Vulnerability Analysis of Weighted Indian Power Grid Network Based on Complex Network Theory

Premananda Panigrahi
Department of Electrical Engineering,
National Institute of Technology,
Rourkela, India.
Email: prempanigrahi@outlook.com

Somnath Maity
Department of Electrical Engineering,
National Institute of Technology,
Rourkela, India.
E-mail: somnatheeiitkgp@gmail.com

***Abstract*—In power grid (PG) networks some critical bus and transmission line has the major impact on the cascading failures and large-scale blackouts. In this work, we have investigated the vulnerability of Indian power grid (PG) and IEEE 118 bus for intentional and random attack strategies using complex network (CN) theory. We show that the PG's are vulnerable to intentional attacks and robust to random failures. We apply eight different attack strategies to unweighted and weighted PG networks. Here our approach based on CN theory does not aim to focus on the detailed operation of a PG networks, rather it gives details about its structural vulnerability. We concluded that weighted network analysis could give more accurate result since the weight is related to the electrical concept of PG. This process can help to identify the most vulnerable transmission lines and nodes, whose protection can increase the robustness and reliability of any PG network.**

***Index Terms*—Cascading failures, Centrality metrics, Complex systems, Physical attacks.**

I. Introduction

The power grid (PG) is a critical infrastructure, whose efficient operation, reliability and robustness, mostly affects national economics, politics, and people's everyday life. A small disturbance within a grid may propagate and cause significant damage or may lead to cascading failure. The disturbance may occur due to natural phenomena (lightning, flooding, high wind), intentional attack or due to imbalances between load and generation. A series of cascading failure can be widespread the blackout [1], [2]. The occurrence of blackout can't be avoided, so efforts have been made by many researchers to find restorative and preventive methods to deal with widespread of catastrophic failures [1].

From 1970 the CN theory has significant applications in social, biological and telecom networks and now slowly it is making its way for the topological analysis of PG networks [3]–[5]. More and more researchers are applying this complex theory for modeling and analysis of PG [2], [6]–[9]. But there needs to be more improvement when CN characteristic is directly applied to the real PG. The identification of the vulnerable component in a PG is not so easy, for which accuracy and perfection are needed [10]. The failure of these components may have a larger impact on the performance of the whole system. If this vulnerable component can be identified, then the overall system security and reliability can be increased by proper maintenance and monitor them.

The investigation completely depends on historical records and enumeration of the critical points of a PG. The blackout in the US, Canada, Italy and some European countries have been studied using the CN and electrical engineering tool (EET) [6], [11]. Most of the studies have focused on CN analysis due to complexity in EET to investigate the blackout in PG [10], [12]. The CN matrices like degree centrality, degree distribution, betweenness centrality are used to identify the most vulnerable lines and nodes in a network. Many researchers applied this approach in real PG network, but most of them considered the network as unweighted and undirected [11], [13], [14]. These approaches do not include any information of the link weights, which is a key difference about the contributions by very few researchers, where links have been considered as weighted to enhance the analysis of the PG [12]. In particular, in a PG network transmission line weight like reactance is related to electric concepts such as in a DC grid, maximum power can be transmitted through the less reactance line [15]. Hence this work is motivated by the concept of CN to identify critical lines and nodes by considering the PG as the weighted network.

This paper is divided into five section and organized as follows: Section II discusses the fundamental of CN and introduces a methodology for identifying the most critical nodes of transmission grids. Also in Section-II structural details of both the PG network are given. Section III and IV illustrates the simulation result of unweighted and weighted Indian PG and IEEE 118 bus networks. Section V concludes the paper with future model additions and extensions

II. Complex Networks Fundamentals

A PG can be represented as a network in which generators, loads, transmission buses are represented as nodes, while edges related to the transmission lines between the nodes. Mathematically a PG network can be represented by using a graph $G = (N, E)$ where N is the number of nodes, and E denotes the number of edges. The following list gives some important definitions and concepts of topological matrices that will help better understand the CN:

1) In a unweighted network, the degree k_i of a node i is the number of edges that are adjacent to node i, i.e.

$$k_i = \sum_{j}^{N} a_{ij}. \tag{1}$$

Here a_{ij} is the edge a connected between node i and j. In a weighted network, the degree of a node is the sum of all the link weight connected to that node.

2) The mean of all the shortest path between nodes in a network is called average path length

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} l_{ij}, \tag{2}$$

here l_{ij} is the total number of shortest path between node i and j. In a weighted network, the shortest path between two nodes is the smallest sum of weights of lines connected between that two nodes

$$L^w = \frac{N(N-1)}{\sum\limits_{i=1}^{N} \sum\limits_{j \neq i}^{N} \frac{1}{W_{ij}}}, \tag{3}$$

where W_{ij} is the weighted shortest path between node i and j.

3) The clustering coefficient of a network is capturing the density of triangles, and it is a local property. Basically, two nodes that are connected to a third node are also directly connected to each other. Thus a node i in a network has k_i links that connect it to k_i other nodes. Mathematically the average clustering coefficient of the network can be defined as:

$$C = \frac{1}{N} \sum_{i} c_i, \tag{4}$$

where c_i is the clustering coefficient of node i.

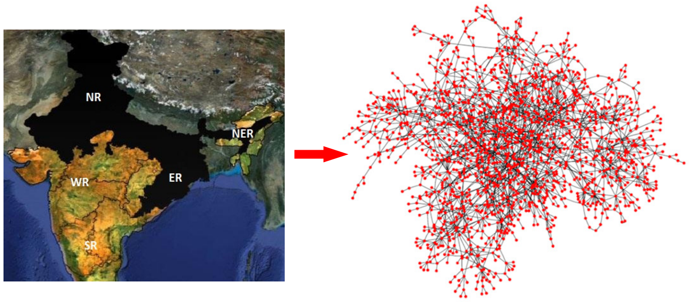


Figure 1: Topological transformation of Indian PG with 1634-nodes and 2549-edges. Node represent substations, loads and power generating stations. Edge represent transmission lines. The transmission data has been extracted from northern, eastern, north-east and few part of western region.

4) The betweenness centrality is the number of shortest paths through a vertex or edge, that is,

$$B(v) = \sum_{i}^{N} \sum_{j}^{N} \frac{l_{ij}(v)}{l_{ij}} \tag{5}$$

and

$$B(l) = \sum_{i}^{N} \sum_{j}^{N} \frac{l_{ij}(l)}{l_{ij}}. \tag{6}$$

Here $l_{ij}(v)$ is the number of shortest path between i and j, that passes through node v and $l_{ij}(l)$ is the total number of shortest path between i and j that passes through line l.

A. Structural Details

Fig.1 shows the mapping of Indian PG, contains information about major substation, power plant and 132–765 kV power transmission line. Our model represents the PG as a topological network of 1634 nodes substations! and 2549 edges power transmission lines!. The structure of a PG can be categories based on small world or scale free model. Most of the researchers show that CNs exhibit the small-world property [4]. This type network is also called Watts & Strogatz model discovered in 1991 [3]. A small world network formed by rewiring a regular lattice without altering the no of nodes and lines with some probability, which is an intermediate of the regular and random network. This type of networks are highly clustered (C) and have minimum average path length (L). These two measures L and C used by Watts & Strogatz to know small-worldness of a unweighted and undirected network.

$$\begin{cases} L \geq L_r, & C \gg C_r \\ L_r = \frac{\ln(N)}{\ln(k)}, & C_r = \frac{k}{N}. \end{cases} \tag{7}$$

Here L_r and C_r are the average path length and clustering coefficient of a random network generated with the number of nodes and lines equivalent to a real network. The work in [16] approaches a new measures to calculate small-worldness of a network. This method works for both unweighted and weighted network. In this work, we adopted both the approach to know the small-worldness of the Indian PG and IEEE 118 bus network.

$$\eta = \frac{C}{C_r}, \ \ \eta \geq 1; \ \ \tau = \frac{L}{L_r}, \ \ \tau \gg 1. \tag{8}$$

Then the quantitative metric to check small-world-ness of network is $\sigma = \eta/\tau$, which must give $\sigma > 1$. Based on this concept we have tested our networks. In table I we can see that the actual average path length L and clustering coefficient C are greater than random L_r and C_r in Indian PG, IEEE 118 bus as well as $\delta > 1$. These two network showing the behavior of small-world network. To test whether these PG networks have scale-free characteristics, we have calculated k_{min}, gamma and p-value as described in Clauset et.al.(2009) [17]. Where k is a vector of degree of a PG to which we fit the power-law distribution $P(k) \sim k^{-\gamma}$ for $k \geq k_{min}$. If $p > 0$, the tested data could fit the power law [17]. As $p = 0$ for both

Table I: Identifying Small-World-Ness of Indian PG and IEEE 118 bus

Network	L_a	L_r	C_a	C_r	δ
Indian PG	8.582	6.271	0.175	0.00305	37.3
IEEE 118	6.309	4.298	0.175	0.0275	4.3354

Table II: Identifying Scale-free-ness of Indian PG and IEEE 118 bus

Network	k_{min}	γ	p
Indian PG	4	2.99	0
IEEE 118	2	2.65	0.0100

the network, it seems that they did not have any scale-free properties. We computed δ and p for both Indian PG and IEEE 118 bus network. We found that both the networks are small-world network.

B. Attack Strategies

The selection of different attack strategies in which nodes and lines are removed is an open choice. In this work, we have adopted attack strategies from CN theory. Broadly these attack strategies are classified in terms of static and dynamic approach. The details are given below in a pipeline structure.

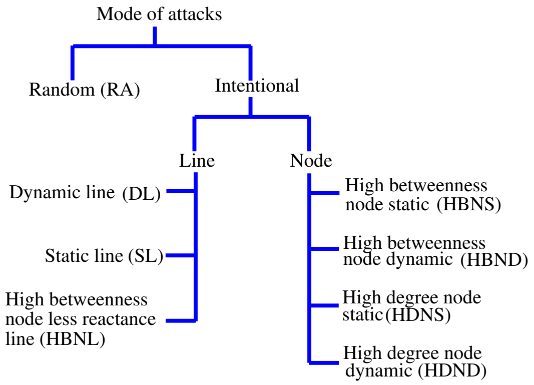

Mode of attacks
Random (RA)
Intentional
Line
Node
Dynamic line (DL)
Static line (SL)
High betweenness node less reactance line (HBNL)
High betweenness node static (HBNS)
High betweenness node dynamic (HBND)
High degree node static (HDNS)
High degree node dynamic (HDND)

Figure 2: Pipeline structure of different attack strategies

1) Node Attack: In this work, the performance of Indian PG and IEEE 118 bus network has been analyzed based on eight different attack scenario. Among all these strategies more tractable choice is to select the node in the descending order of degree in the initial network before any attack. We remove one by one node and calculate topological efficiency and giant component size of the network. This type of attack strategy is called high degree node static attack (HDNS). Similarly, for high degree node dynamic (HDND) approach, we recalculate degree distribution at each time and identify the high degree node to be removed.

In CN theory, the most vulnerable elements can also be identified based on centrality analysis, in which we can identify and rank the most critical lines and nodes. In this work, the critical nodes are identified based on static and dynamic high betweenness approach (HBNS & HBND). The concept of static and dynamic are same as in degree based attacks. Here the betweenness based node removal is a global strategy, and the degree based removal is a local one. Another important difference between these approaches is that degree based attack reduces the number of edges in the network, whether the other one removes the shortest path between two nodes. Among these, we expect that dynamic based approach is more harmful than static approach.

2) Line Attack: In this subsection, we study the vulnerability of network against various edge attack strategies. Generally speaking, the edge removal may be not efficient as node removal, since at each time we are removing a single edge, which has very less impact on network structure. The study presented here is different from other approaches, in which the assumption was that the failure of a single transmission line might propagate cascading removal of other lines. But here we do not make such assumption, but the removal of the shortest line can change the path between other two nodes, which can result in a structural shift in the network. The line attack is categories into dynamic (DL), static (SL), random (RA) and high betweenness node less reactance line (HBNL). The last approach is based on the DC power flow concept, where the transmission line is considered to be loss less. As the resistance is seen as negligible, the power flow will be dependent on the reactance and node voltage. In such case, the active power flow from node i to j of any power network can be given by the following equations

$$P = \frac{v_i v_j}{x_{ij}} \sin \alpha_{ij}. \tag{9}$$

For simplicity we have ignored the node voltage and phase angle, now we can see from the Eq. 8 that the active power flowing through any line is inversely proportional to the reactance of that line i.e. $P = {}^{1}/_{x_{ij}}$. Hence less the reactance means more the power will flow.

C. CN-Based Vulnerability Metrics

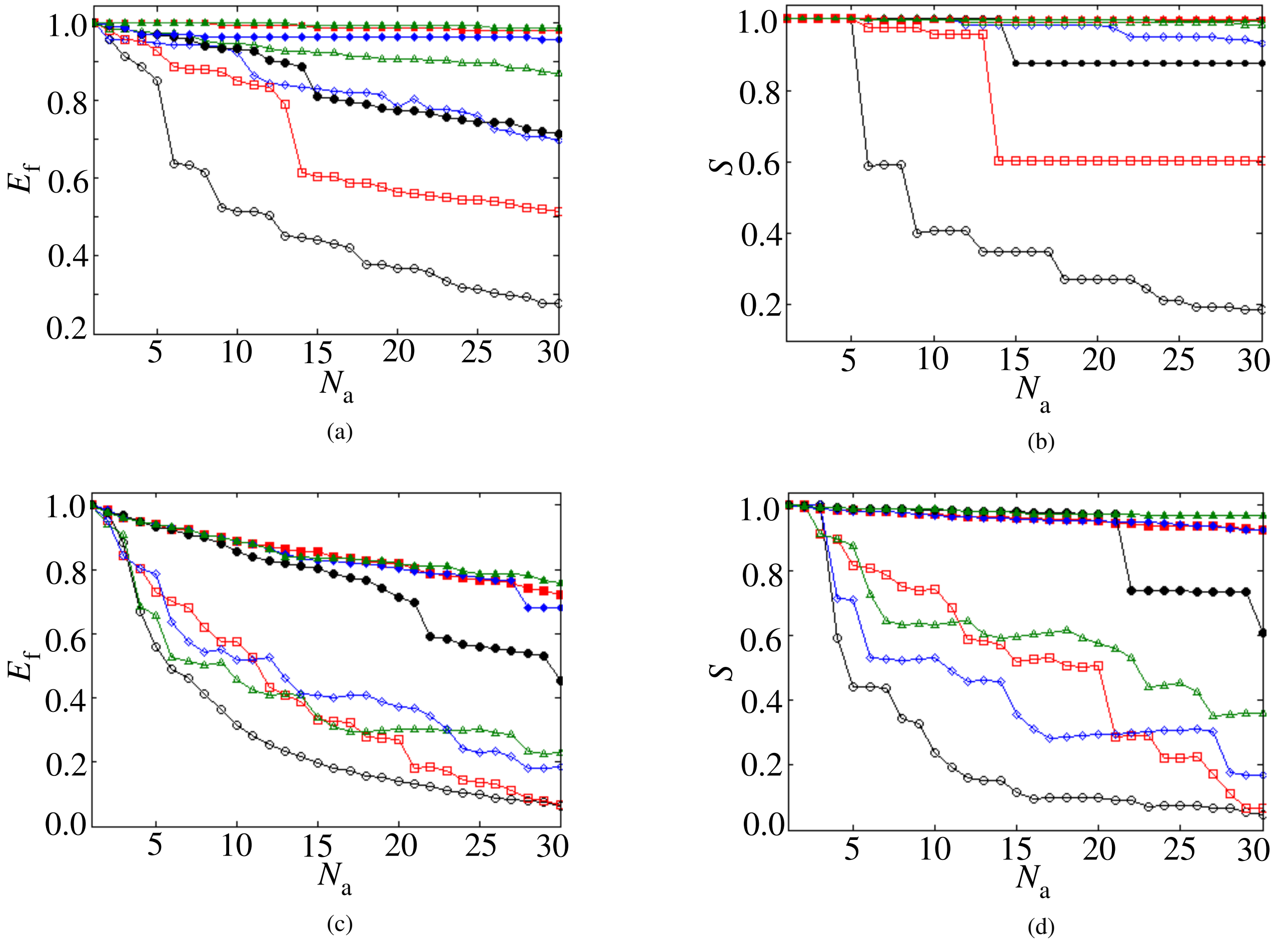
The vulnerability of a PG can be defined in terms of its performance drop when a disruptive event emerges. The key point is that such performance can be measured by using a variety of metrics. In this paper, we consider the following performance matrices.

1) The giant component is the largest connected sub graph in a network. It is studied both numerically and analytically as a function of the progressive removal of nodes and lines, which is defined as $S = {}^{N_a}/_{N_i}$. Here N_i and N_a are the numbers of nodes in the largest connected component before and after the event. Comparatively, the change of network topology can be revealed by the network efficiency since it will decrease with the increasing of path lengths after a failure.
2) The efficiency E_f is the measure of the network performance under the assumption that the efficiency for sending load (electricity, information, etc.) between two nodes i and j is proportional to the reciprocal of their shortest distance. Mathematically it can be defined as:

$$E_f = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{l_{ij}} \tag{10}$$

III. Simulation and Result of Unweighted Networks

In this section, we study the attack vulnerability of Indian PG and IEEE 118 bus by using lines and nodes attack strategies as described in Section–II. The detailed behavior



(a)

(b)

(c)

(d)

Figure 3: Connectivity loss and change in topological efficiency in the Indian and IEEE 118 bus PG due to the removal of lines and nodes. We remove N_a number of nodes and lines with eight different attack strategies. The Y-Axis represents the connectivity loss and efficiency. (a) Efficiency plot for line attack on Indian PG and IEEE 118 model, (b) Drop in giant component size due to line attack on Indian PG and IEEE 118 bus (c)-(d) Drop in efficiency and giant component size due to node attack in both the network. Eight different attack strategies are used here represented by different colors, SL: blue (diamond), DL: black (circle), HBNL: red (square), RA: green (triangle). The symbol used for node attacks are filled with parent color, HBND: black (circle), HBNS: green (triangle), HDND: red (square), HDNS: blue (diamond). Empty symbols represent attack strategies applied on IEEE 118 network and the filled symbol for Indian PG.

of both the grid for lines and nodes attack are summarized in Fig. 3. The performance of the grid was measured by the giant component size S and topological efficiency E_f. The Fig. 3 (a) and (b), shows the vulnerability for various line attack approaches. Both the network shows some distinct behavior for HBNL and SL attack strategies, but almost equally harmful to DL attack. By comparing both the network, we can observe the giant component size and topological efficiency of IEEE 118 bus network decay exponentially for DL and HBNL attack, while the Indian PG is less affected due to HBNL attack. So we concluded that large networks are robust to this type of attack. From the initial analysis, it was confirmed that the performance of the grid is not affected due to SL and RA line attack. So the dynamic based attack strategies are more suitable quantity to measure the importance of a line. For example, in case of IEEE 118 bus network after 5^{th} DL attack the efficiency and giant component size of the network drop to 60% (see Fig. 3 (a) and (b)). Similarly, in Indian PG after 15^{th} DL attack the efficiency and giant component size fall to approximately 80%. When a significant part of the network becomes detached from the giant component, both S and E_f drops simultaneously.

In case of node attack strategies, one can expect that both degree based and betweenness based attack strategies should result in similar vulnerability behaviors. However, the detailed behaviors show a variety of interesting differences between these two networks. Fig. 3 (c) and (d) summarizes the result of the node attacks measured by efficiency E_f and the giant component size S. The Indian PG and IEEE 118 bus show very distinct behaviors for dynamic based node attacks. In case of IEEE 118 network, the HDND and HBND attack strategies are almost equally harmful while the Indian PG is more vulnerable to HBND attack only (see Fig. 3 (c) and (d)). After the 5^{th} HBND attack, we can see a sudden drop in the efficiency and giant component size (approximately 40%) and Indian PG, the drop in network efficiency is 60% after 30^{th} (2% of the total node) attack. So it is sufficient to remove 10% of the total node to destroy the Indian PG completely.

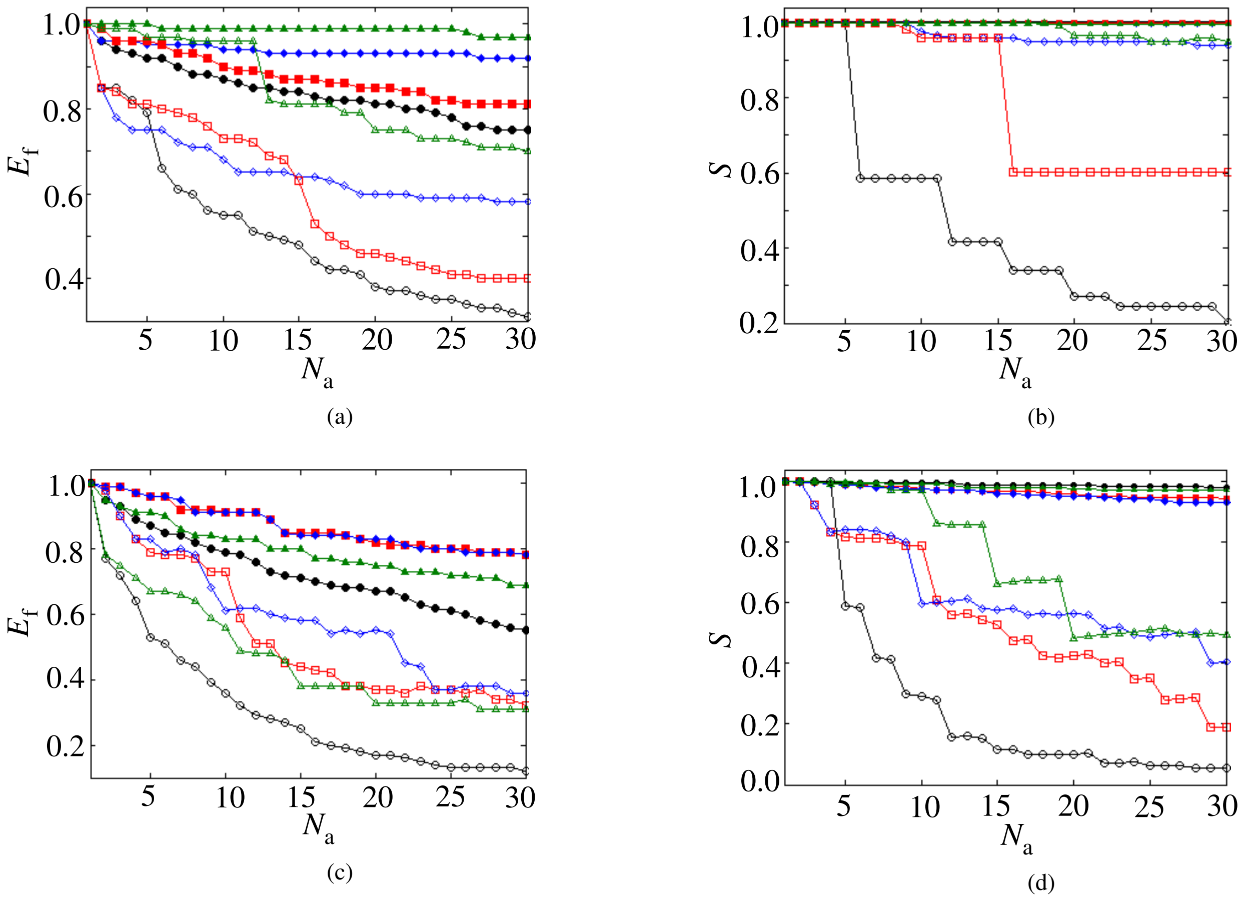


Figure 4: The weighted network vulnerability for the same networks as in Fig. 3 subject to eight different edge and node attack strategies (see Sec. III). N_a is the number of attacks and the other symbols and notations are the same as in Fig. 3.

It is very important to know that whether a graph model is representing a grid by considering either weighted or unweighted links. Most of the paper studied the power network by viewing it as unweighted and undirected. However, a weighted network analysis can enhance the representation of the PG. In particular, weight is related to the electrical concepts, such as the reactance of a line can reveal the maximum power flow that can be transmitted to a DC grid. The PG as a unweighted graph is mostly used to analyze the structural vulnerability, which is a pure topological concept. In our work in Section IV, we have considered reactance as the weight of line, but not to represent an electrical principle. We have identified the critical lines and nodes based on the attack strategies obtain from weighted and unweighted network analysis.

IV. Simulation and Result of Weighted Networks

An unweighted network is simple to build and easy for computation, for which it draws the attentions of many researchers. Such attentions resulted in several significant findings in CN theory such as the small world and the scale-free networks. Even the increase in popularity of unweighted network, it has some drawback like it ignores the important information of lines. To verify this, we simulate the Indian PG and IEEE 118 bus as weighted networks and consider reactance as the weight of transmission line. The attack strategies and method of simulation same as given in section-III.

First, we investigate the drop in efficiency due to line attacks. The result shows both the grids are affected due to DL and HBNL attack strategies. There is an almost 20% drop in efficiency of Indian PG and 60%-70% in IEEE 118 bus after the removal of thirty number of lines based on these two attacks strategies (Fig. 4 (a)). Both the grids are robust to static and random line attacks. In the efficiency plot of node attack, we can see that both the networks are vulnerable to HBND and HBNS attacks and robust to degree based attacks. The efficiency of Indian PG drops to 50% of its initial value due to the removal of 2% node based on HBND attack procedure(Fig. 4 (c)). Similarly, after 20^{th} HBND attack in IEEE 118 bus, the efficiency falls to 20%, which is sufficient to collapse the grid entirely. In Indian PG the connectivity loss is around 6% and 7% for approximately 2% loss of nodes due to HDNS and HDND based attacks. But in the case of IEEE 118 bus, the connectivity loss is more than 90% after 30^{th} attack for HBND and DL attack strategy (see Fig. 4 (d)). This section gives the details of the structural vulnerability of weighted

Indian and IEEE 118 bus networks.

V. Conclusion

It is necessary to identify the vulnerable lines and nodes to mitigate blackout risk so that their proper maintenance can improve efficiency and reliability of PG networks. This paper not proposed any new method to mitigate blackout but did a comprehensive topological analysis on the structural vulnerability of Indian PG. This paper proposes a weighted network analysis, which can enhance the representation of PG and effectively identify the critical lines and nodes in Indian PG network. The centrality index defined here is used to rank the critical lines and nodes based on the concept of CN theory. In the future work, the proposed approaches can be further improved from several aspects. Considering only topological measures in real PGs can mislead the results. So we need to synchronize both topological measures and power flow properties to get more accurate results. Further, the proposed work will be extended by including bifurcation theory, which gives more details about the phase transition in PGs.

References

[1] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, p. 026103, 2007.

[2] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Physical review E*, vol. 69, no. 2, p. 025103, 2004.

[3] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world'networks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[4] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

[5] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.

[6] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the italian electric power grid," *Physica A: Statistical mechanics and its applications*, vol. 338, no. 1, pp. 92–97, 2004.

[7] K. Sun, "Complex networks theory: A new method of research in power grid," in *2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific*. IEEE, 2005, pp. 1–6.

[8] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the european power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2465–2475, 2007.

[9] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the european power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, p. 026102, 2008.

[10] M. Rosas-Casals, S. Bologna, E. F. Bompard, G. D'Agostino, W. Ellens, G. A. Pagani, A. Scala, and T. Verma, "Knowing power grids and understanding complexity science," *International Journal of Critical Infrastructures*, vol. 11, no. 1, pp. 4–14, 2015.

[11] E. Cotilla-Sanchez, P. D. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the north american electric power infrastructure," *IEEE Systems Journal*, vol. 6, no. 4, pp. 616–626, 2012.

[12] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, 2015.

[13] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[14] E. I. Bilis, W. Kröger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

[15] P. Panigrahi, "Topological analysis of power grid to identify vulnerable transmission lines and nodes," Ph.D. dissertation, 2013.

[16] M. D. Humphries and K. Gurney, "Network 'small-world-ness': a quantitative method for determining canonical network equivalence," *PloS one*, vol. 3, no. 4, p. e0002051, 2008.

[17] A. Clauset, C. R. Shalizi, and M. E. Newman, "Power-law distributions in empirical data," *SIAM review*, vol. 51, no. 4, pp. 661–703, 2009.