaly detection techniques for all the imbalanced datasets in a microgrid communication stages. This system uses K-NN, SVM techniques to detect anomaly. A better performance was optimized by using the hierarchical three-layer smart grid.

Saeed Ahmed, Youngdoo Lee, et.al [6] In this paper, the authors propose machine learning model to find a cyber deception assault in the position of estimation–measurement for the data that are acquired through a microgrid communication network. The optimize detection accuracy and reduce computational complexity was achieved by different characteristic like genetic algorithm feature selection in scheme.

Defu Wang, Xiaojuan Wang, et.al [7] The paper suggests a model to encounter attacks for a power-based system, then instructed by using data and logs composed by phasor measurement units (PMUs), later the proposed model is compared with models of other methods using evaluation metrics in order to identify and counteract the attacks.

Ali Sayghe, Yaodan Hu, et.al [8] In this paper, false data injection attacks are investigated. They have tried to overcome the drawbacks of existing BDD [Bad Data Detection] approaches. ML algorithms such as Supervised and Deep learning have been used. In Conclusion, the above-mentioned algorithms achieve the highest detection rates.

Mohammad Ashrafuzzaman, Saikat Das, et.al [9] The paper proposes a scheme to detect FDIA attacks based on State estimation. Ensemble learning is used where decisions given by the individual classifiers are classified again. Supervised classifiers and unsupervised classifiers are used.

Mario R. Camana, Saeed Ahmed, et.al [10] In the paper, they balanced the computational complexity of every Machine Learning based schemes which are considered by applying KPCA (Kernel Principal Component Analysis) technique for the perception of SCA (Side Channel Attack) attacks in smart grid network systems.

Nebrase Elmrabit, Feixiang Zhou, et.al [11] created a machine learning model which will detect anomaly. This paper they have used 12 ML algorithms to check in terms of their capacity to find anomalous behaviors in the network. Mainly three datasets (i.e., UNSW-NB15, CICIDS-2017, and ICS cyberattack) were used for the methods. Finally, results RF classification provides better accuracy, recall in most of cases and among the other methods.

Manikant Panthi [12] In regard to various existing system. This paper detects the cyberattack caused against the power system. Various machine learning Algorithms like Jripper, Random Forest, one-R, Naive Bayes methods. It involved a three-class dataset -No events, Attack and natural.

Yasir Ali Farrukh, Zeeshan Ahmad,Irfan Khan, et.al [13] In this paper, the authors aim to have more accuracy in increasing the detection of cyber-attacks so proposed a two-layer hierarchical machine learning model. The model is used first layer to differentiate between cyberattack or normal state. The other layer is used to classify different types of cyberattacks.

Qi, R.; Rasband, C.; Zheng, et.al [14] Most existing systems detect cyber-attacks in power systems based on Supervised Machine learning which require a lot of historical data for it to be a good model, this paper proposes a new model for using PMU data, that uses semi-supervised anomaly detection and deep learning. The former only uses the instances of a normal events for training, thereby easier to for find unknown attack events. Semi-supervised algorithms are better when compared to the existing system. Performance can be better by using deep representation learning.

III. CONCLUSION AND FUTURE WORK

In this paper, we have briefly reviewed the need for security in the Microgrids. Further we have discussed attacks like Data Integrity and Anomaly Attacks that can happen in the smart meter. We also discuss literature review and the

various methodologies that they have implemented to capture/catch attacks that happen to occur by hackers.

Our Future work is to build an attack detection model using deep learning algorithms with better accuracy to detect anomaly attacks.

REFERENCES

[1] Xinyu Yang, Peng Zhao, Xialei Zhang, Jie Lin and Wei Yu, "A Gaussian-Mixture Model Based Detection Scheme against Data Integrity Attacks in the Smart Grid", IEEE, August 2016.

[2] Jie Duan, Wente Zeng and Mo-Yuen Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack", IEEE, November 2016.

[3] Omar Ali Beg, Taylor T. Johnson, "Detection of False-data Injection Attacks in Cyber-Physical DC Microgrids", IEEE, January 2017.

[4] Qingyu Yang, Donghe Li, Wei Yu, Yuanke Liu, Dou An, Xinyu Yang and Jie Lin, "Towards Data Integrity Attacks Against Optimal Power Flow in Smart Grid", IEEE, October 2017.

[5] Christian Promper, Dominik Engel, Robert C. Green II "Anomaly Detection in Smart Grids with Imbalanced Data Methods" ,IEEE 2017.

[6] Ahmed, S., Lee, Y., Hyun, S.-H., Koo, I., 2018. "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning". IEEE Access 6, 27518–27529.

[7] D. Wang, X. Wang, Y. Zhang and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning", Journal of Information Security and Applications, vol. 46, pp. 42-52, 2019.

[8] Ali Sayghe, Yaodan Hu, Ioannis Zografopoulos, XiaoRui Liu, "A Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems", ResearchGate, August 2020.

[9] Mohammad Ashrafuzzaman, Saikat Das, Yacine Chakhchoukh, Sajjan Shiva, Frederick T Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning." IEEE Systems Journal, October 2020.

[10] Camana-Acosta, M.R., Ahmed, S., Garcia, C.E., Koo, I., 2020. "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks". IEEE Access 8, 19921–19933.

[11] Elmrabit, N, Zhou, F, Li, F & Zhou, H 2020, "Evaluation of machine learning algorithms for anomaly detection". IEEE, International Conference on Cyber Security and Protection of Digital Services, 15/06/20.

[12] Manikant Panthi," Anomaly Detection in Smart Grids using Machine Learning Techniques", 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T).

[13] Yasir Ali Farrukh, Irfan Khan, Zeeshan Ahmad, "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System", August 2021.

[14] Qi, R.; Rasband, C.; Zheng,J.; Longoria, R. Detecting Cyber Attacks in Smart Grids Using Semi-Supervised Anomaly Detection and Deep Representation Learning.Information 2021, 12, 328.

[15] M. H. K. Tushar, C. Assi, M. Maier, and M. F. Uddin, "Smart microgrids: Optimal joint scheduling for electric vehicles and home appliances," IEEE Transactions on Smart Grid, vol. 5, no. 1, pp. 239–250, 2014.