Using Machine Learning to Recognize Attacks on Power Grids

Layhan Mishra   Md Rakibul Ahasan   Abdulrahman Takiddin

Cyber-Physical Machine Learning Lab at Florida State University

FSU UNDERGRADUATE RESEARCH OPPORTUNITY PROGRAM
CENTER FOR UNDERGRADUATE RESEARCH & ACADEMIC ENGAGEMENT

Abstract

Many hackers perform cyberattacks on power grids to reduce their utility bills. This research was conducted to determine which machine-learning models are most effective in detecting such cyberattacks on power grids. Given a dataset from an Irish power company with information on several users' power usage and whether they artificially reduced their utility bills, multiple machine-learning models were trained on a large portion of the dataset and then tested on a smaller portion. The models were then evaluated on 4 metrics: accuracy, precision, recall, and F1 score. Because of the variety of statistics evaluated and the variety of machine learning models, there is no clear-cut best-performing machine learning model. However, taking all data into account, there were three models that performed the best: the random forest, decision tree and CNN. Out of these three, the random forest performed the best consistently across all metrics. However, it should be said that the decision tree and CNN also detected attacks at a very high rate and could be better than the random forest for different instances of this scenario (different power companies, cities, and power grids). For this particular scenario, any of these three could realistically be used to detect cyberattacks on power grids with the random forest classifier being the best.

Introduction

Today, many power grids are instances of cyber-physical systems. One threat to these grids is a false data injection attack (FDIA). In this research, machine learning models will be trained and evaluated on their ability to detect FDIAs on the power grid.

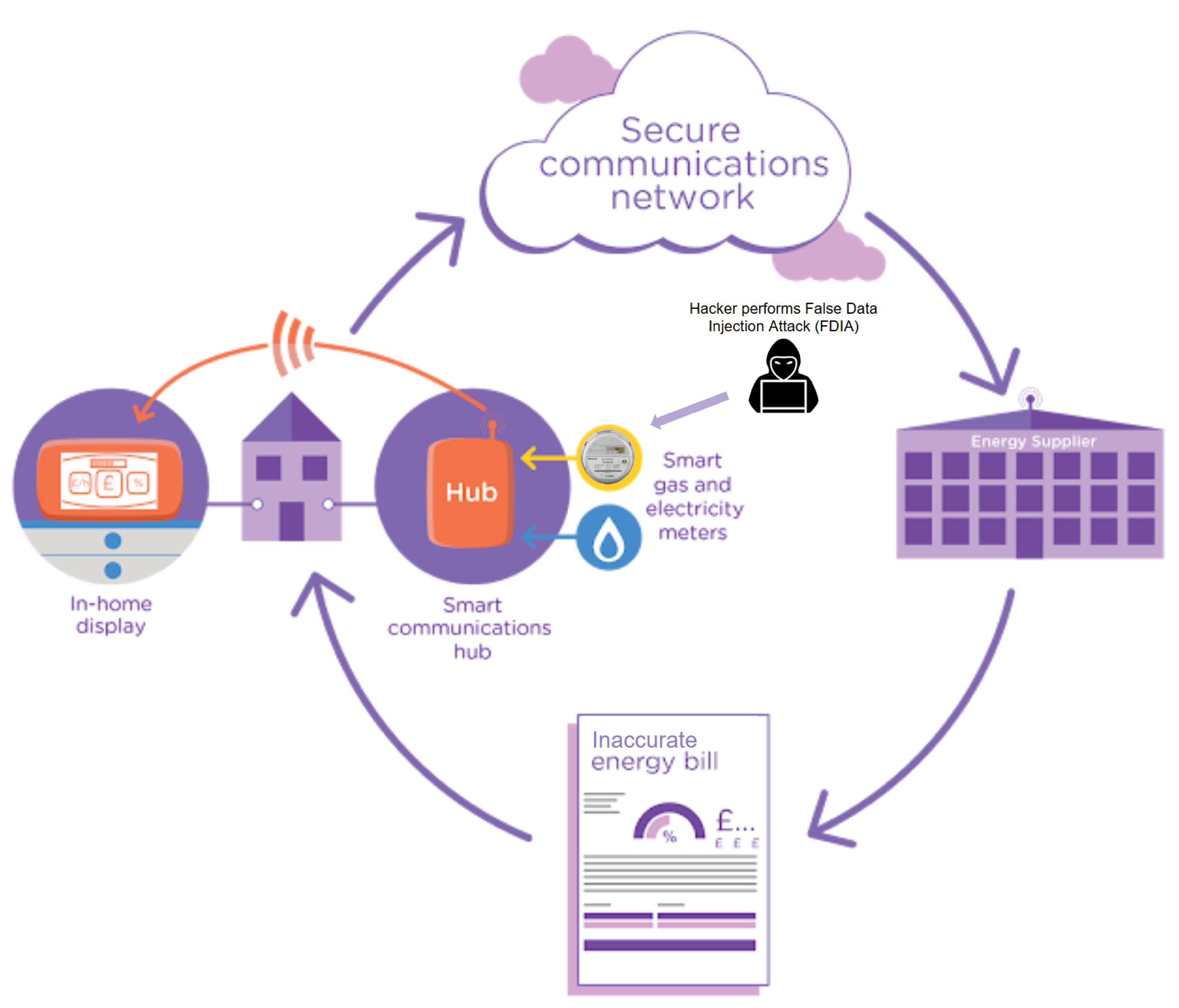


Figure 1. False Data Injection Attack (FDIA)

Models

In this research, two types of machine learning models were used to detect FDIAs. Shallow machine learning models and deep machine learning models (or neural network models).

A shallow machine learning model refers to machine learning models with limited depth, usually involving one or two layers of processing. Commonly used in traditional machine learning tasks, shallow learning models include algorithms like logistic regression, support vector machines (SVM), and decision trees.

A deep machine learning model refers to a type of machine learning model that uses artificial neural networks with multiple layers to process data, mimicking the structure of the human brain to learn complex patterns from large datasets, often performing tasks like image recognition, natural language processing, and speech recognition,

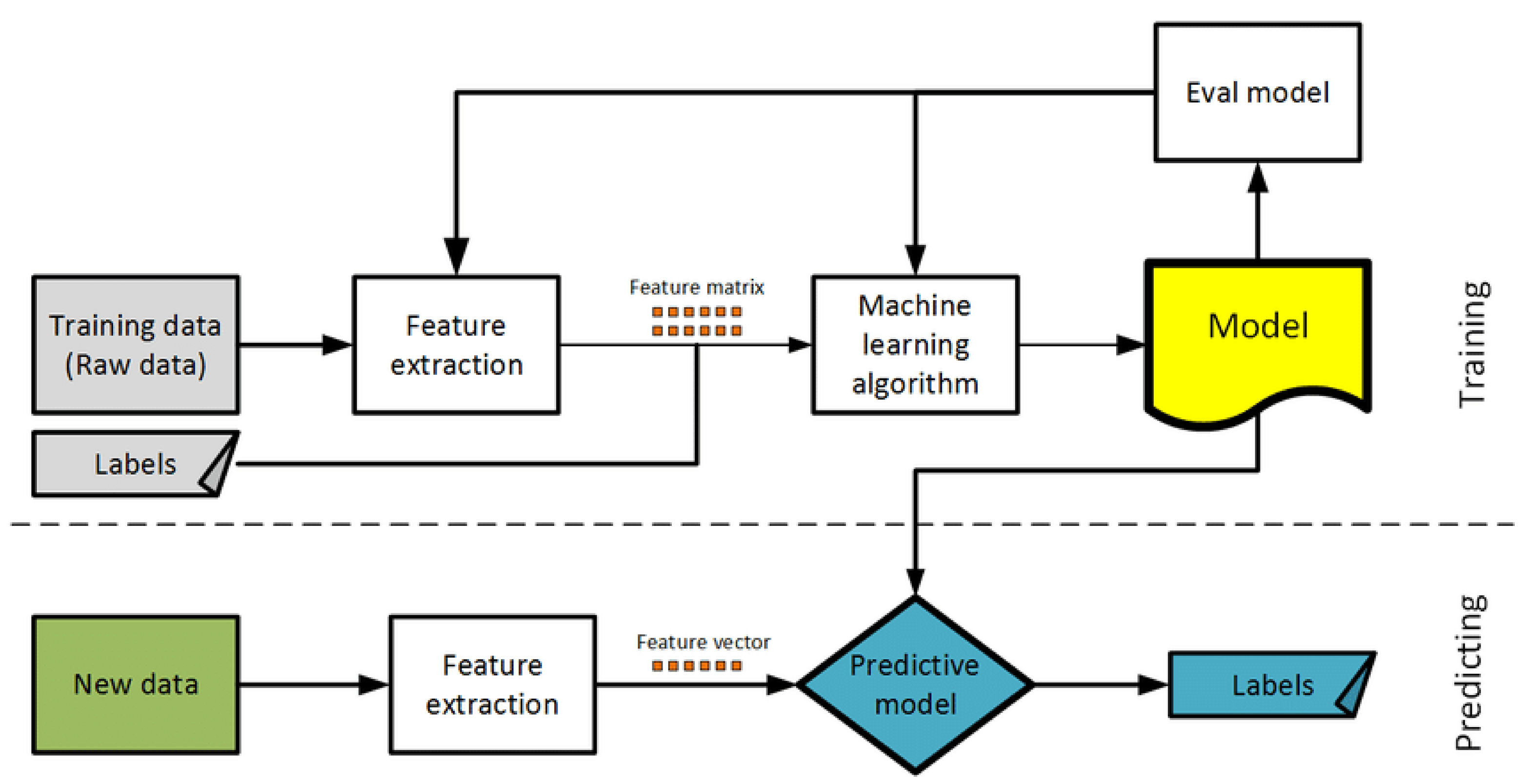


Figure 2. Machine learning model flowchart

Model Evaluation

Four metrics were used to evaluate the performance of the models: accuracy, precision, recall, and F1 score. These metrics were chosen because they provide the best picture of how well the models are predicting regular or irregular activity in the power grid dataset.

ACTUAL VALUES	POSITIVE	NEGATIVE
POSITIVE	TP	FN
NEGATIVE	FP	TN

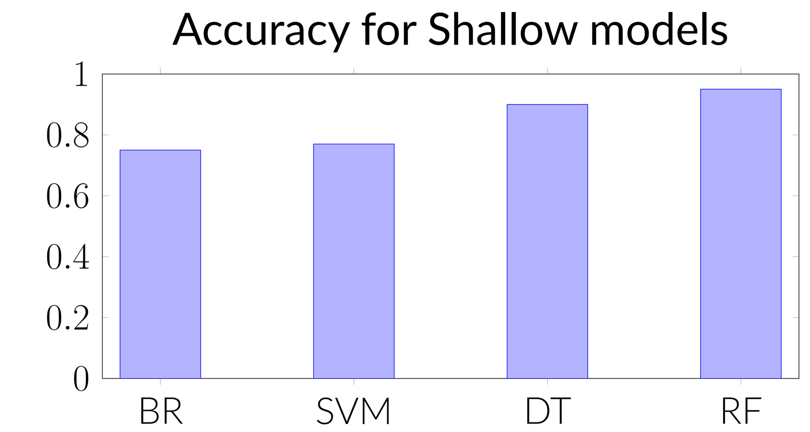
$$Precision = \frac{TP}{TP + FP} \qquad Recall = \frac{TP}{TP + FN}$$

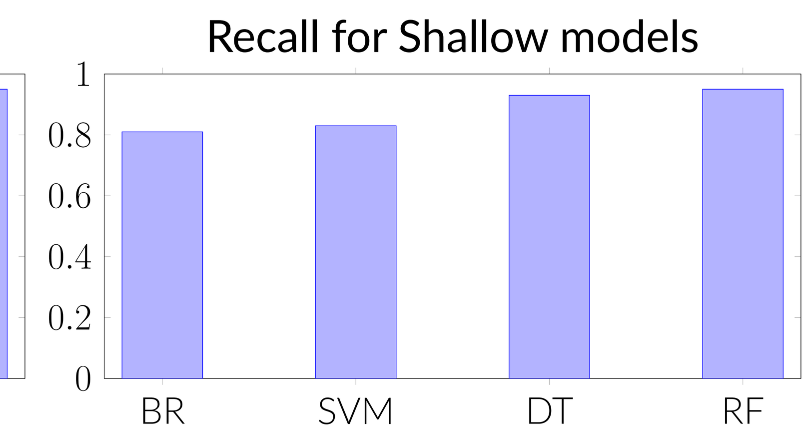
$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Figure 3. Calculation of accuracy, precision, recall, and F1 score

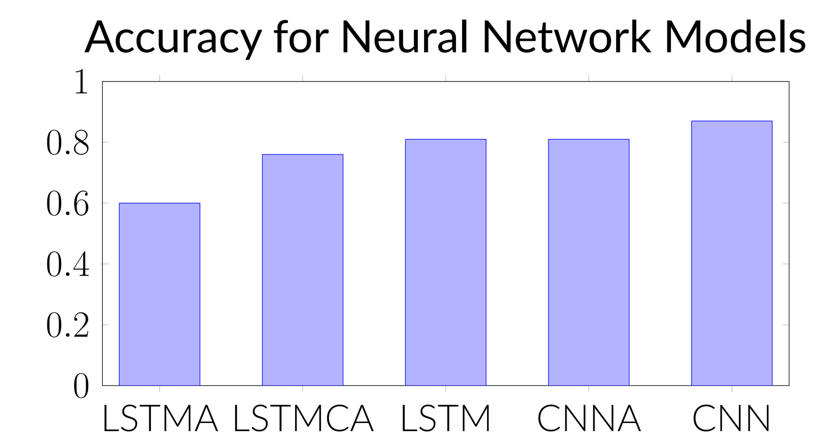
Shallow Learning Model Results

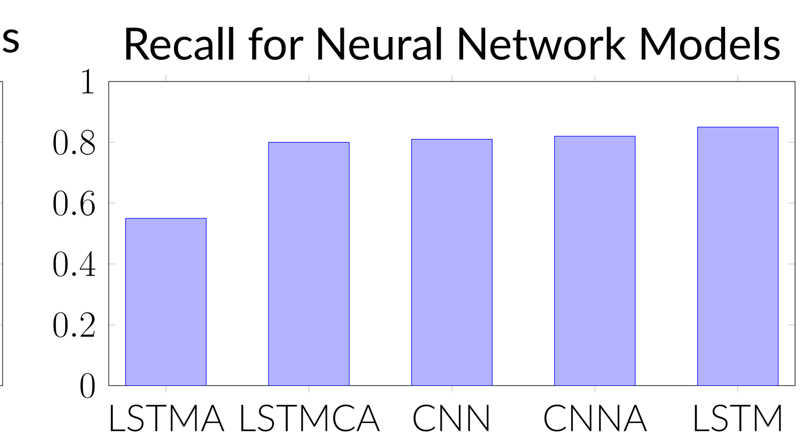




Notes: SVM = Support vector machine, RF = Random forest, DT = Decision tree, BR = Bayesian ridge

Neural Network Model Results





Notes: LSTM = Long short-term memory model, LSTMA = Long short-term memory model w/ autoencoder, LSTMCA = Long short-term memory model w/ CNN autoencoder, CNN = Convolutional neural network model, CNNA = Convolutional neural network model w/ autoencoder

Conclusion and Implications

For the shallow learning models, the random forest model performed the best as it had a higher accuracy and recall than all the other shallow models. This indicates that in a real world scenario, the random forest model would likely work the best in detecting FDIAs. For the neural network models, the CNN, CNNA, and LSTM performed the best as those three had the highest accuracy and recall out of the neural network models. Again, in a real world scenario, these models would likely be the best in detecting FDIAs.

References

Acknowledgements

I would like to express my gratitude to Md Rakibul Ahasan and Abdulrahman Takiddin, along with all the other members of the cyber-physical machine learning lab, for their contributions to this research.

lem24a@fsu.edu