
Seminar Title	: Vulnerability Analysis of Power Grid Using Complex Network Theory
Speaker	: Premananda Panigrahi (Rollno : 514ee6033)
Supervisor	: Prof. Somnath Maity
Venue	: Seminar Room (EE-401), Department of Electrical Engineering
Date and Time	: 18 Jun 2024 (4.30 PM)
Abstract	: The topological analysis of complex networks provides essential information about the structural and vulnerability assessment of real-world power grids (PGs). However, there are many ways to represent a complex network as a graph. The electrical complex PG (CPG) can be analyzed as a simple graph by ignoring the electrical dynamics and considering it as an unweighted and undirected network. These methods do not include the weight of lines, which is a disadvantage of such an analysis. For a PG network, weights (impedance) relate to electrical concepts, such as maximum power through the line. Therefore, a weighted network assessment can be efficiently used to improve the PG network representation.

Here, we explore the structural analysis of various synthetic and real-world PGs such as the IEEE 39, 118, 300 bus networks, and the Indian PG based on both topological and electrical connectivity. The topological analysis is carried out by taking into account these networks as unweighted and weighted networks. Our work is here divided into three categories. Firstly, we analyze the structural details of the PG networks. Secondly, through the centrality matrices adapted from complex network theory, we identify the most critical or vulnerable transmission lines and buses/nodes. We estimate the impact on the performance of the electrical PG by modeling cascade events from the removal of these lines and nodes. Based on these removal strategies, the AC optimal power flow problem is solved and then compared for both weighted and unweighted networks. It is shown that a weighted network can provide a better insight for the vulnerability assessment in comparison to an unweighted network.

We also utilize these two graph models, e.g., unweighted and weighted graphs, to compute the centrality metrics for targeted/intentional node attacks. Based on these centrality measures (CMs), we develop various node-attack strategies and empirically examine the effects of targeted attacks on the structural and operational performance of the CPGs. These measures help us describe the transfer capability and performance under normal operation and evaluate the vulnerability of the power system under cascading failures. Through a series of simulations on IEEE 118, 300 bus, and Indian PG networks, we demonstrate that key nodes with high electrical centrality can be effectively identified. The resulting cascading failures can also lead to a significant reduction in the size of the giant component and capacity index, thereby confirming the accuracy and effectiveness of the proposed analysis.

Moreover, the CM measure is one of the most fundamental metrics for evaluating the efficiency and vulnerability analysis of CPGs. Despite an abundance of different CMs for individual nodes, there are only a few metrics available to measure the centrality of individual lines without geodesic shortest path-length. Here, we also propose the current-flow line centrality to identify the ranking of lines, where each set of lines is associated with a different level of importance. We find the CMs using effective resistance and apply it not only to identify the important lines in a commonly used IEEE 118 bus network but also to analyze the efficiency and vulnerability of the CPGs.