iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59222

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Machine Learning Methods for Attack Detection in Smart Grid

P. Sravanthi[1], Md. Moqeed[2], P. Shiva Charan[3], S. Neeraj Kumar[4]
[1]*Assistant Professor, Department of Computer Science, CMR College of Engineering and Technology (of Affiliation JNTUH) Medchal, Telangana, India*
[2, 3, 4]*Student, Department of Computer Science, CMR College of Engineering and Technology (of Affiliation JNTUH) Medchal, Telangana, India*

Abstract: ***In the realm of smart grids attack detection, statistical learning poses challenges across various attack scenarios, whether measurements are obtained either online or in batch mode. This approach categorizes measurements into two groups: secure and attacked, leveraging machine learning algorithms. The suggested method offers a framework for detecting attacks, aiming to address limitations arising from the sparse nature of the problem and leveraging any available past system knowledge. Through decision- and feature-level fusion, established batch and online learning methods are employed to tackle the attack detection challenge. To uncover unobservable attacks using statistical learning techniques, the relationships between the geometric and statistical characteristics of the attack vectors within the attack scenarios and the learning algorithms are scrutinized.***

Keywords: Sparse optimization, phase transition, smart grid security, attack detection, and categorization.

I. INTRODUCTION

Machine learning methods are utilized attracted considerable attention in the realm of smart grids, offering avenues for monitoring, managing power systems, and improving energy efficiency. We suggest a framework for intelligent system design that utilizes machine learning algorithms to predict component failures and enhance the management of load and energy sources in smart grid networks. Moreover, machine learning techniques have been studied for their potential to detect malicious activity and stop intrusions within a smart grid communication systems, especially at the network layer. This paper focuses on addressing the detection of false data injection attacks in the smart grid, specifically at the physical layer. Our approach adopts the distributed sparse attacks model, where False data is injected by intruders into local measurements observed by network operators or intelligent phasor measurement units within a hierarchical network structure characterized by clustered measurements. Network operators utilizing statistical learning algorithms for attack detection possess a thorough understanding of the network topology, measurements observed within clusters, and the measurement matrix. The system's state is first calculated from observable data in methods for detecting attacks that use state vector estimation (SVE). Then, if the difference between the estimated and observed measures is more than a pre-established threshold, a assault using data injection is identified. In sparse networks, however, when the Jacobian measurement matrix is sparse, precisely recovering state vectors presents difficulties Although strategies for sparse reconstruction can be useful with this problem, the sparsity of state vectors limits their usefulness. Furthermore, these false data injection attacks, also referred to as undetectable assaults, cannot be detected if the false data Vectors that have been injected are found within the column space of the Jacobian measurement matrix and meet certain sparsity requirements, such as having at most $\kappa*$ nonzero elements (limited by the size of the Jacobian matrix).

II. EXISTING SYSTEM

For a range of attack situations where measurements are recorded in either a batch or online environment attack detection issues in the smart grid are posed as statistical learning challenges. Machine learning methodologies are employed in this method to label readings as secure or attacked.

A. False Data Injection Attacks Against State Estimation in Electric Power Grids

A power grid is a complex network of interconnected power transmission and distribution systems that connects electric power providers and consumers over a large geographic area. System monitoring is essential to the dependability of the power grid, and state estimate is used in this process to examine power system models and meter readings and establish the power grid's condition as precisely as possible.

©IJRASET: All Rights are Reserved

Several methods have been established to detect and identify incorrect measurements, including the interaction of inaccurate measurements generated by arbitrary, nonrandom sources. Initially, it appears as though these techniques can also get over harmful safeguards that attackers have put in place. In this work, we present and examine a new class of attacks against current flawed measurement detection methods, dubbed false data injection attacks, uncovering a previously unknown weakness.

B. Merits, Demerits, and Challenges Merits

1) *Disruption of Operations:* By injecting false data into the state estimation process, attackers can manipulate the perceived state of the power grid, leading to incorrect decisions in grid operations.
2) *Stealthy Attacks:* Attacks using fake data injection can be challenging to identify, especially if the data injection is carefully crafted to resemble legitimate measurements.
3) *Potentially Widespread Impact:* Manipulating the state estimation process can have cascading effects on grid operations, potentially leading to widespread outages or other disruptions.
4) *Low Cost:* Attacks involving the injection of false data may not require sophisticated tools or resources, making them attractive to adversaries with limited capabilities.

C. Demerits and Challenges

1) *Trustworthiness of Data:* Attacks involving the injection of false data undermine the reliability of the data utilized in state estimation, potentially eroding confidence in the overall integrity of the power grid.
2) *Regulatory Concerns:* Incidents involving Attacks involving the injection of false data may trigger regulatory scrutiny and enforcement actions, leading to financial penalties and reputational damage for utilities and grid operators.

III. PROPOSED METHOD

Methods of machine learning have been proposed in various publications in the smart grid literature for monitoring and controlling power grids. Rudin et al. suggest an intelligent paradigm for machine learning-based system design
techniques to predict component failures. Anderson et al. use machine learning strategies for controlling loads and energy sources in smart grid networks. Machine learning methods have been investigated to detect intrusions and foresee malicious activity at the network layer of smart grid communication networks. We investigate the difficulty of identifying physical-layer assaults using false data injection on the smart grid in this work. Utilizing the distributed sparse attack model first presented in, we launch a network attack.

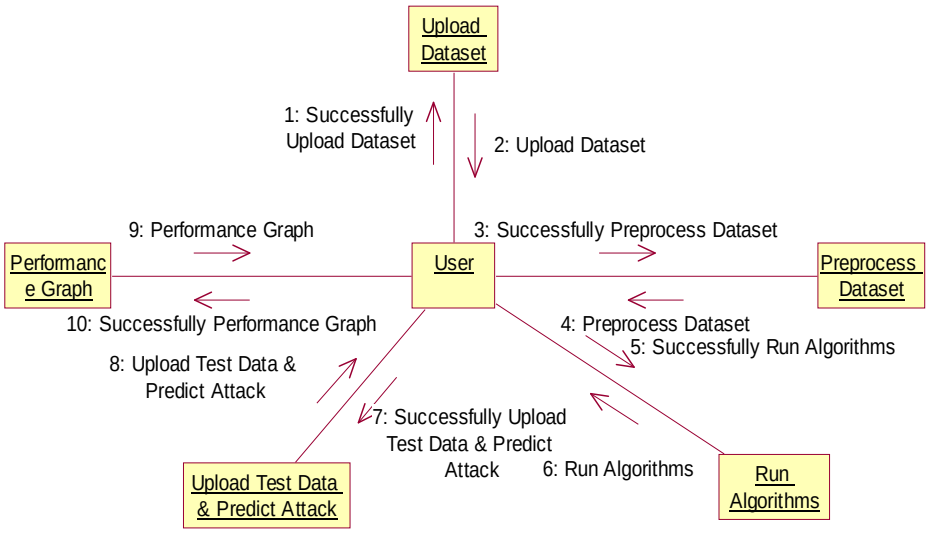
A. Advantages of Proposed System

1) High Accuracy
2) Quick response

B. Modules Information

The project encompasses the implementation of four distinct machine learning algorithms: Perceptron, KNN, SVM, and Logistic Regression. It's structured into the following modules:
Upload Dataset: This module enables users to upload the smart grid dataset to the application.
Preprocess Dataset: The dataset often contains missing values, null values, and non-numeric values. This module handles preprocessing tasks by replacing such values with 0. Additionally, it splits the dataset into training and testing sets, allocating 80% for educating the machine learning algorithms and reserving 20% for testing the prediction accuracy of these algorithms.
Run Algorithms: This module involves Each of the four algorithms for machine learning using the dataset prepared in the previous step. Following the phase of training, The performance of each algorithm is assessed using a variety of criteria, including Accuracy, Precision, Recall, and FSCORE.
Upload Test Data & Predict Attack: Users can upload test data through this module. Subsequently, the application predicts whether the test smart grid data is normal or contains an attack based on the trained algorithms.
Performance Graph:This module generates performance graphs, plotting the metrics obtained from each algorithm. These graphs offer a visual depiction of how well the various machine learning algorithms used in the project perform in comparison to one another.

IV. ARCHITECTURE



V. ALGORITHMS

A. K-Nearest Neighbours (K-NN)

1) The k-Nearest Neighbors (k-NN) algorithm operates by classifying a data point through a majority vote among its k nearest neighbors. Here's the mathematical operation involved:

2) Calculate the distance between each training sample and the query instance.

3) Identify the k-nearest Neighbors according to the computed distance.

4) Assign the class label by taking a majority vote among the k-nearest neighbors.

5) The formula to compute the distance between two locations (x1, y1) and (x2, y2) in Euclidean space is given as:

Formula

- Distance between two locations (x1, y1) and
- (x2,y2)Euclidean-space:

$$\sqrt{(x2 - x1)^2 + (y2 - y1)^2}$$

This formula computes the Euclidean distance between two locations in a two-dimensional space, facilitating the identification of nearest neighbors in the k-NN algorithm

B. Support Vector Machine (SVM)

1) Support Vector Machines (SVM) is a technique for supervised learning that determines the optimal hyperplane for classifying data points.

2) Mathematical operation:

3) SVM aims to identify the hyperplane with the maximum margin between the classes.

4) It transforms the data entered into a higher-dimensional space using kernel functions (e.g., linear, polynomial, Gaussian) to make the data linearly separable.

5) The optimization problem involves to identify the optimal separating hyperplane by maximizing the margin and minimizing classification errors.

Formula:

- Decision function: $f(x) = sign\left(\sum_{i=1}^{n} \propto_i y_i K(x_i, x) + b\right)$
- Margin : $\frac{2}{\|w\|}$
- Objective function: $\min_{w,b} \frac{1}{2}\|w\|^2$ **subject to** $yi(w^T x_i + b) \geq 1$

C. *Perceptron*

The perceptron is a simple binary classification algorithm that learns a linear decision boundary.

Mathematical operation

- To generate predictions, it adds up all of the input features and uses a step function.
- To reduce errors during training, weights are changed depending on samples that were incorrectly classified.

Formula

- Weighted Sum **:** $Z = \sum_{i=0}^{n} w_I x_i + b$
- Activation function(step function) : $\hat{y} = \begin{cases} 1 \ if \ z > 0 \\ 0 \ otherwise \end{cases}$
- Weight update rule: $w := w + \alpha(y - \hat{y})x$

D. *Logistic Regression*

Logistic regression models the probability that a given input belongs to a particular class.

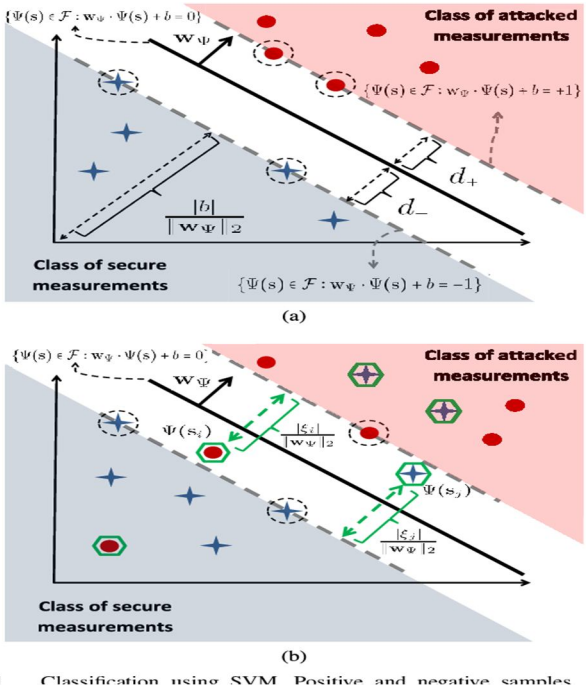
Mathematical operation:

- It applies the logistic function (sigmoid) to the linear combination of input features to produce a probability score.
- During training, parameters (weights) are calculated by utilizing the highest likelihood estimation or gradient descent to minimize the logistic loss function.

Formula:

- Logistic function : $\sigma(Z) = \frac{1}{1+e^{-z}}$
- Probability prediction: $\sigma(w^T x + b)$
- Logistic loss function**:** $J(w,b) = -\frac{1}{m}\sum_{i=1}^{m}[\, y(i) \ \ log(\hat{y}^{(i)}) + (1 - y^{(i)})\log(1 - \hat{y}^{(i)})\}$

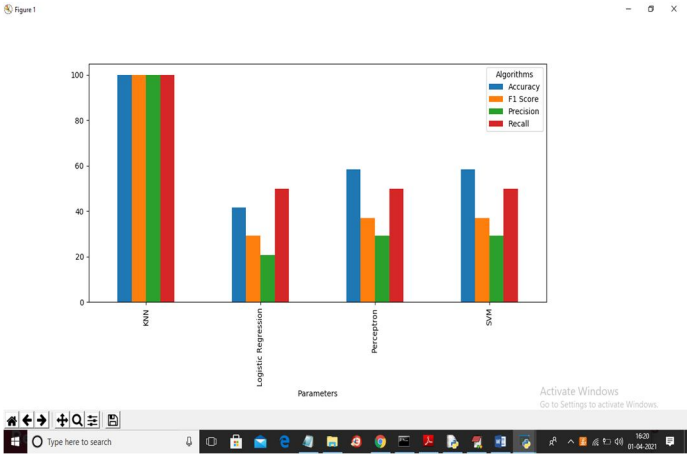
VI. RESULT



Fig(1) Workdown structure

This image illustrates Support Vector Machine (SVM) application for classifying measurements into two categories: "Secure" and "Attacked." In both scenarios depicted (a and b), there are distinct classes of data points: "Secure Measurements" represented by green solid circles, and "Attacked Measurements" represented by red dotted circles. The decision boundary, depicted by blue arrows, separates these two classes.

In Diagram (a), the separation between the classes is clear, and the equations in mathematics provide the criteria for classification. Conversely, Diagram (b) portrays a more intricate scenario where there is an overlap between the classes, suggesting a increased degree of classificational complexity. This overlap suggests that certain data points could be incorrectly classified or present a more difficult classification problem.



Fig(2) Percentage of algorithms

In the graph above, the x-axis represents the algorithm name, and the y-axis represents each algorithm's accuracy, precision, recall, and FSCORE. We can infer from this graph that KNN yields better outcomes.

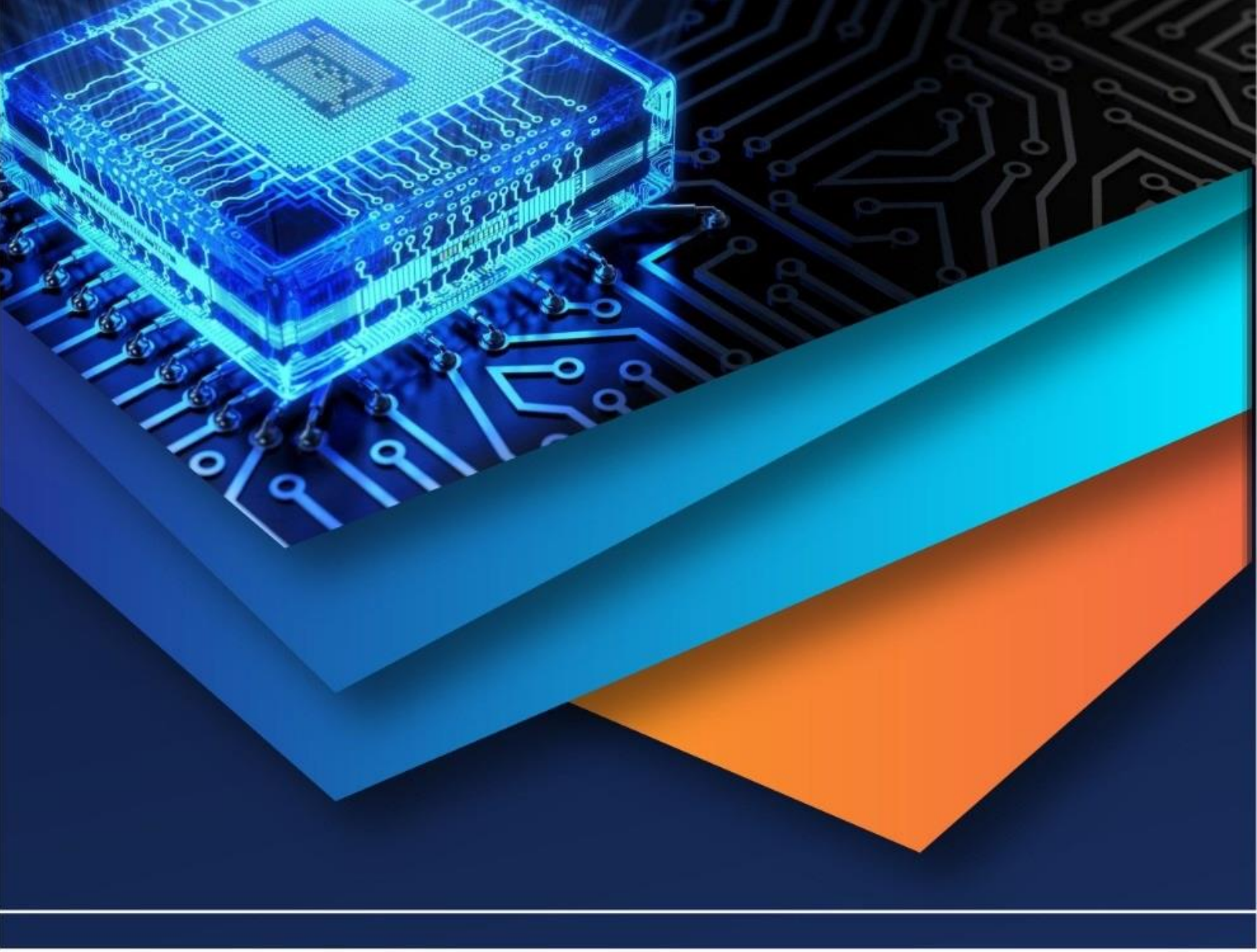
VII. CONCLUSION

This paper addresses the detection of bogus data injection attacks in smart grid systems as a machine learning task and assesses the performance of several algorithms under various attack scenarios. The assessment of online learning, classifier and feature fusion, supervised, semi-supervised, and other learning algorithms showed that the state-of-the-art machine learning algorithms outperform traditional detection methods. Notably, k-NN performs differently depending on the data imbalance and is more susceptible to system size than perceptron. With a phase transition seen at κ∗, which indicates the minimum available measurements for generating unobservable assaults, SVMs function well in large-scale systems. SVMs must contend with issues with kernel selection and system sparsity sensitivity. When it comes to data sparsity, semisupervised techniques outperform supervised learning. techniques for fusion, like Adaboost

REFERENCES

[1] C. Lin and Y. Lai, "A SVM-based Approach for Attack Detection in Smart Grid," 2015 worldwide gathering on Information Networking (ICOIN), Siem Reap, Cambodia, 2015, pp. 148-152.
[2] Reference: "An Approach Using Artificial Neural Networks for Anomaly Detection in Smart Grids," R. Lu, X. Lin, X. Liang, X. Shen, and X. Shen, 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, pp. 1-6.
[3] Hagras, "Real-time Cyber Attack identifing System for Smart Grids Using Random Forest," 2018 worldwide gathering on Industrial Informatics and Computer Systems (CIICS), Alexandria, Egypt, 2018, pp. 1-6.
[4] Reference: Y. Yuan, S. G. Ghiocel and A. M. Guran, "Convolutional Neural Network Based Cyber-Physical Attack Detection in Smart Grids," 2018 IEEE worldwide gathering on Communications, Control, and CN Technologies for Smart Grids , Aalborg, Denmark, 2018, pp. 1-6.
[5] Reference: T. Yu, Z. Zhou, L. Wu, J. Xiao and J. Lü, "A Decision Tree Approach for Detecting Cyber Attacks on Smart Grid Communication Networks," 2019 IEEE Innovative Smart Grid Computing Technologies Asia (ISGT Asia), 2019, pp. 918-922.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)