e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

Online Identification and Data Recovery for PMU Data Manipulation Attack

Mr. N.M.K Ramalingamsakthivelan[1], B. Ramya[2]

Associate Professor, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India[1]

M.E II[nd] Year, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India [2]

ABSTRACT: Due to their ever-increasing reliance on information and communications technologies, some of the most recent smart grid infrastructures, such as phasor measurement units (PMUs), are susceptible to cyberattacks. Sensing and communication networks' redundancy and/or security levels are the main focus of current cyberattack mitigation strategies. These solutions cost a lot of money because they require a lot of offline work. Additionally, when it comes to dealing with dynamic attacks, they are typically ineffective. A novel density-based spatial clustering strategy for online data recovery, classification, and detection of data manipulation attacks on PMU measurements is presented in this paper. The approach that has been proposed is based solely on data and can handle simultaneous multi-measurement attacks without requiring any additional hardware for the infrastructure that is already in place. Additionally, the proposed method does not depend on the conventional state estimation (SE). The proposed method's efficacy is demonstrated by extensive case studies.

KEYWORDS*:* PMU.DBSCAN, data mining, data manipulation, data recovery, and cybersecurity.

I. INTRODUCTION

Phasor measurement units (PMUs), for instance, are one example of SMART grid technologies that are rapidly being incorporated into power systems. These technologies, on the one hand, give life to the electricity grid by making the system more reliable, making it easier to control things faster, and making it easier to connect a lot of distributed energy resources (DERs). Power systems, on the other hand, are susceptible to cyberattacks because they are heavily dependent on information and communications technologies. At this time, the following six types of cyberattacks can be categorized in relation to PMU measurements: physical attack, denial-of-service attack, Man-in-the-Middle (MITM) attack, malicious code injection, data spoofing, and packet analysis Data spoofing and MITM both fall under the category of data integrity attacks. Telemetered data, which is also the primary concern of this paper, include power injections, line flows, voltage measurements from PMUs, and status information for breakers and switches. Telemetered data are also susceptible to such an attack.

PMUs send voltage and current phasors to control centers in a specified format after collecting them in real time across the electric power grid. Attacks on the transmission chain of data can occur at any point. Untrue measurements can have an impact on the normal operation of a control center and threaten the power grid's stability. At the moment, state estimation is one of the most important applications for identifying and rejecting bad data. However, if malicious attackers design stealthy attack vectors, it has been demonstrated that false data injection (FDI) attacks can be undetectable to state estimation. In general, the current cyberattack protections against PMU measurements can be divided into two groups.

The first method improves system observability by putting PMUs in the right places. Through data encryption or masking, the second type of approach raises the security levels of the communication network. In practice, these methods are expensive to put into practice because they require a lot of offline work. Additionally, power system topology and operating conditions are constantly shifting, and cyberattacks can be highly dynamic and unpredictable. These current methods are difficult to adapt to, and they are frequently restrictive and inadequate for dealing with dynamically evolving cyber threats in a changing system environment.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

Several sophisticated intrusion detection systems (IDSs) have been developed in recent years to combat evolving cyber threats. Due to their independence from existing bad data detection schemes, these solutions are more resistant to various types of data manipulation attacks. However, the majority of IDSs either require precise system configurations to be known beforehand or can only detect attacks without the ability to recover data, which can be crucial for power systems. An online anomaly detection algorithm that combines PMU data, generation schedules, and forecasted load is proposed by the authors. The efficacy of this strategy is heavily reliant on the precision of load forecasting, which is itself highly uncertain. Through the evaluation of transmission line equivalent impedances, the authors propose a method for attack detection. This method can identify the measurement under attack by detecting abnormal changes in transmission line (TL) parameters. However, multiple measurement channel attacks cannot be detected using this approach. Data tampering can be detected with the help of a protocol that makes use of a random time hopping sequence. However, there is no data recovery solution, and again, accurate system configuration must be known, which is difficult in practice. Attack solely driven by data

Although it has not been fully edited, this article has been accepted for publication in a future issue of this journal. Before it is published, the content may change. Smart Grid Transactions in Citation > CHANGE THIS LINE WITH YOUR PAPER IDENTIFICATION NUMBER (DOUBLE-CLICK HERE TO EDIT) Two detection mechanisms, for example, typically rely on historical attacking data for model training. Cross-validating other regional substations is how the authors of this paper detected the data integrity attack; however, these methods are ineffective against attacks that target multiple substations. In addition, work on data recovery is not being done because it is more important in attack scenarios where multiple measurements have been compromised.

Data manipulation attacks on the wide area monitoring system (WAMS) are identified and fixed using a novel data mining-based strategy that is presented in this paper. Density-based spatial clustering of applications with noise (DBSCAN), which has been shown to be very effective for PMU bias error correction, is the main algorithm proposed in this paper. This framework has made significant contributions, including:

- A sensitive attack detection mechanism that can detect attacks as small as one to four parts per trillion.
- A precise method for recovering corrupted PMU measurements from one or more channels.
- A robust and adaptable algorithm for changing and incorrect system configuration information.

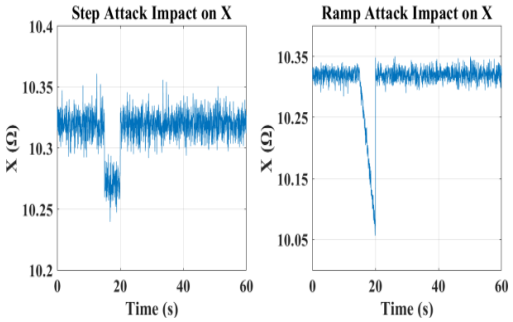
THREAT MODEL DESCRIPTION

PMUs output voltage and current phasors that are truly synchronized and accurate at critical power grid substations. Those estimations can be utilized by the nearby Autonomous Framework Administrator (ISO) to screen and control the framework recurrence changes, ongoing power stream and so on. By manipulating the current and voltage phasor measurements, an attacker can divert the system from an established (optimal) operational trajectory, which is appealing from an economic and security standpoint. Over the past few years, these kinds of attacks have received a lot of attention. The Economic Dispatch Problem (EDP) solution can be altered economically by manipulating PMU measurements. For instance, the manipulated EDP solution can schedule more generation from high-cost units, causing the existing electricity market mechanism to be maliciously destroyed. The resulting market shift may result in greater financial gains for the adversaries. The cost of crime is significantly less than the potential economic benefits because of the attacks' concealment. From a security standpoint, such attacks can cause the grid control/dispatch center to issue harmful commands by tampering with the measurement data of the power system and disrupting the normal dispatching operation of the power system. Along these lines, a digital fear based oppressor can straightforwardly compromise the power supply and, surprisingly, public safety. As a result, the attackers are sufficiently motivated to carry out such malicious attacks.

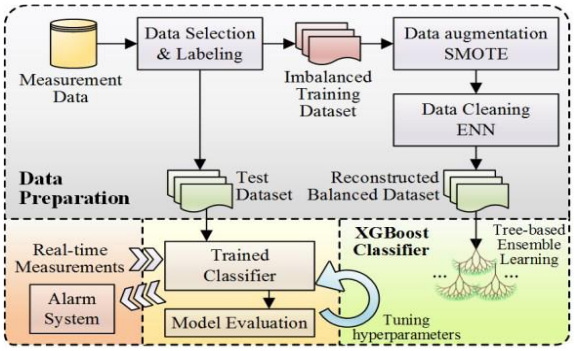
| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

CYBERATTACK FRAMEWORK



TRAINING AND TEST DATASETS



II. RELATED WORK

While the issue of detecting malicious changes in PMU data has received some recent attention, the detection of bad data in power systems has received significant research. The literature on the issue of detecting data manipulations in power systems is reviewed in this section. In order to identify large errors brought on by malfunctions in telemetry or sensors, conventional bad data detection methods typically make use of redundant measurement data to calculate measurement residuals. The 2-norm of the difference between the observed measurement vector and the estimated states is compared to a threshold in bad data detection techniques to identify bad measurements. Even though these conventional methods are quite effective against random measurement noises that interact with each other, they are unable to detect highly structured manipulated data that conforms to the network topology and some applicable physicallaws.

The first to demonstrate that an attacker armed with the current grid configuration information can successfully inject arbitrary errors into specific state variables without being detected by standard bad data processing methods are the authors of From the attacker's perspective, they presented a new category of attacks known as false data injection attacks and conducted analysis. The authors looked at false data injection attacks from an operator's perspective in order to determine how to defend against such attacks in the context of smart meters. Based on the findings of indices that quantify the least effort needed by attackers to achieve attack goals while avoiding bad data detection, these indices are related to the critical measurements without which observability is lost. In such attacks, highly-structured and coordinated data tampering can mislead the state estimation process without raising an alarm.

III. PROPOSED SYSTEM

An innovative method for online data recovery, classification, and detection of data manipulation attacks on PMU measurements using density-based spatial clustering. The approach that has been proposed is based solely on data and can handle simultaneous multi-measurement attacks without requiring any additional hardware for the

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

infrastructure that is already in place. Additionally, the proposed method does not depend on the conventional state estimation (SE). The proposed method's efficacy is demonstrated by extensive case studies.

ADVANTAGES

Compared to the typical one measurement every two to four seconds provided by conventional SCADA systems, PMUs offer up to 60 measurements per second. Because all PMU data is time-stamped using GPS data, PMUs have a big advantage over traditional methods of collecting data. The voltage and current phasors of the three-phase network can be measured by PMUs, which typically report between 30 and 60 samples per second. The system's frequency is reported at 30–60 samples per second and internally computed at a higher sampling rate.

IV. SYSTEM ARCHITECTURE

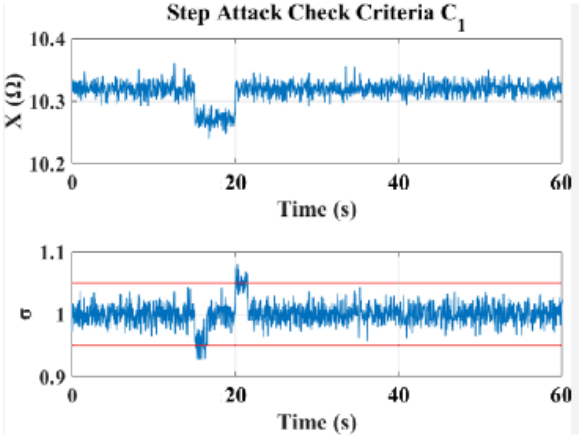


Fig.1.1 System Architecture

IMPLEMENTATION

The project's implementation Employment of information security analysts is projected to grow 35 percent from 2021 to 2031, much faster than the average for all occupations. About 19,500 openings for information security analysts are projected each year, on average, over the decade.

TESTING

The theoretical design becomes a working system during the project's implementation phase. This is the most common method for converting a new framework into a functional one, and it is the final and most important stage of the framework life cycle.

UNIT TESTING

Unit testing is a set of tests performed by a single programmer before a unit is integrated into a larger system. The module interface is put through tests to make sure that data enters and exits the program unit correctly. At each stage of an algorithm's execution, the local data structure is examined to guarantee that the temporarily stored data will remain the same. The module is tested under boundary conditions to guarantee that it works as intended within processing restrictions.

BLOCK BOX TESTING

Black-box testing is a method of software testing that examines an application's functionality without examining its internal workings or design. This approach makes it possible to test virtually every level of software testing.

V. CONCLUSION

A novel framework for the detection, identification, and data recovery of data integrity attacks on PMU measurements is presented in this paper. The approach that is being proposed has four major advantages over the other options: 1) capable of providing bad data recovery solutions that maintain the data consistency, 2) effective for simultaneous attacks on multiple channels, 3) sensitive and robust to small attacking signals, which are difficult to detect with

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 6, June 2023 |

existing bad data detection methods, and 4) independent of system topological changes and therefore adaptive and effective for changing system configurations.

REFERENCES

[1] C. Beasley, X. Zhong, J. Deng, etc., "A Survey of Electric Power Synchrophasor Network Cyber Security," 5th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Istanbul, Turkey, 2014.
[2] K. Chatterjee, V. Padmini and S. A. Khaparde, "Review of Cyber Attacks on Power System Operations," 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, 2017, pp. 1-6.
[3] A. Abur, and A. G. Exposito, Power System State Estimation: Theory and Implementation. CRC Press, 2004.
[4] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," ACM Transactions on Information and System Security, vol. 14, no. 1, Article 13, May 2011.
[5] J. Chen, and A. Abur, "Placement of PMUs to Enable Bad Data Detection in State Estimation," IEEE Trans. Power Syst., vol. 21, no. 4, pp. 1608–1615, Nov. 2006.
[6] G. B. Denegri, M. Invernizzi, and F. Milano, "A Security Oriented Approach to PMU Positioning for Advanced Monitoring of a Transmission Grid," Inter. Conf. Power System Technology, vol. 2, pp. 798-803, 2002.
[7] Q. Yang, D. An, etc., "On Optimal PMU Placement-based Defense against Data Integrity Attacks in Smart Grid," IEEE Trans. Information Forensics and Security, vol. 12, no. 7, July 2017.
[8] G. Dan, and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in Proc. IEEE Int. Conf. Smart Grid Commun., pp. 214–219, 2010.
[9] M. Jamei, E. Stewart, etc., "Micro Synchrophasor-based Intrusion Detection in Automated Distribution Systems: Toward Critical Infrastructure Security," IEEE Internet Computing, vol. 20, no. 5, pp. 18-27, Oct. 2016.
[10] A. Mazloomzadeh, O. A. Mohammed, and S. Zonouzsaman, "Empirical Development of a Trusted Sensing Base for Power System Infrastructures," IEEE Trans. Smart Grid, vol. 7, no. 5, Sep. 2015.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com