

Machine Learning to Detect Cyber-Attacks and Discriminating the Types of Power System Disturbances

Diane Tuyizere^{1*} and Remy Ihabwikuzo²

Carnegie Mellon University Africa Kigali, Rwanda

*Corresponding Author

Diane Tuyizere, Carnegie Mellon University Africa Kigali, Rwanda.

Submitted: 2023, July 10; Accepted: 2023, Aug 23; Published: 2023, Sep 28

Citation: Tuyizere, D., Ihabwikuzo, R. (2023). Machine Learning to Detect Cyber-Attacks and Discriminating the Types of Power System Disturbances. *J Electrical Electron Eng*, 2(3), 328-331.

Abstract

This research proposes a machine learning-based attack detection model for power systems, specifically targeting smart grids. By utilizing data and logs collected from Phasor Measuring Devices (PMUs), the model aims to learn system behaviors and effectively identify potential security boundaries. The proposed approach involves crucial stages including dataset pre-processing, feature selection, model creation, and evaluation. To validate our approach, we used a dataset used, consist of 15 separate datasets obtained from different PMUs, relay snort alarms and logs. Three machine learning models: Random Forest, Logistic Regression, and K-Nearest Neighbour were built and evaluated using various performance metrics. The findings indicate that the Random Forest model achieves the highest performance with an accuracy of 90.56% in detecting power system disturbances and has the potential in assisting operators in decision-making processes.

Keywords: Machine Learning, Cyber-attack

1. Introduction

Although Cyber-physical system has many advantages in areas such as power distribution grids and wastewater treatment plants, it also has some disadvantages and threats. A smart grid is an electrical grid equipped with automation, communication, and information technology systems that can monitor power flows from points of generation to points of consumption [1]. If these systems fail, it can result in massive damage or loss to people as well as the shutdown of all infrastructure.

Nowadays, most businesses have regulations and policies in place to ensure their security. Phasor Measurement Units (PMUs) have been used to increase system performance as power systems become increasingly complex in their architecture [2]. It provides information that can help to make quick decisions. Hackers, on the other hand, can create a trigger that will cause the system to fail and cause significant damage to smart grids. Machine learning techniques can be used to find pattern recognition, learning abilities, and rapid identification of potential security boundaries [3]. This paper proposes a machine learning approach for detecting system behaviors by learning from historical data and relevant information. Mainly we present a machine learning-based attack detection model for power systems that can be taught using data and logs collected by PMUs.

To accomplish this, the dataset was preprocessed, for model selection, 10-fold cross-validation was used to build a random forest, logistic regression, and k-Nearest neighbor models, and the results were compared using four performance metrics: f1

macro, recall, accuracy, and precision scores. Furthermore, feature selection was performed, and the results were compared to models without feature selection; the best model found was Random Forest, and finally, optimization of the best model was performed.

The structure of this paper is as follows: Section 2 provides an overview of related research in the field. In Section 3, we detail our proposed approach by highlighting the conducted data processing, model building, testing various machine learning methods, and experimental results as well as discussing the findings. Lastly, Section 4 offers concluding remarks.

2. Literature Review

Smart grids, are vulnerable to cyber-attacks due to their reliance on automation, communication, and information technology systems. Hackers target these systems to disrupt the power supply, cause damage, or gain unauthorized access to critical infrastructure. As highlighted the consequences of successful attacks on power systems can be severe, leading to widespread power outages, financial losses, and even endangering public safety. Therefore, there is an urgent need for effective detection and mitigation strategies to protect power systems from cyber threats.

Machine learning techniques have emerged as promising approaches for enhancing the security of power systems. These techniques offer the ability to analyze large volumes of data, detect patterns, and identify anomalies indicative of potential attacks [4]. Phasor Measurement Units (PMUs) play a crucial

role in this context, as they provide real-time data on power system dynamics, enabling the development of accurate machine learning models [5]. By leveraging historical data and logs collected by PMUs, these models can learn system behaviors and detect deviations that may indicate cyber-attacks.

Several intrusion detection systems (IDS) approaches have been proposed for smart grid security, including anomaly-based detection techniques, communication traffic analysis, and leveraging power system theories. However, these approaches have limitations in terms of detecting different types of attacks, scalability, and capturing invalid changes in the physical system.

In this study, our goal is to utilize machine learning to detect cyber-attacks and accurately classify different types of power system disturbances. We hypothesize that machine learning algorithms can effectively detect disturbances and classify potential security threats in power systems. By addressing the limitations of existing approaches and harnessing the power of machine learning, we aim to enhance the security and resilience of power systems against cyber-attacks.

3. Proposed Approach

3.1 Dataset

The dataset downloaded was about power system disturbance. It was made up of 15 separate datasets that were collected and recorded by PMUs 1–4, relay snorts alarms, and logs. Each has 129 columns, and the target attribute was having three classes such as No event, Natural, and Attack as shown in Figure 1.

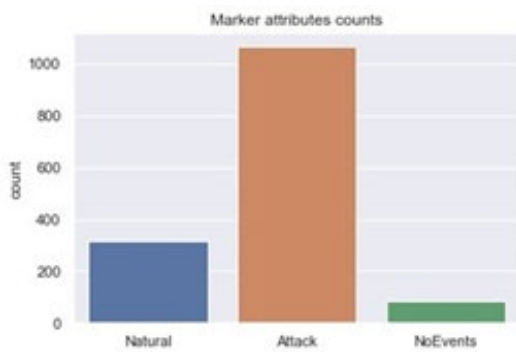


Figure 1: Graph Shows the Number of Each Category

All columns were numerical except target attributes which were categorical. Moreover, the total number of observations of all datasets was 73037. After combining all datasets 2 % from all datasets was collected for this experiment. In the dataset, there were no duplicates or missing values found. However, infinity values were found, and the outlier was detected by using Isolation Forest and Principal component analysis was used to visualize the detected outliers Figure 2.

4. Data Preprocessing and Preparation

To prepare the dataset for analysis, several preprocessing steps were performed. Firstly, any infinity values present in the dataset were eliminated. Additionally, outliers were identified using the

Isolation Forest algorithm and subsequently removed. To handle non-numerical values, a label encoder was applied to convert them into numerical representations. Moreover, as observed in Figure 1, the dataset.

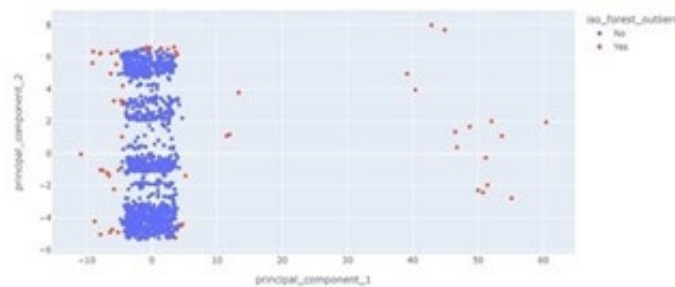


Figure 2: PCA for Normal and Outliers in the Dataset

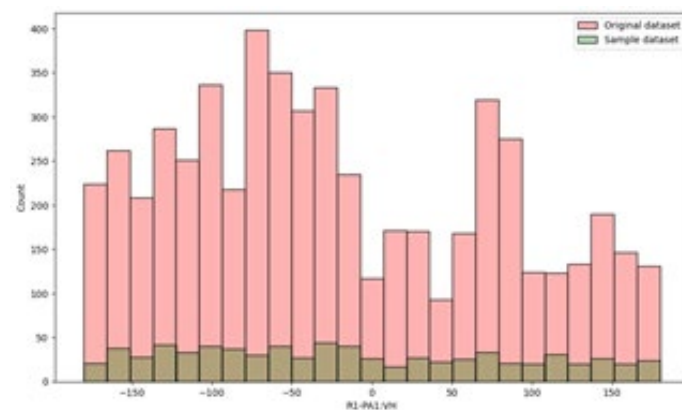


Figure 3: Distribution of the Sampled and Original Dataset

Exhibited class imbalance. To address this issue, the Synthetic Minority Oversampling Technique (SMOTE) was employed to augment the samples in the minority class. Lastly, to ensure uniformity in the dataset, standardization was carried out by scaling all the features using standard scalers.

5. Exploratory Data Analysis and Data Visualization

To explore the data and understand the pattern among features. The distribution of each feature was examined, and an example was presented in Figure 3 using a histogram. The distribution of the RI-PA1:VH feature closely resembled that of the original dataset, indicating that this particular sample serves as a representative example of the overall dataset.

Furthermore, correlation analysis was performed to assess the relationships between the features and the target variable. The results were presented in Figure 4, showcasing the most correlated variables. It was found that the top 14 features exhibited strong correlations with the target variable. This suggests that these features hold valuable information and have a significant impact on predicting the target variable. The correlation analysis aids in selecting the most relevant features for subsequent modeling and analysis, ensuring that the chosen variables capture important patterns and relationships within the dataset.

R2-PA6: IH	0.085646
R3-PA6: IH	0.080989
R2-PM1: V	0.064549
R2-PM7: V	0.058754
R2-PM2: V	0.051900
R3-PM1: V	0.051511
R2-PM12: I	-0.052484
R2-PM11: I	-0.053124
R1-PA6: IH	-0.054157
R3-PA: ZH	-0.054255
R2-PA: ZH	-0.055303
R4-PA3: VH	-0.057977
R4-PA6: IH	-0.058016
R1-PA3: VH	-0.060139

Figure 4: The Best 14 Features Which are Very Correlated to the Marker

6. Model Creation and Evaluation

Three machine learning models, namely Random Forest, Logistic Regression, and K-Nearest Neighbor, were constructed for analysis. To evaluate the performance of each model, 10-fold cross-validation was applied, ensuring robustness and reliable results. Various metrics were used to assess the models, including F1 macro, Precision macro, Recall macro, and Accuracy. Since the dataset underwent resampling to address the class imbalance, these metrics were particularly relevant in evaluating the models' performance on the balanced dataset.

To determine the impact of feature selection on model performance, the comparison among models was conducted both on the full set of features and after feature selection. The feature selection method employed was mutual information, which measures the dependency of features on the target value. This approach assists in identifying the most informative and relevant features for accurate predictions.

Based on the comparison, the Random Forest model emerged as the best-performing model. Subsequently, hyperparameter tuning was carried out to optimize the selected features. The parameters adjusted during hyperparameter tuning included the number of trees, maximum depth, and criterion selection. By fine-tuning these parameters, the Random Forest model can be optimized to achieve the best possible performance and accuracy for the specific task at hand.

7. Experiments Results

In general, certain features within the dataset were found to exhibit a high correlation with each other, as illustrated in Figure 4. Notably, features such as 'R3-PM9:V', 'R2-PM9:V', 'R4-PM1:V', and 'R3-PM8:V' displayed a strong correlation. However, when considering the correlation between these features and the target variable, the relationship was relatively weaker.

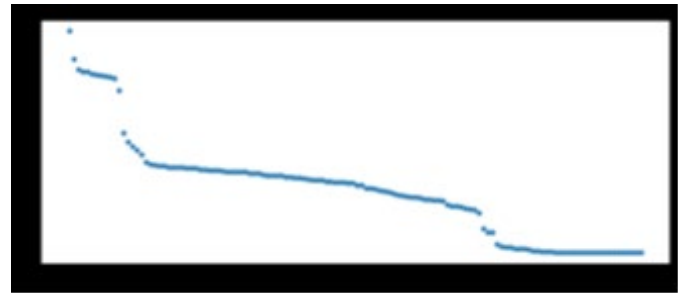


Figure 5: Information Gain for Each Feature

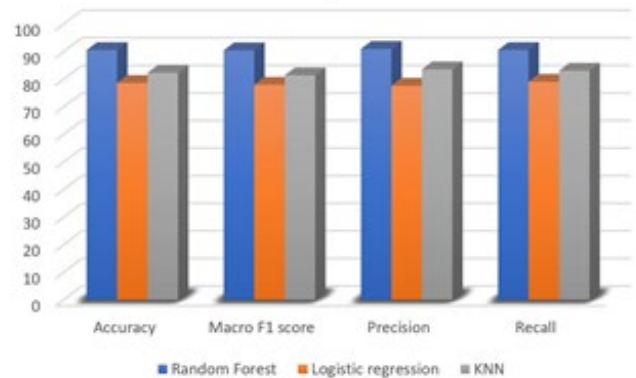


Figure 6: The Models' Performance without Feature Selection

Additionally, a comparison was conducted among the KNearest Neighbor (KNN), Random Forest, and Logistic Regression models. The results demonstrated that the Random Forest model performed the best, achieving an F1 macro score of 90.46%, an accuracy of 90.56%, a precision macro score of 90.97%, and a recall macro score of 90.57%. Figure 6 provides a visual representation of these findings. The second-best performing model was the KNN model, although the specific metrics associated with its performance were not mentioned in the provided context.

Furthermore, the Mutual Information technique was utilized to select the best features from the dataset. Figure 5 illustrates the scores assigned to each feature based on their relevance. From this analysis, the top 40 features with the highest scores were selected for further modeling.

Using these selected features, the same machine learning algorithms were constructed and compared once again. The performance of each model was evaluated using metrics such as F1 score, precision, recall, and accuracy, Figure 7. Notably, the Random Forest (RF) model demonstrated strong performance, achieving a Macro F1 score of 86.16%.

Surprisingly, when comparing the model built with feature selection to the one without, it was found that the model utilizing all features performed better. This unexpected result could be attributed to the potential overfitting of the data since we only used a subset of features.

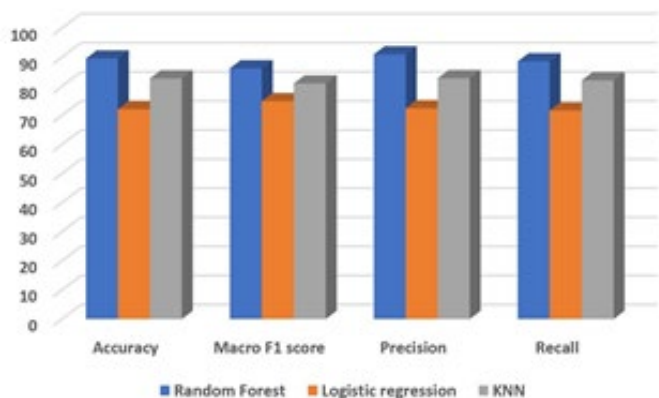


Figure 7: Comparison of the performance of the models with FS

Additionally, it was observed that the Logistic Regression model did not perform well in this analysis, indicating that it may not be suitable for capturing the complexities present in the dataset or may require further refinement in terms of hyperparameter tuning or feature engineering. Moreover, the benchmark model found is Random Forest Figure7, then it was used for Hyperparameter tuning and the accuracy score was improved from 89.54% to 90.08%. As a result, it can be concluded that model parameters have to be optimized based on the usage scenario. The model is more sensitive to data collected in the power system and can better distinguish the situations corresponding to the data because of optimization.

8. Discussion

Previous studies have recommended the application of preprocessing techniques to improve the performance of classifiers, such as balancing the dataset [6]. These findings align with the results obtained in the current study, which also demonstrate that Random Forests exhibit strong precision performance [7]. Furthermore, when comparing different algorithms, the tree-based algorithm Random Forest outperforms KNN and Logistic Regression.

According to Junejo and Goh, the success of the Random Forest algorithm can be attributed to the fact that the Programmable Logic Controller (PLC) used in power systems is programmed using relational ladder logic. Ladder logic is a rule-based language that executes rules in sequential order, resembling a control logic system. The tree-based algorithms, including Random Forest, attempt to relearn this control logic or understand the normal behavior of the system. This compatibility between the underlying logic of the power system and the tree-based

algorithms could explain the superior performance of Random Forest in this context.

9. Conclusion

This report utilizes Random Forest, KNN, and Logistic Regression machine learning algorithms to detect power system disturbance. All the approaches used for evaluating models showed that random forest remained the best algorithm among others; therefore, it is recommended to be used for classifying the scenarios related to detecting cyberattacks and controlling system operations. However, an increased amount of data may increase accuracy and time complexity. Moreover, as a recommendation, deep learning and big data can be integrated for future work.

References

1. Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014, August). Machine learning for power system disturbance and cyber-attack discrimination. In 2014 7th International symposium on resilient control systems (ISRC) (pp. 1-8). IEEE.
2. Hadeli, H., Schierholz, R., Braendle, M., & Tudu, C. (2009, September). Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration. In 2009 IEEE Conference on Emerging Technologies & Factory Automation (pp. 1-8). IEEE.
3. Dondossola, G., Szanto, J., Masera, M., & Nai Fovino, I. (2008). Effects of intentional threats to power substation control systems. International journal of critical infrastructures, 4(1-2), 129-143.
4. Mitchell, R., & Chen, R. (2013). Behavior-rule based intrusion detection systems for safety critical smart grid applications. IEEE Transactions on Smart Grid, 4(3), 1254-1263.
5. Thomas, H., Morris, Shengyi, Pan., Jeremy, Lewis., Jonathan, Moorhead., Nicolas, H., Younan, Roger, L. King., Mark, Freund., and Vahid, Madani. (2011). Cybersecurity risk testing of substation phasor measurement units and phasor data concentrators. In Cyber Security and Information Intelligence Research Workshop.
6. Ten, C. W., Hong, J., & Liu, C. C. (2011). Anomaly detection for cybersecurity of the substations. IEEE Transactions on Smart Grid, 2(4), 865-873.
7. Zhang, Y., Wang, L., Sun, W., Green II, R. C., & Alam, M. (2011). Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid, 2(4), 796-808.

Copyright: ©2023 Diane Tuyizere, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.