Detecting the Most Central Nodes for the Vulnerability of Power Networks

Yeşim Aygül
Department of Computer Engineering,
İzmir Bakırçay University
İzmir, Türkiye
yesim.aygul@bakircay.edu.tr
0000-0003-0605-9604

Melike Karatay
Department of Computer Engineering,
İstanbul Esenyurt University
İstanbul, Türkiye
melikekaratay@esenyurt.edu.tr
0000-0001-6941-4752

Onur Ugurlu
Department of Computer Engineering,
İzmir Bakırçay University
İzmir, Türkiye
onur.ugurlu@bakircay.edu.tr
0000-0003-2743-5939

***Abstract*—Understanding the vulnerability of power networks is crucial for ensuring the stability and efficiency of modern infrastructure. Identifying the most central nodes that significantly impact network resilience helps prevent potential failures and disruptions. In this study, we analyze the effectiveness of three traditional centrality metrics—Degree Centrality, Betweenness Centrality, and Closeness Centrality — in maximizing the Rupture Degree, which assesses the robustness and resilience of a network by analyzing the impact of node removals. By iteratively removing the highest-ranked nodes based on these centrality measures across eight real-world power networks, we assess their impact on RD. The results indicate that DC generally achieves higher RD values compared to BC and CC; however, in certain networks, BC proves to be a more effective indicator of node criticality. These findings highlight the importance of selecting appropriate centrality metrics in vulnerability analysis and provide insights for enhancing the resilience of power networks.**

Keywords—power networks, network vulnerability, rupture degree, central nodes

I. INTRODUCTION

Understanding the vulnerability of networks is crucial, particularly in infrastructure systems where disruptions can have severe societal and economic consequences. Vulnerability analysis in complex networks is essential for assessing how failures, attacks, or natural disasters impact connectivity and overall functionality [10]. Among various types of complex networks, power networks are particularly significant due to their critical role in ensuring the continuous functioning of modern infrastructure. The stability and efficiency of these networks rely heavily on the resilience of their structural components. Fig. 1 illustrates a real-world power network (power-494-bus [8]).

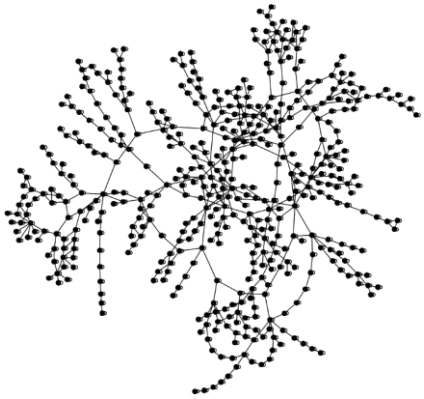

Fig. 1. Illustration of power-494-bus network

In graph theory, the Rupture Degree (RD) is an advanced vulnerability metric that measures the impact of node removal on the overall connectivity of a network [7]. It plays a crucial role in assessing network resilience, as it quantifies how the removal of a single node can lead to fragmentation or even complete disconnection. Several studies have explored the applications and effectiveness of RD in different network domains. Fan et al. [3] conducted a comprehensive analysis of power communication networks, which are integral to the support structure of electric power grids. They proposed a model that evaluates nodes across multiple layers—physical topology, traffic distribution, and service importance—and developed a multi-layer critical node identification algorithm by calculating node importance within each layer. Wen et al. [11] explored the vulnerability of distribution networks by introducing a method that integrates complex network theory with an optimized Technique for Order Preference by Similarity to Ideal Solution. This approach provided a more refined identification of vulnerable nodes by considering both the structural characteristics of the network and its operational parameters. Qi et al. [9] advanced the field by developing a fusion power network security risk evaluation algorithm that combines the flash search algorithm with a support vector machine. This innovative approach enhanced the accuracy of security risk assessments within power networks by effectively identifying critical nodes and evaluating their impact on network vulnerability.

Another essential phenomenon in graph theory is the central nodes, which play a pivotal role in network structure and functionality. Several centrality metrics have been introduced to quantify node importance from different perspectives. Given their significance in network analysis, investigating the effectiveness of centrality metrics regarding the RD is important for understanding their impact on network vulnerability. In this study, we investigate the effectiveness of three traditional centrality metrics—Degree Centrality (DC), Betweenness Centrality (BC), and Closeness Centrality (CC) in maximizing the RD, thereby identifying the most critical nodes in power networks. Understanding how these metrics correlate with network vulnerability provides valuable insights into enhancing the resilience of power systems, contributing to more robust and failure-resistant infrastructure.

The remainder of this paper is organized as follows: Section 2 provides the fundamental background of the study. Section 3 describes the methodology used, and Section 4 presents the computational results. Finally, Section 5 concludes the paper by summarizing the findings and outlining potential directions for future research.

II. Basic Definitions and Preliminaries

Graph theory serves as a crucial tool in analyzing complex networks, including power grids, transportation systems, and communication networks. Formally, a graph consists of a set of nodes and a set of edges that establish connections between pairs of nodes. Let $G = (V, E)$ be a simple, undirected graph, where V represents the set of nodes and E represents the set of edges, with $n = |V|$ and $m = |E|$. The density of a graph, denoted as D, is computed by dividing the actual number of edges by the maximum possible number of edges in the graph. The degree of a node v is defined as the number of edges incident to it. A path in a graph is a sequence of distinct vertices and edges that allows traversal from one vertex to another by following the edges [2]. Given a cut set S, we denote the number of connected components in the remaining graph $G - S$ as $\omega(G - S)$, and the size of the largest connected component after removal as $m(G - S)$.

Rupture Degree has been proposed by Li et al. [7]. The RD of a graph G, denoted by $r(G)$, is defined as:

$$r(G) = max\{\omega(G - S) - |S| - m(G - S): S \subset V(G)\}$$

Centrality metrics are fundamental measures used to assess the importance of nodes within a network. In this study, we consider the three well-known centrality metrics:

- **Degree centrality** measures a node's importance based on the number of direct connections it has with other nodes [6].
- **Betweenness centrality** evaluates a node's significance by determining the proportion of shortest paths between all node pairs that pass through it [4].
- **Closeness centrality** quantifies how efficiently a node can reach all other nodes in the network, considering the sum of shortest path lengths [1].

Each of these centrality measures provides a different perspective on node importance. While DC highlights local connectivity, BC emphasizes a node's role in facilitating communication across the network. CC captures how quickly information can spread from one node to all others. This study analyzes these metrics in relation to RD to identify the most central nodes that significantly impact network vulnerability.

III. Material And Method

This section details the methodology, including dataset characteristics and the iterative node removal process.

A. Dataset

The dataset used in this study consists of eight real-world power networks [8], each represented as a graph where nodes correspond to buses (substations or junction points) and edges represent transmission lines.

Table I summarizes the fundamental characteristics of these networks. The number of nodes in the networks ranges from 494 to 5300, reflecting their varying sizes and structural complexity. A key characteristic of these networks is their sparse connectivity, as indicated by low-density values, which remain close to zero across all instances. The clustering coefficient (C), which quantifies the tendency of nodes to form tightly connected local clusters, varies significantly between networks, with values ranging from 0.007 to 0.432. This variation suggests that while some networks exhibit strong local connectivity structures, others are more loosely connected.

TABLE I. Basic characteristics of 8 real-world networks

Instance Name	*n*	*m*	*D*	*C*	*AvDeg*
power-494-bus	494	1080	0.009	0.042	4.372
power-662-bus	662	1568	0.007	0.046	4.737
power-685-bus	685	1967	0.008	0.172	5.743
power-1138-bus	1138	2596	0.004	0.087	4.562
power-eris1176	1176	9864	0.014	0.432	16.776
power-bcspwr09	1723	4117	0.003	0.076	4.779
power-US-Grid	4941	6594	0.001	0.080	2.669
power-bcspwr10	5300	13571	0.001	0.088	5.121

Additionally, the average degree ($AvDeg$), representing the mean number of connections per node, ranges from 2.669 to 16.776. These variations highlight the structural diversity of power networks, which is influenced by factors such as geographical constraints, operational requirements, and engineering considerations.

B. Solution Framework

To evaluate the effectiveness of centrality metrics in relation to RD across different power networks, we employ an iterative node removal approach. In this process, nodes are ranked based on their centrality values, and at each step, the node with the highest centrality score is removed. After each removal, the RD is recalculated to analyze how network vulnerability evolves as critical nodes are eliminated.

Algorithm Rupture Degree Computation

Input: $G = (V, E)$
Output: Maximum RD r^*

$r^* \leftarrow 1 - n$
while $\exists v \in V$ such that $\deg(v) > 1$ **do**
  Find the most central node v
  $G' \leftarrow G \setminus \{v\}$
  Compute rupture degree r_v of G'
  if $r_v > r^*$ **then**
    $r^* \leftarrow r_v$
  end if
end while
return r^*

Fig. 2. Calculation of rupture degree using centrality metrics

The algorithm given in Fig. 2 outlines the step-by-step procedure of the iterative node removal approach. The process begins by assigning a centrality score to each node based on one of the three selected metrics: DC, BC, and CC. The node with the highest centrality score is then determined and removed from the network. After each removal, the remaining network is updated, and the RD is recalculated to determine the resulting change in the network. If the newly computed RD exceeds the previously recorded maximum, the value is updated accordingly. This process continues iteratively until no further removals can be performed. At the end of the process, the highest recorded RD is reported as a measure of network vulnerability.

By applying this approach separately for each centrality metric, we systematically compare their effectiveness in identifying the most critical nodes regarding RD within power

networks. This analysis provides insights into whether local connectivity measures (such as DC) or global influence measures (such as BC and CC) offer a more accurate indication of network fragility and resilience.

IV. Results

This section presents the computational results of the analysis conducted on real-world power networks.

Table II provides a comparative assessment of DC, BC, and CC in their ability to identify the most critical nodes affecting network vulnerability. The RD values for each network correspond to the highest values obtained through the iterative node removal process. The results indicate that DC generally achieves higher RD values compared to BC and CC. For instance, in the power-494-bus network, BC-based removal results in an RD of 94, while CC-based removal yields an RD of 90, both of which are lower than the RD obtained using DC (102). This suggests that, in many networks, locally well-connected nodes contribute more significantly to overall network vulnerability than nodes that facilitate long-range connectivity. However, in power-eris1176, DC-based removal results in a negative RD (-49), whereas BC-based removal produces a significantly higher RD (102). This suggests that, in certain networks, DC may not always be a reliable indicator of node criticality when assessing network vulnerability. For some networks, such as power-685-bus and power-bcspwr09, RD remains zero across all centrality metrics, indicating that these networks exhibit structural robustness, where the removal of even the most central nodes does not significantly disrupt overall connectivity. Such networks may possess high redundancy or alternative pathways, making them more resilient to targeted node failures.

TABLE II. Comparison of Centrality Measures

Instance Name	***DC***	***CC***	***BC***
power-494-bus	102	90	94
power-662-bus	106	87	101
power-685-bus	0	0	0
power-1138-bus	275	254	267
power-eris1176	-49	-29	102
power-bcspwr09	0	0	0
power-US-Grid	1035	904	994
power-bcspwr10	398	179	310

The variation in RD across different power networks highlights the influence of network topology on vulnerability analysis. In densely connected networks with high clustering coefficients, such as power-eris1176, DC and CC exhibit weaker performance, whereas BC proves to be more effective in identifying crucial nodes. Conversely, DC remains a strong predictor of node importance in sparser networks, such as power-US-Grid, as highly connected nodes in these networks function as essential bridges. However, as demonstrated in multiple instances, global connectivity measures like BC often provide a more accurate representation of critical nodes. These findings reinforce the importance of selecting appropriate centrality metrics when assessing power network resilience.

V. Conclusion

This study investigates the relationship between centrality metrics and network vulnerability by analyzing their impact on the RD across eight real-world power networks. The results demonstrate that DC, BC, and CC perform differently depending on network topology. While the DC is generally effective in maximizing RD, BC often provides a more accurate representation of critical nodes in specific network structures. The findings reveal that networks with high clustering coefficients tend to be more resilient to node removals, whereas sparser networks are more vulnerable, particularly when BC-based nodes are removed. Additionally, some networks exhibit structural robustness, where central node removals do not significantly disrupt connectivity.

These insights have practical implications for power grid design and resilience planning. Future work could explore hybrid centrality-based approaches to improve the identification of critical nodes and develop more effective strategies for preventing cascading failures in power networks.

Acknowledgment

Y. Aygul thanks TUBITAK for its scholarship support under the BIDEB 2211-A program.

References

[1] Bavelas, A. (1950). Communication patterns in task-oriented groups. *The journal of the acoustical society of America*, *22*(6), 725-730.

[2] Diestel, R. (2024). Graph theory. Springer (print edition); Reinhard Diestel (eBooks).

[3] Fan, B., Zheng, C. X., Tang, L. R., & Wu, R. Z. (2020). Critical nodes identification for vulnerability analysis of power communication networks. *IET Communications*, *14*(4), 703-713.

[4] Freeman, L. C. (1977). A set of measures of centrality based on betweenness. Sociometry.

[5] Freeman, L. C. (1978). Centrality in social networks conceptual clarification, Social Networks 1 (3), 215–239.

[6] Kleinberg, J. M., Kumar, R., Raghavan, P., Rajagopalan, S., & Tomkins, A. S. (1999). The web as a graph: Measurements, models, and methods. In Computing and Combinatorics: 5th Annual International Conference, COCOON'99 Tokyo, Japan, July 26–28, 1999 Proceedings 5 (pp. 1-17). Springer Berlin Heidelberg.

[7] Li, Y., Zhang, S., & Li, X. (2005). Rupture degree of graphs. *International Journal of Computer Mathematics*, *82*(7), 793-803.

[8] Network Repository, Jan. 2025 [online] Available: https://networkrepository.com/power.php

[9] Qi, H., Zhu, W., Ye, M., Hu, Y., & Wang, Y. (2024). Construction of power network security risk assessment model based on LSA-SVM algorithm in the background of smart grid. *Scientific Reports*, *14*(1), 9077.

[10] Wang, J. W., & Rong, L. L. (2009). Cascade-based attack vulnerability on the US power grid. *Safety science*, *47*(10), 1332-1336.

[11] Wen, J., Lin, S., Qu, X., & Xiao, Q. (2023). A TOPSIS-Based Vulnerability Assessment Method of Distribution Network Considering Network Topology and Operation Status. *IEEE Access*.