A Survey on Detection of False Data Injection Attacks in Smart Grid Communication Systems

Dr.R. Lalitha
Professor, Department of Computer Science and Engineering, Rajalakshmi Institute Of Technology, Chennai.
Email: lalitha.r@ritchennai.edu.in
Praveen.P
Student, Department of Computer Science and Engineering, Rajalakshmi Institute Of Technology, Chennai.
Email: praveen.p.2015.cse@ritchennai.edu.in
Prasanna K
Student, Department of Computer Science and Engineering, Rajalakshmi Institute Of Technology, Chennai.
Email: prasanna.k.2015.cse@ritchennai.edu.in
Monash K
Student, Department of Computer Science and Engineering, Rajalakshmi Institute Of Technology, Chennai.
Email: monash.k.2015.cse@ritchennai.edu.in

----------Abstract----------

The transformation of ancient energy networks to smart grids will assist in revolutionizing the energy business in terms of dependability, performance and tractability. On the opposite hand, the augmented property of facility assets for bidirectional communications presents very high security vulnerabilities. Few matching approaches is found to be strong for detective work false knowledge injection attacks still as different attacks within the good grids. Once the attack is detected, system will take preventive action and alarm the manager to require preventative action to limit the danger. This paper is a survey of varied such methodologies to sight the attacks from the provided knowledge.

Keywords- **False Data Injections (FDI), Power Grid Security, Supervised Learning Algorithms, Smart Grid Systems**

I. INTRODUCTION

A smart grid technology provides simple integration and reliable service to the consumers. It is conjointly one amongst the economical ways that of the supply-consume energy by providing bi-directional energy flow and communications. It is a self-sufficing electricity network system that relies on digital automation technology to watch, management and to research at intervals the chain. The consumption, acquisition and transmission of high-granularity period of time power grid knowledge is expedited through the combination of communications, computing, and advanced management technologies. As explicit within the paper [1], the electricity felony is one amongst the forbidding threat for numerous industries. The dependence on the knowledge technology, raises inquiries to the results of cyber-attacks on power grid operations.

There numerous analysis that was developed on proposing various FDI attacks and developing the potential methods to develop. The subsequent methods are few that are developed by few authors. Yang et al. [2] developed the least-effort attack strategy and planned a protection-based defence theme and a detection-based defence scheme. Ozay et al. [3] modelled the attack strategy victimization Gaussian method and used machine learning strategies for attack detection. Liu et al. [4] developed an FDI detection mechanism by victimization the properties of the low spatial property of measurements and meagerness of attacks. In [5], the equivalent mensuration transformation and also the largest weighted residual technique were integrated for detective work the FDI attacks.

On the opposite hand, malicious attacks are often launched to bypass the prevailing dangerous mensuration detection techniques and acquire the results of state by capitalizing the configuration of power grid, calculable at random. As a result, this survey targets at providing a short review on numerous techniques employed in detective work false knowledge for acute results. The paper is divided into numerous sections- wherever Section two presents an outline of the scope and methodologies associated with detection of false data whereas Section three contains of table that contains previous works- the info supply and also the result together with the limitation and the final section, Section four concludes the survey.

II. SCOPE AND METHODOLOGY

Researchers have proposed a variety of methods to detect false data injection attacks. Some of the mechanisms and algorithms are discussed here.

2.1. Adaptive Cusum (Cumulative Sum) Test

Yi Huang et al. [1] have proposed the adaptive CUSUM algorithm for detecting false data injection attack in smart grid. The planned work for grid state estimation composes 2 interleaved stages: Stage one introduces the linear unknown parameter problem solver technique, and Stage two applies the multi-thread CUSUM algorithmic rule for determining the possible existence of adversary at the control center as quickly as possible without violating the given constraints while maintaining a certain low level of detection error rate. An adaptive CUSUM algorithm, which assumes that the state variables of the smart grid follows a Gaussian prior with some known mean and covariance, an, also assumes that the FDIA is always

positive and small so that the first-order approximation to the decision statistic is valid.

Y. Huang et a. [2] have used a CUSUM-type algorithm based on the residuals. The Rao test statistic is utilized to construct the decision statistic. However in many cases, such decision statistic cannot be evaluated due to the singularity of the covariance of the residuals.

M. N. Kurt et al. [3], have proposed a CUSUM-type algorithm based on the Kalman filter which relies on the assumption that the state variables of the smart grid evolve over time by following a known linear model. On the contrary, in this paper, no assumption is made on the dynamic of the time-varying state variables. In addition, no performance analysis is provided for the proposed algorithm.

2.2. Machine Learning

Rehan Nawaz et al. [4] have presented a paper on detection of false data injection using machine learning. Communication is the main feature of smart grid and also the vulnerable one. By attacking in communication line any load shading power theft or any other purpose can be achieved. In FDI using Linear Regression, we assumed that our data is linear and applied linear regression. Attack vector is constructed and we showed that our attack vector has bypassed BDD and SVM.

Can Yung et al. [5] have proposed a paper for comparing four outlier detection methods, namely one-Class SVM, Robust covariance, Isolation forest and Local outlier factor method from machine learning. All the four outlier detectors perform better once the contamination rate becomes smaller, no matter in respect of accuracy or precision, which is a benefit for detecting those small-scale attacks that are unobservable in traditional detections.

BaoyiWanga et al. [6] have viewed supervised binary classification problems, where the attacked and safe measurements are marked as two independent categories. In the experiment, they have observed that machine-learning algorithm shows better performance and can detect FDIA more effectively. Meanwhile, KNN is very sensitive to the size of system than various algorithms. The performance of SVM is better for large scale systems than other algorithms. Figure 1.1 briefs the steps involved in machine learning.

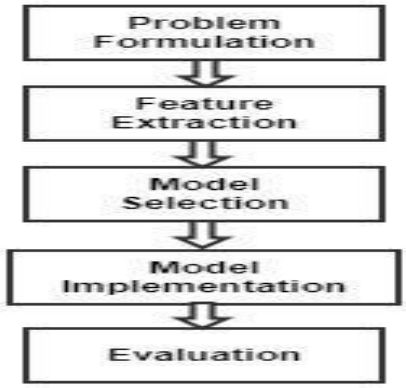

Figure 1.1 Steps in Machine Learning

2.3. Sparse Optimization

Lanchao Liu [7] have proposed a mechanism that exploits the temporal correlation of the time-series state measurements, as well as the sparse nature of the malicious attacks, to detect the false data injection in power grid. The false data detection problem is formulated as the matrix separation problem. Two methods, the nuclear norm minimization method and low rank matrix factorization method, are proposed to recover the electric power states as well as detect the malicious attacks in the power grid. The proposed methods can also deal with missing measurements. Numerical simulations are performed to evaluate the performance of proposed algorithms. The effects of the missing measurement ratio, attack ratio and dimension of measurements are also analysed.

Jingxuan Wang et al. [8] have examined the problem of detecting data injection attacks in smart grid networks. They proposed a detection framework named F-DDIA, which can recover the initial system state and also the real measurement readings. Due to the sparse nature of false data injection attacks, minimization technique including Douglas-Rachford can be applied. The proposed detection algorithm is validated using load data from NYISO. This detector works well in both linear and nonlinear systems.

2.4. Short-Termstateforecasting-Aided Method

Junbo Zhao et al. [9] have proposed a general linear measurement model which is derived to handle both SCADA and PMU measurements. The generic FDIA based on this model is derived and the error tolerance of such attacks is analysed. Then, the short-term state forecasting method considering temporal correlation is used to exploit the measurement consistency between the forecasted measurements and the received measurements. In addition the measurement consistency test is integrated with the alpha–norm and L2-norm based measurement residual analysis to construct the necessary detection metric.

2.5. Detection Algorithm

Yun Liu et al. [10] have presented a paper where the principle of false data injection is stated, and proposed two distributed detect algorithms. One is DOID

(Distributed Observable Island Detection algorithm), which relies on observable islands theory. If a line connected by two nodes which pass through different observable islands, then false data injection is detected in this line. The second algorithm is DTAD (Distributed Time Approaching Detection algorithm). At one measuring point, if the state estimation values vary a lot, then nearly 190 attack can be detected. The simulation shows this methods can detect false data injection with low cost in an efficient way.

Table : Survey And Performance Analysis

No	Authors	Journal, year of publication	Methodology and tools	Data source and result
1	Lanchao Liu, Mohammad Esmalifalak,Qifeng Ding,Valentine A. Emesih,,Zhu Han [7]	IEEE Transactions on Smart Grid, March 2014	Sparse Optimization	**Dataset:** Readings from remote electrical meters **Result:** A model that exploits temporal correlation of time-space measurements and also the nature of the attacks. It also deals with the missing parameters.
2	Mete Ozay,IñakiEsnaola,FatosTunayYarmanVural,Sanjeev R. Kulkarni, H. Vincent Poor [13].	IEEE Transactions On Neural Networks And Learning Systems	Machin Learning methods	**Dataset:** Positive and negative samples that are each linearly separable and non-separable **Result:** Analysed on-line learning strategies for detection issues of real-time attacks. **Limitation:** For smaller values of input within SVM, the model fails and the computational complexity is high
3	Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and MansoorAlam [14].	IEEE Transactions On Smart Grid, December 2011	Smart grid distributed intrusion detection system (SGDIDS)	**Dataset:** NSL-KDD dataset is employed for training and testing **Result:** Utilizes the straified and distributed intrusion detection system within the wireless mesh network and additionally finds an optimum routing for smart grid communications. **Limitation:** Performance has got to be improved in the upcoming models
4	Junbo Zhao,Gexiang Zhang, Massimo La Scala,Zhao Yang Dong, Chen-Chen,Jianhui Wang[9]	IEEE Transactions On Smart Grid, December 2015	Short-Term State Forecasting-Aided Method	**Dataset:** 20 SCADA measurements and PMU measurements **Result:** Measurement

				consistency between the forecasted measurements and also the received measurements are compared
5	Yi Huang,HushengLi,Kristy. A Campbell,Zhu Han[1]	IEEE, 2011	Adaptive CUSUM Test	**Dataset:** Injection of false data in random intervals **Result:** Defends false data in 2 stages
6	Bo Tang, Jun Yan, Steven Kay, and Haibo He[11]	IEEE Conference on Communications and Network Security, 2016	Colored Gaussian Noise, Auto-regressive process	**Dataset:** Data with Gaussian Noise **Result:** Considered the noise within the data and addressed the problem with the proposed state estimator **Limitation:**Potency is relatively less
7	Anurag Srivastava, Thomas Morris,Timothy Ernster,Shengyi Pan,CeemanVellaithura, UttamAdhikari[12]	IEEE Transactions on Smart Grid, March 2013	Physical vulnerability algorithms	**Dataset:** Dataset with Aurora attack and mechanical input **Result:** Integrated cyber physical vulnerability of smart grid with restricted information is projected **Limitations:** Mitigation techniques has to be improved

III. CONCLUSION

This survey paper discusses on the varied methodologies to observe the false information injection attacks in good Grid. The present models use supervised learning algorithms and generalized chance magnitude relation detectors are planned for good grid security with restricted variety of meters compromised. The generalized chance magnitude relation detector depends on constant quantity inferences however isn't applicable to non-parametric inferences supported perform estimation. These techniques depend on a training information set that is employed as a regard to observe the attacks in new measurements. This approach may well be compromised throughout coaching part and/or the newer attacks as well as false information injection attacks might go undetected. None of those ways contemplate security techniques for false-data injection attacks in good grid systems, that don't seem to be applicable for all the things.

REFERENCE

[1] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test", 45th Annual Conference Inf. Sci. Syst. Baltimore, MD, USA, March 2011, pp. 1–6.

[2] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis", IEEE Syst. J., vol. 10, no. 2, pp. 532–543, 2016.

[3] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid", IEEE Transactions Information Forensics Security, vol. 13, no. 8, pp. 2015–2030, 2018.

[4] Rehan Nawaz, Muhammad Awais Shahid, Ijaz Mansoor Qureshi, Muhammad Habib Mehmood, "Machine Learning based False Data Injection In Smart Grid", IEEE 2018.

[5] Can Yang, Yong Wang, Yuhao Zhou, JiongmingRuan, Wei Liu, "False Data Injection Attacks Detection in Power System Using Machine Learning Method", Journal of Computer and Communications, 2018.

[6] YadongZhaob , ShaominZhangc , Bihe Lia, BaoyiWanga, "Study of Monitoring False Data Injection Attacks Based on Machine-learning in Electric Systems", Journal of Electronics and Information Science,2017.

[7] Lanchao Liu, Mohammed Esmalifalak,QIfengDing,Valnetine A Emesih, Zhu Han, "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization", IEEE Transactions on Smart Grid,2014.

[8] Jingxuan Wang, Lucas C. K. Hui, S. M. Yiu, Gang Zhou, and Ruoqing Zhang Hindawi ,"F-DDIA: A Framework for Detecting Data Injection Attacks in Nonlinear Cyber-Physical Systems", Security and Communication Networks ,Volume 2017.

[9] Junbo Zhao, Gexiang Zhang, Massimo La Scala, Fellow, IEEE, Zhao Yang Dong, Chen Chen, Member, Jianhui Wang, "Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks", IEEE TRANSACTIONS ON SMART GRID,2015

[10] Yun Liu, Lei Yan, Jian-wei Ren, Dan Su, "Research on Efficient Detection Methods for False Data Injection in Smart Grid" 2014 IEEE International Conference on Wireless Communication and Sensor Network.

[11] Bo Tang, Jun Yan, Steven Kay, and Haibo He, "Detection of False Data Injection Attacks in Smart Grid under Colored Gaussian Noise", IEEE Conference on Communications and Network Security, 2016

[12] Anurag Srivastava, Thomas Morris, Timothy Ernster, Shengyi Pan, CeemanVellaithura, UttamAdhikari, "ModelingCyber-PhysicalVulnerabilityoftheSmart Grid With Incomplete Information", IEEE Transactions on Smart Grid, March 2013

[13] Mete Ozay, InakiEsnaola, FatosTunayYarmanVural, Sanjeev R.Kulkarni,H Vincent Poor,, "Machine Learning Methods for Attack Detection in the Smart Grid", IEEE Transactions.

[14] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and MansoorAlam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE Transactions on Smart Grid, December 2011.

[15] Israel Akingeneye, Jingxian Wu, "Low Latency Detection of Sparse False Data Injections in Smart Grids", 2018 IEEE Translations.

[16] Wen-Long Chin, Chun-Hung Lee, Tao Jiang, "Blind False Data Attacks against AC State Estimation based on Geometric Approach in Smart Grid Communications", IEEE Transactions on Smart Grid ,2016.

[17] Ruzhi Xu, Rui Wang, Zhitao Guan, Longfei Wu, Jun Wu, Xiaojiang Du, "Achieving Efficient Detection against False Data Injection Attacks in Smart Grid", 2017 IEEE Translations.

[18] KebinaManandhar, Xiaojun Cao, Fei Hu, Yao Liu, "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter", IEEE Transactions on Control of Network Systems-2013.

[19] Mohammad Esmalifalakt, Nam Tuan Nguyent, Rong Zheng, and Zhu Rant, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid", Globecom 2013-Communication and Information System Security Symposium.

[20] Wang Jianqiao, Chen Cailian, Guan Xinping, "An Overlapping Distributed State Estimation and Detection Method In Smart Grids", IEEE-2015.

[21] Jeilin, Wei yu, Xinyu yang, "On False Data Injection Attack against Multistep Electricity Price in Electricity Market in Smart Grid", Globecom 2013-Communication and Information System Security Symposium.

[22] Md. Ashfaqur Rahman and HamedMohsenian-Rad, "False Data Injection Attacks Against Nonlinear State Estimation in Smart Power Grids", 2013 IEEE.

[23] Abdelrahman Ayad, Hany E.Z. Farag, Amr Youssef and Ehab F. El-Saadany, "Detection of False Data Injection Attacks in Smart Grids using Recurrent Neural Networks",2018-IEEE.

[24] AnuparpBoonsongsrikul, Kyung-sukLhee and ManPyo Hong, "Securing Data Aggregation against False Data Injection in Wireless Sensor Networks", ICACT-2010.

[25] Satoshi Katsunuma, Hiroyuki Kurita, RyotaShioya, Kazuto Shimizu, "Base Address Recognition with Data Flow Tracking for Injection Attack Detection" , 12th Pacific Rim International Symposium on Dependable Computing (PRDC'06)