False Data Injection & DoS Attack Simulation & Detection on the IEEE 14-Bus System

Ashish Tirupati Bollam (2021EEB1158)
Chirag Ghodke (2021EEB1162)
Siddhartha Arora (2021EEB1213)
Divyansh Verma (2022CSB1081)

April 27, 2025

1 Executive Summary

The objective of this project is to simulate and detect False Data Injection (FDI) and Denial-of-Service (DoS) attacks on smart grids, with the expected outcome of achieving robust real-time anomaly detection. Using a Simulink-based IEEE 14-bus model, real-time voltage and current data are streamed over UDP, intercepted by a Python Man-in-the-Middle (MITM) proxy that injects false readings (FDI) and drops or delays packets (DoS). The system data is then analyzed on a live dashboard server and the attacks are detected using machine learning for FDI detection and DoS detection. This setup enables the exploration of integrated integrity and availability threat mitigation in cyber-physical power systems.

2 Introduction

The IEEE 14-Bus System

The IEEE 14-bus system is a standard test model representing a simplified electrical grid with 14 buses connected by transmission lines, some linked to generators and others to loads. It is widely used to study power flow, system stability, and response to disturbances. In this project, we use the IEEE 14-bus model to simulate a realistic smart grid environment for injecting and detecting False Data Injection (FDI) and Denial-of-Service (DoS) attacks, enabling a controlled evaluation of cyber-physical threats.

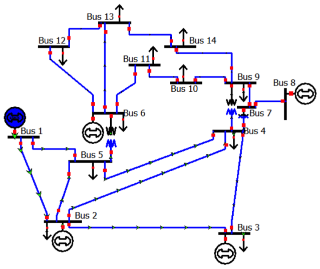


Figure 1: IEEE 14 bus system

3 Objectives and Scope

3.1 Objectives

- Simulate and detect False Data Injection (FDI) attack on the IEEE 14 bus system.
- Simulate and detect Denial of Service (DoS) attack on the IEEE 14 bus system.
- Develop and deploy a supervised machine learning model for attack detection.
- Build a real-time monitoring and visualization dashboard.
- Demonstrate the integrated system for real-time anomaly detection.

3.2 Limitations and Assumptions

- The machine learning model is trained on simulated data; performance on real-world test beds may vary a bit.
- Assumes ideal UDP communication without real-world network congestion or loss (except induced DoS attacks).

4 Literature Survey

- S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational Detection of False Data Injection Attack in Smart Grid: A Multi-label Classification Approach," Link.
- A. Chawla, P. Agrawal, B. K. Panigrahi, and K. Paul, "Deep-learning-based Data-Manipulation Attack Resilient Supervisory Backup Protection of Transmission Lines." Link.

5 Methodology

Here is a flow diagram that describes the whole architecture of the project.

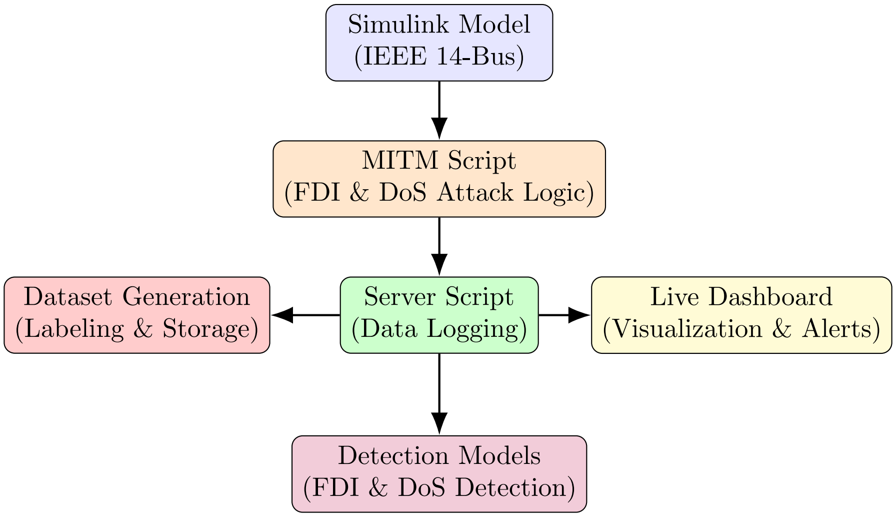


Figure 2: System Architecture for FDI and DoS Attack Simulation and Detection

5.1 Simulink Model

We used a Simulink model of the IEEE 14-bus system that continuously generates 3-phase voltage and current measurements for all 14 buses.

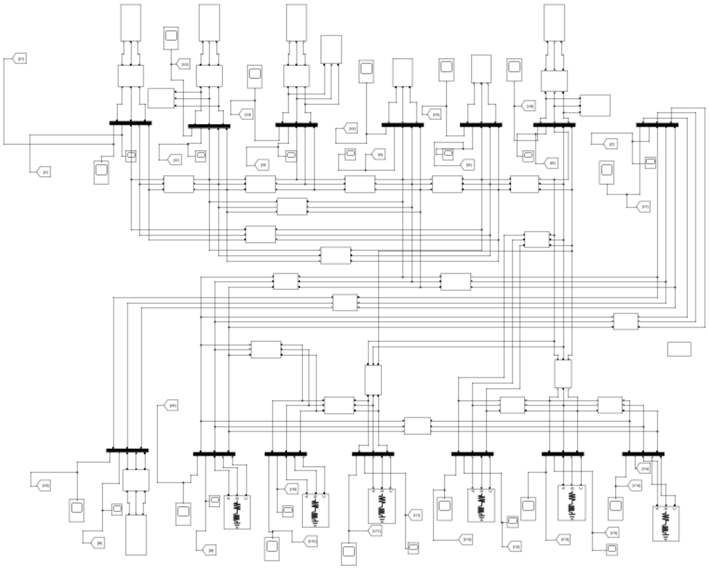


Figure 3: Simulink Model of the 14-Bus Smart Grid

5.2 Attack Script

We implemented a Man-in-the-Middle (MITM) proxy server between the MATLAB Simulink model and the main server to simulate False Data Injection (FDI). Along with this, we also implemented Denial-of-Service (DoS) attack. The attack script listens for UDP packets on port 5005, applies attack logic, and forwards the modified packets to port 5006. The attack routines are as follows:

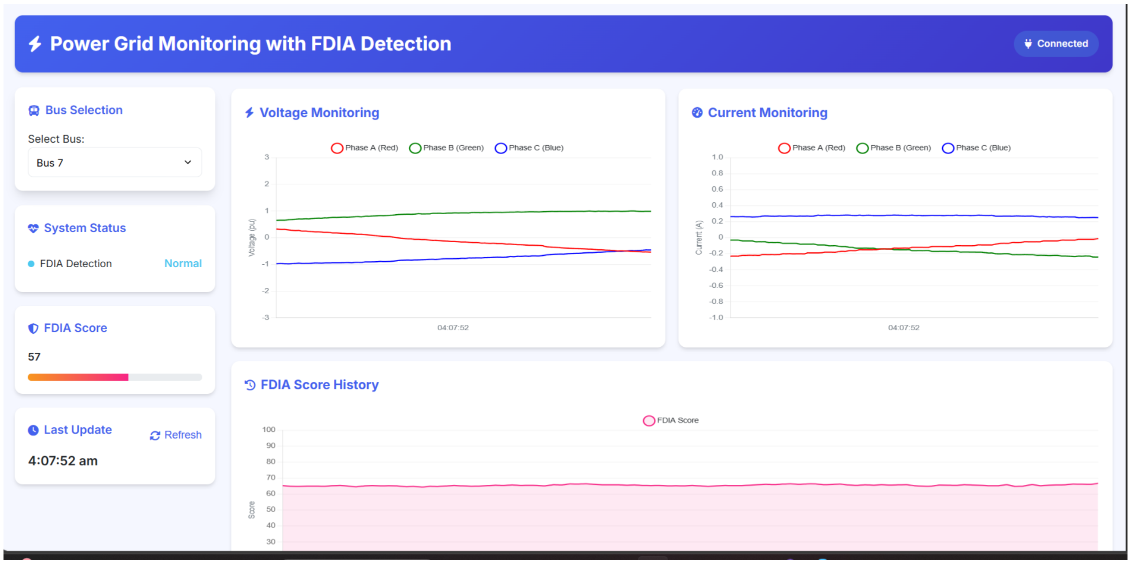
- Receives JSON-formatted voltage and current measurements from Simulink on port 5005 and forwards the (potentially tampered) data to the server on port 5006.
- For FDI simulation, randomly selects some variables out of the 84 total measurements and alters their values by approximately 15–20%.
- For DoS simulation, with a probability of 70%, corrupts entire packets by setting all voltage and current values to zero.

5.3 Server Script

- The server script sits on UDP port 5006, receiving each JSON-encoded measurement and immediately logging it with the timestamp.
- The logged data is used to create a dashboard, where the 3 phase voltage and current data can be observed using plots.

5.4 Dashboard for Real-Time Visualization

We created a web interface that displays the current V & I values, live grid status and attack alerts.



Power Grid Monitoring with FDIA Detection

Connected

Bus Selection

Select Bus: Bus 7

System Status

FDIA Detection Normal

FDIA Score

57

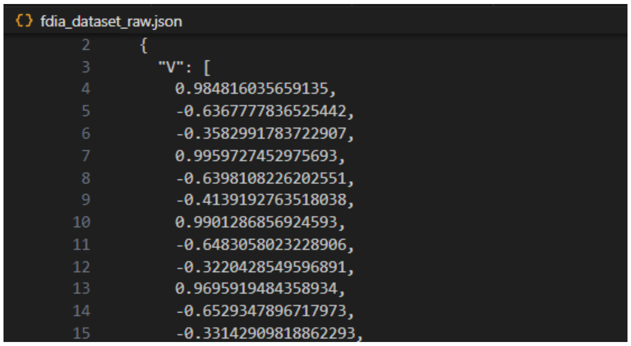
Last Update

4:07:52 am

Figure 4: Dashboard for real-time visualization

5.5 Dataset Generation Using MATLAB

- Simulated and recorded 500,000 timestamps using the MATLAB model and MITM script.
- Captured 84 variables per timestamp (3 voltages and 3 currents for each of the 14 buses).
- Manually injected False Data Injection (FDI) during selected intervals.
- Labeled each record as normal (0) or attacked (1).
- Stored the dataset in both JSON and CSV formats.



fdia_dataset_raw.json

```
  {
    "V": [
      0.984816035659135,
      -0.6367777836525442,
      -0.3582991783722907,
      0.9959727452975693,
      -0.6398108226202551,
      -0.4139192763518038,
      0.9901286856924593,
      -0.6483058023228906,
      -0.3220428549596891,
      0.9695919484358934,
      -0.6529347896717973,
      -0.33142909818862293,
```

Figure 5: Dataset Snippet

5.6 FDI Detection Model

To detect False Data Injection (FDI) attacks in smart grids, a supervised classification model was developed using time-series voltage and current data from 14 buses (84 total features).

5.6.1 Model Architecture and Implementation

- CSVs were loaded in chunks, and features were transformed with Yeo-Johnson to normalize distributions and preserve negative values for stability.
- A Histogram-Based Gradient Boosting Classifier was chosen for its high performance on structured data and optimizations like binning, early stopping, and regularization.
- Data was split 80-20 stratified. Hyperparameters were tuned with grid search and 3-fold cross-validation, while early stopping (15 rounds) prevented overfitting. Results are shared in the results section.
- The trained model and preprocessing pipeline were saved as a `.joblib` file for real-time FDI detection in the dashboard.

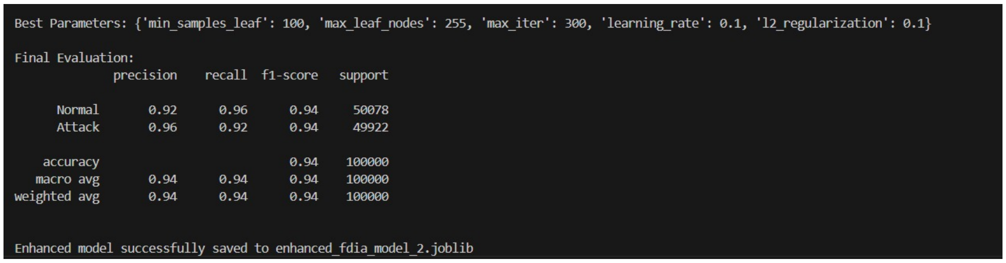
6 Results

6.1 Model Results

The enhanced model achieved 94% accuracy on the test set. It showed strong class-wise performance:

- **Normal:** Precision = 0.92, Recall = 0.96, F1 = 0.94
- **Attack:** Precision = 0.96, Recall = 0.92, F1 = 0.94

Macro and weighted F1-scores were both 0.94, indicating consistently high performance across both classes. The model demonstrates efficient and interpretable detection of FDI attacks, suitable for real-time deployment in smart grid systems.

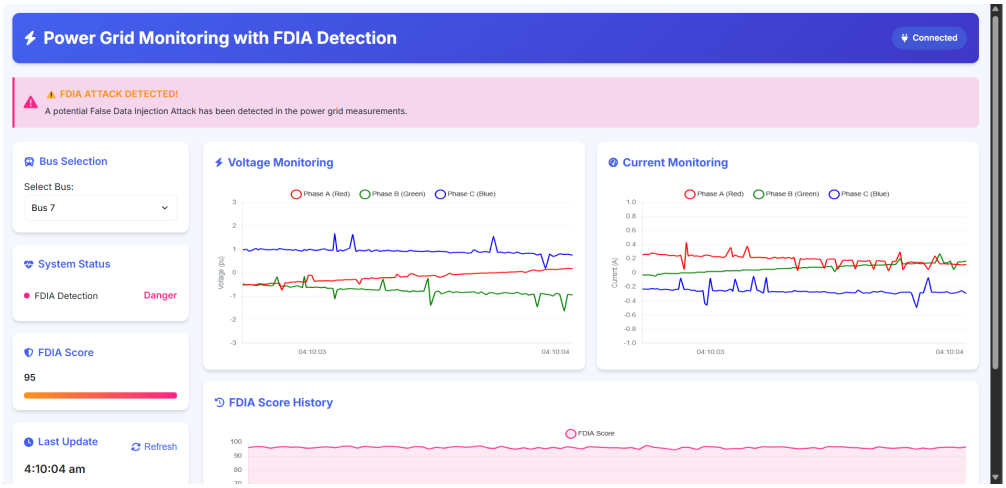


```
Best Parameters: {'min_samples_leaf': 100, 'max_leaf_nodes': 255, 'max_iter': 300, 'learning_rate': 0.1, 'l2_regularization': 0.1}

Final Evaluation:
              precision    recall  f1-score   support

      Normal       0.92      0.96      0.94     50078
      Attack       0.96      0.92      0.94     49922

    accuracy                           0.94    100000
   macro avg       0.94      0.94      0.94    100000
weighted avg       0.94      0.94      0.94    100000


Enhanced model successfully saved to enhanced_fdia_model_2.joblib
```

Figure 6: Results of the model training

6.2 FDI Detection

False Data Injection (FDI) attacks were detected in real-time by using our ML model. Alerts were triggered whenever the trained model classified incoming data as tampered. The dashboard visualization below highlights an example where the system successfully identified FDI attacks.



Power Grid Monitoring with FDIA Detection

⚠ FDIA ATTACK DETECTED!

A potential False Data Injection Attack has been detected in the power grid measurements.

Select Bus: Bus 7

FDIA Detection: Danger

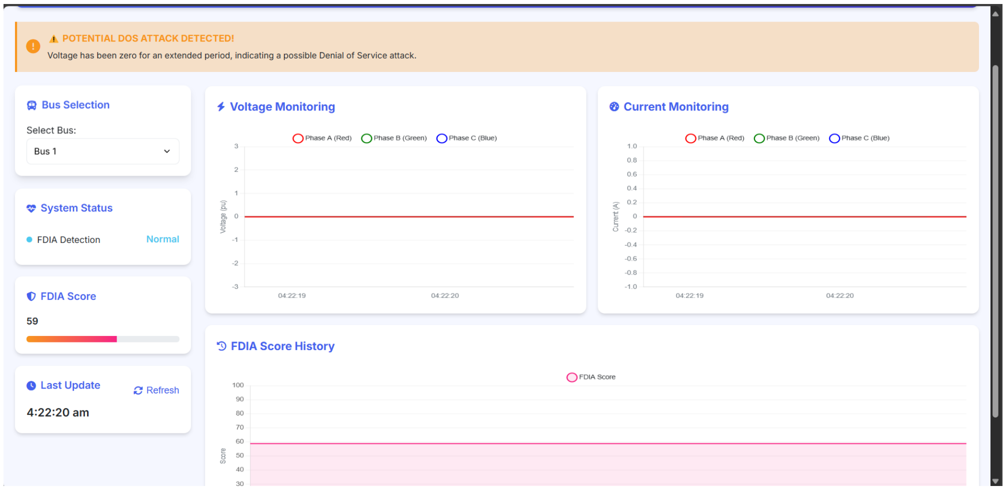
FDIA Score: 95

Last Update: 4:10:04 am

Figure 7: Dashboard visualization showing real-time FDI detection

6.3 DoS Detection

Denial-of-Service (DoS) attacks were detected by observing patterns of missing or zeroed voltage and current readings. The server flagged events where consecutive corrupted packets were received, indicating potential DoS conditions. The dashboard below showcases a scenario where the system successfully detected a DoS attack.



⚠ POTENTIAL DOS ATTACK DETECTED!

Voltage has been zero for an extended period, indicating a possible Denial of Service attack.

Select Bus: Bus 1

FDIA Detection: Normal

FDIA Score: 59

Last Update: 4:22:20 am

Figure 8: Dashboard visualization showing real-time DoS detection

7 Analysis

7.1 Insights from Results

The model achieved high detection accuracy for FDI attacks (94%), demonstrating that supervised machine learning can effectively identify subtle anomalies in voltage and current readings. For DoS attacks, detection was successfully handled at the server level based on missing data patterns without requiring an ML model.

7.2 Comparison with Existing Approaches

Compared to existing literature relying heavily on deep learning methods or complex graph-based techniques, our lightweight Histogram-based Gradient Boosting Classifier proved to be highly efficient, interpretable, and easier to deploy for real-time smart grid applications.

8 Future Work

- Expand detection to stealthier attack types, including false sequence injection and combined FDI-DoS attacks.
- Enhance dataset realism by building and training on data collected from physical testbed experiments.
- Building a dashboard that can track multiple power systems at once.

9 Conclusion

In line with our objective of building a robust and real-time cyberattack detection framework for smart grids, we successfully designed and implemented a comprehensive solution spanning attack simulation, data generation, model development, and real-time visualization. The major outcomes of the project are as follows:

- Successfully simulated both False Data Injection (FDI) and Denial-of-Service (DoS) attacks on the IEEE 14-bus smart grid using a combined Simulink+MITM proxy setup.
- Generated a labeled dataset of 500 000 timestamps with 84 features each, enabling robust supervised learning for anomaly detection.
- Developed and deployed a Histogram-Based Gradient Boosting Classifier that achieved 94% accuracy and F1-scores of 0.94 for both normal and attack classes.
- Built a real-time web dashboard that integrates live data streaming, attack injection, ML inference, and alert visualization.
- Demonstrated a scalable, interpretable, and low-latency detection pipeline, laying the groundwork for future testbed validation and edge-based deployment.

10 References

- S. Wang, S. Bi, and Y.-J. A. Zhang, “Locational Detection of False Data Injection Attack in Smart Grid: A Multi-label Classification Approach,” Link.
- A. Chawla, P. Agrawal, B. K. Panigrahi, and K. Paul, “Deep-learning-based Data-Manipulation Attack Resilient Supervisory Backup Protection of Transmission Lines.” Link.

11 Team Contributions

- **Ashish Tirupati Bollam (2021EEB1158):** Designed the MITM attack simulation script and integrated the data and detection models with a real-time web dashboard.
- **Siddhartha Arora (2021EEB1213):** Built the MITM labelled dataset, the FDI Detection ML model and connecting it to the dashboard.
- **Chirag Ghodke (2021EEB1162):** Did literature survey for smart grid and developed the IEEE 14-bus smart grid simulation model in MATLAB and connected it with python over UDP.
- **Divyansh Verma (2022CSB1081):** Implemented the Denial-of-Service (DoS) attack simulation and detection using heuristic approach.