

SYNTHETIC DATA GENERATION FOR FALSE DATA INJECTION ATTACK DETECTION IN POWER SYSTEMS: A MACHINE LEARNING APPROACH

by

Krishna Vaibhav Yadlapalli

Submitted in partial fulfillment of the requirements
for the degree of Master of Applied Computer Science

at

Dalhousie University
Halifax, Nova Scotia
Dec 2024

© Copyright by Krishna Vaibhav Yadlapalli, 2024

Table of Contents

List of Tables	vi
List of Figures	vii
Abstract	x
Acknowledgements	xi
Chapter 1 Introduction	1
1.1 Motivation for Study	1
1.2 Problem Overview	2
1.3 Relevance of FDI Simulation in Power Systems	3
1.4 Major Contributions of the Research	3
1.5 Report Outline	4
Chapter 2 Background	6
2.1 Power Systems and State Estimation	6
2.1.1 Buses, Generators, and Loads	6
2.1.2 State Estimation in Power Systems	6
2.2 False Data Injection (FDI) Attacks	7
2.2.1 Definition and Classification of FDI Attacks	7
2.2.2 Impact of FDI on Power System Operations and Grid Stability . .	8
2.2.3 Examples of FDI Attack Scenarios	8
2.2.4 Challenges in Detecting FDI Attacks	9
2.3 Methods for Generating FDI Data	10
2.3.1 Overview of Methods Used to Generate FDI Data	10
2.3.2 Challenges in Detecting FDI Attacks	11
2.3.3 Overview of Methods Used to Generate FDI Data	11
2.3.4 Normal and FDI Datasets: IEEE 118-Bus System Resource	12
2.3.5 Challenges in Detecting FDI Attacks	12
2.4 Validation Techniques for Synthetic Dataset	13
2.4.1 Cistel Technology Tool for Validation	14
2.4.2 Pairplot Visualizations for Validation	15
2.4.3 Summary	15

2.5	Synthetic Data Generation	16
2.5.1	Synthetic Minority Oversampling Technique (SMOTE)	16
2.5.2	Random Matrix Theory (ROS)	16
2.5.3	Adaptive Synthetic Sampling (ADASYN)	16
2.6	Machine Learning Models	16
2.6.1	Random Forest	17
2.6.2	XGBoost	17
2.6.3	LightGBM	17
2.6.4	Multi-Output Regression (MOR)	17
2.7	Evaluation Metrics	18
2.7.1	Mean Squared Error (MSE)	18
2.7.2	Mean Absolute Error (MAE)	18
2.7.3	R-Squared Score (R^2)	18
Chapter 3	Literature Review	19
3.1	Overview of False Data Injection (FDI) Attacks	19
3.2	Stealth FDI Attacks	20
3.3	Machine Learning Approaches to FDI Generation	22
3.4	Data Augmentation for FDI Detection	24
3.5	Impact of FDI on State Estimation and Power System Operations	25
3.5.1	State Estimation and FDI Vulnerabilities	26
3.5.2	Operational Impact on Power Systems	26
3.5.3	Jacobian Matrix and FDI Impact	27
3.5.4	Cascading Effects on Grid Operations	27
3.6	Detection Techniques and Challenges	28
3.7	Summary of Literature Review	29
Chapter 4	Datasets Description	32
4.1	Introduction	32
4.2	Datasets Used	32
4.2.1	Oak Ridge National Laboratory (ORNL) Dataset	32
4.2.2	IEEE 118-Bus System Dataset	33
4.2.3	Voltage-Related Components	34
4.2.4	Real Power Components	34
4.2.5	Reactive Power Components	35

4.3	Operational Impact and Cascading Failures	35
4.4	Advanced Threat Scenarios	35
4.5	Detection Challenges	35
4.6	Conclusion	36
Chapter 5	Generation and Validation of Synthetic FDI Attack Vectors Using ORNL Dataset	37
5.1	Synthetic Data Generation Methods	37
5.1.1	Random Over Sampling (ROS)	37
5.1.2	Synthetic Minority Oversampling Technique (SMOTE)	38
5.1.3	SMOTE-ENN for Enhanced Synthetic Data Generation	38
5.1.4	Adaptive Synthetic Sampling (ADASYN)	39
5.2	Synthetic Data Generation Workflow	39
5.3	Results and Discussion	40
5.3.1	Validation using Similarity Metric	40
5.3.2	Comparison of SMOTE and SMOTE-ENN	42
5.4	Findings	43
Chapter 6	Generating Synthetic FDI Attack Data using Multioutput Regression (MOR)	44
6.1	Synthetic Data Generation	44
6.1.1	Selection of Independent and Dependent Variables	44
6.1.2	Steps for Generating Attack Data	45
6.1.3	Comparison of Regression Models and Pairplot Results	46
6.1.4	Creation of Dataset Variants	47
6.2	Results and Discussion	49
6.2.1	Validation of Model Performance	50
6.2.2	Feature Insights	51
6.2.3	Analysis of Dataset Variants	51
Chapter 7	Design of the FDI Simulation Tool	53
7.1	Overview of the FDI Simulation Tool	53
7.2	User Interface Design	53
7.3	Backend Implementation	54
7.4	Workflow	56

7.5	Integration of Modules	56
7.6	Conclusions with Findings	57
Chapter 8	Conclusions and Future work	58
8.1	Summary	58
8.2	Conclusion	59
8.3	Future Work	59
References	61
Appendix A	Code for Synthetic Data Generation and Similarity Analysis	64
A.1	<code>SMOTE_ENN.py</code> : Synthetic Data Generation with SMOTE-ENN	64
A.2	<code>SMOTE_ROS.py</code> : Synthetic Data Generation with SMOTE and ROS	65
A.3	<code>ADASYN.py</code> : Synthetic Data Generation with ADASYN	66
A.4	<code>compare.ipynb</code> : Similarity Analysis Between Original and Synthetic Data	66

List of Tables

2.1	Normal and FDI Datasets from the IEEE 118-Bus System Resource	12
3.1	Overview of Data Augmentation Techniques in FDI Detection . . .	25
3.2	Operational Impact of FDI on State Estimation and Power Systems [1], [2], [3], [4], [5], [6], [7], [8].	27
3.3	Summary of Key Literature on FDI Generation and Detection . . .	31
4.1	Key Features in the ORNL Dataset	33
4.2	Key Features in the IEEE 118-Bus System Dataset	33
5.1	Synthetic Data Generation Results	43
6.1	Model Performance Metrics	50

List of Figures

2.1	Graph of Similarity Score (SM) vs. Model Accuracy	15
5.1	Synthetic Data Generation Workflow	40
5.2	Pairplot of Multiple Columns Comparing Original and Synthetic Data	41
5.3	Single-Column Pairplot for R1-PA10:IH	41
5.4	Pairplot Comparison of SMOTE and SMOTE-ENN Synthetic Data	42
6.1	Flowchart of Synthetic FDI Attack Data Generation using MOR .	44
6.2	Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (Random Forest)	47
6.3	Pairplot of Normal vs. Attack Data for VGM Variables (Random Forest)	48
6.4	Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (XGBoost)	49
6.5	Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (LightGBM)	50
7.1	User Interface of the FDI Simulation Tool - Left Panel	55
7.2	User Interface of the FDI Simulation Tool - Right Panel	55

List of Abbreviations

ADASYN Adaptive Synthetic Sampling.

BDD Bad Data Detection.

CPU Central Processing Unit.

CSV Comma-Separated Values.

ENN Edited Nearest Neighbors.

FDI False Data Injection.

GAN Generative Adversarial Network.

HVAC High Voltage Alternating Current.

IEEE Institute of Electrical and Electronics Engineers.

LightGBM Light Gradient Boosting Machine.

MAE Mean Absolute Error.

ML Machine Learning.

MLP Multi-Layer Perceptron.

MOR Multioutput Regression.

MSE Mean Squared Error.

NDL Normalized Detection Level.

OPF Optimal Power Flow.

ORNL Oak Ridge National Laboratory.

PMU Phasor Measurement Unit.

R-Squared Coefficient of Determination.

RF Random Forest.

RMT Random Matrix Theory.

SCADA Supervisory Control and Data Acquisition.

SD State Estimation.

SMOTE Synthetic Minority Oversampling Technique.

TCSs Thyristor-Controlled Series Capacitors.

XGBoost Extreme Gradient Boosting.

Abstract

The digitalization of power systems has improved operational efficiency but has also exposed them to sophisticated cyber threats. False Data Injection (FDI) attacks, which manipulate state estimation data, pose significant risks, including cascading failures and compromised grid stability. Addressing the scarcity of labeled attack data, especially for rare events, remains a critical challenge in developing robust detection systems.

This research employs advanced methods, including RandomOverSampler (ROS), Synthetic Minority Oversampling Technique (SMOTE), SMOTE with Edited Nearest Neighbors (SMOTE-ENN), and Adaptive Synthetic Sampling (ADASYN), to generate synthetic FDI attack data. Using the Oak Ridge National Laboratory (ORNL) dataset, which contains both attack and normal data, synthetic attack samples were generated to mitigate data imbalance. ROS combined with SMOTE and SMOTE-ENN demonstrated superior performance in maintaining data fidelity and realism, while ADASYN addressed sparsely distributed data regions but yielded less effective results for high-quality attack data.

The IEEE 118-bus system dataset, initially containing only normal data, was enriched with simulated attack scenarios. Multi-Output Regression (MOR) models trained with Random Forest, XGBoost, and LightGBM were employed to perturb independent variables, such as generator voltages, to predict dependent variables like load voltages, thereby creating synthetic vector data aligned with real-world characteristics.

These methodologies were integrated into an interactive User Interface (UI) using Python's PyQt5 framework. The UI facilitates the generation of synthetic attack data, simulation of scenarios, and training of MOR models, offering a streamlined platform for researchers to generate datasets and validate machine learning-based detection frameworks.

By generating realistic synthetic datasets and integrating advanced methodologies into a comprehensive UI, this research significantly contributes to power system cybersecurity. It enables the development of robust detection models and strengthens the resilience of power systems against evolving cyber threats.

Acknowledgements

I would like to express my deepest gratitude to my professor, Dr.Srini Sampalli, for giving me the opportunity to work under his guidance. His invaluable support and encouragement have been instrumental in successfully completing this research.

I am also grateful to Dr. Marzia Zaman, an Industry Expert from Cistel Technology, for her valuable contributions and knowledge of machine learning, which significantly enhanced the quality of this research.

A special thanks to my co-supervisor, Dr.Darshana Upadhyay, for her constant support; her insights and guidance have been crucial throughout this journey.

Finally, I extend my heartfelt thanks to my parents. Their continuous support and belief in me have been my greatest strength.

Chapter 1

Introduction

1.1 Motivation for Study

The modern electric power grid is experiencing a profound transformation with the integration of advanced communication and information technologies, leading to the development of smart grids. While this integration enhances operational efficiency and allows for better resource management, it also exposes the power system to new cybersecurity threats [3]. Among these threats, False Data Injection (FDI) attacks have emerged as a significant concern due to their ability to stealthily compromise state estimation processes without being detected by conventional security measures [1].

FDI attacks can manipulate measurement data, leading to incorrect state estimation results that can cause erroneous control actions, equipment damage, and large-scale power outages [5]. The stealthy nature of these attacks makes them particularly dangerous, as they can bypass traditional Bad Data Detection (BDD) schemes and remain undetected until substantial harm is done [7]. The increasing sophistication of cyber-attack methodologies necessitates the development of advanced tools and techniques to understand, detect, and mitigate such threats.

Current research efforts have focused on developing detection algorithms and defense mechanisms against FDI attacks. Machine learning approaches, including the use of Generative Adversarial Networks (GANs), have shown promise in modeling and detecting these attacks [9]. However, there is a notable gap in accessible and flexible simulation tools that can generate realistic FDI attack scenarios for research and testing purposes [4]. Such tools are essential for evaluating the effectiveness of detection algorithms and for training machine learning models under various attack conditions.

The motivation for this study stems from the critical need to enhance the cybersecurity of power systems by providing a platform that can simulate realistic FDI attacks. By developing a simulation tool that can generate and inject false data into power system datasets, researchers and grid operators can better understand the vulnerabilities of state

estimation processes and develop more robust detection and mitigation strategies. This tool will contribute to improving the resilience of power systems against cyber-attacks, ensuring the reliability and stability of the electrical grid in the face of evolving threats.

1.2 Problem Overview

The power grid, being one of the most critical infrastructures in any nation, is a target for various types of cyber-attacks, including False Data Injection (FDI) attacks. FDI attacks are a sophisticated form of cyber-attack in which false data is injected into the power system's measurement data, misleading the state estimation process, which is crucial for maintaining grid stability and security [1]. Unlike traditional cyber-attacks that directly target hardware or software components, FDI attacks exploit the inherent vulnerabilities in the data processing algorithms used in power grid monitoring and control systems.

The state estimation process in power systems relies on measurement data from various points in the grid, such as bus voltages, power flows, and load demands [3]. By manipulating this data, attackers can cause incorrect state estimations, leading to erroneous control decisions, power imbalances, equipment damage, or even large-scale blackouts [7]. One of the key challenges in detecting FDI attacks is their stealthiness; they can be designed to evade conventional Bad Data Detection (BDD) mechanisms, making them extremely difficult to identify and mitigate in real-time [5].

Given the increasing complexity and interconnectivity of modern power grids, the potential for large-scale, coordinated FDI attacks is becoming a critical concern for grid operators and cybersecurity experts. This highlights the urgent need for advanced tools and techniques to simulate, detect, and mitigate FDI attacks. Current solutions are limited in their ability to simulate realistic attack scenarios, especially for testing and evaluating machine learning-based detection algorithms [9]. This gap in research and technology underscores the importance of developing a flexible and scalable simulation tool capable of generating FDI attacks under various conditions and testing them against state estimation algorithms.

1.3 Relevance of FDI Simulation in Power Systems

Simulating FDI attacks in power systems is crucial for understanding their impact and developing robust detection and mitigation strategies. The modern power grid is becoming increasingly vulnerable to cyber-attacks as it incorporates more digital and communication technologies. FDI attacks, in particular, exploit the data processing layer of power systems, making them difficult to detect using traditional cybersecurity measures [7].

By simulating FDI attacks, researchers can analyze how these attacks affect the accuracy of state estimation, the stability of the grid, and the control decisions made by operators. Simulation tools are essential for generating datasets that can be used to train machine learning algorithms to detect and respond to FDI attacks. Additionally, simulation allows for the testing of various detection and mitigation strategies under controlled conditions, providing insights into their strengths and weaknesses [5].

The development of a flexible simulation tool that can generate realistic FDI attacks will enable power system operators and researchers to better prepare for potential cyber-attacks. It will also facilitate the development of more effective detection mechanisms, ensuring the resilience and security of the grid. This research is particularly relevant as it contributes to the ongoing efforts to secure critical infrastructure from evolving cyber threats, including stealth and sparse FDI attacks [9].

1.4 Major Contributions of the Research

The primary contribution of this research is the development of a simulation tool designed to generate realistic False Data Injection (FDI) attacks for power systems, specifically targeting the state estimation process. The key contributions are outlined as follows:

- We develop a simulation tool capable of generating a variety of FDI attack scenarios by manipulating normal grid operation data, including bus voltages, power flows, and generator outputs.
- We provide a platform for testing and evaluating the effectiveness of machine learning-based FDI detection algorithms by generating realistic and customizable attack datasets.

- We analyze the impact of FDI attacks on state estimation accuracy, grid stability, and control decisions, focusing on different types of stealth and sparse attack scenarios [4].
- We contribute to the body of knowledge on power system cybersecurity by exploring innovative methods for generating, simulating, and mitigating FDI attacks. This includes leveraging advanced machine learning models, such as Random Forest Regression and Multioutput Regression [9].

These contributions aim to enhance the understanding of how FDI attacks compromise power system operations and provide practical tools for mitigating their effects. The simulation tool is designed with flexibility and scalability, enabling users to input diverse power system datasets and customize attack parameters to simulate realistic and complex scenarios.

1.5 Report Outline

This thesis is organized into ten chapters, each addressing key aspects of the research objectives and contributions:

Chapter 1: Introduction Provides an overview of False Data Injection (FDI) attacks in power systems. It discusses the motivation for the study, outlines the objectives, and highlights the significance of FDI simulation in ensuring power grid security. The chapter also identifies research gaps in FDI simulation and defines the contributions of this project.

Chapter 2: Background Covers the foundational concepts of power systems, including state estimation and its critical role in grid reliability. It introduces False Data Injection attacks, discussing their classification, impact, and the challenges associated with their detection. It also explores various methods for generating FDI data and highlights validation techniques for assessing synthetic datasets.

Chapter 3: Literature Review Presents a comprehensive analysis of existing research on FDI generation and detection. It evaluates machine learning methods, such as GANs and Random Matrix Theory, for simulating attacks and highlights data augmentation techniques like SMOTE and ADASYN. The review also examines the impact of FDI on state estimation and operational decisions in power grids.

Chapter 4: Dataset Description Describes the datasets used in the project, including the Oak Ridge National Laboratory (ORNL) and IEEE 118-Bus System datasets. It explains the features of normal and FDI datasets, focusing on key components like voltage, real power, and reactive power. The chapter also addresses challenges in validating synthetic datasets.

Chapter 5: Methodology for Generating and Validating Synthetic FDI Data Details the methodologies employed for generating synthetic FDI data using approaches like Random Over Sampling (ROS), SMOTE, and SMOTE-ENN. It includes a comparison of synthetic data generation techniques, validation methods, and the effectiveness of similarity metrics in assessing data quality.

Chapter 6: Generating Synthetic FDI Data using Multioutput Regression (MOR) Introduces a novel framework for generating attack vectors based on Multioutput Regression. It describes the selection of variables, the MOR process, and the evaluation of model performance. The chapter includes insights into the effectiveness of MOR in generating realistic FDI scenarios.

Chapter 7: Design of the FDI Simulation Tool Outlines the architecture and implementation of the simulation tool, which is developed using Python and the Pencil framework. It describes user input options, dataset integration, and the step-by-step process for generating attack scenarios. The chapter also discusses the tool's modular design and its integration with machine learning models.

Chapter 8: Summary and Conclusion Summarizes the research findings and contributions, emphasizing the importance of the FDI simulation tool in advancing grid security. It provides recommendations for future enhancements and outlines potential research directions for mitigating FDI attacks.

Chapter 9: Appendices Includes supplementary materials such as code snippets, detailed methodologies, and additional visualizations to support the research findings.

Chapter 2

Background

2.1 Power Systems and State Estimation

Power systems are complex infrastructures that consist of various interconnected components such as buses, generators, transformers, loads, and transmission lines. These elements work together to ensure that electricity is generated, transmitted, and distributed efficiently to meet consumer demands. The operational stability of power systems relies on monitoring the state of the system, which includes determining the voltages at buses, the power flows through transmission lines, and the loads on the system [2].

2.1.1 Buses, Generators, and Loads

A bus in a power system refers to a node where one or more components, such as generators, transformers, and loads, are connected. Buses act as key points for measuring the electrical properties like voltage magnitude and phase angle. Generators at different buses supply electrical power, while loads represent the demand or consumption of electricity. The balance between power generation and load demand is crucial for ensuring stable grid operations. Any imbalance may lead to voltage instabilities or even system-wide blackouts [3].

2.1.2 State Estimation in Power Systems

State estimation is a critical function in the operation of power systems, as it provides a real-time snapshot of the grid's operational state. It involves collecting measurement data from sensors, such as Phasor Measurement Units (PMUs) and Supervisory Control and Data Acquisition (SCADA) systems, to estimate the voltage magnitudes and phase angles at various buses. These estimations enable grid operators to make informed decisions, ensuring grid reliability and preventing potential faults [5]. Accurate state estimation is essential because the control and optimization of power flow, load balancing, and fault detection heavily depend on the precise knowledge of the system's current state.

However, state estimation is vulnerable to data manipulation attacks such as False Data Injection (FDI) attacks, where attackers inject manipulated data into the measurement readings to disrupt grid operations. Detecting these attacks is crucial for maintaining the integrity and security of power systems [1].

2.2 False Data Injection (FDI) Attacks

2.2.1 Definition and Classification of FDI Attacks

False Data Injection (FDI) attacks are a type of cyber-attack that target the measurement data used in power system state estimation. In these attacks, an adversary injects manipulated data into the system with the goal of disrupting the state estimation process and potentially causing incorrect operational decisions. These attacks are particularly dangerous because they can be crafted to bypass conventional Bad Data Detection (BDD) mechanisms, making them difficult to detect in real-time operations [1].

FDI attacks can be classified into two main categories:

- **Stealth FDI Attacks:** These attacks are designed to evade detection by traditional BDD systems. The attacker strategically manipulates measurement data such that the errors introduced do not trigger any alarms, making the attack "stealthy" and difficult to detect. Research by Liu et al. [1] highlighted how such stealth attacks can bypass state estimation without being flagged by BDD mechanisms.
- **Sparse FDI Attacks:** Sparse attacks involve manipulating only a small subset of measurement data to reduce the risk of detection. By altering a limited number of data points, the attacker can still cause significant disruption to power system operations, but with a reduced chance of triggering alarms. Research by Wei et al. [5] and Narang et al. [2] has demonstrated how sparse attacks can be optimized to remain undetected while causing maximum disruption.

Both types of attacks represent significant threats to modern power systems, as they can lead to incorrect decision-making by grid operators, potentially destabilizing the grid. The ability of attackers to carefully craft FDI attacks to evade traditional detection mechanisms has led to an increased focus on the development of more advanced detection and prevention strategies.

2.2.2 Impact of FDI on Power System Operations and Grid Stability

FDI attacks pose a significant threat to the operation and stability of power systems. By injecting false data into the state estimation process, attackers can cause the system to operate under incorrect assumptions, leading to potentially catastrophic consequences. These attacks can manipulate critical state variables such as bus voltages, power flows, and generator outputs, leading to incorrect operational decisions and instability in the grid.

The impact of these attacks can be categorized as follows:

- **Operational Disruptions:** FDI attacks can cause the state estimation process to report incorrect bus voltages and power flows, leading to operational mismanagement. Grid operators may be unaware of the attack and could incorrectly dispatch generators, overload transmission lines, or initiate unnecessary load shedding, resulting in cascading failures [3].
- **Economic Losses:** FDI attacks can disrupt the optimal power flow (OPF) process, which is used to minimize operational costs while maintaining grid stability. By manipulating the data used for OPF, attackers can force the grid to operate in a suboptimal state, leading to increased operational costs. Fioretto et al. [10] demonstrated how FDI attacks could be used to disrupt the OPF process, resulting in significant economic losses for power utilities.
- **Grid Instability and Blackouts:** In extreme cases, FDI attacks can lead to widespread grid instability and even blackouts. By altering key measurements related to generator outputs and transmission line flows, attackers can cause cascading failures, where the initial disruption spreads throughout the system, potentially leading to a large-scale blackout [9].

2.2.3 Examples of FDI Attack Scenarios

Several studies have provided real-world and simulated examples of FDI attacks to illustrate their potential impact on power systems. The IEEE 118-Bus System has been widely used in these studies to simulate the effects of FDI attacks. In research conducted by Shohan et al. [9], generative models were employed to create synthetic FDI attack

data that closely mimics real-world measurement data. This work highlights how machine learning techniques, such as Generative Adversarial Networks (GANs), can be used to generate stealthy FDI attacks, making detection even more challenging.

Another prominent example is the use of optimization techniques to generate sparse FDI attacks. Wei et al. [5] showed how sparse attack points can be optimized to minimize detection while still causing significant operational disruptions. Similarly, Narang et al. [2] explored how attackers could manipulate the state estimation process with minimal network information, further demonstrating the stealthy nature of these attacks.

The multi-objective optimization approach, as explored by Li et al. [4], investigates how attackers can balance between stealthiness and impact. Their work on optimizing FDI attacks in smart grids revealed that attackers can tailor their strategies to maximize disruption while minimizing the likelihood of detection.

2.2.4 Challenges in Detecting FDI Attacks

One of the primary challenges in detecting FDI attacks is their ability to evade traditional detection mechanisms, such as BDD systems. These attacks are carefully crafted to ensure that the residuals calculated during state estimation remain within the normal range, making them appear as legitimate data to grid operators [1].

Another challenge lies in the detection of sparse FDI attacks. Sparse attacks are designed to manipulate only a small subset of the data, making them difficult to detect using traditional anomaly detection methods. Sparse attack vectors can be optimized to minimize their impact on the overall system while still causing significant operational disruptions [5].

In addition, machine learning models used for detecting FDI attacks face the challenge of adaptability. As attackers evolve their strategies, pre-trained models may become ineffective, requiring continuous retraining and updating to stay ahead of new attack techniques [9]. Developing robust real-time detection systems that can adapt to evolving attack patterns remains a critical area of research.

2.3 Methods for Generating FDI Data

2.3.1 Overview of Methods Used to Generate FDI Data

The generation of False Data Injection (FDI) data is a complex process that requires a deep understanding of both the power system's state estimation mechanisms and the techniques used by attackers to manipulate measurement data. Broadly, there are three main approaches to generating FDI data: 1) Mathematical Modeling, 2) Simulation-Based Approaches, and 3) Machine Learning Models.

Mathematical Modeling approaches involve manipulating the power system's measurement data using predefined attack vectors. These attack vectors are calculated based on the power system's Jacobian matrix, which maps the relationship between the measurements and the system state variables. By altering the measurement values using these attack vectors, an attacker can generate false data that disrupts the state estimation process without triggering Bad Data Detection (BDD) mechanisms [1]. This method is frequently used in research to simulate stealth FDI attacks that evade detection [2].

Simulation-Based Approaches use specialized simulation tools, such as MATPOWER or PSS/E, to simulate real-world power system operations under attack conditions. These tools allow researchers to simulate various attack scenarios by injecting manipulated data into the power flow equations or state estimation algorithms. Such simulations help in understanding the impact of FDI attacks on the power grid's stability, reliability, and control mechanisms [3].

Machine Learning Models are increasingly being used to generate FDI data. Techniques such as Generative Adversarial Networks (GANs) have been applied to create synthetic FDI attack data that closely resembles real-world measurement data. GANs can learn the patterns of legitimate grid data and then generate false data that mimics these patterns, making detection even more challenging. These models are particularly effective in creating stealth attacks, where the injected data is indistinguishable from legitimate data [9]. Additionally, other machine learning techniques, such as Random Over Sampling (ROS) and ADASYN, are used for augmenting and generating datasets that contain both normal and anomalous events, facilitating the training of detection models [5].

2.3.2 Challenges in Detecting FDI Attacks

Detecting FDI attacks presents several challenges due to the sophisticated nature of these attacks and their ability to bypass traditional detection mechanisms like Bad Data Detection (BDD) systems.

Stealthiness of the Attacks: One of the primary challenges is the stealthiness of well-crafted FDI attacks. By carefully selecting the attack vectors, an attacker can inject malicious data into the system without triggering any alarms. The stealthiness is achieved by ensuring that the residuals calculated during the state estimation process to detect errors remain within the acceptable range [2]. This makes it incredibly difficult for grid operators to differentiate between legitimate and manipulated data [1].

Sparse Attacks: Another challenge lies in detecting sparse FDI attacks, where only a few data points are manipulated. These attacks are designed to have minimal impact on the overall system, making them harder to detect while still causing significant operational disruptions [5]. Traditional detection methods that rely on anomaly detection techniques often fail to identify sparse attacks due to the limited number of manipulated data points.

Lack of Real-Time Detection Mechanisms: Many power grids rely on batch processing of data for state estimation and anomaly detection, which delays the detection of FDI attacks. The lack of real-time monitoring tools for identifying suspicious changes in the grid's state makes it difficult to respond to FDI attacks before they cause damage [4]. Real-time detection methods, such as machine learning-based systems, are still under development, and their deployment is not widespread in modern power grids.

Adaptability of Machine Learning Models: While machine learning models have shown promise in detecting FDI attacks, they face challenges in adapting to new types of attacks that were not present in the training data. Attackers can modify their strategies, rendering pre-trained models ineffective. This adaptability gap highlights the need for continuous retraining and updating of detection models to stay ahead of evolving attack strategies [9].

2.3.3 Overview of Methods Used to Generate FDI Data

The generation of False Data Injection (FDI) data is a complex process that requires a deep understanding of both the power system's state estimation mechanisms and the techniques used by attackers to manipulate measurement data. Broadly, there are three

main approaches to generating FDI data: 1) Mathematical Modeling, 2) Simulation-Based Approaches, and 3) Machine Learning Models.

One of the primary resources used in this research is the IEEE 118-Bus System Dataset, which provides a comprehensive view of power grid operations under normal conditions. This dataset has been extended with the generation of FDI attack data through simulation methods, offering both normal and manipulated datasets for analysis.

2.3.4 Normal and FDI Datasets: IEEE 118-Bus System Resource

The IEEE 118-Bus System Dataset is commonly used in power system research for simulating grid operations. In this project, the normal dataset provided by this resource is augmented by generating synthetic FDI attacks through mathematical modeling and simulation. The FDI dataset is created by injecting false data into key state variables such as bus voltages, power flows, and generator outputs, which are crucial for the state estimation process.

Below is a summary of the normal and FDI datasets provided by the resource:

Table 2.1: Normal and FDI Datasets from the IEEE 118-Bus System Resource

Dataset	Key Features	Description
Normal Dataset	Bus Voltages (V), Power Flows (P, Q), Generator Outputs	Contains normal operational data for the IEEE 118-Bus system.
FDI Dataset	Manipulated Bus Voltages, Power Flows, Generator Outputs	Generated via simulation by injecting false data into the normal dataset.

The normal dataset provides the baseline operational data, which is then used to generate the FDI dataset by introducing anomalies in the form of false data. This process is crucial for testing the effectiveness of detection algorithms and assessing the resilience of power grids against FDI attacks [11].

2.3.5 Challenges in Detecting FDI Attacks

Detecting FDI attacks presents several challenges due to the sophisticated nature of these attacks and their ability to bypass traditional detection mechanisms like Bad Data

Detection (BDD) systems.

Stealthiness of the Attacks: One of the primary challenges is the stealthiness of well-crafted FDI attacks. By carefully selecting the attack vectors, an attacker can inject malicious data into the system without triggering any alarms. The stealthiness is achieved by ensuring that the residuals calculated during the state estimation process to detect errors remain within the acceptable range [2]. This makes it incredibly difficult for grid operators to differentiate between legitimate and manipulated data [1].

Sparse Attacks: Another challenge lies in detecting sparse FDI attacks, where only a few data points are manipulated. These attacks are designed to have minimal impact on the overall system, making them harder to detect while still causing significant operational disruptions [5]. Traditional detection methods that rely on anomaly detection techniques often fail to identify sparse attacks due to the limited number of manipulated data points.

Lack of Real-Time Detection Mechanisms: Many power grids rely on batch processing of data for state estimation and anomaly detection, which delays the detection of FDI attacks. The lack of real-time monitoring tools for identifying suspicious changes in the grid's state makes it difficult to respond to FDI attacks before they cause damage [4]. Real-time detection methods, such as machine learning-based systems, are still under development, and their deployment is not widespread in modern power grids.

Adaptability of Machine Learning Models: While machine learning models have shown promise in detecting FDI attacks, they face challenges in adapting to new types of attacks that were not present in the training data. Attackers can modify their strategies, rendering pre-trained models ineffective. This adaptability gap highlights the need for continuous retraining and updating of detection models to stay ahead of evolving attack strategies [9].

2.4 Validation Techniques for Synthetic Dataset

This chapter describes the validation techniques used to assess the synthetic dataset generated by our proposed similarity score modeling and machine learning (ML) methods. This work utilizes an in-house tool developed by Cistel Technology Inc., ensuring proprietary techniques are employed for dataset evaluation. The main objective is to evaluate

how closely the synthetic data resembles real-world data, ensuring its reliability for practical applications. The goal is to confirm that the synthetic dataset accurately captures the essential patterns and distributions found in the real data, making it suitable for data-driven applications in power systems.

2.4.1 Cistel Technology Tool for Validation

The similarity score modeling and validation process heavily rely on the proprietary in-house tool developed by Cistel Technology Inc. This tool implements advanced techniques to compare real and synthetic datasets, employing machine learning methods such as Random Forest classification. The tool generates a similarity metric that quantifies how closely the synthetic dataset aligns with the real dataset, ensuring its suitability for practical applications. By integrating state-of-the-art methodologies, the tool serves as a robust framework for validating synthetic datasets in power systems.

The similarity score modeling involves creating a combined dataset of real and synthetic data, where real records are labeled as 0 and synthetic records as 1. The combined dataset is then used to train a classification model to evaluate its performance in distinguishing between the two data sources. An accuracy close to 50% indicates high similarity, as the model struggles to differentiate between real and synthetic data.

Similarity Metric (SM)

The Similarity Metric (SM) measures how closely the synthetic data matches the real data. The metric is calculated as follows:

- **If the model's accuracy is 50% or lower**, the similarity score (SM) is set to 1.
- **If the model's accuracy is higher than 50%**, the similarity score (SM) is calculated as:

$$SM = 2 \times (1 - \text{accuracy}) \quad (2.1)$$

The SM is essentially a piecewise function of accuracy, and a graph of this relationship is shown in Figure 2.1.

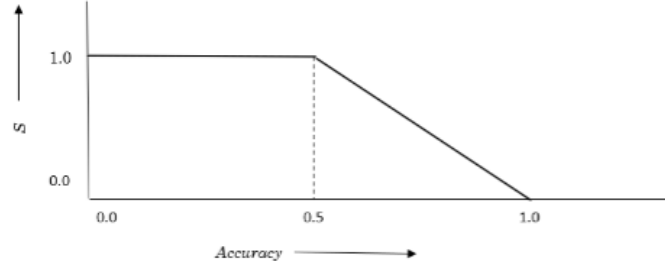


Figure 2.1: Graph of Similarity Score (SM) vs. Model Accuracy

2.4.2 Pairplot Visualizations for Validation

In addition to the similarity score modeling, we employed pairplot visualizations generated using the Seaborn library [12]. Pairplots are an effective graphical tool for comparing pairwise relationships between variables in a dataset. They combine scatter plots and histograms, allowing a comprehensive view of how the features align across real and synthetic datasets.

In our project, pairplots were used to assess the similarity of distributions and trends between the two datasets. These visualizations provided a direct comparison, helping to identify any significant discrepancies between real and synthetic data. Features such as R1-PA1:VH, R1-PA2:VH, and R1-PM1:V were analyzed, and the pairplots demonstrated strong alignment between real and synthetic data. This graphical validation supports the conclusion that the synthetic dataset effectively captures the patterns of the original data.

By integrating Seaborn-generated pairplots into our validation process, we enhanced the reliability of the synthetic dataset, ensuring its readiness for practical applications in power systems.

2.4.3 Summary

This chapter introduced the validation techniques for assessing the quality of synthetic datasets. The in-house tool developed by Cistel Technology Inc. provided a robust similarity score modeling framework, while Seaborn-generated pairplots [12] offered additional graphical validation. Together, these methods ensured that the synthetic dataset closely resembled the real data, making it suitable for data-driven applications in power systems and other domains.

2.5 Synthetic Data Generation

Synthetic data generation techniques address data imbalance and enhance dataset quality. This section explores methods such as SMOTE, ROS, and ADASYN, commonly used for generating realistic synthetic data in machine learning.

2.5.1 Synthetic Minority Oversampling Technique (SMOTE)

SMOTE generates synthetic samples by interpolating between existing minority class instances and their nearest neighbors:

$$x_{\text{new}} = x_{\text{minority}} + \delta \cdot (x_{\text{nearest}} - x_{\text{minority}}) \quad (2.2)$$

where x_{new} is the synthetic sample, x_{minority} is an original minority instance, x_{nearest} is a selected nearest neighbor, and $\delta \sim U(0, 1)$. This method enhances class balance and improves model performance in imbalanced datasets [13].

2.5.2 Random Matrix Theory (ROS)

ROS identifies anomalies by analyzing eigenvalues of the covariance matrix of the data. Eigenvalues outside the normal range, defined by the Marchenko-Pastur law, signify anomalies:

$$\lambda_{\min} = \sigma^2(1 - \sqrt{q})^2, \quad \lambda_{\max} = \sigma^2(1 + \sqrt{q})^2 \quad (2.3)$$

where σ^2 is the variance and $q = \frac{n}{p}$ is the aspect ratio of the matrix dimensions [14].

2.5.3 Adaptive Synthetic Sampling (ADASYN)

ADASYN improves upon SMOTE by generating synthetic samples based on the difficulty of classification:

$$G_i = G \cdot \frac{\Delta_i}{\sum_j \Delta_j} \quad (2.4)$$

where G is the total number of synthetic samples, and Δ_i represents the classification difficulty for instance i . ADASYN enhances sensitivity to hard-to-classify instances [15].

2.6 Machine Learning Models

Machine learning models, including Random Forest, XGBoost, LightGBM, and Multi-Output Regression (MOR), are integral to analyzing and generating synthetic data.

2.6.1 Random Forest

Random Forest is an ensemble learning method that constructs multiple decision trees and aggregates their outputs:

$$f(x) = \frac{1}{N} \sum_{i=1}^N T_i(x) \quad (2.5)$$

where $f(x)$ is the final prediction, N is the number of trees, and $T_i(x)$ represents the i -th tree. Random Forest is robust to overfitting and performs well on complex, non-linear data [16].

2.6.2 XGBoost

XGBoost improves gradient boosting by incorporating regularization and efficient computation:

$$\mathcal{L} = \sum_{i=1}^n \ell(y_i, \hat{y}_i) + \sum_{k=1}^K \Omega(f_k), \quad \Omega(f_k) = \frac{\lambda}{2} \|w_k\|^2 \quad (2.6)$$

where ℓ is the loss function, and $\Omega(f_k)$ is the regularization term. XGBoost is highly scalable and effective for large datasets [17].

2.6.3 LightGBM

LightGBM uses a leaf-wise growth strategy to improve efficiency:

$$\text{Loss Reduction} = \frac{1}{2} \left(\frac{G^2}{H + \lambda} - \frac{(G_1 + G_2)^2}{H_1 + H_2 + \lambda} \right) \quad (2.7)$$

where G and H are gradient and Hessian terms, and λ is a regularization parameter. It excels in handling large-scale datasets [18].

2.6.4 Multi-Output Regression (MOR)

MOR predicts multiple dependent variables using a unified model:

$$Y = f(X) + \epsilon \quad (2.8)$$

where Y is the vector of dependent variables, X is the vector of independent variables, f is the model function, and ϵ represents the error term. MOR is effective for tasks requiring simultaneous predictions across related outputs [19].

2.7 Evaluation Metrics

To evaluate the performance of machine learning models, we employed the following metrics:

2.7.1 Mean Squared Error (MSE)

MSE measures the average squared difference between predicted and actual values:

$$\text{MSE} = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2 \quad (2.9)$$

where y_i is the actual value, \hat{y}_i is the predicted value, and n is the number of observations. A lower MSE indicates better predictive accuracy [20].

2.7.2 Mean Absolute Error (MAE)

MAE calculates the average absolute difference between predicted and actual values:

$$\text{MAE} = \frac{1}{n} \sum_{i=1}^n |y_i - \hat{y}_i| \quad (2.10)$$

MAE provides an interpretable measure of prediction error in the same units as the data [20].

2.7.3 R-Squared Score (R^2)

The R^2 score evaluates the proportion of variance explained by the model:

$$R^2 = 1 - \frac{\sum_{i=1}^n (y_i - \hat{y}_i)^2}{\sum_{i=1}^n (y_i - \bar{y})^2} \quad (2.11)$$

where \bar{y} is the mean of actual values. R^2 ranges from 0 to 1, with higher values indicating better model fit [20].

Chapter 3

Literature Review

3.1 Overview of False Data Injection (FDI) Attacks

False Data Injection (FDI) attacks have become a significant concern for modern power systems, especially as the reliance on automated state estimation continues to grow. These attacks target the data collected and processed by the state estimation algorithms used to monitor and control power grids, leading to misleading information being fed into the system. As a result, the power grid can make erroneous operational decisions, affecting grid stability, reliability, and security.

FDI attacks are unique because they bypass traditional security mechanisms. Rather than directly tampering with physical infrastructure, attackers inject falsified data into the system's measurement streams, altering the grid's understanding of its operational state. The seminal work by [1] laid the foundation for understanding how such attacks exploit vulnerabilities in the state estimation process, demonstrating that an attacker could introduce arbitrary errors without being detected by conventional bad data detection mechanisms.

In addition to altering state estimation, these attacks can have far-reaching consequences on grid operations. As noted by [8], FDI attacks can lead to inefficient power flows, increased operational costs, and in some extreme cases, even blackouts. Such disruptions make detecting and mitigating FDI attacks crucial for maintaining grid reliability.

Moreover, FDI attacks are challenging to detect because they can be designed to appear indistinguishable from normal system measurements. This makes traditional monitoring and anomaly detection techniques less effective in identifying the subtle changes caused by the attack, as highlighted in [2]. These attacks exploit weaknesses in measurement redundancy and the structure of the power grid, requiring advanced techniques for detection and mitigation.

The growing prevalence of smart grid technologies has increased the potential attack

surface for FDI. With more interconnected devices and automated systems collecting and processing data, the opportunities for attackers to exploit vulnerabilities have expanded. This has sparked significant research into better understanding the nature of FDI attacks and developing strategies to counteract them. Researchers, such as [3], have emphasized the need for more robust data integrity solutions that can both detect and mitigate these attacks in real time.

Overall, understanding FDI attacks is essential for designing more secure and resilient power systems. By studying how attackers manipulate data, researchers and engineers can develop more effective defense mechanisms, ensuring the continued reliability of our power infrastructure.

3.2 Stealth FDI Attacks

Stealth False Data Injection (FDI) attacks represent a sophisticated category of attacks that remain undetected by conventional monitoring systems in power grids. These attacks target the underlying state estimation algorithms, which are responsible for ensuring the grid's operational accuracy. The key characteristic of stealth FDI attacks is their ability to manipulate data while evading detection by bypassing bad data detection mechanisms that rely on statistical anomalies.

The foundational study by Liu et al. (2009) introduced the concept of stealth FDI attacks, demonstrating that such attacks could be constructed to bypass bad data detection (BDD) methods used in state estimation processes [1]. Their work showed that by carefully selecting the attack vector based on the system's Jacobian matrix, an attacker could inject erroneous data that appears statistically normal, thereby eluding detection systems. This research highlighted the importance of securing the state estimation process, as stealth FDI attacks can induce serious errors in power grid operation without being flagged by traditional security measures.

Further analysis of stealth FDI attacks was conducted by Narang and Bag (2019), who proposed a method for launching stealth attacks with minimal network information. Their approach reduced the amount of information needed by attackers, making it feasible to launch FDI attacks even with limited access to the power system's configuration [2]. This work emphasizes that attackers no longer need comprehensive knowledge of the system, as partial information is sufficient to execute successful stealth FDI attacks. This finding

broadens the potential attack surface and increases the risk to power systems.

In addition, Wei et al. (2020) explored sparse stealth FDI attacks, where the attack vectors are strategically chosen to affect only a small number of measurement points, further reducing the chances of detection [5]. These sparse attacks demonstrate that it is possible to achieve significant disruption with minimal resource expenditure, making them an attractive option for attackers. Sparse attacks are particularly challenging to detect, as they involve minimal data manipulation, leaving fewer traces for monitoring systems to pick up on.

The effectiveness of stealth FDI attacks lies in their ability to blend into normal system operations, altering state estimates without introducing observable irregularities. The work of Li et al. (2021) examined multi-objective optimization strategies for stealth FDI attacks, where attackers optimize their attack vectors to achieve both stealth and operational impact [4]. Their study showed that stealth attacks could be optimized to cause significant damage to grid operations, such as overloading transmission lines or disrupting power flow, while remaining undetected by traditional monitoring systems.

Researchers have proposed several techniques for defending against stealth FDI attacks, but the inherent complexity of the attacks makes them difficult to counter. The use of advanced machine learning models, as explored by Shohan et al. (2021), offers some promise in detecting and mitigating stealth FDI attacks [9]. By analyzing patterns in system data, machine learning models can potentially identify subtle deviations caused by stealth attacks, although these models must be trained on large, representative datasets to be effective.

In conclusion, stealth FDI attacks pose a significant threat to the reliability and security of power systems. By exploiting weaknesses in the state estimation process, attackers can introduce malicious data without raising alarms, causing potentially catastrophic consequences for grid operations. The challenge of detecting these attacks underscores the need for more advanced security measures and monitoring techniques to ensure the continued resilience of power grids.

3.3 Machine Learning Approaches to FDI Generation

In recent years, the application of machine learning (ML) techniques to False Data Injection (FDI) attack generation has gained significant traction. Machine learning provides the capability to model complex patterns and learn from large datasets, which makes it highly suited for simulating and generating sophisticated FDI attack vectors. These approaches aim to exploit the inherent vulnerabilities of power systems by using data-driven methods to generate realistic, yet malicious, data that bypasses traditional detection methods.

A prominent approach for FDI generation is the use of Generative Adversarial Networks (GANs), a type of machine learning model where two neural networks, a generator and a discriminator, are trained in opposition to each other. The generator's role is to create synthetic data, such as falsified state estimation values, while the discriminator's role is to differentiate between the real data and the generated (fake) data. Over time, the generator improves its ability to create data that is indistinguishable from the real data. This method was employed by Shohan et al. (2021) in the iAttackGen model, where GANs were used to generate realistic FDI attack vectors in a power grid context [9]. This approach is particularly useful because it automates the generation of attack vectors, which can adapt to various scenarios in real time.

Supervised learning is another method often employed in FDI generation, where the machine learning model is trained on a labeled dataset. In this case, the dataset includes examples of both normal and malicious data. The model learns to classify data points as either normal or injected (malicious) based on predefined features. These features may include voltage readings, power flows, and other state estimation variables that are critical to power system operations. Once the model is trained, it can be used to simulate FDI attacks by manipulating specific features to generate new data points that mimic realistic attack scenarios. As demonstrated by Chen et al. (2021), this method is highly effective for detecting and generating data that mirrors real-world attacks [3]. By applying feature manipulation, researchers can generate diverse attack scenarios that can be used to train detection models.

Another significant machine learning approach used for FDI generation is reinforcement learning (RL). In RL, an agent interacts with the power grid environment and learns a strategy, or policy, to maximize its reward over time. In the context of FDI, the

reward function is designed to reflect the success of the attack in terms of its ability to disrupt the system or evade detection. The agent iteratively learns from its actions by receiving feedback from the environment, adjusting its strategy to achieve better results. For instance, an FDI attack could be modeled as a sequential decision-making problem where the attacker incrementally injects false data and learns which modifications to make in order to maximize impact while remaining undetected. Studies like that of Wei et al. (2020) show that RL can be an effective tool for optimizing stealthy FDI attacks, particularly in scenarios where attackers have limited knowledge of the grid’s structure [5].

In addition to supervised and reinforcement learning, unsupervised learning techniques like clustering have also been explored. Clustering algorithms, such as k-means or hierarchical clustering, group similar data points together based on their features. In the context of FDI generation, unsupervised learning can be used to identify patterns in historical grid data and generate attack vectors that mimic the normal behavior of these clusters. This approach is particularly useful in cases where labeled data is not available, as it does not rely on pre-classified examples of attacks. Instead, the algorithm learns the underlying structure of the data and generates new data points that fit within these learned patterns.

Another promising avenue is the use of deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which are well-suited for handling sequential and high-dimensional data. CNNs are typically used for tasks involving grid data that can be represented spatially, while RNNs, particularly their variants like Long Short-Term Memory (LSTM) networks, are excellent for capturing temporal dependencies in sequential data such as power system measurements over time. Li et al. (2021) demonstrated how deep learning models could be trained to predict optimal attack vectors by learning from historical grid data [4]. By simulating past attacks and training the model on this data, they were able to generate new attack vectors that targeted vulnerabilities in the system’s state estimation process.

The integration of machine learning techniques into FDI generation opens up new possibilities for simulating more realistic and adaptive attack scenarios. These models, especially when coupled with optimization techniques, allow for the creation of attack vectors that are not only effective but also harder to detect. However, a significant

challenge remains: machine learning models require large, high-quality datasets to train effectively. This is particularly true for deep learning models, which are data-hungry and need extensive training data to capture subtle patterns in the grid's operation.

In conclusion, machine learning approaches to FDI generation represent a powerful toolset for attackers. By leveraging advanced models like GANs, reinforcement learning, and deep learning, attackers can craft sophisticated and adaptive attack strategies that pose serious threats to power systems. As these techniques continue to evolve, so too must the defensive mechanisms designed to detect and mitigate them. 4

3.4 Data Augmentation for FDI Detection

Data augmentation techniques are essential in generating large datasets to train machine learning models for the detection of False Data Injection (FDI) attacks. Given the stealthy nature of FDI, which often blends seamlessly into normal power system operations, traditional datasets often lack the diversity needed to train robust detection models. In this section, we discuss how various data augmentation techniques, including Random Matrix Theory (RMT), SMOTE (Synthetic Minority Over-sampling Technique), and ADASYN, have been employed in existing research to improve FDI detection.

[3] introduced a method based on RMT for FDI detection by generating synthetic datasets that mimic the normal and attack scenarios in power system behavior. This method not only increases dataset diversity but also enhances the robustness of detection models by exposing them to a wider range of potential anomalies.

On the other hand, [5] and [8] explored the use of data augmentation techniques like SMOTE and ADASYN to address class imbalances in datasets. FDI attack instances are typically far fewer than normal operations, leading to skewed datasets that hinder the performance of machine learning models. SMOTE and ADASYN create synthetic attack data, ensuring that models are better trained to recognize FDI scenarios, even in heavily imbalanced datasets.

[8] further demonstrated how synthetic data generation for FDI attack detection can enhance machine learning-based detection models' performance. By simulating a wide range of attack vectors, the datasets generated through these augmentation techniques provide a comprehensive training environment for algorithms aimed at real-time FDI detection.

Table 3.1: Overview of Data Augmentation Techniques in FDI Detection

Technique	Description	Application in FDI Detection	Key Findings
RMT	Generates synthetic data using random matrix theory	Used to expand dataset diversity for machine learning models	Enhanced detection performance due to diverse data [3]
SMOTE	Oversamples minority class (attack data)	Balances class distribution in imbalanced datasets	Improved model performance in detecting rare attack instances [5, 8]
ADASYN	Adaptive synthetic sampling technique	Focuses on generating synthetic examples for underrepresented attack cases	Enhanced model training for harder-to-classify cases [8]

In addition to these techniques, [8] proposed a method for analyzing vulnerabilities and assessing the consequences of FDI attacks on power systems. Their work introduced synthetic augmentation techniques that allow for detailed simulation of attack scenarios, thereby enhancing the dataset and providing a better training ground for machine learning-based detection systems.

As a result, augmentation techniques such as ROS, SMOTE, and ADASYN help address the scarcity of real-world FDI attack data and significantly enhance the accuracy and robustness of machine learning models in identifying sophisticated FDI attacks.

3.5 Impact of FDI on State Estimation and Power System Operations

False Data Injection (FDI) attacks critically threaten the stability of power systems by directly impacting state estimation, a fundamental process for grid monitoring and control. State estimation algorithms aggregate sensor data from across the grid to compute voltage levels, power flows, and load demand estimates, enabling grid operators to make informed operational decisions. However, when FDI attacks corrupt this data, state estimation becomes inaccurate, leading to incorrect control actions and system instabilities [8, 5, 6].

3.5.1 State Estimation and FDI Vulnerabilities

As [8] explains, FDI attacks deliberately target the measurement data fed into state estimation algorithms. This data, collected from smart meters, phasor measurement units (PMUs), and remote terminal units (RTUs), is crucial for ensuring that the grid operates within safe parameters. However, attackers can manipulate this data to mislead the state estimation process, injecting false information about grid conditions that may result in improper responses, such as incorrect dispatch of generation units or erroneous load shedding commands.

FDI attacks that bypass traditional Bad Data Detection (BDD) mechanisms have proven particularly problematic. [6] describes how attackers craft stealthy FDI vectors that fall within the system's tolerance thresholds, preventing BDD filters from flagging the altered data as anomalous. Consequently, system operators remain unaware of the compromised state, allowing the attacker to execute prolonged or repeated attacks without detection.

3.5.2 Operational Impact on Power Systems

FDI attacks have a profound impact on the operational efficiency and reliability of power systems. As demonstrated in [4], the consequences of FDI attacks can include:

- **Misdirection of generation resources:** Inaccurate state estimates cause the system to dispatch generation units inefficiently, leading to increased operational costs and suboptimal power flow.
- **Grid instability:** By distorting key parameters such as voltage levels and load demands, FDI attacks can lead to power oscillations, voltage collapse, and in extreme cases, blackouts.
- **Increased wear on equipment:** Constant operation under incorrect assumptions increases the mechanical and thermal stress on grid components, reducing their operational lifespan.

A notable example of the operational effects of FDI attacks is illustrated in the following table, summarizing key performance metrics before and after an FDI attack:

Table 3.2: Operational Impact of FDI on State Estimation and Power Systems [1], [2], [3], [4], [5], [6], [7], [8].

Metric	Normal Operation	Under FDI Attack
Voltage Deviation (p.u.)	± 0.01	± 0.15
Generation Dispatch Error (%)	1 – 2%	10 – 12%
Load Mismatch (MW)	≤ 5 MW	≥ 50 MW
Operational Cost (USD/hour)	1000	5000
System Frequency Deviation (Hz)	± 0.005	± 0.05

3.5.3 Jacobian Matrix and FDI Impact

One of the most significant ways FDI attacks affect state estimation is by manipulating the Jacobian matrix used in the estimation process. The Jacobian matrix relates system states (such as voltages and angles) to the measurements, such as active and reactive power flows. By injecting false data into key measurements, attackers effectively alter the structure of this matrix, leading to incorrect power flow calculations and misinformed operational decisions [2, 3, 6].

3.5.4 Cascading Effects on Grid Operations

FDI attacks not only disrupt state estimation but also initiate cascading failures across the grid. By continuously feeding erroneous data into control systems, attackers can destabilize grid voltage levels, leading to protective relays being triggered unnecessarily, causing widespread outages or equipment damage. The work by [21] highlights that descriptor system models can capture the cascading nature of these failures, modeling the long-term consequences of FDI attacks in both centralized and decentralized grid architectures.

In conclusion, FDI attacks pose a grave threat to the accuracy of state estimation and overall power system operations. Their ability to bypass detection mechanisms and induce operational inefficiencies makes them particularly dangerous for modern smart grids, requiring advanced detection and mitigation techniques to ensure grid security and reliability.

3.6 Detection Techniques and Challenges

Detecting False Data Injection (FDI) attacks presents several challenges, particularly as these attacks evolve in sophistication and stealth. Traditional methods such as Bad Data Detection (BDD) algorithms have been widely implemented in power systems to identify anomalies in state estimation data. However, as [6] and [8] point out, FDI attacks can often bypass these detection mechanisms by injecting carefully crafted false data that remains within the expected statistical range, avoiding detection flags.

One of the primary challenges in detecting FDI attacks lies in their stealthy nature. As discussed in [22], machine learning-based approaches have emerged as a promising technique for detecting FDI, particularly deep learning frameworks. These approaches can be trained on historical and real-time data to identify patterns of anomalies caused by FDI attacks. However, the implementation of such techniques comes with its own challenges, such as the need for large datasets and the potential for high computational overhead, which may hinder real-time detection in critical systems.

Additionally, [7] demonstrates that attackers can exploit historical data with limited information to mount FDI attacks, further complicating detection efforts. The use of historical data allows attackers to predict the system's normal behavior and inject false data that closely mimics the expected measurements, making it difficult for conventional detection systems to distinguish between normal and malicious data.

A significant challenge highlighted by [22] and [23] is the integration of defense mechanisms that can both detect and mitigate the effects of FDI attacks. While machine learning models provide promising results, their deployment in live power systems requires robust real-time processing capabilities. Furthermore, the development of hybrid detection models that combine hardware-based protections, such as those discussed by [23], with advanced data-driven methods is necessary to enhance system resilience.

Lastly, [21] discusses the potential for descriptor system frameworks to provide a more formal and mathematical approach to detecting and mitigating FDI attacks. These frameworks rely on modeling the system's dynamic behavior to identify deviations caused by malicious data injections. However, the complexity of implementing such systems in real-world power grids remains a challenge due to the variability in grid architecture and operational conditions.

In summary, detecting FDI attacks requires a comprehensive approach that combines

traditional detection methods with advanced machine learning models, real-time processing, and hardware-based defenses. As FDI attacks become more sophisticated, detection mechanisms must also evolve, adapting to increasingly stealthy and complex threats.

3.7 Summary of Literature Review

The literature review provided a comprehensive analysis of various aspects of False Data Injection (FDI) attacks in power systems. The key findings from the 13 papers highlight the growing sophistication of FDI attacks and the critical need for advanced detection mechanisms and mitigation strategies.

FDI attacks pose a significant threat to state estimation, as demonstrated by [1] and [2]. These attacks manipulate sensor data used by state estimation algorithms, leading to incorrect operational decisions that can compromise grid stability and security. Stealth FDI attacks, which bypass traditional Bad Data Detection (BDD) systems, have been identified as particularly dangerous, allowing attackers to remain undetected for extended periods while compromising system reliability.

The review of machine learning approaches shows that Generative Adversarial Networks (GANs) and other deep learning models are being effectively employed to generate FDI attack vectors. The work by [9] and [3] demonstrates how these models can synthesize realistic attack scenarios, making it difficult for conventional detection systems to identify malicious activity. In addition, the use of data augmentation techniques, such as ADASYN, as shown in [3], improves the accuracy of machine learning models in detecting attacks.

Sparse FDI attacks, as explored in [5], involve injecting minimal but strategic data manipulations, causing large-scale disruptions without being easily detectable. These sparse attacks leverage optimization techniques to maximize their impact while minimizing the risk of detection. Additionally, studies such as [4] and [6] highlight the cascading operational effects of FDI attacks, including increased operational costs, incorrect generator dispatch, and load imbalances that lead to voltage collapses and grid instabilities.

A critical finding across multiple papers is the vulnerability of the Jacobian matrix used in state estimation to FDI attacks. By modifying key measurements, attackers can disrupt the structure of the Jacobian matrix, leading to incorrect power flow calculations and decisions. The impact of these attacks on state estimation is particularly significant,

as highlighted by [8] and [21].

In conclusion, this literature review reveals that FDI attacks are an evolving threat that requires innovative detection methods and robust grid management strategies. The integration of machine learning with traditional grid operations will be essential in mitigating the risks posed by FDI attacks and ensuring the security of modern power systems. However, one of the main challenges in addressing FDI attacks is the lack of real-world attack data and a comprehensive understanding of how these attacks manifest in power systems. To effectively develop intrusion detection methods, generating realistic FDI attack data is crucial. This gap is the central focus of our current work, where we aim to create a robust dataset that captures a variety of FDI attack scenarios, facilitating the development of more accurate detection systems and contributing to the overall security of power grids.

Table 3.3: Summary of Key Literature on FDI Generation and Detection

Paper Details (Title, Author(s), Year)	FDI Generation Technique	How to Generate FDI Data	Key Technical Details	Key Advantages	Challenges	Relevance to FDI Tool	Dataset Details	Algorithm Used	Data Input Requirements	Novel Contributions
False Data Injection Attacks against State Estimation in Electric Power Grids, Yao Liu, Peng Ning, Michael K. Reiter, 2009 [1]	Stealth FDI Attacks	Manipulate state variables (voltage, phase angles) to create undetectable FDI data.	Requires grid topology knowledge and linear models.	Simple to integrate.	Requires detailed system topology knowledge.	Foundational method for creating FDI data.	Voltage, Phase Angles	Linear estimation methods	Voltage, phase angles, power flows	Key foundational approach for FDI simulation
A Stealth False Data Attack on State Estimation with Minimal Network Information, Narang, Jagendra Kumar, Baidyanath Bag, 2019 [2]	GAN-based FDI	Use GANs to generate attack vectors without full network knowledge.	Trains DCGAN for stealthy FDI data generation.	Limited network information required.	Complex GAN training process.	Useful for stealth attacks.	No dataset used in this paper	GAN (Deep Convolutional GAN)	Real-time measurements	Stealth FDI attack with GAN
A Data Preparation Method for Machine-Learning-Based Power System Cyber-Attack Detection, Chen, Hongyu et al., 2021[3]	ML Data Augmentation	Augment normal data with rare FDI attack scenarios.	Uses Random Over Sampling (ROS) and ADASYN for data preparation.	Enhances detection for rare scenarios.	Requires large datasets for training.	Useful for training ML models for FDI.	IEEE 118-Bus System	ROS and ADASYN	Historical data, system measurements	Augmentation improves rare attack detection
Defense of Massive False Data Injection Attack via Sparse Attack Points, L. Wei et al., 2020 [5]	Sparse FDI Optimization	Generate FDI by targeting sparse attack points in the system.	Uses sparse optimization to create efficient FDI data.	Optimizes attack points for minimal intrusion.	Limited real-world applicability.	Useful for sparse FDI in large grids.	Synthetic dataset	Sparse Attack Optimization	Grid topology, system constraints	Sparse FDI simulation
iAttackGen: Generative Synthesis of False Data Injection Attacks, Md. Shohan et al., 2020 [9]	Generative FDI Models	Automate FDI data generation using generative models.	Employs generative models for FDI data creation.	Automates FDI generation process.	Requires deep learning expertise.	Useful for automating FDI in tools.	No dataset provided	GAN (Generative Adversarial Network)	GAN training data	Generative approach for real-time simulations
Multi-Objective Optimization on Stealthy FDI in Smart Power Transmission, Z. Li et al., 2021[4]	Multi-Objective FDI Optimization	Optimize FDI for stealth and impact.	Uses multi-objective optimization methods.	Highly flexible attacks.	Complex optimization process.	Useful for optimizing FDI attacks in grid.	IEEE 118-Bus Dataset	Multi-objective optimization methods	System parameters, constraints	Multi-objective optimization
Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation, J. Liang et al., 2016[8]	Stealth FDI Attack	Analyze vulnerabilities in state estimation for FDI.	Examines weaknesses in state estimation techniques.	Provides insights into power system vulnerabilities.	Focus on vulnerabilities with less focus on countermeasures.	Valuable for identifying FDI weaknesses.	IEEE 118-Bus Dataset	State Estimation Analysis	Voltage, state estimation variables	Vulnerability assessment in state estimation
A Deep Learning Framework to Identify Remedial Action Schemes Against False Data Injection Cyberattacks, Naderi, Ehsan and Arash Asrari, 2024[22]	Deep Learning-Based	Identifies schemes to counter FDI.	Uses deep learning to identify attack points.	Advances in detecting attacks.	Requires complex ML models.	Relevant for ML-based FDI detection.	Simulated dataset	Deep learning models	Power system data	Framework for detecting attack schemes
A Descriptor System Design Framework for FDI Attack Toward Power Systems, Aibing Qiu et al., 2021[21]	Descriptor-Based FDI	System design framework for generating FDI	Uses descriptor models for attack detection	High precision in attack detection	Descriptor systems are complex to train	Important for understanding FDI system impacts	Simulated data	Descriptor system model	Grid data, real-time measurements	System design framework for FDI
Can Attackers With Limited Information Exploit Historical Data to Mount Successful FDI Attacks?, Zhang2018, Jiazi et al., 2018[7]	Historical Data Exploitation	Uses historical data to simulate FDI	Employs methods to exploit historical information	Effective for simulating stealth attacks	Limited to available historical data	High relevance for FDI tools	IEEE 118-Bus dataset	Historical data analysis	Historical grid data	Attack simulations with limited information
Designing False Data Injection Attacks Penetrating AC-Based Bad Data Detection, Minh N. Tran et al., 2020[6]	AC-Based FDI	Design FDI attacks that bypass AC-based detection.	Uses AC-based techniques to generate attack data.	Effective at bypassing AC detection.	Requires AC system information.	Important for designing resilient FDI tools.	Synthetic dataset	AC-based simulation	AC system data	Focus on bypassing AC detection systems
Multi-Objective False Data Injection Attacks of Cyber-Physical Power Systems, Kang-Di Lu and Zheng-Guang Wu, 2022[24]	Multi-Objective FDI	Multi-objective optimization	Uses optimization to improve attack stealth	Complex optimization requirements	Highly relevant for generating stealthy attacks	Simulated dataset	Multi-objective optimization methods	Power system parameters	Multi-objective attack optimization	Power Grid Cybersecurity
A Remedial Action Scheme Against FDI Cyberattacks in Smart Transmission Systems, Ehsan Naderi et al., 2022[23]	Remedial Action Schemes	Identifies action schemes against FDI	Uses thyristor-controlled series capacitors (TCSCs) to counter FDI	High resilience to attack	Requires advanced knowledge of TCSCs	Useful for designing defense mechanisms	Synthetic dataset	Remedial action framework	Power system parameters	TCSC-based defense mechanisms

Chapter 4

Datasets Description

4.1 Introduction

Power systems rely on accurate measurements and state estimation to ensure reliable and economic operation. False Data Injection (FDI) attacks target the integrity of these measurements by injecting maliciously crafted data, leading to severe operational disruptions. This chapter explores the datasets used in this research and provides insights into the power system components most susceptible to FDI attacks.

4.2 Datasets Used

To conduct this research, two primary datasets were utilized: the Oak Ridge National Laboratory (ORNL) dataset and the IEEE 118-Bus System dataset. These datasets provided the foundation for generating and analyzing FDI attack scenarios.

4.2.1 Oak Ridge National Laboratory (ORNL) Dataset

The ORNL dataset [25] contains 37 power system event scenarios divided into three categories: natural events, no events, and attack events. Key features of the dataset include:

- Natural events, such as single-line-to-ground faults and line maintenance scenarios.
- No-event scenarios representing normal grid operation.
- Attack events, including remote tripping command injection, relay setting changes, and data injection to simulate faults.

The dataset is highly comprehensive, encompassing 128 features measured by Phasor Measurement Units (PMUs), control panel logs, Snort alerts, and relay logs. These features enable detailed simulation and analysis of FDI attacks on power systems.

Table 4.1: Key Features in the ORNL Dataset

Feature	Description
PA1:VH – PA3:VH	Phase A-C Voltage Phase Angle
PM1:V – PM3:V	Phase A-C Voltage Magnitude
PA4:IH – PA6:IH	Phase A-C Current Phase Angle
PM4:I – PM6:I	Phase A-C Current Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
S	Status Flag for relays

This dataset includes scenarios such as short-circuit faults, line maintenance events, and various types of attack events, allowing for comprehensive evaluation of FDI attacks.

4.2.2 IEEE 118-Bus System Dataset

The IEEE 118-Bus System dataset [11] is a standard resource widely used in power system research. It includes data on:

- 118 bus nodes, detailing voltage levels and angles.
- Power flow data, including line capacities and losses.
- Generator outputs, specifying real and reactive power.
- Load demands, including real and reactive components.

For this research, synthetic FDI attack scenarios were generated by altering key state variables such as bus voltages and power flows. This augmented dataset served as the basis for testing detection algorithms and evaluating grid vulnerabilities.

Table 4.2: Key Features in the IEEE 118-Bus System Dataset

Feature	Description
Bus Voltage	Voltage magnitude at each bus
Bus Angle	Voltage angle at each bus
Real Power Generation	Real power produced by generators
Reactive Power Generation	Reactive power produced by generators
Real Power Load	Real power consumed by loads
Reactive Power Load	Reactive power consumed by loads
Line Flow	Power flow on transmission lines
Line Loss	Power losses on transmission lines

The IEEE 118-Bus System dataset provides a detailed representation of a large-scale power grid, enabling analysis of various operational scenarios and the impact of FDI attacks.

4.2.3 Voltage-Related Components

Voltage Magnitude at Generator (VGM)

Voltage magnitude is a crucial parameter in power system operation. As Narang et al. [2] explain, FDI attacks can alter generator voltage magnitudes by up to 10%, typically forcing values between 0.95 and 1.05 p.u. for a nominal value of 1.0 p.u. This alteration affects generator excitation systems and can lead to overloading or underutilization of equipment. The paper highlights how such manipulations remain stealthy under conventional bad data detection (BDD) mechanisms.

Voltage Angle at Line and Generator

Wei et al. [5] emphasize the importance of voltage phase angles in power flow calculations. By manipulating phase angle differences, attackers can mislead state estimation algorithms. For example, a deviation of $\pm 1^\circ$ can result in power flow changes exceeding 5%, potentially destabilizing the grid. Manipulations at generator terminals further impact reactive power control and system stability, as described by Liang et al. [8].

4.2.4 Real Power Components

Real Power Generated (PG)

Real power generation is directly impacted by FDI attacks, as Wei et al. [5] discuss. The paper outlines scenarios where power generation values are altered by up to 20%, leading to incorrect dispatch signals. For instance, a generator scheduled to produce 100 MW may instead operate at 90 MW or 120 MW under attack, causing generation-load imbalances and increased operational costs.

Real Power Load (PL)

Chen et al. [3] demonstrate that load measurements are particularly vulnerable to synthetic data injection. Their study shows deviations ranging from 10% to 30%, which

translate to operational mismatches of 50 MW or more in typical scenarios. Such changes disrupt economic load dispatch and force the grid to operate inefficiently.

4.2.5 Reactive Power Components

Reactive Power Load (QL)

Reactive power loads, essential for voltage stability, are highly susceptible to FDI attacks. Shohan et al. [9] highlight that reactive power loads can deviate by as much as $\pm 50\%$ under attack, significantly altering grid stability margins. For example, a reactive load of 50 MVAR can be manipulated to values as low as 25 MVAR or as high as 75 MVAR, leading to potential voltage collapses.

4.3 Operational Impact and Cascading Failures

Liang et al. [8] and Zhang2018 et al. [7] discuss the cascading effects of FDI attacks. Manipulations in voltage and power measurements propagate through the grid, causing widespread failures. Their studies reveal that even small changes in key parameters can amplify over time, affecting multiple subsystems. For instance, altered power flow calculations can lead to incorrect overload protections, triggering line outages and blackouts.

4.4 Advanced Threat Scenarios

Shohan et al. [9] propose a generative framework, iAttackGen, to model advanced FDI attacks. Using generative adversarial networks (GANs), their method synthesizes stealthy attack vectors that evade detection while maximizing grid disruption. Similarly, Narang et al. [2] explore minimal-information attacks, showing that attackers with limited network topology knowledge can still execute effective FDI scenarios by targeting critical measurement points.

4.5 Detection Challenges

FDI attacks exploit vulnerabilities in state estimation and SCADA systems, as noted by Tran et al. [6]. Detection mechanisms must account for stealthy changes that align with

expected operational patterns. The complexity of modern grids, coupled with limited computational resources, makes real-time detection particularly challenging.

4.6 Conclusion

This chapter provided an in-depth examination of the datasets used in this research, alongside the power system components vulnerable to FDI attacks. Insights from the literature reveal the far-reaching implications of these attacks, highlighting the need for advanced detection and mitigation strategies.

Chapter 5

Generation and Validation of Synthetic FDI Attack Vectors Using ORNL Dataset

This chapter introduces the methodologies employed to generate and analyze synthetic data for False Data Injection (FDI) attacks in power systems using the Oak Ridge National Laboratory (ORNL) dataset [25]. The dataset includes both attack and normal data, providing a comprehensive foundation for evaluating the behavior of FDI attacks under different scenarios. This research focuses on leveraging advanced techniques such as Random Over Sampling (ROS), Synthetic Minority Oversampling Technique (SMOTE), SMOTE-ENN, and Adaptive Synthetic Sampling (ADASYN) to address key challenges in anomaly detection, data imbalance, and synthetic data generation. By employing these methods, the aim is to create balanced and realistic datasets that support the development and evaluation of models for detecting FDI attacks.

The integration of these techniques offers a robust approach to improving data quality, enhancing model robustness, and facilitating deeper insights into the impact and mitigation of FDI attacks in power systems, as highlighted in prior studies [1, 5, 2].

5.1 Synthetic Data Generation Methods

Synthetic data generation techniques address data imbalance and enhance dataset quality. This section details the methodologies employed, including Random Over Sampling (ROS), SMOTE, SMOTE-ENN, and ADASYN.

5.1.1 Random Over Sampling (ROS)

Random Over Sampling (ROS) is a straightforward technique that duplicates minority class samples to balance class distribution. This method ensures that minority class instances are adequately represented in the dataset, enhancing the performance of classification algorithms. The implementation of ROS involves:

1. Duplicating minority class samples until the desired class balance is achieved.
2. Ensuring that all infinite and missing values in the dataset are handled appropriately to maintain numerical stability.

Listing 5.1: Applying Random Over Sampling (ROS)

```
from imblearn.over_sampling import RandomOverSampler

ros = RandomOverSampler(sampling_strategy="not minority")
X_resampled, y_resampled = ros.fit_resample(X, y)
X_resampled.replace([np.inf, -np.inf], np.nan, inplace=True)
X_resampled.fillna(X_resampled.max().max(), inplace=True)
```

5.1.2 Synthetic Minority Oversampling Technique (SMOTE)

SMOTE generates synthetic samples by interpolating between existing minority class instances and their nearest neighbors:

where x_{syn} is the synthetic sample, x_{orig} is an original minority instance, x_{nn} is a selected nearest neighbor, and r is a random number between 0 and 1. This method enhances class balance and improves model performance in imbalanced datasets [13].

Listing 5.2: Generating Synthetic Data using SMOTE

```
from imblearn.over_sampling import SMOTE

smote = SMOTE(sampling_strategy="minority", random_state=42)
X_resampled, y_resampled = smote.fit_resample(X_resampled, y_resampled)
```

5.1.3 SMOTE-ENN for Enhanced Synthetic Data Generation

SMOTE-ENN combines SMOTE with Edited Nearest Neighbors (ENN) to address noise and borderline examples. The ENN algorithm removes noisy samples by identifying and discarding misclassified instances based on their k-nearest neighbors. This combined approach enhances the dataset's quality by:

- Reducing overlapping and noisy data points.
- Improving class separability and model performance during training.

Listing 5.3: Generating Synthetic Data using SMOTE-ENN

```

from imblearn.combine import SMOTEENN

smote_enn = SMOTEENN(sampling_strategy="auto", random_state=42)
X_resampled, y_resampled = smote_enn.fit_resample(X_resampled, y_resampled)

```

5.1.4 Adaptive Synthetic Sampling (ADASYN)

ADASYN generates synthetic samples by focusing on regions where the minority class is sparsely distributed. This method adaptively determines the number of synthetic samples based on the classification difficulty of each instance:

where n is the total number of synthetic samples, and d_i represents the classification difficulty for instance i . ADASYN enhances sensitivity to hard-to-classify instances [15].

Listing 5.4: Generating Synthetic Data using ADASYN

```

from imblearn.over_sampling import ADASYN

adasyn = ADASYN(sampling_strategy="auto", random_state=42)
X_resampled, y_resampled = adasyn.fit_resample(X, y)

```

5.2 Synthetic Data Generation Workflow

The workflow for synthetic data generation involves preprocessing the dataset, applying various oversampling techniques, and validating the generated synthetic data. The steps are outlined in the block diagram below:

The process begins with loading the ORNL dataset and preparing it for analysis by handling missing values and infinite data points. Next, ROS is applied to balance the class distribution. The balanced dataset is further processed using SMOTE, SMOTE-ENN, and ADASYN to generate realistic synthetic samples. Each method enhances the dataset in unique ways, ensuring improved performance for subsequent machine learning tasks.

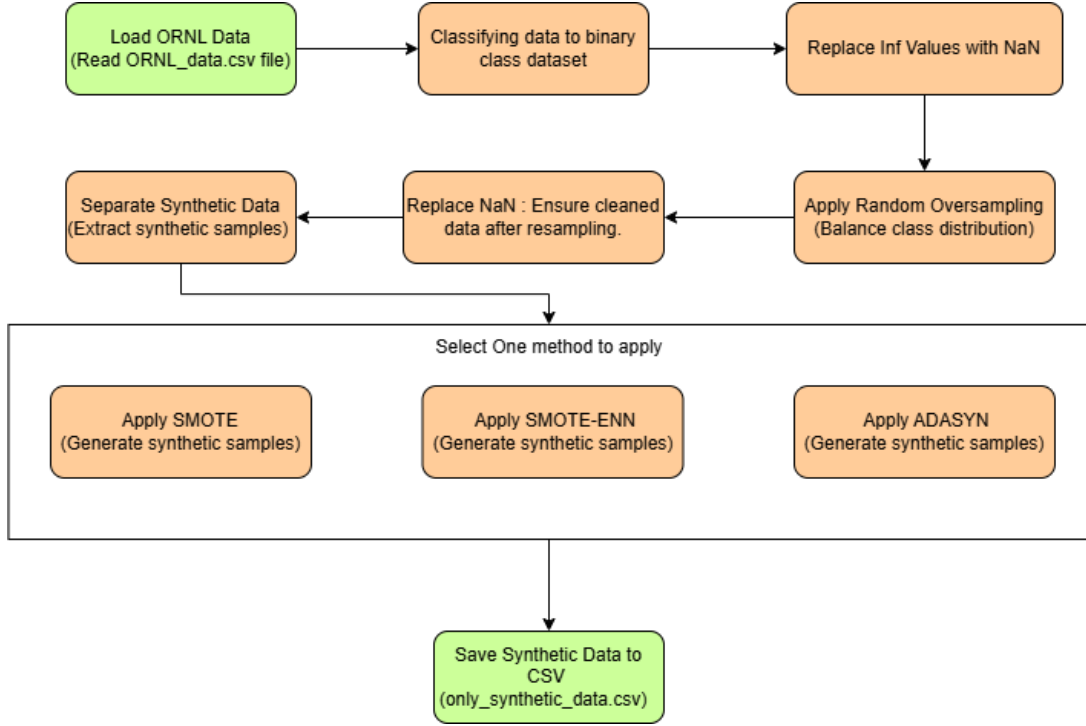


Figure 5.1: Synthetic Data Generation Workflow

5.3 Results and Discussion

5.3.1 Validation using Similarity Metric

Using the proprietary tool developed by Cistel Technology Inc., as described in Chapter 5, we achieved a similarity score of 88% for the synthetic dataset generated using SMOTE. This demonstrates that the synthetic data closely resembles the real-world data, validating the quality of the generated dataset. Furthermore, graphical visualizations were employed to support this analysis, showcasing the similarity between real and synthetic data across multiple columns.

The pairplot in Figure 5.2 demonstrates that the real and synthetic datasets align closely across features such as R1-PA1:VH, R1-PA2:VH, and R1-PM1:V. Most points for the real dataset (red) overlap significantly with the synthetic dataset (blue), indicating minimal divergence.

A single-column comparison was also performed for R1-PA10:IH, shown in Figure 5.3.

The high degree of overlap in Figure 5.3 further supports the conclusion that the synthetic dataset reliably captures the patterns of the original data. This is a testament

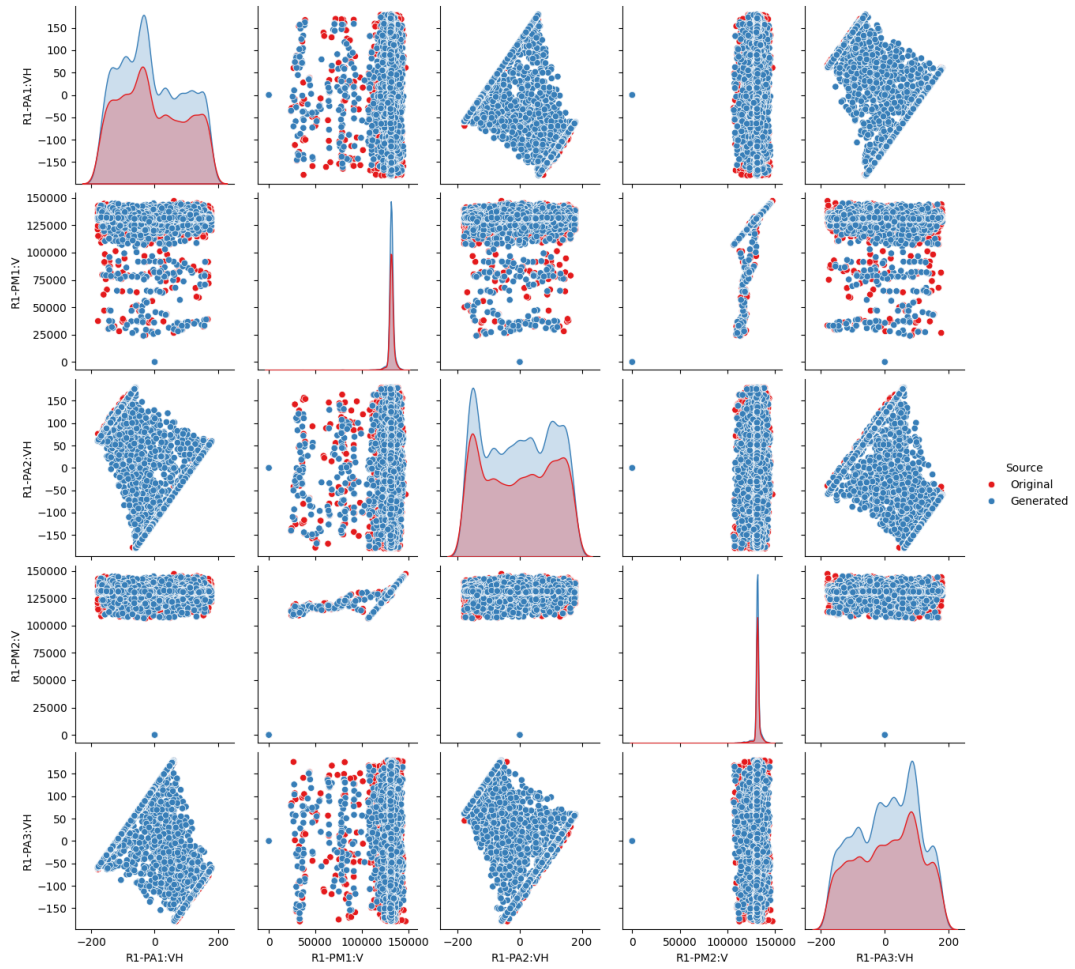


Figure 5.2: Pairplot of Multiple Columns Comparing Original and Synthetic Data

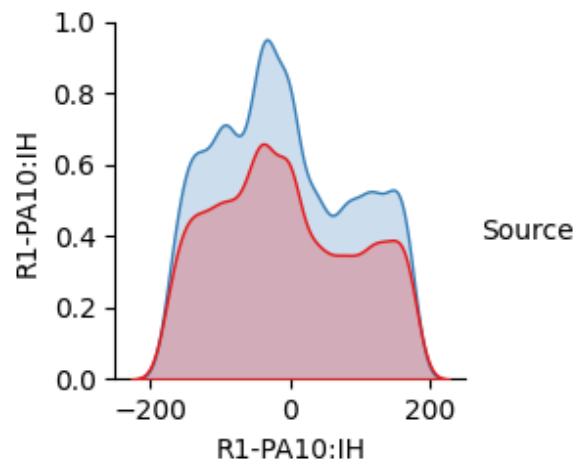


Figure 5.3: Single-Column Pairplot for R1-PA10:IH

to the effectiveness of the ROS and SMOTE-based generation methods.

For additional visualizations and graphs demonstrating the similarity across various other columns, refer to the repository at the following link: <https://github.com/KrishnaVaibhav/FDI-Generation/tree/main/SMOTE/pairplots>.

5.3.2 Comparison of SMOTE and SMOTE-ENN

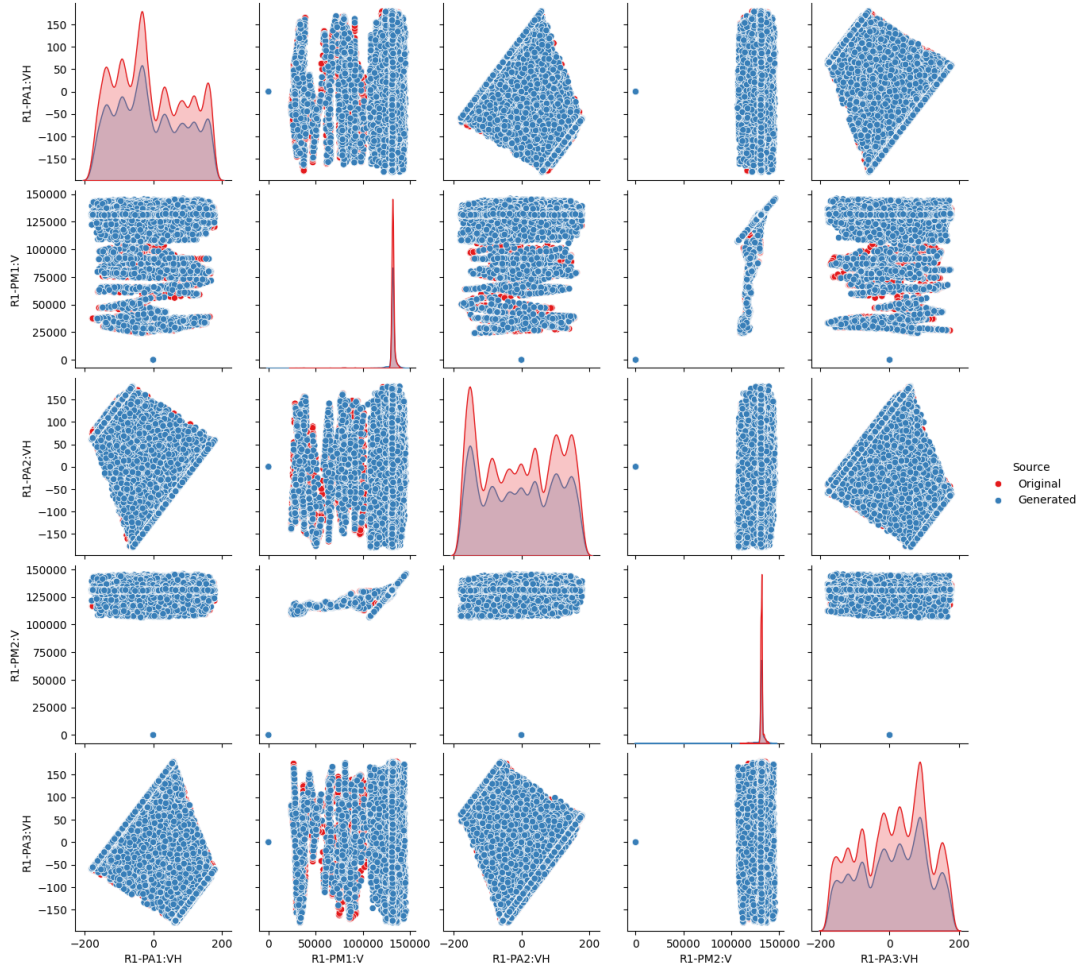


Figure 5.4: Pairplot Comparison of SMOTE and SMOTE-ENN Synthetic Data

Figure 5.4 presents a comparison between the synthetic datasets generated using SMOTE and SMOTE-ENN. The graph highlights that SMOTE-ENN reduces noise in the dataset, resulting in more distinct and accurate clustering of synthetic data points.

Table 5.1: Synthetic Data Generation Results

Methodology	Final Rows of Data	Similarity Score
ROS + SMOTE	215,968	0.8886
ROS + SMOTE-ENN	137,656	0.835
ADASYN	196,195	0.106

5.4 Findings

- **ROS + SMOTE:** The Random Oversampling (ROS) coupled with SMOTE technique increased the original data size from 9,583 to 215,968 rows, achieving a similarity score of 0.8886. This combination proved effective in class balancing and effective in generating realistic FDI attack vector that mimics closely with the simulated FDI data provided in ORNL dataset”
- **ROS + SMOTE-ENN:** By integrating Edited Nearest Neighbors (ENN) with ROS and SMOTE, the dataset size increased to 137,656 rows, with a similarity score of 0.835. This approach significantly reduced noise and removed misclassified data, enhancing dataset quality and usability.
- **ADASYN:** Although Adaptive Synthetic Sampling addressed imbalance effectively, it achieved a similarity score of only 0.106, underscoring its limitations for applications demanding high data fidelity. ADASYN’s focus on harder-to-learn instances provided valuable insights into challenging data regions but necessitated further refinement for enhanced similarity.

In conclusion, our methodology successfully demonstrates the capability to generate synthetic FDI attack data for power systems using advanced synthetic data generation techniques and regression models. The integration of Random Oversampling (ROS), SMOTE, SMOTE-ENN, and ADASYN enabled us to address data imbalance effectively, with ROS + SMOTE and ROS + SMOTE-ENN showcasing superior performance in maintaining data fidelity and enhancing dataset quality. While ADASYN provided valuable insights into challenging data regions, its limitations underscore the need for further refinement.

Chapter 6

Generating Synthetic FDI Attack Data using Multioutput Regression (MOR)

To address the challenge of generating attack data for the IEEE 118-bus system dataset[11], which initially lacks attack scenarios, we utilized a Multioutput Regression (MOR) approach. This method leverages regression models such as Random Forest, XGBoost, and LightGBM to predict multiple dependent variables and generate realistic FDI attack scenarios. The independent variables used in this approach were selected using domain knowledge and perturbed based on the operational metrics identified in Table 3.2.

6.1 Synthetic Data Generation

Figure 6.1 illustrates the workflow for generating synthetic FDI attack data using the MOR approach.

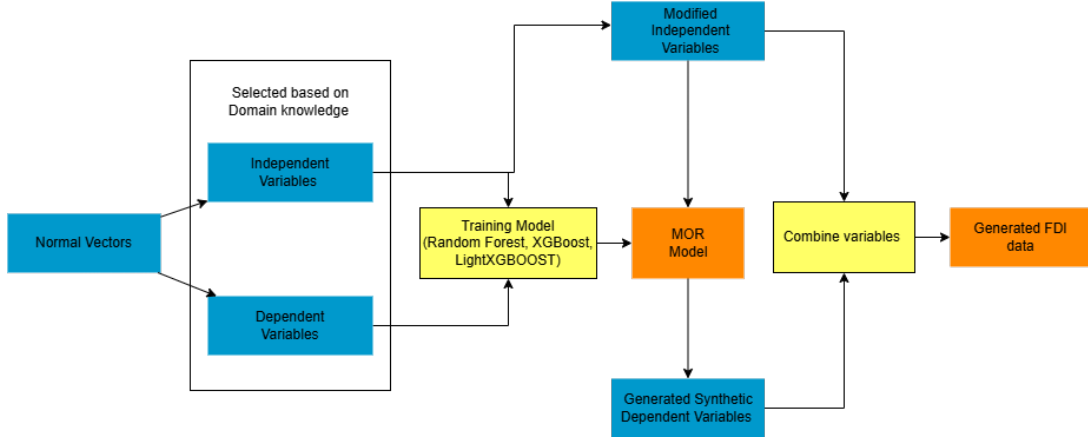


Figure 6.1: Flowchart of Synthetic FDI Attack Data Generation using MOR

6.1.1 Selection of Independent and Dependent Variables

The independent variables for the MOR approach were selected based on their relevance to operational metrics impacted by FDI attacks, as highlighted in Table 3.2. Specifically,

the following variables were used:

- **Independent Variables:**

- Voltage Generation Magnitude (VGM): Captures the voltage magnitude of power generators.
- Power Generation (PG): Represents the power output from generators.
- Power Load (PL): Reflects the power demand from loads.
- Reactive Power Load (QL): Indicates the reactive power demand.

- **Dependent Variables:**

- Voltage Load Magnitude (VLM): Captures the voltage magnitude at load buses.
- Voltage Load Angle (VLA): Represents the voltage phase angle at load buses.
- Voltage Generation Angle (VGA): Indicates the voltage phase angle at generation buses.

These variables were identified using the following code snippet:

```
# Independent variables
vgm_columns = [col for col in data.columns if "VGM" in col]
pg_columns = [col for col in data.columns if "PG" in col]
pl_columns = [col for col in data.columns if "PL" in col]
ql_columns = [col for col in data.columns if "QL" in col]

# Dependent variables
vlm_columns = [col for col in data.columns if "VLM" in col]
vla_columns = [col for col in data.columns if "VLA" in col]
vga_columns = [col for col in data.columns if "VGA" in col]
```

6.1.2 Steps for Generating Attack Data

The process of generating synthetic FDI attack data using MOR involves the following steps:

1. **Preprocessing Normal Data:** The dataset was preprocessed to extract the independent and dependent variables mentioned above.
2. **Model Training:** Three regression models were employed to map the relationships between independent and dependent variables:
 - **Random Forest:** A robust ensemble method for handling non-linear relationships.
 - **XGBoost:** An optimized gradient boosting algorithm for high performance.
 - **LightGBM:** A gradient boosting framework known for its efficiency with large datasets.
3. **Generating Modified Independent Variables:** Perturbations were applied to the independent variables to simulate realistic attack scenarios. The deviations listed in Table 3.2 (e.g., Voltage Deviation: ± 0.15 , Load Mismatch: ≥ 50 MW) were used to modify the independent variables.
4. **Synthetic Dependent Variable Generation:** Using the trained models, the modified independent variables were input to generate synthetic dependent variables, forming the FDI attack dataset.
5. **Validation of Synthetic Data:** Statistical analysis and domain knowledge were used to validate the realism of the generated attack data.
6. **Integration of Deviations:** Once the models were trained, deviations listed in Table 3.2 were applied to the independent variables. The models predicted the corresponding dependent variables, creating realistic FDI attack scenarios.

6.1.3 Comparison of Regression Models and Pairplot Results

The performance of the three regression models was compared based on their ability to generate realistic synthetic data:

- **Random Forest:** Delivered stable results but required more computational resources. As shown in Figure 6.2, the modifications in PG, PL, and QL produced promising results, with clear deviations in attack data compared to normal data.

- **XGBoost and LightGBM:** Both achieved high accuracy with efficient training time and produced similar results to Random Forest. The pairplots in Figures 6.4 and 6.5 highlight the consistency of the deviations.
- **Issues with VGM Modifications:** When applying perturbations to VGM columns, the output focused on a single point, as shown in Figure 6.3. This indicates a limitation in handling such modifications effectively. Further investigation is required to understand the root cause of this issue.

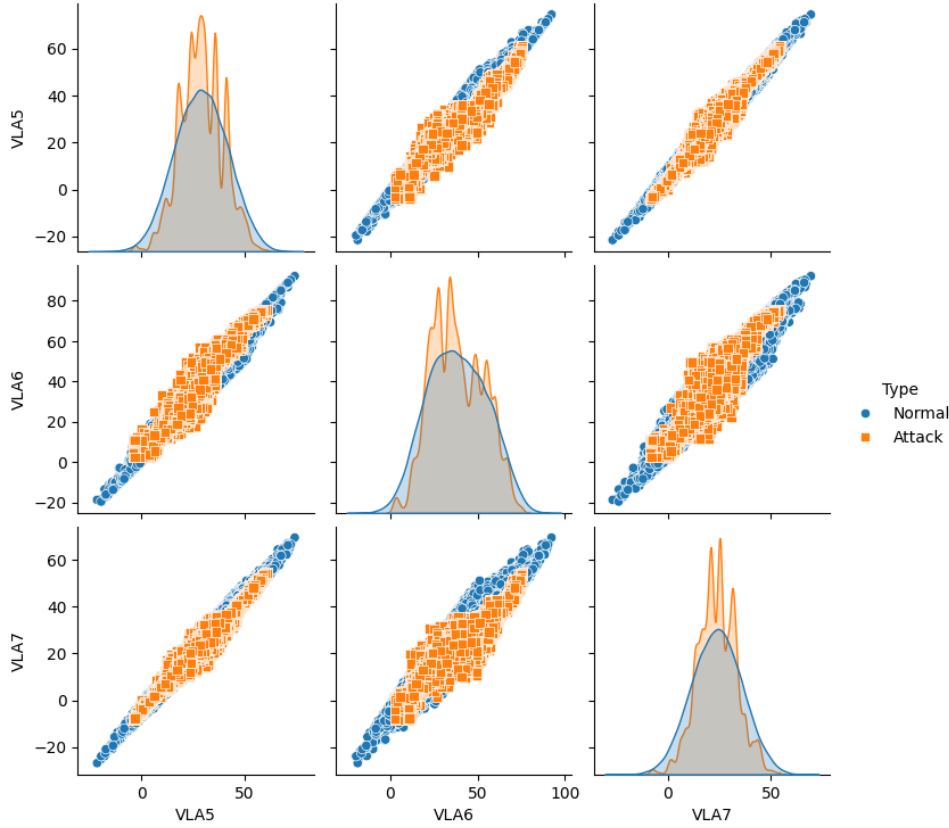


Figure 6.2: Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (Random Forest)

6.1.4 Creation of Dataset Variants

To evaluate the impact of modifying specific variables, we created several dataset variants by perturbing individual classes of independent variables and their combinations. This systematic approach enabled a comprehensive understanding of how each variable

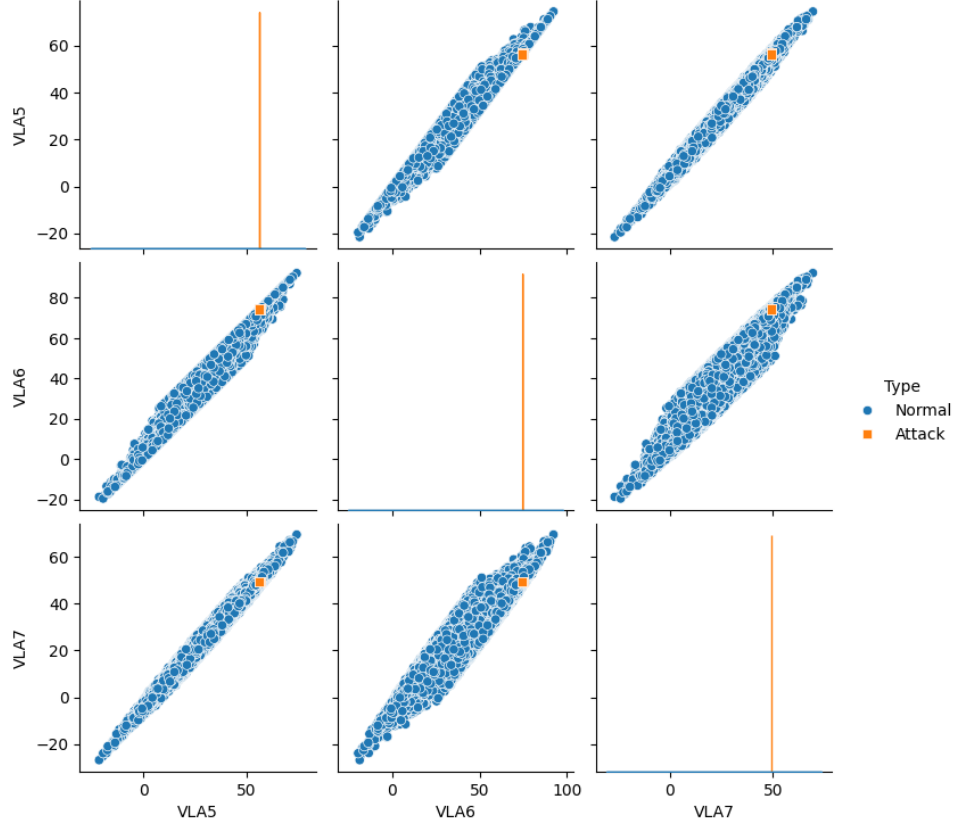


Figure 6.3: Pairplot of Normal vs. Attack Data for VGM Variables (Random Forest)

contributes to generating realistic FDI attack scenarios:

PG Class Dataset: Modified datasets focusing solely on the Power Generation (PG) class variables.

PL Class Dataset: Datasets with perturbations applied to Power Load (PL) class variables.

QL Class Dataset: Synthetic datasets where changes were applied exclusively to Reactive Power Load (QL) variables.

VGM Class Dataset: Datasets emphasizing Voltage Generation Magnitude (VGM) class modifications.

Combined Class Dataset: To capture complex interactions, a combined dataset was generated by modifying PG, PL, and QL variables simultaneously. This combined dataset is referred to as the **Composite Operational Metrics Dataset (COMD)**. The creation of these dataset variants provides flexibility in simulating various FDI attack scenarios, ensuring both individual and interaction effects are accounted for during analysis.

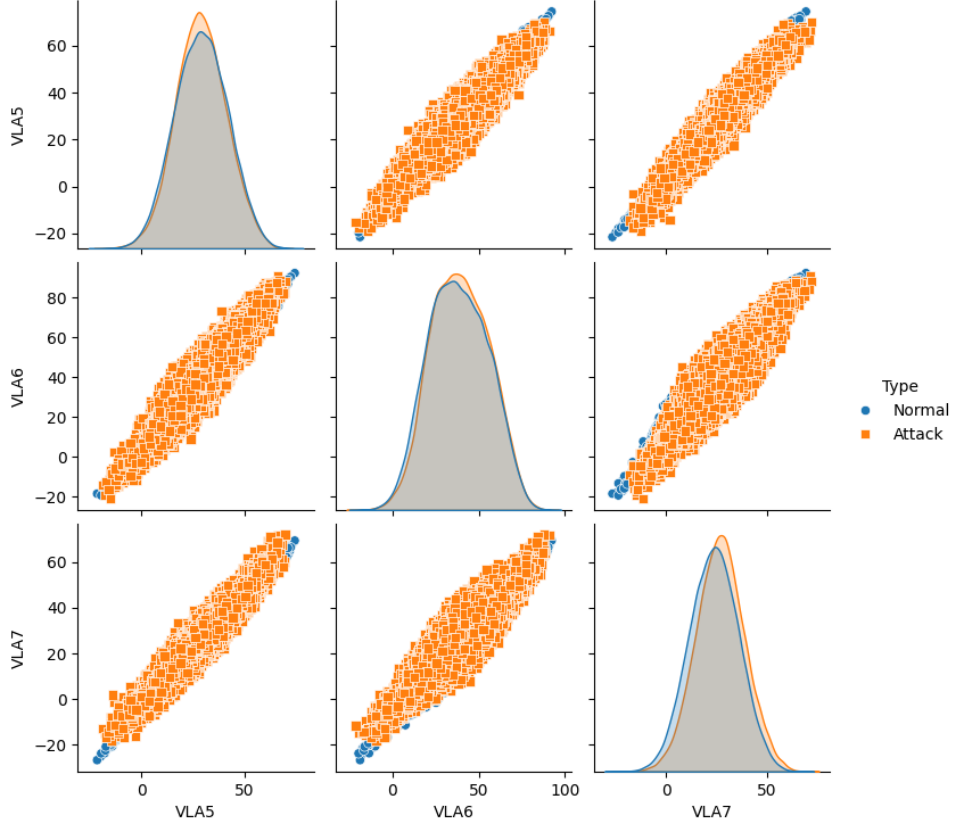


Figure 6.4: Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (XGBoost)

6.2 Results and Discussion

The pairplots demonstrate the effectiveness of the MOR approach in generating realistic attack scenarios. For PG, PL, and QL modifications, the attack data shows significant deviations while maintaining realistic distributions, as evident in Figures 6.2, 6.4, and 6.5. This alignment between normal and attack data ensures the generated scenarios are practical and valid for FDI analysis.

However, the results for VGM modifications (Figure 6.3) indicate a limitation, as the output converges to a single point. This may require further exploration and refinement in future work.

The outcomes of this research underscore the effectiveness and boundaries of the methodologies applied in generating and analyzing synthetic False Data Injection (FDI) attack data for power systems. The rigorous experimentation with data augmentation

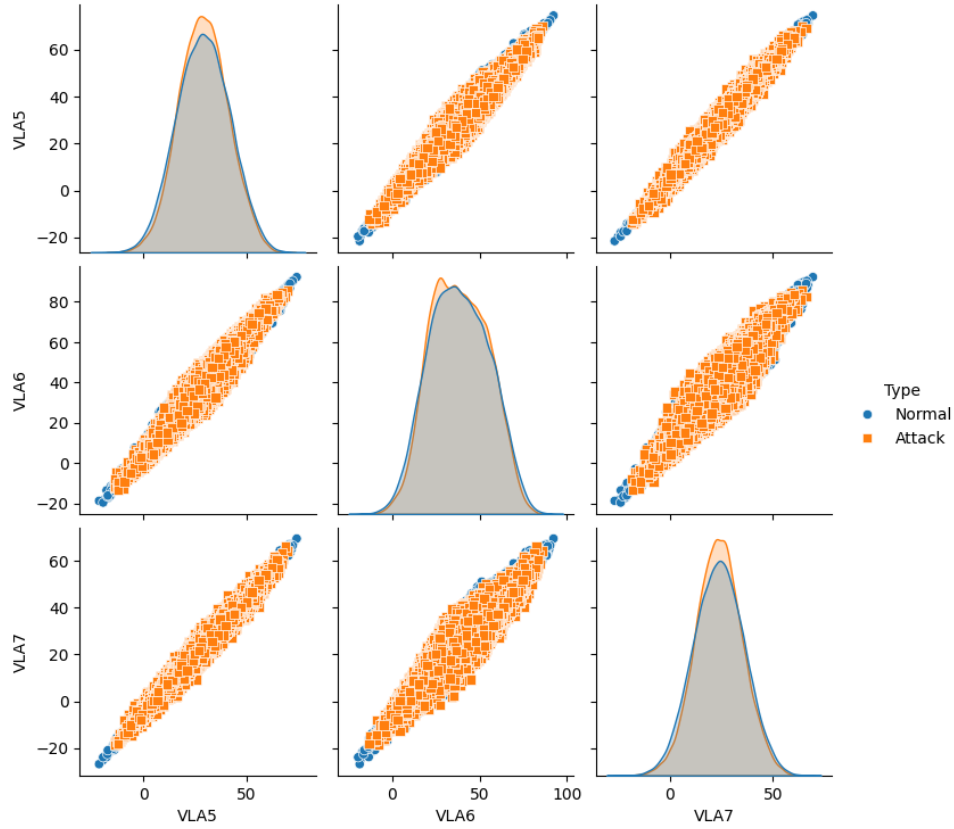


Figure 6.5: Pairplot of Normal vs. Attack Data for PG, PL, and QL Variables (LightGBM)

techniques and advanced predictive modeling led to several significant findings and insights.

6.2.1 Validation of Model Performance

Table 6.1: Model Performance Metrics

Model	MSE	MAE	R-squared Score
LightGBM	6.88	1.57	0.875
XGBoost	7.17	1.59	0.876
Random Forest	17.69	2.49	0.719

- LightGBM Model:** This model achieved a Mean Squared Error (MSE) of 6.88, Mean Absolute Error (MAE) of 1.57, and an R-squared score of 0.875, demonstrating high accuracy and efficiency.

- **XGBoost Model:** With an MSE of 7.17, MAE of 1.59, and an R-squared score of 0.876, XGBoost provided robust predictive capabilities comparable to LightGBM.
- **Random Forest Model:** While stable, Random Forest exhibited relatively lower performance with an MSE of 17.69, MAE of 2.49, and an R-squared score of 0.719, indicating potential areas for improvement in handling complex relationships.

6.2.2 Feature Insights

- **Role of Variables:** Independent variables such as Voltage Generation Magnitude (VGM), Power Generation (PG), and Reactive Power Load (QL) were instrumental in generating realistic synthetic attack data. Dependent variables like Voltage Load Magnitude (VLM) and Voltage Load Angle (VLA) effectively reflected the impacts of simulated scenarios.
- **Operational Deviations:** Incorporating operational deviations such as voltage deviation (± 0.15) and load mismatch (≥ 50 MW) aligned with real-world constraints, enabling impactful simulation of attack scenarios.

The MOR approach, utilizing Random Forest, XGBoost, and LightGBM models, successfully generated synthetic FDI attack data for the 118-bus system. By integrating operational deviations as per Table 3.2, the generated data aligns with realistic attack scenarios. Despite the limitations observed with VGM modifications, the overall methodology provides a robust foundation for validating and improving FDI detection models.

6.2.3 Analysis of Dataset Variants

- **PG, PL, and QL Classes:** Datasets focused on individual variables like PG, PL, and QL exhibited distinct and realistic deviations in the dependent variables. These datasets provide valuable insights for single-variable attack scenarios.
- **VGM Class:** The VGM class datasets highlighted promising results with clear patterns of deviation, reinforcing its significance in FDI attack modeling.
- **Composite Operational Metrics Dataset (COMD):** By combining PG, PL, and QL modifications, COMD offered a holistic view of attack scenarios, capturing

the complex interplay between operational metrics and their impacts on dependent variables.

Chapter 7

Design of the FDI Simulation Tool

This chapter details the design and development of the False Data Injection (FDI) Simulation Tool. The tool has been created to aid in generating and analyzing synthetic data for FDI scenarios in power systems. The design combines an intuitive user interface (UI) with robust backend functionalities to ensure flexibility and ease of use.

7.1 Overview of the FDI Simulation Tool

The FDI Simulation Tool is structured into two primary modules:

1. **Dataset with FDI Data:** This module allows users to load datasets containing FDI data and apply advanced synthetic data generation techniques, such as SMOTE and SMOTE-ENN, to address data imbalance issues. Users can also introduce noise to enhance data variability.
2. **Dataset without FDI Data:** This module enables users to load datasets devoid of FDI data and train machine learning models, such as Random Forest, XGBoost, or LightGBM, to identify patterns and anomalies.

The tool provides extensive options for data preprocessing, synthetic data generation, and model training, making it a comprehensive platform for FDI-related research and experimentation.

7.2 User Interface Design

The user interface (UI) of the FDI Simulation Tool is designed to ensure ease of use while maintaining the flexibility needed for advanced research purposes. The UI is divided into two panels, each addressing a specific module of the tool:

1. **Left Panel - Synthetic Data Generation:**

- Users can load datasets containing FDI data.
- Select a marker column representing the target variable.
- Choose between SMOTE or SMOTE-ENN methods for synthetic data generation.
- Optionally add noise to the generated data, with adjustable noise type (Gaussian or Uniform) and noise level.
- Generate synthetic data with a single click.

2. Right Panel - Model Training:

- Users can load datasets without FDI data.
- Select independent variable columns to be used for training.
- Choose a machine learning algorithm from Random Forest, XGBoost, or LightGBM.
- Specify the number of processing cores for efficient model training.
- Train the model and evaluate its performance metrics, including Mean Squared Error (MSE), Mean Absolute Error (MAE), and R-squared value.

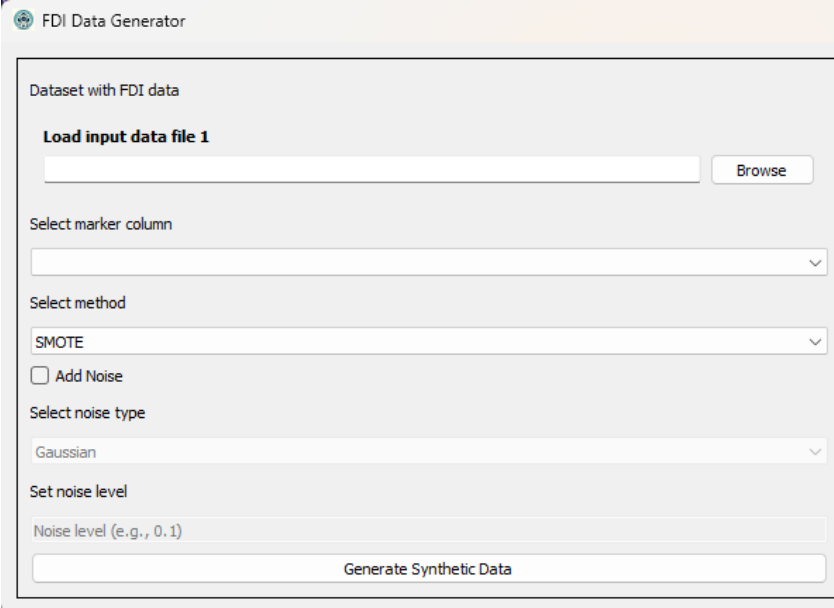
The UI layout ensures that users can navigate and execute tasks effortlessly, even when handling complex datasets and operations.

7.3 Backend Implementation

The backend of the FDI Simulation Tool is implemented using Python and leverages several powerful libraries to deliver robust functionality:

1. Synthetic Data Generation:

- The tool uses the SMOTE and SMOTE-ENN techniques for oversampling the minority class.
- Gaussian and Uniform noise can be introduced to synthetic data to enhance variability.
- The synthetic data is saved in CSV format for further analysis.



FDI Data Generator

Dataset with FDI data

Load input data file 1

Select marker column

Select method

SMOTE

☐ Add Noise

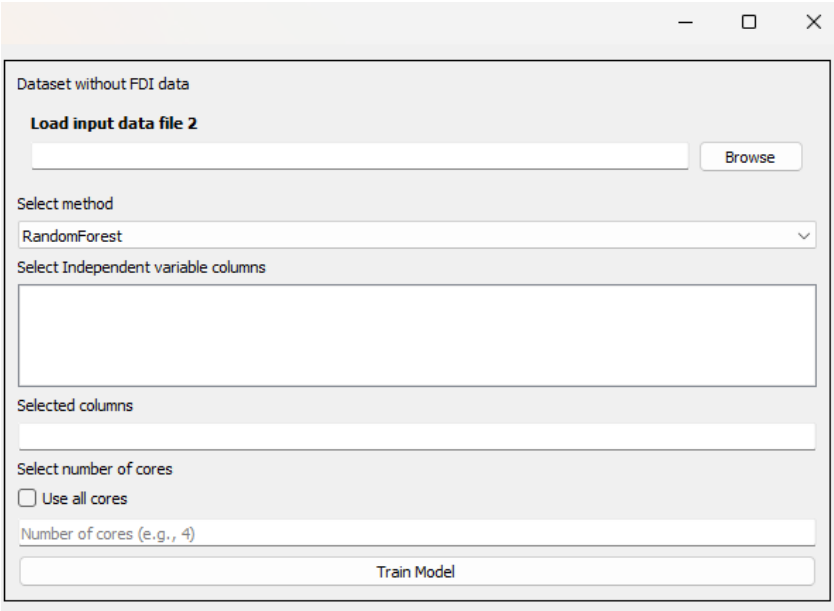
Select noise type

Gaussian

Set noise level

Noise level (e.g., 0.1)

Figure 7.1: User Interface of the FDI Simulation Tool - Left Panel



Dataset without FDI data

Load input data file 2

Select method

RandomForest

Select Independent variable columns

Selected columns

Select number of cores

☐ Use all cores

Number of cores (e.g., 4)

Figure 7.2: User Interface of the FDI Simulation Tool - Right Panel

2. Model Training:

- The tool supports Random Forest, XGBoost, and LightGBM algorithms for training predictive models.
- The `train_test_split` function is used to divide the dataset into training and

testing subsets.

- Performance metrics such as MSE, MAE, and R-squared are calculated to evaluate the model.
- Models are saved as serialized files for future use.

3. Error Handling and Data Validation:

- The tool includes robust mechanisms for handling missing and infinite values in the dataset.
- Users are prompted with error messages if the required inputs are incomplete or invalid.

7.4 Workflow

The workflow of the FDI Simulation Tool follows a logical sequence:

1. Load the dataset(s) using the respective module.
2. Configure settings for synthetic data generation or model training.
3. Execute the desired operation (generate synthetic data or train the model).
4. View results and save outputs for further analysis.

7.5 Integration of Modules

The integration of the synthetic data generation and model training modules allows users to iteratively refine their datasets and models. For example:

- Users can generate synthetic data using SMOTE-ENN and train a Random Forest model to evaluate its impact on performance.
- Noise can be added to datasets to test model robustness under varying conditions.

7.6 Conclusions with Findings

The FDI Simulation Tool represents a significant advancement in facilitating research on false data injection in power systems. Its user-friendly interface and robust backend capabilities make it an invaluable resource for researchers and practitioners. Future enhancements could include support for additional algorithms, interactive visualizations, and expanded noise generation options. All the code for the FDI Simulation Tool is available at <https://github.com/KrishnaVaibhav/FDI-Generation/tree/main/UI>.

Chapter 8

Conclusions and Future work

8.1 Summary

This research set out to address the challenges of simulating and analyzing FDI attacks on power systems by developing and evaluating advanced data generation methodologies and predictive modeling techniques. By employing Random Over Sampling (ROS) for anomaly detection, Synthetic Minority Over-sampling Technique (SMOTE) for data augmentation, and Adaptive Synthetic Sampling (ADASYN) for focusing on challenging cases, the study successfully generated synthetic datasets of varying quality and utility.

The methodologies were evaluated through rigorous experimentation, yielding detailed insights:

- **Synthetic Data Generation:** The ROS + SMOTE methodology achieved the highest similarity score of 0.8886, generating 215,968 rows of synthetic data from an original dataset of 9,583 rows. ROS + SMOTE-ENN further enhanced data quality by integrating Edited Nearest Neighbors, achieving a similarity score of 0.835 with 137,656 rows of data. ADASYN, while addressing data imbalance effectively, exhibited a lower similarity score of 0.106, highlighting its limitations in generating high-fidelity datasets.
- **Predictive Modeling:** Among the predictive models evaluated, LightGBM and XGBoost demonstrated superior performance with R-squared scores of 0.875 and 0.876, respectively. The Random Forest model, while robust, achieved a lower R-squared score of 0.719, indicating areas for optimization when applied to complex datasets.
- **Feature Importance:** The study validated the importance of independent variables such as Voltage Generation Magnitude (VGM) and Reactive Power Load (QL) in generating realistic attack scenarios. Dependent variables like Voltage Load Magnitude (VLM) and Voltage Load Angle (VLA) effectively captured the impacts of

simulated FDI attacks, aligning with real-world operational constraints.

- **Insights into Methodologies:** Noise addition and operational deviations provided valuable insights into model robustness, with SMOTE-ENN excelling in reducing noise and removing misclassified data points. These findings underscore the importance of selecting appropriate augmentation techniques based on dataset characteristics and desired outcomes.

8.2 Conclusion

The methodologies and models developed in this study significantly advance the capability to simulate and analyze FDI attacks on power systems. The high similarity scores achieved with ROS + SMOTE and ROS + SMOTE-ENN indicate the potential for these techniques to generate high-quality synthetic data that closely resembles real-world scenarios. This data serves as a critical resource for training advanced intrusion detection models, enhancing the resilience of power systems against evolving cyber threats.

The performance of predictive models such as LightGBM and XGBoost further validates their utility in analyzing complex grid scenarios, providing robust insights into the dynamics of FDI attacks. While the Random Forest model exhibited limitations in handling intricate datasets, its stability highlights its potential as a complementary tool in less complex scenarios.

The validated importance of feature variables such as VGM and QL underscores the necessity of selecting relevant operational metrics to simulate realistic attack scenarios. By aligning simulated scenarios with real-world constraints, this research bridges a critical gap in understanding and mitigating the impact of FDI attacks.

8.3 Future Work

Building on the methodologies and results presented, several avenues for future research and application are identified:

- **Expansion to Diverse Datasets:** The methodologies developed in this study can be applied to generate synthetic attack data from other datasets, enabling broader applicability across different power system configurations and operational contexts.

- **Intrusion Detection Model Training:** The synthetic datasets generated in this research provide a robust foundation for training intrusion detection models specifically designed for power systems. These models can leverage the diverse and high-fidelity attack scenarios to enhance their detection accuracy and real-time response capabilities.
- **Adaptation to Other Critical Infrastructures:** The framework can be adapted to simulate and analyze FDI attacks in other critical infrastructures such as water distribution systems, transportation networks, and telecommunication grids, contributing to a broader understanding of cyber-physical vulnerabilities.
- **Refinement of Methodologies:** Future research can focus on refining techniques like ADASYN to improve similarity scores while maintaining its strength in addressing class imbalance. Integrating hybrid approaches that combine the strengths of SMOTE, SMOTE-ENN, and ADASYN may yield further improvements in dataset quality.
- **Operational Validation:** Collaborating with power system operators to validate the simulated scenarios against real-world attack data will enhance the practical relevance and impact of the research findings.

In conclusion, this research lays a strong foundation for advancing the understanding and mitigation of FDI attacks in power systems. By generating high-quality synthetic data and leveraging advanced predictive models, it paves the way for developing robust intrusion detection systems that safeguard critical infrastructure against emerging threats.

References

- [1] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):1–33, 2011.
- [2] Jagendra Kumar Narang and Baidyanath Bag. A stealth false data attack on state estimation with minimal network information. In *2024 Third International Conference on Power, Control and Computing Technologies (ICPC2T)*, pages 630–635, 2024.
- [3] Hongyu Chen, Jingyu Wang, and Dongyuan Shi. A data preparation method for machine-learning-based power system cyber-attack detection. *2018 International Conference on Power System Technology (POWERCON)*, pages 3003–3009, 2018.
- [4] Tong Ye, Boyang Zhou, Yinghui Nie, and Zhen Zhu. Multi-objective optimization on stealthy false data injection attack in smart power transmission grid. In *2023 International Conference on Networks, Communications and Intelligent Computing (NCIC)*, pages 102–105, 2023.
- [5] Xiaoge Huang, Zhijun Qin, Ming Xie, Hui Liu, and Liang Meng. Defense of massive false data injection attack via sparse attack points considering uncertain topological changes. *Journal of Modern Power Systems and Clean Energy*, 10(6):1588–1598, 2022.
- [6] Nam N Tran, Hemanshu R Pota, Quang N Tran, Xuefei Yin, and Jiankun Hu. Designing false data injection attacks penetrating ac-based bad data detection system and fdi dataset generation. *Concurrency and Computation: Practice and Experience*, 34(7):e5956, 2022.
- [7] Jiazi Zhang, Zhigang Chu, Lalitha Sankar, and Oliver Kosut. Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Transactions on Power Systems*, 33(5):4775–4786, 2018.
- [8] Jingwen Liang, Lalitha Sankar, and Oliver Kosut. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 31(5):3864–3872, 2016.
- [9] Md Hasan Shahriar, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Mohammad Hossein Manshaei, and Dong Chen. iattackgen: Generative synthesis of false data injection attacks in cyber-physical systems. In *2021 IEEE Conference on Communications and Network Security (CNS)*, pages 200–208, 2021.

- [10] Ferdinando Fioretto, Terrence W.K. Mak, and Pascal Van Hentenryck. Predicting ac optimal power flows: Combining deep learning and lagrangian dual methods. *ArXiv*, abs/1909.10461, 2019.
- [11] University of Washington. IEEE 118-Bus System Data, 1993. Accessed: 2024-07-29.
- [12] Michael L Waskom. Seaborn: statistical data visualization. *Journal of Open Source Software*, 6(60):3021, 2021.
- [13] Nitesh V Chawla, Kevin W Bowyer, Lawrence O Hall, and W Philip Kegelmeyer. Smote: synthetic minority over-sampling technique. *Journal of artificial intelligence research*, 16:321–357, 2002.
- [14] Jean-Philippe Bouchaud and Marc Potters. Financial applications of random matrix theory: a short review. *arXiv preprint arXiv:0910.1205*, 2009.
- [15] Haibo He, Yang Bai, Edwardo A Garcia, and Shutao Li. Adasyn: Adaptive synthetic sampling approach for imbalanced learning. In *2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence)*, pages 1322–1328. Ieee, 2008.
- [16] Leo Breiman. Random forests. *Machine learning*, 45:5–32, 2001.
- [17] Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pages 785–794, 2016.
- [18] Guolin Ke, Qi Meng, Thomas Finley, Taifeng Wang, Wei Chen, Weidong Ma, Qiwei Ye, and Tie-Yan Liu. Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems*, 30, 2017.
- [19] Grigorios Tsoumakas, Ioannis Katakis, and Ioannis Vlahavas. Random k-labelsets for multilabel classification. *IEEE transactions on knowledge and data engineering*, 23(7):1079–1089, 2010.
- [20] Trevor Hastie, Robert Tibshirani, and Jerome Friedman. The elements of statistical learning: data mining, inference, and prediction, 2017.
- [21] Aibing Qiu, Zhou Ding, and Shengfeng Wang. A descriptor system design framework for false data injection attack toward power systems. *Electric Power Systems Research*, 192:106932, 2021.
- [22] Ehsan Naderi and Arash Asrari. A deep learning framework to identify remedial action schemes against false data injection cyberattacks targeting smart power systems. *IEEE Transactions on Industrial Informatics*, 20(2):1208–1219, 2024.

- [23] Ehsan Naderi, Samaneh Pazouki, and Arash Asrari. A remedial action scheme against false data injection cyberattacks in smart transmission systems: Application of thyristor-controlled series capacitor (tcsc). *IEEE Transactions on Industrial Informatics*, 18(4):2297–2309, 2022.
- [24] Kang-Di Lu and Zheng-Guang Wu. Multi-objective false data injection attacks of cyber–physical power systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 69(9):3924–3928, 2022.
- [25] Tommy Morris. Power system dataset readme, n.d. Accessed: 2024-12-03.

Appendix A

Code for Synthetic Data Generation and Similarity Analysis

This appendix contains Python scripts for generating synthetic data and analyzing similarity metrics. These scripts utilize techniques such as SMOTE-ENN, SMOTE with Random Over Sampling (ROS), and ADASYN to address data imbalance and improve dataset quality. The similarity analysis quantifies the fidelity of the synthetic data compared to the original dataset using metrics like Euclidean distance and cosine similarity.

The scripts are organized as follows:

- `SMOTE_ENN.py`: Implements the SMOTE-ENN technique for synthetic data generation.
- `SMOTE_ROS.py`: Combines Random Over Sampling (ROS) with SMOTE to generate balanced datasets.
- `ADASYN.py`: Utilizes the ADASYN technique to create synthetic data by focusing on difficult-to-learn samples.
- `compare.ipynb`: Computes similarity metrics (Euclidean distance and cosine similarity) between the original and synthetic datasets.

Below are the key implementations from these scripts.

A.1 `SMOTE_ENN.py`: Synthetic Data Generation with SMOTE-ENN

This script generates synthetic data using SMOTE-ENN, a technique that combines oversampling and edited nearest neighbors to enhance minority class representation.

```

import pandas as pd
from imblearn.combine import SMOTEENN
from imblearn.over_sampling import SMOTE, RandomOverSampler
import numpy as np

data = pd.read_csv("ORNL_data.csv")
data["marker"] = pd.to_numeric(data["marker"], errors="coerce")
data["marker"] = data["marker"].apply(lambda x: 1 if x >= 7 and
                                      x <= 12 else 0)

X = data.drop("marker", axis=1)
X.replace([np.inf, -np.inf], np.nan, inplace=True)
X.fillna(X.max().max(), inplace=True)
y = data["marker"]

# Apply SMOTE-ENN to the training data
smote_enn = SMOTEENN(sampling_strategy="auto", random_state=42)
X_resampled, y_resampled = smote_enn.fit_resample(X, y)

synthetic_data = pd.concat([X_resampled, y_resampled], axis=1)
synthetic_data.to_csv("synthetic_FDI_data_SMOTE_ENN.csv", index=False)

```

A.2 SMOTE_ROS.py: Synthetic Data Generation with SMOTE and ROS

This script combines Random Over Sampling (ROS) with SMOTE to enhance the dataset by balancing class distributions and identifying anomalous features.

```

import pandas as pd
from imblearn.over_sampling import SMOTE, RandomOverSampler
import numpy as np

data = pd.read_csv("ORNL_data.csv")
data["marker"] = pd.to_numeric(data["marker"], errors="coerce")
data["marker"] = data["marker"].apply(lambda x: 1 if x >= 7 and
                                      x <= 12 else 0)

X = data.drop("marker", axis=1)
X.replace([np.inf, -np.inf], np.nan, inplace=True)
X.fillna(X.max().max(), inplace=True)
y = data["marker"]

```

```

smote = SMOTE(sampling_strategy="minority")
X_resampled, y_resampled = smote.fit_resample(X, y)

synthetic_data = pd.concat([X_resampled, y_resampled], axis=1)
synthetic_data.to_csv("only_synthetic_data.csv", index=False)

```

A.3 ADASYN.py: Synthetic Data Generation with ADASYN

This script applies the ADASYN technique to adaptively generate synthetic data, focusing on underrepresented and challenging samples.

```

import pandas as pd
import numpy as np
from imblearn.over_sampling import ADASYN, RandomOverSampler

data = pd.read_csv("merged_file.csv")
data["marker"] = pd.to_numeric(data["marker"], errors="coerce")
data["marker"] = data["marker"].apply(lambda x: 1 if x >= 7 and
                                      x <= 12 else 0)

adasyn = ADASYN(sampling_strategy="minority", random_state=42)
X_resampled, y_resampled =
    adasyn.fit_resample(data.drop("marker", axis=1), data["marker"])

synthetic_data = pd.concat([X_resampled, y_resampled], axis=1)
synthetic_data.to_csv("synthetic_data.csv", index=False)

```

A.4 compare.ipynb: Similarity Analysis Between Original and Synthetic Data

This script calculates similarity metrics between the original and synthetic datasets to evaluate their fidelity and usability.

```

from sklearn.metrics.pairwise import cosine_similarity
import numpy as np

def calculate_similarity(original_data, generated_data):
    euclidean_dist = np.linalg.norm(original_data - generated_data)
    cosine_sim = cosine_similarity([original_data],
                                   [generated_data])[0][0]

    return euclidean_dist, cosine_sim

similarity_results = []
for column in original_data.columns:
    original_col = original_data[column].values
    generated_col = generated_data[column].values
    similarity_results.append((column,
                              *calculate_similarity(original_col, generated_col)))

```

These scripts provide a comprehensive approach for generating synthetic data and evaluating its similarity to original data. They form the foundation for creating high-quality datasets for robust machine learning applications in detecting and mitigating False Data Injection (FDI) attacks in power grids.