Northeast Journal of Complex Systems (NEJCS)

Volume 6
Number 1 *Special Issue: NERCCS 2024 Papers*

Article 2

June 2024

Enhancing Electrical Network Vulnerability Assessment with Machine Learning and Deep Learning Techniques

M Mishkatur Rahman
North Dakota State University, mmishkatur.rahman@ndsu.edu

Ayman Sajjad Akash
North Dakota State University, ayman.akash@ndsu.edu

Harun Pirim
North Dakota State University, harun.pirim@ndsu.edu

Chau Le
North Dakota State University, chau.le@ndsu.edu

Trung Le
University of South Florida, tqle@usf.edu

See next page for additional authors

Recommended Citation

Rahman, M Mishkatur; Akash, Ayman Sajjad; Pirim, Harun; Le, Chau; Le, Trung; and Yadav, Om Prakash (2024) "Enhancing Electrical Network Vulnerability Assessment with Machine Learning and Deep Learning Techniques," *Northeast Journal of Complex Systems (NEJCS)*: Vol. 6 : No. 1 , Article 2.
DOI: 10.22191/nejcs/vol6/iss1/2
Available at: https://orb.binghamton.edu/nejcs/vol6/iss1/2

Enhancing Electrical Network Vulnerability Assessment with Machine Learning and Deep Learning Techniques

Authors

M Mishkatur Rahman, Ayman Sajjad Akash, Harun Pirim, Chau Le, Trung Le, and Om Prakash Yadav

Enhancing Electrical Network Vulnerability Assessment with Machine Learning and Deep Learning Techniques

M Mishkatur Rahman[1], Ayman Sajjad Akash[1], Harun Pirim[1*],
Chau Le[2], Trung (Tim) Q. Le[3] and Om Prakash Yadav[4]

[1]Dept. of Industrial and Manufacturing Engineering, North Dakota State University, Fargo, ND, USA

[2]Dept. of Civil, Construction and Environmental Engineering, North Dakota State University, Fargo, ND, USA

[3]Dept. of Industrial and Management Systems Engineering, University of South Florida, Tampa, FL, USA

[4]Dept. of Industrial and Systems Engineering, North Carolina A&T State University, Greensboro, NC, USA

[*]Corresponding Author: harun.pirim@ndsu.edu

Abstract

This research utilizes advanced machine learning techniques to evaluate node vulnerability in power grid networks. Utilizing the SciGRID and GridKit datasets, consisting of 479, 16,167 nodes and 765, 20,539 edges respectively, the study employs K-nearest neighbor and median imputation methods to address missing data. Centrality metrics are integrated into a single comprehensive score for assessing node criticality, categorizing nodes into four centrality levels informative of vulnerability. This categorization informs the use of traditional machine learning (including XGBoost, SVM, Multilayer Perceptron) and Graph Neural Networks in the analysis. The study not only benchmarks the capabilities of these models in network analysis but also explores their potential in identifying critical nodes using features beyond centrality metrics alone, enhancing their applicability in real-world scenarios. The research addresses a significant gap in effectively assessing the vulnerability of electrical networks, marked by isolated use of traditional centrality metrics and a lack of integration between these combined metrics with both tradiational and advanced machine learning models. The study integrates various centrality measures into a comprehensive metric and advocates for the application of advanced machine learning models, particularly GNNs. It underscores the need for larger and more complex datasets to unlock the full potential of GNNs in network vulnerability assessments. By comparing the performance of GNN models with traditional machine learning approaches across datasets of different sizes and complexities, the study provides insights into optimizing model selection for network analysis, thereby contributing significantly to the field of network vulnerability assessment.

1 Introduction

The term ”vulnerability” has its origins in a political academic concept, referring to the potential outcomes of system changes within an interdependent system. It suggests that both large-scale organizations and independent individuals have inherent weaknesses, making vulnerabilities inevitable [1]. The idea of vulnerability was initially introduced in research on natural disasters by scholar Timmerman in [2], and has since expanded into various fields including network research such as the internet[3], transportation[4], [5], and power systems[6]. In one study, an indicator for assessing system vulnerability against DoS attacks on the internet was introduced[7]. This indicator was then utilized to evaluate commonly used data structures within network mechanisms. In the realm of electrical network analysis, the assessment of power grid network vulnerabilities is of paramount importance. These networks, crucial for sustaining societal and industrial functions, directly impact community resilience and economic stability [8]. The complexity of power grids and the critical need for a reliable power supply underscore the importance of accurate vulnerability assessments. The advances in machine learning offers new perspectives in network vulnerability analysis. Conventional approaches to evaluating the susceptibility of electrical networks, such as stochastic modeling, converting bi-level to single-level optimization problems, employing algorithms for constraint and column generation, utilizing Benders decomposition, conducting system reliability assessments, and implementing evaluations based on Acyclic Oriented Electrical Network (AOEN) structures, often do not fully encompass the intricate dynamics of power grid networks [9], prompting the need for more innovative and computational approaches [10]. Machine learning, with its capacity to process large datasets and identify intricate patterns, stands as a promising tool to enhance the accuracy and depth of these assessments.Past studies often used machine learning in isolation, relying on traditional centrality metrics that may not fully capture the complex dynamics of power grids. This approach overlooks the interconnected and nonlinear characteristics of nodes, potentially leading to less effective vulnerability assessment. The need for this research stems from the limitations in dataset size and complexity, which may restrict the effectiveness of more sophisticated models like GNNs, and the lack of integration between combined centrality metrics and advanced machine learning techniques.

The purpose of this research is to improve the evaluation of power grid node vulnerability by utilizing machine learning and deep learning models. Our goal is to increase the precision with which network vulnerabilities are identified by utilizing machine learning’s capacity to recognize intricate patterns in large datasets. Notably, XGBoost performed the best out of all the models examined. However, we see tendency of GNNs to perform better on larger datasets.

https://orb.binghamton.edu/nejcs/vol6/iss1/2
DOI: 10.22191/nejcs/vol6/iss1/2

The contributions of this study are pivotal for advancing the field of power grid vulnerability assessment. We used two datasets, a small and a larger one, to test models across varying network complexities also explored distinct methodologies for addressing missing data. By comparing traditional machine learning and deep learning, our research analyzes complex interdependencies and nonlinear behaviors in power grids. Additionally, the integration of entropy-weighted centrality scores with these models has refined our ability to pinpoint critical network nodes, thus improving predictive accuracy and operational reliability in real-world scenarios.

2 Literature Review

The assessment of power grid network vulnerabilities has been an area of extensive research, given the critical role these networks play in modern society. Studies have primarily focused on identifying key nodes whose failure could cause significant disruptions. Traditional approaches have often utilized centrality metrics such as betweenness, degree, and PageRank to determine the importance of nodes within these networks [11]. However, a notable gap in the literature is the isolated use of these centrality metrics, which may not comprehensively capture the complex dynamics of networks [12]. This limitation has motivated our research to explore more holistic methods that integrate various centrality measures into a unified metric. Our study builds upon the work of[13], which discusses an entropy-weighted Combined Centrality Score (CCS). This approach synthesizes betweenness, degree, and PageRank metrics, offering a more inclusive view of node significance. This method addresses the shortcomings of using single centrality metrics, as identified in previous studies [12]. Recent progress in machine learning, particularly in the realm of Graph Neural Networks (GNNs), has created novel opportunities for conducting network analysis [14]. These methods have shown potential in identifying critical nodes using complex patterns within network data, which traditional statistical approaches may overlook. A critical analysis of existing methodologies reveals a lack of integration between traditional network analysis techniques and advanced machine learning models.Traditional centrality metrics offer valuable insights into power grid dynamics; however, they often overlook the non-linear and interconnected characteristics inherent in power grids. In contrast, machine learning models, particularly Graph Neural Networks (GNNs), demonstrate the capability to capture and analyze the complex interdependencies and non-linear behaviors within power grids[15]. In aligning with our research objectives, this study aims to bridge this gap by combining the robustness of traditional centrality metrics with the advanced analytical capabilities of machine learning. By doing so, we contribute to the development of more comprehensive tools for vulnerability assessment in power grid networks.

3 Network System Description

Our study uses the SciGRID dataset version 0.2, which provides a detailed layout of the European electrical transmission network with 479 nodes and 765 edges. This effort is supported by the German Federal Ministry of Education and Research[16] and is focused on creating automated models for the European electrical grid to aid various research areas.

We also draw on the GridKit network model, which comes from OpenStreetMap data, to examine the North-American high-voltage power grid[17]. This model was put together by the Next Energy research institute as part of the SciGRID project and is particularly useful for analyzing power system operations and planning. The GridKit model offers a comprehensive view with its 16,167 nodes and 20,539 edges.

Our aim with these tools is to predict the vulnerability of particular spots within these power networks, even when we don't have all the details about the network's setup, like how everything is connected or the importance of certain points. Our findings are meant to help make the power networks, especially in the U.S., more reliable by pinpointing and planning for potential weak spots. These datasets are key to our work, giving us a broad overview of power networks across Europe and North America.

3.1 Nodes and Edges:

The transmission network is represented by graph $G = (N, E)$. The network's topology, defined by these nodes N and edges E, offers insights into the operational dynamics of the power grid. The nodes in the dataset represent electrical substations or power stations, crucial for the distribution of electrical power. The edges denote the transmission lines, interconnecting these nodes.

3.2 Centrality Metrics

The importance of each node is assessed using several centrality metrics:

Degree Centrality (C_D):

$$C_D(v) = \frac{\deg(v)}{|N| - 1} \tag{1}$$

where $\deg(v)$ is the degree of node v and $|N|$ is the total number of nodes.

PageRank Centrality (C_P):

$$C_P(v) = \frac{1 - d}{|N|} + d \sum_{u \in B_v} \frac{C_P(u)}{L(u)} \tag{2}$$

where B_v is the set of nodes linking to v, $L(u)$ is the number of links from node u, and d is the damping factor[11].

Betweenness Centrality (C_B):

$$C_B(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3}$$

where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths passing through v .

4 Node Importance

A key focus of this research is identifying critical nodes within power grid networks. Traditional centrality metrics such as betweenness, degree, and PageRank have been widely used in assessing the significance of nodes in networks. Betweenness centrality quantifies the frequency at which a node appears on the shortest paths between other nodes, indicating its role in controlling information flow. Degree centrality measures the number of direct connections a node has, reflecting its immediate influence. PageRank, a concept developed by Google researchers, evaluates the significance of nodes in a network by considering two main factors: the quantity and quality of incoming edges. Nodes with a higher number of incoming edges are deemed more crucial. Moreover, the influence of these nodes is further enhanced if the incoming edges originate from nodes that are themselves highly ranked by PageRank, thus recognizing the nodes' prominence within the overall structure. Additionally, the PageRank algorithm takes into account the distribution of a node's influence through its outgoing links. A node's PageRank is divided equally among its outgoing links, meaning that a node linking to many others spreads out its influence more thinly, as opposed to concentrating it on a few nodes. This balance between a node's incoming and outgoing links is central to calculating its PageRank, ensuring that a node's significance is determined not just by how many, but also by how important its connections are. However, these metrics individually may not capture the multifaceted aspects of node importance comprehensively. To address this limitation, our study adopted the formula of an entropy-weighted Combined Centrality Score (CCS), as described in [18] in which we implemented different centrality metrics for our analysis. This CCS amalgamates betweenness, degree, and PageRank into a single score, offering a more holistic view of node vulnerability and significance within the network. By leveraging entropy as a weighting mechanism in the CCS, we aim to quantify the inherent uncertainty and information diversity of network nodes.

Entropy can be defined as a fundamental measure of unpredictability or information content within a system. We used the Shannon Entropy formula to merge centrality metrics.

Shannon Entropy Formula: The Shannon entropy of a discrete random variable X with possible values $\{x_1, x_2, \ldots, x_n\}$ and probability mass function $p(x)$ is defined as:

$$E(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) \tag{4}$$

Here x_i would be a specific centrality value (like a node having a degree of 4), and $p(x_i)$ would be the proportion of nodes in the network that have that specific centrality value. This formula, denoted as $E(X)$ representing Shannon Entropy, is a fundamental concept in information theory, used to quantify the uncertainty or complexity in a data set [19].

Weights for Centrality Measures: The weight ω_j for each centrality measure is calculated as:

$$\omega_j = \frac{1 - E_j}{3 - (E_D + E_P + E_B)} \tag{5}$$

Here we have entropy measures E_D, E_P, E_B for degree, PageRank, and betweenness respectively where ω_j represents the weight for each centrality measure, based on their entropy values. Here, j is an index over the centrality measures.

Combined Centrality Score:

$$C_{\text{combined}} = \omega_1 C_D + \omega_2 C_P + \omega_3 C_B \tag{6}$$

C_D, C_P, C_B are centrality measures for degree, PageRank, and betweenness respectively. This equation defines the Combined Centrality Score, indicating the significance of a node within the network based on weighted centrality metrics[18].

We use combined centrality scores to label centrality, vulnerability level of transmission network nodes followed by training machine learning models, including traditional ones and graph neural networks (GNNs). Their performance in detecting critical nodes with node and edge features are evaluated. This innovative approach aims to extend the utility of machine learning models in real-world scenarios beyond the limitations of conventional centrality metrics. In conclusion, this research benchmarks the capabilities of both traditional and advanced machine learning models in assessing the vulnerability of electrical networks and contributes

to the development of more resilient power infrastructure through refined analytical methods.

5 Methodology

The robustness of electrical networks is paramount, particularly because their components are susceptible to failure from natural disasters, human errors, or malicious attacks. Such failures can propagate through the network, causing widespread disruption due to the interconnected nature of its elements—a phenomenon known as the cascading effect. Within the framework of graph theory, these components are represented as nodes, and identifying those that are critical is essential for maintaining network integrity. Ensuring these nodes receive adequate protection or reinforcement is crucial to mitigate the risk of cascading failures [20].

Addressing the challenge of predicting node criticality is compounded by the scarcity of comprehensive data and the intricacies of the factors involved. Therefore, the development of a predictive model leveraging the topological characteristics of the electrical network, alongside any available functional attributes, is essential. Advanced machine learning makes it is possible to anticipate the vulnerability of these critical nodes and implement preemptive strategies to safeguard the electrical network.

Our methodology employs both classical machine learning (CML) and graph neural networks (GNN) to evaluate the vulnerability of electrical transmission systems. The process begins with data collection, focusing on node and edge information from a publicly accessible source. Using Python NetworkX library, a weighted directed network is constructed, facilitating the calculation of various centrality measures: degree centrality, PageRank centrality, and betweenness centrality [21]. These metrics are amalgamated into a combined centrality score using the Shannon entropy method.

Afterwards, each node in the network is assigned one of the four criticality levels: low, moderate, high, and severe, assigned based on the combined criticality scores and CML and GNN algorthims are used to predict this level for specific node in later portion of the study. To augment the limited node features in the dataset, additional features are generated from the network topology. Subsequently, three CML algorithms—XGBoost, Multilayer Perceptron Neural Network, and SVM—are implemented. Hyperparameters for each algorithm are optimized through grid search with cross validation.

In the next phase, both node and edge features are processed through various GNN algorithms. These algorithms include Graph Neural Network (GNN), Graph Convolutional Network (GCN), and Graph Attention Network (GAT). To implement these algorithms, the PyTorch Geometric library is utilized, a widely rec-

ognized and efficient framework for graph-based deep learning tasks within the PyTorch ecosystem [22]. This library provides optimized and user-friendly implementations of GNN, GCN, and GAT models, facilitating the effective application and comparison of these techniques in our study. After evaluating these models, the most effective GNN algorithm is identified for comparison with classical ML algorithms. Python is employed throughout this research, known for its extensive libraries and tools conducive to machine learning and network analysis [23]. The main steps of the proposed methodology are shown in figure 1.

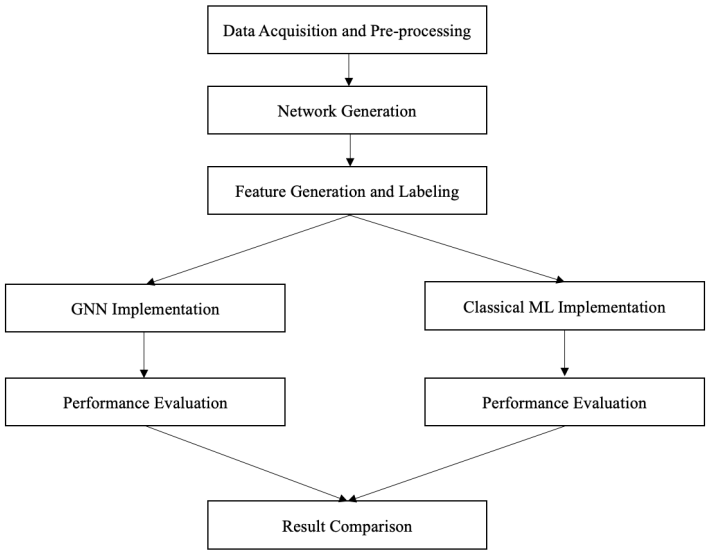

Figure 1: Main Steps of the Proposed Methodology.

5.1 Data Description and Preprocessing

Our methodology was implemented in two datasets. The first one was obtained from the SciGRID project, which focuses on the automated creation of models for electricity grids, serving research and related applications. The second dataset utilized in our study is sourced from GridKit. Both the dataset are similar in their structure and divided into two key components: vertices and edges, symbolizing the nodes and their interconnections within the electrical network. The dataset description is provided in Table 1.

Table 1: Node and Edge data description from the dataset

Variable Index	Variable	Description	Dataset
1	v_id	Unique identifier for the vertex (node)	Node
2	lon	Longitude of the node	Node
3	lat	Latitude of the node	Node
4	typ	Type of node, e.g., substation	Node
5	voltage	Voltage level(s) at the node, multiple separated by semicolon	Node
6	geom	Geometric information, typically coordinates in WKT format	Node
7	l_id	Unique identifier for the edge (line)	Edge
8	v_id_1	Identifier for the starting vertex of the edge	Edge
9	v_id_2	Identifier for the ending vertex of the edge	Edge
10	voltage	Voltage level of the edge	Edge
11	cables	Number of cables in the edge	Edge
12	wires	Number of wires in the edge	Edge
13	frequency	Operating frequency of the edge	Edge
14	length_m	Length of the edge in meters	Edge
15	r	Resistance of the edge	Edge
16	x	Reactance of the edge	Edge
17	c	Capacitance of the edge	Edge
18	i_th_max	Maximum thermal current limit of the edge	Edge
19	geom	Geometric information, typically line coordinates in WKT format	Edge

The vertices dataset encompasses essential information about the nodes in the electrical network and edges dataset includes essential features of the electrical lines. A directed network was built by utilizing an edge list that incorporates the voltage of each line as the weights for individual links within the network. Additionally, we computed network centrality measures like degree centrality, PageRank, and betweenness centrality.

A Shannon entropy-based method was then applied to these centrality measures to assign criticality levels to the nodes. The edges dataset provides detailed information about the connections between nodes. Like the vertices, these were incorporated into our graph model, adding depth to our network analysis.

In the preprocessing phase, the 'geom' column, which contained spatial data in Well-Known Binary (WKB) format, from both datasets. This exclusion was done to streamline the data for machine learning analysis, as this spatial information was not relevant to our specific study objectives focused on network structure and electrical characteristics. The vertices dataset had missing entries in the voltage column, which were handled through median imputation. This approach is effective for addressing missing numerical data and maintaining the data's central tendency [24]. Where multiple voltage values were present, we selected the maximum value to assume maximum capacity.

The edge dataset presented missing values in several columns (wires, r, x, c, i_th_max), which we imputed using the k-Nearest Neighbors (kNN) algorithm. This method ensures data consistency by utilizing the similarity patterns within the dataset [25].

Table 2: Node features used for CML and GNN

Feature Index	Feature Name	Description
1	lon	Longitude of the node
2	lat	Latitude of the node
3	typ	Type of node, e.g., substation
4	voltage	Maximum voltage level at the node
5	eigen_centrality	A measure of the influence of a node in a network
6	closeness_centrality	Proximity of a node to all other nodes in the network
7	clustering_coefficient	Degree to which nodes tend to cluster together
8	load_centrality	Distribution of shortest paths going through a node
9	avg_shortest_path_length	Average distance from the node to all other nodes in the network
10	average_neighbor_degree	Average degree of the neighborhood of a node
11	node_strength	Sum of weights of edges incident to the node

Additionally for the GridKit dataset, in addressing the absence of values in the r, x, c, and i_th_max columns, a regression model was developed leveraging the SciGRID dataset, noted for its robust and detailed data in these specific fields. Then this regression model was employed to predict the missing values in the GridKit

dataset. The application of regression analysis, a machine learning technique, allowed for precise estimation of missing data by utilizing the inherent relationships within the SciGRID dataset. This method ensured the consistency of the dataset but also aligned with the analytical demands of our study [26].

Various network centrality measures are added to existing node features for CML. For GNN approaches, the edge features were integrated to effectively capture the network's relational dynamics. Table 2 shows the node features used for the application of the CML and GNN. Apart from node attributes, all edge attributes outlined in Table 1 have been incorporated into the GNN analysis.

5.2 Assigning Criticality Levels

For both of the classification and deep learning tasks, each node within the network are assigned a criticality level, categorized into one of four classes: low, moderate, high and severe. These criticality levels serve as the target variable in this study. First, the combined criticality scores for each node is computed using equation (6) and then they are segmented into the four aforementioned categories. This segmentation is methodically executed based on the quantile distribution of the combined centrality scores. To elaborate, scores that fall at or below the 25th percentile are designated as 'Low'. Those exceeding the 25th percentile yet not surpassing the 50th percentile are deemed 'Moderate'. Scores advancing beyond the 50th percentile but remaining at or below the 75th percentile are identified as 'High'. Scores that exceed the 75th percentile threshold are classified as 'Severe'. This quantile-based approach ensures an equitable distribution of criticality levels across the dataset.

5.3 Machine Learning Algorithms

Numerous AI and machine learning algorithms are documented in the field, yet an exhaustive review of all extends beyond the scope of this research. The focus is on commonly used multi-classification algorithms renowned for superior performance. XGBoost, MLPNN, and SVM have been chosen for classical machine learning, and GNN, GCN, and GAT for graph neural network applications.

In this project, both classical ML algorithms and GNNs were utilized to analyze and compare their performance, given that the electrical network naturally forms a graph. This approach enabled to determine the most effective method for understanding and predicting vulnerabilities in the electrical grid.

5.4 CML Algorithms

Extreme Gradient Boosting (XGBoost): XGBoost is a machine learning algorithm that employs distributed gradient boosting to build gradient boosted decision trees. Renowned for its efficiency, flexibility, and portability, XGBoost excels in processing complex datasets with enhanced speed and performance, often resulting in superior analytical outcomes [27].

Multilayer Perceptron Neural Network (MLPNN): MLPNN is a type of feedforward artificial neural network characterized by its multiple layers of nodes. It is adept at recognizing complex patterns and classifying data, effectively handling non-linear relationships inherent within diverse datasets. MLPNN is implemented in many deep learning frameworks, offering robust solutions for a variety of machine learning challenges [28].

Support Vector Machine (SVM): SVM is a robust supervised learning model introduced by Vapnik [29]. It is particularly effective for both linear and nonlinear classification, capable of distinguishing between data classes by computing the optimal separating hyperplane. This feature makes SVM an invaluable tool in the domain of data categorization and is widely supported by machine learning libraries for its reliability in classification tasks.

5.5 GNN Algorithms

Graph Neural Network (GNN): GNNs are specialized neural network architectures that process data represented as graphs. These networks are adept at capturing the complex relationships and interdependencies between nodes, making them particularly useful for datasets that inherently form graphs, such as social networks, molecular structures, and more [30].

Graph Convolutional Network (GCN): GCNs represent an evolution of GNNs that incorporate the principles of convolutional neural networks to graph data. By aggregating features from a node's immediate neighbors, GCNs can effectively leverage local graph structures, enabling them to learn representations that reflect both the topology and features of the graph [31]..

Graph Attention Network (GAT): GATs further enhance the capabilities of GNNs by introducing attention mechanisms into the graph domain. This innovation allows the network to focus on the most relevant parts of the input graph dynamically, assigning varying levels of importance to different nodes within a node's neighborhood based on their contributions to the model's output. This selective focus helps in improving the predictive accuracy of the network for tasks such as node classification and link prediction [32]. The GNN codes for the study were adapted from the book [33], which provides practical techniques and architectures for construct-

ing powerful graph and deep learning applications with PyTorch.

5.6 Model Evaluation

In evaluating the models, the accuracy score was utilized as the primary metric. The accuracy score is calculated using the formula:

$$Accuracy\ Score = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ prediction} \tag{7}$$

For each model, this score was computed to assess its performance. Both of the dataset were partitioned in a 70/30 ratio, where 70% constituted the training set and the remaining 30% was used as the testing set. The training set was employed to train each model, including XGBoost, MLPNN, SVM, GNN, GCN, and GAT. Subsequently, the testing dataset, which consists of previously unseen data, was used to evaluate the models.

The accuracy score for each model was determined by comparing the model's predictions on the testing set against the actual values. This approach allowed for an objective assessment of each model's ability to accurately predict outcomes, particularly in terms of identifying critical nodes within the electrical network.

Upon evaluating the accuracy scores across various models, a feature importance analysis on the top-performing model will be conducted. This analysis will pinpoint the specific network features that significantly influence the model's predictions. By doing so, a comprehensive understanding of the key factors that shape network behavior can be developed, thereby enhancing our insights into the underlying dynamics of the model.

6 Result and Discussion

The electrical transmission system was represented as a weighted directed network, characterized by specific nodal and edge attributes. The SciGrid network comprised a total of 479 nodes and 765 edges.

Extending our methodology, we applied it to a second network, the GridKit Network, which encompasses a larger scale with 16,167 nodes and 20,539 edges. Unlike the SciGrid network, the GridKit Network was not fully connected. Consequently, we focused on the largest connected component of the GridKit Network, which contained 14,490 nodes and 20,881 edges, to maintain analytical consistency and ensure the robustness of our network analysis. Upon constructing NetworkX directed graph objects for both datasets, the edge counts were adjusted to 633 for SciGrid and 19,073 for GridKit. This modification occurred because NetworkX, by default, merges edges that share identical 'from' and 'to' node information, leading

to a consolidated representation of the networks. The construction of the SciGrid network and GridKit network largest component is shown in Figure 2 and Figure 3 respectively. The size of the nodes is determined based on the outgoing degree. As a result, it is prominent that few hub nodes are present in both of the network

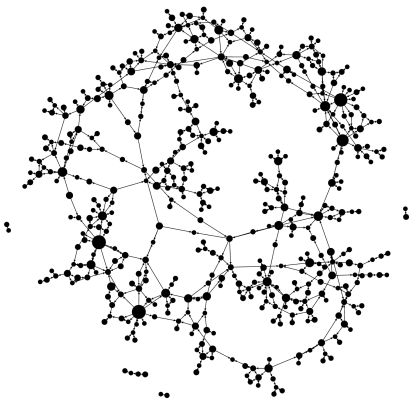

Figure 2: Network representation of the SciGrid network.

In order to examine the vulnerability of electrical transmission systems, both classical machine learning algorithms and Graph Neural Networks (GNNs) were applied to the SciGrid network, observing varied performance levels across different models. For the classical algorithms, after initial model development, grid search with cross-validation was applied to ensure each model is rigorously optimized. This method effectively identify the set that maximizes the accuracy of each model by exploring a range of potential hyperparameter combinations. In contrast, for the GNNs, manual hyperparameter tuning was utilized for GNNs, as direct Grid Search Cross-Validation support is generally not available for these models. This approach facilitated a systematic exploration and refinement of hyperparameter combinations, ensuring optimized accuracy for the distinct architecture of GNNs. In terms of performance, XGBoost led the way with an accuracy of 84.72%, followed by the Support Vector Machine (SVM) at 83.33%, while the Multilayer Perceptron Neural Network (MLP) trailed at 79.86%. Diving into the realm of GNNs, the results varied: the generic GNN model achieved a test accuracy of 46.94%, the Graph Convolutional Network (GCN) recorded 61.22%, and the Graph Attention Network (GAT) reached 71.43%. Although insightful, the performance of the GNN models was notably lower compared to the classical machine learning approaches. Figure 4 illustrates the performance accuracy of all six models

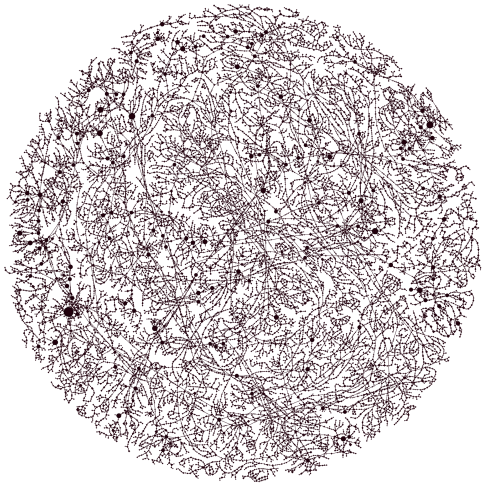

Figure 3: Network representation of the GridKit network largest connected component.

as applied to the SciGrid network.

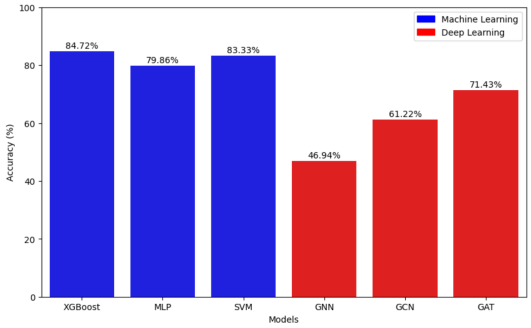

Figure 4: Model Performance Comparison for SciGrid Network.

In the next step, the same Machine Learning methodology was applied to the larger GridKit network. The classical machine learning algorithms exhibited diverse performance levels. Figure 5 shows the results achieved from applying the alogorithms to GridKit dataset. XGBoost continued its strong performance with an accuracy of approximately 83.14%, while the Multilayer Perceptron Neural Network (MLP) and Support Vector Machine (SVM) lagged behind, recording accuracies of 41.78% and 38.76% respectively. In contrast, the exploration with Graph Neural Networks (GNNs) yielded closely contested results: the generic GNN model

achieved a test accuracy of 65.24%, the Graph Convolutional Network (GCN) followed at 66.98%, and the Graph Attention Network (GAT) outperformed both with an accuracy of 65.04%. These outcomes emphasize the variance in model performance when scaling up to the more complex GridKit network, underlining the critical role of model selection in relation to the specific characteristics of the network being analyzed.

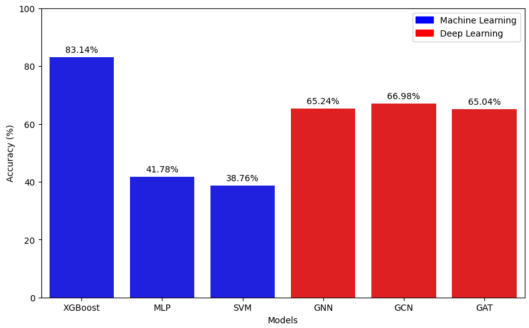

Figure 5: Model Performance Comparison for GridKit Network.

The comparative analysis of classical machine learning (CML) algorithms and Graph Neural Networks (GNNs) across two different datasets, SciGrid and GridKit, provides insightful findings. In the case of the SciGrid network, GNNs displayed lower performance, which could be attributed to the dataset's limited size and complexity, possibly insufficient to exploit GNNs' full potential. These networks, with their inherent complexity and reliance on large, intricate data, did not outperform the more straightforward CML algorithms, which seem better suited for smaller or simpler datasets. Conversely, when applied to the larger and more complex GridKit network, GNNs demonstrated improved performance, still not surpassing the accuracy achieved by the XGBoost algorithm. This suggests that while GNNs benefit from larger datasets, their effectiveness compared to CML algorithms like XGBoost may vary depending on the network's scale and complexity, as well as the nature of node and edge features.

As XGBoost is the best performing algorithm in case of both the data set, further investigation was done on feature importance analysis specific to this model. Figure 6 and 7 shows the top 5 features in terms of feature importance for SciGrid and GridKit data respectively. In the SciGrid network, 'eigen_centrality' and 'node_strength' emerged as key, highlighting the significant influence of individual node attributes in smaller network dynamics. On the other hand, in the larger and more complex GridKit network, 'closeness_centrality', 'node_strength', and

'typ_joint' were predominant, reflecting the importance of connection, weight of the network and type of nodes in extensive networks. The significance of diverse centrality measures as principal features in the study corresponds closely with anticipated outcomes, given the criticality levels defined by combining degree, pagerank, and betweenness centrality. The importance of 'node strength' in the analysis is closely linked to the network's weight, voltage, underscoring voltage's key role in influencing node robustness and the network's overall structural integrity. Furthermore, the categorization of nodes, evident in the significance of joint/auxiliary T nodes in both datasets, highlights the importance of the node type, particularly emphasizing the extent of a node's connection within the network.

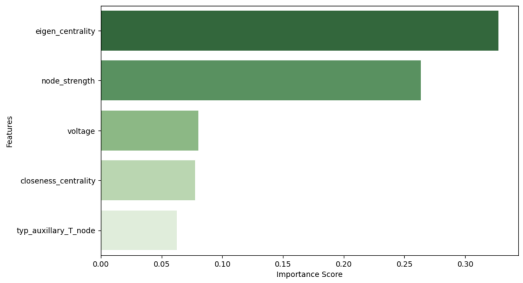

Figure 6: Top 5 important features used for XGBoost on SciGrid Data.

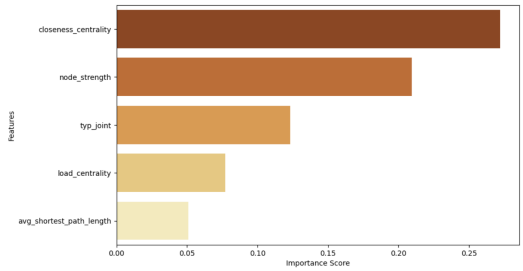

Figure 7: Top 5 important features used for XGBoost on GridKit Data.

Moving forward, it is imperative to investigate these methods further on even larger and more diverse real-world datasets. Such research could ascertain whether increased dataset size and diversity would enhance GNNs' performance, potentially making them more competitive with or even superior to CML algorithms in certain contexts. Additionally, exploring more intricate feature engineering, hyperparameter tuning might unlock new possibilities for improving model accuracy.

These efforts could lead to the development of more sophisticated predictive models, thereby contributing substantially to the safety, resilience, and efficiency of electrical transmission system management. As such, extending these methodologies to broader datasets and identifying the optimized parameters for existing GNN models remain an important direction for future studies, aiming to clarify the scalability and applicability of these models in real-world scenarios. All codes and datasets are available at `https://github.com/CEL-lab/Net_ML`.

7 Conclusion

In conclusion, our study provided comprehensive insights into node vulnerability assessment in power grid networks, utilizing the SciGRID and GridKit datasets. Our findings indicate that traditional machine learning models, including XGBoost, SVM, and Multilayer Perceptron, are more effective in identifying critical nodes than Graph Neural Networks, underscoring their practical utility in current network vulnerability assessments. However, the potential of Graph Neural Networks in network analysis, particularly with larger datasets and refined prediction models, is significant.

The study highlights various implications for power networks. It emphasizes the importance of targeted maintenance and resilience, with predictive strategies focusing on critical nodes to strengthen network robustness. Accurate vulnerability assessments are shown to enhance emergency and disaster responses, especially in natural disaster-prone areas. The potential for advanced models like Graph Neural Networks to develop smarter, more adaptive grids capable of real-time monitoring and rapid responses is evident. Strategic infrastructure investments and long-term network planning are informed by our insights, targeting areas that require reinforcement. Our findings have implications for policy and regulatory decisions, particularly in enhancing cybersecurity and setting safety standards. Improved network analysis can lead to effective demand-side management, resulting in energy savings and better service quality for consumers. Our research also drives future research and development, particularly in refining network analysis algorithms and technologies. Understanding network vulnerabilities, as shown in our study, leads to better grid inter-connectivity and cost-efficient grid management, benefiting both providers and consumers.

It is important to consider the potential effects of the data imputation methods on the outcomes of the study. Missing data in the vertex dataset's voltage column was addressed through median imputation to maintain central tendency, essential for preserving underlying distribution patterns crucial for network analysis. For other attributes in both node and edge datasets, k-Nearest Neighbors imputation was utilized, leveraging similarity patterns to ensure consistency and completeness

of the data. Selected imputation methods aimed to reduce information loss, which could affect conclusions regarding feature importance and classifier performance. While the results are substantial, it is crucial to consider that these methods might introduce slight biases in critical features, like voltage and typ identified in the study. Recognizing such biases is important for ensuring the accuracy of critical node identification in network vulnerability assessments.

Additionally, the impact of dataset size and complexity on model performance also emerged as a key finding, suggesting the need for more extensive datasets in future research to fully exploit the capabilities of advanced machine learning models. Future research should focus on expanding datasets to improve Graph Neural Networks' accuracy in vulnerability prediction, and exploring other deep learning architectures. Additionally, refining centrality measures, particularly building upon the entropy-weighted Combined Centrality Score, will further enhance assessment methodologies in network vulnerability. These areas offer promising directions for advancing the field based on our study's insights.

Acknowledgment

This research is partially supported by the National Science Foundation (NSF) EPSCoR RII Track-2 Program under the grant number OIA-2119691 at North Dakota State University. The findings and opinions expressed in this article are those of the authors only and do not necessarily reflect the views of the sponsors.

References

[1] Z. Li, W. Wu, B. Zhang, and X. Tai, "Analytical reliability assessment method for complex distribution networks considering post-fault network reconfiguration," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1457–1467, 2019.

[2] S. Marrone, R. Nardone, A. Tedesco, P. D'Amore, V. Vittorini, R. Setola, F. De Cillis, and N. Mazzocca, "Vulnerability modeling and analysis for critical infrastructure protection applications," *International Journal of critical infrastructure protection*, vol. 6, no. 3-4, pp. 217–227, 2013.

[3] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[4] B. Liu, G. Zhu, X. Li, and R. Sun, "Vulnerability assessment of the urban rail transit network based on travel behavior analysis," *Ieee Access*, vol. 9, pp. 1407–1419, 2020.

[5] X. Feng, J. Wu, A. K. Bashir, J. Li, A. Shen, and M. D. Alshehri, "Vulnerability-aware task scheduling for edge intelligence empowered trajectory analysis in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, p. 4661–4670, Apr. 2023. [Online]. Available: https://doi.org/10.1109/tits.2023.3241479

[6] I. Kamwa, A. K. Pradhan, and G. Joós, "Automatic segmentation of large power systems into fuzzy coherent areas for dynamic vulnerability assessment," *IEEE Transactions on Power Systems*, vol. 22, no. 4, p. 1974–1985, Nov. 2007. [Online]. Available: https://doi.org/10.1109/tpwrs.2007.907383

[7] U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Vulnerability of network mechanisms to sophisticated ddos attacks," *IEEE Transactions on Computers*, vol. 62, no. 5, p. 1031–1043, May 2013. [Online]. Available: https://doi.org/10.1109/tc.2012.49

[8] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, p. 1334–1340, Jul. 2011. [Online]. Available: https://doi.org/10.1016/j.epsr.2011.01.021

[9] U. Shahzad, "Vulnerability assessment in power systems: a review," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, no. 4, pp. 17–24, 2021.

[10] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Physica A: Statistical Mechanics and Its Applications*, vol. 392, no. 11, p. 2688–2700, Jun. 2013. [Online]. Available: https://doi.org/10.1016/j.physa.2013.01.023

[11] B. Fan, Z. Li, N. C. Shu, and Y. Li, "Identification of key nodes based on pagerank algorithm," *IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Mar. 2021. [Online]. Available: https://doi.org/10.1109/iaeac50856.2021.9390946

[12] Y.-H. Yang, Y. Lei, X. Wang, Z. Zhou, Y. Chen, and K. Tian, "A novel method to evaluate node importance in complex networks," *Physica A: Statistical*

Mechanics and Its Applications, vol. 526, p. 121118, Jul. 2019. [Online]. Available: https://doi.org/10.1016/j.physa.2019.121118

[13] M. Zhao, W. Muqing, L. Qiao, Q. An, and L. Sixu, "Evaluation of cross-layer network vulnerability of power communication network based on multi-dimensional and multi-layer node importance analysis," *IEEE Access*, vol. 10, p. 67181–67197, Jan. 2022. [Online]. Available: https://doi.org/10.1109/access.2021.3109902

[14] H. Cui, W. Dai, Y. Zhu, X. Kan, A. A. C. Gu, J. Lukemire, L. Zhan, L. He, Y. Guo, and C. Yang, "Braingb: a benchmark for brain network analysis with graph neural networks," *IEEE Transactions on Medical Imaging*, vol. 42, no. 2, p. 493–506, Feb. 2023. [Online]. Available: https://doi.org/10.1109/tmi.2022.3218745

[15] C. Nauck, I. Isenhardt, H. Zhang, F. Hellmann, and P. Ennen, "Prediction of power grid vulnerabilities using machine learning," 2020.

[16] C. Matke, W. Medjroubi, and D. Kleinhans, "Scigrid - an open source reference model for the european transmission network (v0.2)," 7 2016.

[17] B. Wiegmans, "Gridkit: European and north-american extracts," https://doi.org/10.5281/zenodo.47317, 2016, [Data set].

[18] M. Zhao, W. Muqing, L. Qiao, Q. An, and L. Sixu, "Evaluation of cross-layer network vulnerability of power communication network based on multi-dimensional and multi-layer node importance analysis," *IEEE Access*, vol. 10, p. 67181–67197, Jan. 2022. [Online]. Available: https://doi.org/10.1109/access.2021.3109902

[19] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[20] M. Newman, *Networks: An Introduction*. Oxford University Press, 3 2010.

[21] A. Hagberg, P. J. Swart, and D. A. Schult, "Exploring network structure, dynamics, and function using networkx," in *7th Python in Science Conference (SciPy2008)*, 2008.

[22] M. Fey and J. E. Lenssen, "Fast graph representation learning with PyTorch Geometric," in *ICLR Workshop on Representation Learning on Graphs and Manifolds*, 2019.

[23] G. V. Rossum and F. L. Drake, "Python 3 reference manual," *Scotts Valley, CA: CreateSpace*, 2009.

[24] R. J. A. Little and D. B. Rubin, *Statistical Analysis with Missing Data*. Wiley, 8 2002.

[25] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*. Springer New York, 2009.

[26] M. B. Richman, T. B. Trafalis, and I. Adrianto, "Missing data imputation through machine learning algorithms," in *Artificial Intelligence Methods in the Environmental Sciences*, S. E. Haupt, A. Pasini, and C. Marzban, Eds. Dordrecht: Springer, 2009, pp. 119–140.

[27] T. Chen and C. Guestrin, "Xgboost." ACM, 8 2016, pp. 785–794.

[28] G. E. Hinton, "Connectionist learning procedures," *Artificial Intelligence*, vol. 40, pp. 185–234, 9 1989.

[29] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273–297, 9 1995.

[30] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, "The graph neural network model," *IEEE Transactions on Neural Networks*, vol. 20, pp. 61–80, 1 2009.

[31] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks." *arXiv preprint arXiv:1609.02907*, 2016.

[32] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks." *arXiv preprint arXiv:1710.10903 (2017)*.

[33] M. Labonne, *Hands-On Graph Neural Networks Using Python: Practical techniques and architectures for building powerful graph and deep learning apps with PyTorch*. Packt Publishing Ltd, 2023.