A Comparative Analysis of Weighted and Unweighted Power Grid Networks

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*—This paper focuses on identification of vulnerable lines and nodes of the power grid (PG) network whose removal disrupt on its operational capability. Here the topological parameters are derived from CN theory, and these are used to identify the most important elements i.e., lines and nodes of the PGs. Based on this concept, the number of attack strategies are illustrated and also applied to different IEEE bus networks, e.g., IEEE 39 and 300 buses. We show that in case of electrical PG network, weights are related to electric concepts, and that can enhance the representation of the PG. This work identifies the vulnerable lines and nodes of both weighted and unweighted networks, and quantify the results by applying the concept to real AC power flow model. We conclude that a weighted network analysis can give a better vulnerability assessment than that of an unweighted network.**

***Index Terms*—Cascading failures, centrality metrics, complex systems, physical attacks, AC OPF.**

I. Introduction

The power grid (PG) is a critical infrastructure whose efficient operation, reliability and robustness, greatly affects national economics, politics, and people's everyday's life. A small disturbance within a grid may propagate and cause significant damage or may lead to cascading failure. The disturbance may also 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. According to National Research Council (NRC) panel of US, the Intentional attack in the key elements i.e., lines and nodes that could lead to long-term multi-state blackout [1]. For example, blackout in India, US, Canada, Italy [2], [3] and some other countries in the European Union [4], [5] have been widely studied using the concept of complex network (CN) [6], [7] and electrical engineering tool (EET) [8], [9]. Most of these studies have been focused on CN analysis due to the complexity in EET. The vulnerability analysis of PG has also been applied to investigate the effect of lines and/or nodes removal [10]. The most vulnerable lines and the nodes are identified using the different CN metrics like degree centrality, degree distribution, betweenness centrality of line and node, etc. However, this type of analysis has its own merit and demerit as it ignores the electrical properties of the PG. To overcome this problem, few works have been focused on a hybrid approach such as a CN theory approach — which has been used to demonstrate the attack scenarios in PG netwoks [11], [12]. Based on this approach works reported in [12], [13] consider that the PG network can be modeled as an unweighted and undirected ones. These investigations, however, may give an unappropriated result. A weighted network analysis therefore can be modelled for better representation of the electrical PG. In particular, the consideration of reactance as line weight can able to add some electrical feature to the topological concept for more accurate analysis [14].

The present work analyzes the both weighted and unweighted IEEE bus networks thoroughly to get the more realistic results. We derive the attack scenarios from topological matrices and apply these result on the real PG model. Section II describes the fundamental of CN and also check the small-world-ness and scale-free-ness of IEEE bus networks. Section III discusses different attack strategies and presents the simulation result of both unweighted and weighted PG network. In Section IV, the attack strategies adopted from CN are applied to IEEE 39 and 300 buses respectively, and their optimal power flow problem is also solved. The conclusion and future aspect are given in Section V.

II. CN Based Vulnerability Matrices

The PG vulnerability usually associated with an unusual event and quantified by performance drop; hence, to analyze it, we have to model its performance based on the event [12]. In this work, the degradation in the performance of PG is measured by giant component size, network efficiency, average path length. Some basic information about these topological measures are given in this section.

A. Vulnerability Matrices

Degree: For a network G, we use $V = \{v\}$ and $K = \{e\}$ to denote the set of nodes and set of lines respectively. Than the degree of a node v in an unweighted network can be defined as no of lines that are adjacent to v, i.e,

$$d_v = \sum_{e \in K} \delta_e^v \tag{1}$$

where

$$\delta_e^v = \begin{cases} 1, & \text{edge } e \text{ adjcent to node } v \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

In a weighted network, the degree of node v is the sum of the weights of all the lines adjacent to v.

Average Path Length: The mean of all the shortest path in a network is called mean path length or average path length

$$L{=}\frac{1}{N(N{-}1)}\sum_{i\neq j} l_{ij}, \tag{3}$$

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

$$L(w) = \frac{N(N-1)}{\sum\limits_{i=1}^{N}\sum\limits_{j\neq i}^{N}\frac{1}{W_{ij}}}, \tag{4}$$

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

Betweenness Centrality: The betweenness centrality defined as, the no of times that the node traversed by the shortest paths between each pair of nodes in the network. It is also valid edge betweenness centrality. Mathematically it can be written as

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

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.

The damage in a PG can be measured in terms of the degradation of its performance. In the topological analysis, performance can calculated mathematically by two parameters, giant component, and efficiency.

Giant Component: The giant component is the largest connected subgraph in a network. The phase transition due to change in giant component size before and after removal of node or line gives idea about behavior at and near the critical point. Mathematically the giant component can be written as $Y\ (k) = G(k)/G(0)$. The $G(0)$ is the biggest connected component before attack and $G(k)$ is the biggest connected component after k time attacks.

Topological Efficiency: It is an assumption that efficiency and distance are inversely proportional, which can measures how efficiently two nodes exchange information. In a unweighted network, the global efficiency is

$$E = \frac{1}{N(N-1)}\sum_{i\neq j}\frac{1}{l_{ij}}, \tag{7}$$

where l_{ij} is the shortest distance between bus i and j. The global efficiency in a weighted network is

$$E\ (w) = \frac{1}{N(N-1)}\sum_{i\neq j}\frac{1}{W_{ij}}. \tag{8}$$

B. Structural Characteristics of PG

Small-World-Ness of PG Networks: 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 are used by Watts & Strogatz to know small-worldness of unweighted and undirected networks

$$\begin{cases} L \geq L_r, \quad C \gg C_r \\ L_r = \frac{\ln(N)}{\ln(k)}, \quad C_r = \frac{k}{N}. \end{cases} \tag{9}$$

Here k is the average degree of the network. Based on this concept we have verified IEEE networks (see table I). It has been seen that the actual average path length L_a and clustering coefficient C_a are greater than random L_r and C_r in IEEE 300 bus. So this network is showing the properties of a small world network. In case of IEEE 39 bus L_r is greater than L_a, that means, it is deviating the small world characteristics.

Table I: Identifying Small-World-Ness of IEEE bus networks

Network	L_a	L_r	C_a	C_r
IEEE 39	4.749	6.271	0.05	0.0604
IEEE 300	9.944	5.6855	0.111	0.009

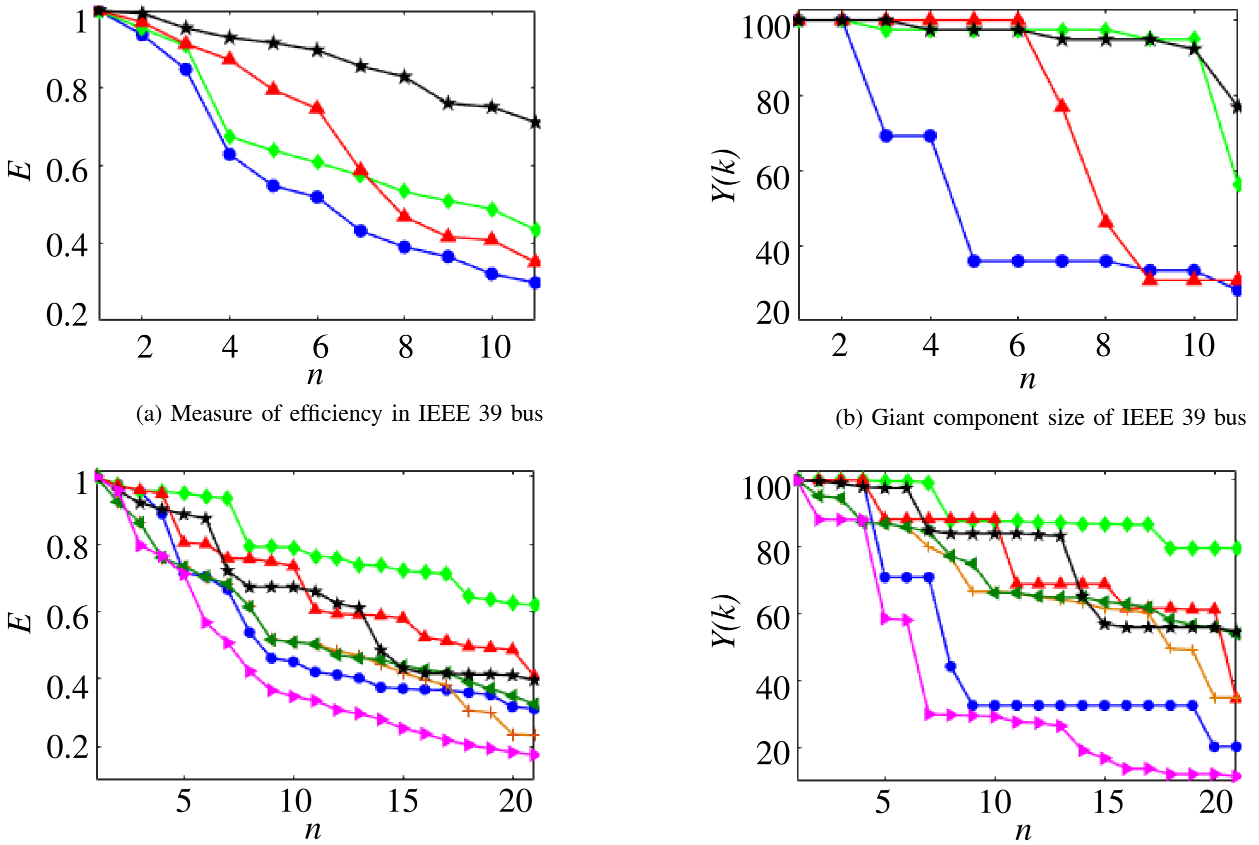
Scale-Free-Ness of PG Networks: To test whether these PG networks have scale-free characteristics, we have calculated k_{min}, γ and p-value as described by Clauset, Shalizi and Newman [15]. Here k is the vector of degree of a PG to which they fit the power-law distribution $p(k) \sim k^{-\gamma}$ for $k \geq k_{min}$. The fitting procedure of power law are also as followed.

1) For each possible choice of k_{min}, γ value is estimated by the method of maximum likelihood, and calculate the Kolmogorov-Smirnov goodness-of-fit statistic KS.
2) Estimate k_{min}. This gives the minimum value KS over all values of k_{min}.
3) Then the degree of each node k is chosen to find out lower cutoff for the power-law behavior k_{min} and computes the p-value for the Kolmogorov-Smirnov test.

Table II: Identifying Scale-Free-Ness of IEEE bus network

Network	k_{min}	γ	p
IEEE 39	2	2.99	0
IEEE 300	3	3.5	0.1380

If $p > 0.1$, the tested data could fit the power law. The tested result is given in table II, from which we found these three IEEE networks not showing any scale free properties.



(a) Measure of efficiency in IEEE 39 bus

(b) Giant component size of IEEE 39 bus

(c) Measure of efficiency in IEEE 300 bus

(d) Giant component size of IEEE 300 bus

Figure 1: Presents the changes in network transmission efficiency *E* and giant component size *Y (k)* due to different attack strategies in unweighted IEEE 39 and 300 bus networks. Here *n* in x-axis signifies the number of attacks. The color code is given to identify different type of attacks, Blue: DLA, Red: HBNL, Green: SHDN, Brown: DHDN, Light green: SLA, Black: SHBN, Pink: DHBN. For IEEE 39 bus Red: HBNL, Blue: DLA, Light green: SLA, Black: RA

III. Attack Strategies

The different attack strategies are developed having topological measures. Here we have divided these attack into lines as well as nodes attacks. The removal process is also fixed up based on dynamic and static concepts. In dynamic attack, every time algorithm was run, and vulnerable line or node is identified and thus removed. This process is repeated several times till the grid collapse completely. However in the case of static attack only once we ran the algorithm and sorted out the high betweenness or degree nodes or lines in descending manner, then remove one by one. Total 8 attack strategies are developed: DLA (dynamic line attack), SLA (static line attack), RA (random attack), HBNL (high betweenness less reactance line attack), DHBN (dynamic high betweenness node), SHBN (static high betweenness node), DHDN (dynamic high degree node), SHDN (static high degree node).

A. Simulation Result of Unweighted Networks

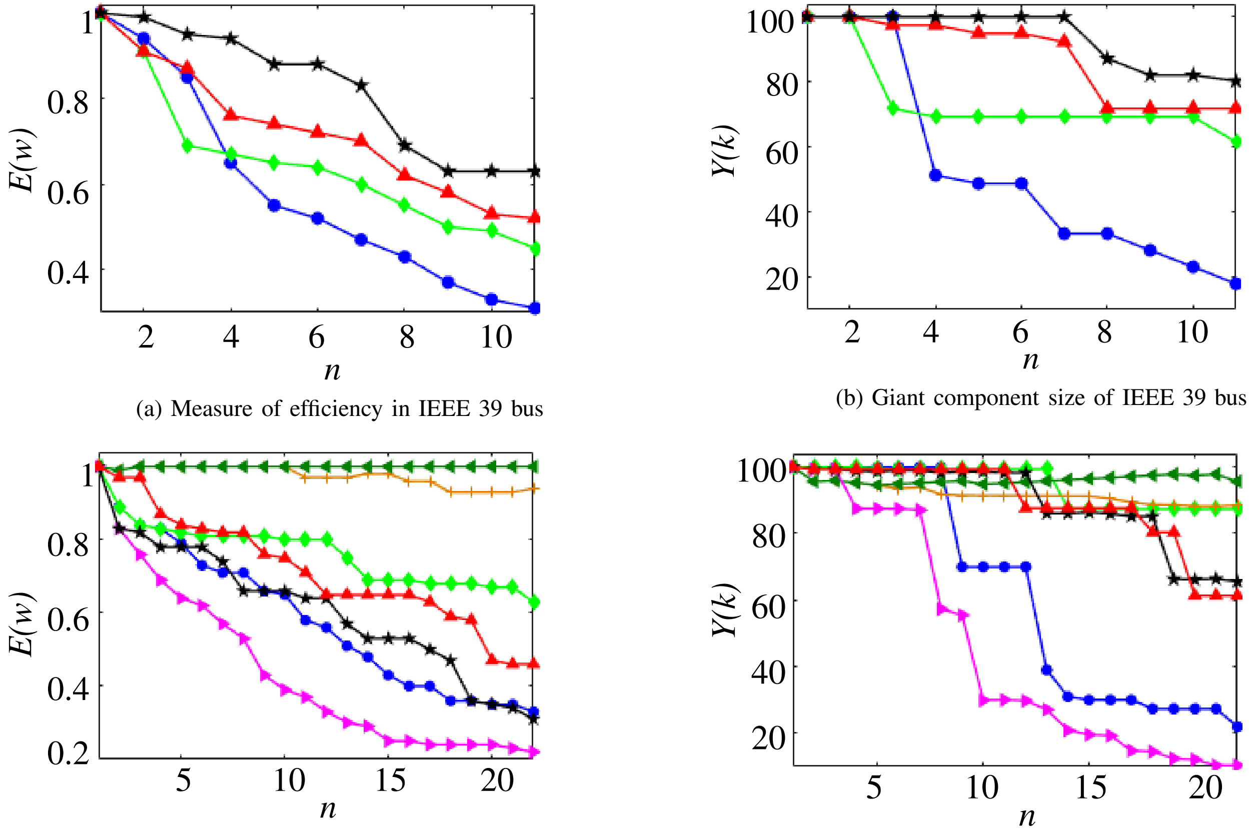
Node Attacks:

From Fig.1, the IEEE PGs shows different features under intentional and random attacks including seven different attacks. The horizontal axis is attack number *n*, and the vertical axis is efficiency *E* and giant component size *Y (k)* respectively. In IEEE 39 bus it is observed that the grid is completely robust to random attacks, which means that decrease in giant component size and efficiency is very less with the increase in the number of node or line attacks (see FIG. 1 (a) and (b)). So we skip random attack strategies in IEEE 300 bus model. However, *E* and *Y (k)* decreases substantially especially in the starting when the network is under intentional attacks. It indicates that small world networks are vulnerable to intentional attacks.

The network transmission efficiency *E* and the giant component size *Y (k)* changes in a similar manner in IEEE 300 bus under dynamic high betweenness node attack (DHBN) (see Figs. 1 (c) and (d)), which is also more destructive than any other type of attacks. Next, to the betweenness based dynamic attack, IEEE 300 bus is vulnerable to dynamic node degree attack (DHDN). After 20 number of such attacks, the drop in efficiency and giant component size is 60-70%. However, this type of attack is more destructive when evaluated using the efficiency *E* (see Fig. 1 (c)). From the result, we found that static based attacks strategies are less effective in comparison to dynamic attacks.

Line Attacks:

From Fig. 1 (b) and (d) it is clear that the dynamic line



(a) Measure of efficiency in IEEE 39 bus

(b) Giant component size of IEEE 39 bus

(c) Measure of efficiency in IEEE 300 bus

(d) Giant component size of IEEE 300 bus

Figure 2: Change in network efficiency $E\ (w)$ and giant component size $Y\ (k)$ in weighted IEEE 39 and 300 bus networks due to different attack strategies. The color codes are same as Fig. 1 color codes.

betweenness attack (DLA) is more destructive in IEEE 39 and 300 bus networks when evaluated by using the giant component index $Y(k)$. In both the networks there is a sudden drop in $Y\ (k)$ of 30% after 2nd and 5th attack receptively. This condition shows the faster structural vulnerability in IEEE 39 and 300 buses to dynamic line attack. The network transmission efficiency E also decay similarly in both the networks for this attack strategy. From Fig. 1 (a) and (b) it was clear that high betweenness node less reactance line (HBNL) attack strategy is more destructive in smaller networks in comparison to large network like IEEE 300 bus. In Fig. 1 (a) and (b) the changes in E and $Y\ (k)$ is very less due to the random attack, which shows the grid robust to this attack strategy.

B. *Simulation Result of Weighted Networks*

Node Attacks:

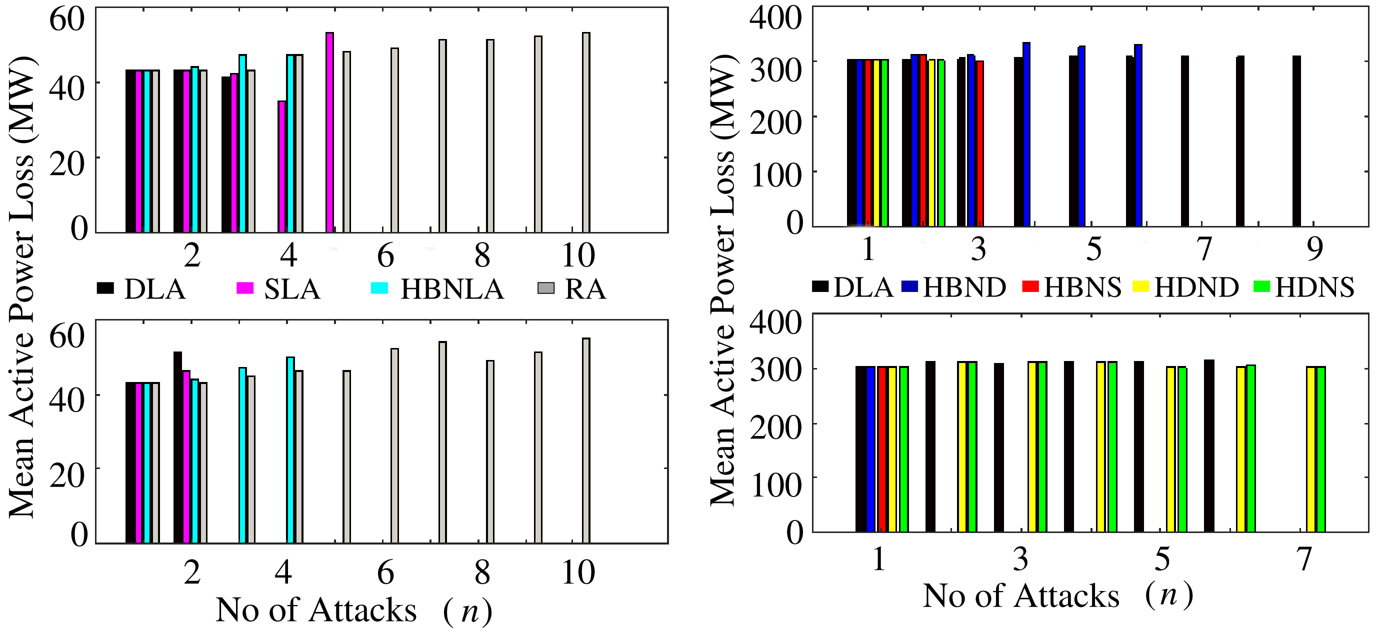
We simulate IEEE models as weighted networks by considering reactance as the weight of transmission line. The attack strategies and method of simulation same as given in Section III. From the previous section, it is clear that in unweighted networks are highly vulnerable to betweenness based dynamic attacks than any other attack strategies. Also during the weighted network analysis, we found this type of attack strategies are more dangerous than any other attacks. Both the indices in IEEE 300 bus drop abruptly under DHBN attack, for which $Y\ (k)$ and $E\ (w)$ decrease nearly to 10% and 20% respectively after the 20th attack and the vulnerability of this small-world PG network is demonstrated clearly (see Fig. 2 (c) and (d)). Here one interesting thing we observe that static high betweenness attack (SHBN) is comparatively more destructive than degree based attacks when evaluated using the efficiency $E\ (w)$ (see Fig. 2 (c)). The efficiency $E\ (w)$ decreases to 89% after 1st SHBN attack but there is no change in $E\ (w)$ after 10th DHDN attack. This result reveals the weighted IEEE 300 bus network is robust to degree based attack strategies.

Line Attacks:

Similar to unweighted networks, in weighted networks also the dynamic line attack is more destructive than any other line attacks (see Fig. 2 (a)-(d)). In IEEE 39 bus, there is also an abrupt change in $E\ (w)$ and $Y\ (k)$ due to static line attack (SLA). After 2nd attack the $E\ (w)$ and $Y\ (k)$ decreases to 70%.

IV. Electrical Analysis of IEEE Networks

The aim of the AC power flow analysis conducted here is to provide the state of the system after the electric PG is unbalanced due to random or intentional attacks. To manifest



(a) Power flow analysis of IEEE 39 bus

(b) Power flow analysis of IEEE 300 bus

Figure 3: The upper plot shows the result of unweighted networks and the bottom one for weighted networks. Different color represents types of attack strategies, DLA: Black, HBND: Blue, HBNS: Red, HDND: Yellow, HDNS: Light green. In case of IEEE 39 bus, SLA: Pink, DLA: Black, HBNL: Cyan, RA: Gray

the feasibility of the approach proposed in weighted networks, we particularized it to analyze the consequences of some physical attack scenarios against the IEEE 39 and 300 bus PG networks. These attack strategies are same as defined in Section III.

A. AC Optimal Power Flow

The objective of the PG is to supply the power to the consumer with lower operation costs and provides economic and social benefits by maintaining the stability of the system. This objective can achieve by the computation of optimal power flow (OPF). The aim of OPF is to minimize the power loss in the system. Mathematically it can be presented as

$$\min F(P,Q) = \sum_{i=1}^{G} P_g(i) - \sum_{j=1}^{L} P_l(j) \tag{10}$$

Here P and Q are the active and reactive power to be determined and G and L are the set of generators and loads buses. The $P_g(i)$ and $P_l(j)$ are the active power at the generator i and load bus j. The OPF includes different constraint like line capacity constraint, generation constraint, and power flow constraint. Here we followed a quasi-dynamic procedure to illustrate the simulation model, based on AC optimal power flow. The process of this simulation is as follows:

1) At initial condition, we run the AC OPF and calculate the active power of generator and losses occurs during power transmission
2) Remove highly loaded lines or nodes and recalculate the AC OPF, and this process continues until the system does not collapse completely.
3) Check whether the computation converges or not. If it converges, then print the result and run the algorithm again. If not then go for next step.
4) Check is there any isolated bus or island formed. If no then, check whether a significant corrective action required or may be there is the probability of complete collapse of the system. If yes then to go to next step.
5) Solve the island problem and Compute the total generation output and total load demand in each island network. Otherwise go back to Step 1.
6) Finally compute the load loss. In this process, the ratio of the total load loss to the total load demand can be used to describe the scale of the blackout.

At each step a line or node is taken out due to intentional attack or mishandling a contingency situation by the operator, an algorithm loop takes place. The simulation is stopped, only when the system completely collapses or blackout. There are several solutions for non-linear OPF methods. For the test case presented here, we use the Newton-Raphson method. For each one of the 360 (300 targeted and 60 random) attack scenarios, we analyze the system response by calculating active power loss. The response was captured based on targeted attack scenario from the weighted and unweighted network. Some assumptions and parameter values are used during the simulation procedure.

1) The attack against a substation leads to its complete incapacitation. No redundancy (e.g., spare or alternate transformers) is taken into account.
2) The double line between two terminals is taken into consideration during the system response analysis.

3) The probability of hidden failure was negligible.
4) During the system response analysis we fixed the power flow capacity of each transmission line.

The Fig. 3 shows bar graph in different colors where each color signifies different attack scenario. The color bars are limited to the number of attacks, and the final progression of the bar shows the occurrence of the blackout in PGs. The result shown in the upper part of the figure is for unweighted networks, and the bottom of the figure illustrates the result of the weighted network. Fig. 3 (a) demonstrate the result of IEEE 39 bus. Here the progression of the bar graph stopped after the second DLA and SLA attack strategies developed from the weighted network analysis, but the grid due to unweighted network attack strategies can sustain few more attacks. It signifies that the blackout is happening more faster in the weighted IEEE 39 network than unweighted network due to these two attack strategies. In the case of weighted IEEE 300 bus network, the load flow problem does not converge to a solution in most of the attack scenario. The grid is not able to sustain even for a single weighted betweenness based attack strategy, but it can resist more than five such attacks defined by unweighted network analysis. But the IEEE 300 bus is robust to the degree based attacks identified from weighted network analysis in comparison to unweighted networks (see Fig. 3 (b) upper plot). It's a natural phenomenon that the degree based attack in unweighted network alway vulnerable than weighted networks. Similarly, we can see the grid collapse completely after 6th dynamic line attack, developed from weighted network analysis, but the grid can sustain up to nine such attacks identified from unweighted network analysis. The above result shows the occurrence of the blackout in the weighted network is faster than unweighted networks.

V. Conclusion

We use CN theory to find out critical lines, and nodes of IEEE 39 and 300 bus networks. We compare both weighted and unweighted PG networks after several targeted attack scenarios. Further, we extend this attack scenario to AC power flow model of IEEE 39 and 300 bus networks that take into account the structure and internal behavior of PG networks. These case studying reveals that the effect of the dynamical betweenness based attacks on the nodes (substation) and lines (transmission lines) derived from weighted network analysis are far greater than the one observed in the unweighted network. The random attacks in both the case have a very negligible effect on grid integrity. Hence the methodology based on weighted network proposed here can help grid operators to identify the critical elements and contingency situations to which an electrical PG is most vulnerable. It can also contribute to choosing the appropriate protection and prevention measures against intentional attacks. This work gives a direction to the use of CN as a weighted network in power system research, which will improve structural vulnerability assessment and identification of important lines and nodes.

In the future work, the proposed approaches can be further improved from several aspects. Only the simple topological measures in real PGs is not enough for the indication of general vulnerability trends. 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 sensitivity analysis like PTDF, LODF concept. We will take entire Indian PG network as a benchmark to investigating the cascading failure, which will be more meaning full.

References

[1] N. R. C. U. C. on Science and T. for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academy Press, 2002.

[2] G. Zhang, Z. Li, B. Zhang, and W. A. Halang, "Understanding the cascading failures in indian power grids with complex networks theory," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 15, pp. 3273–3280, 2013.

[3] U.-C. P. S. O. T. Force, S. Abraham, H. Dhaliwal, R. J. Efford, L. J. Keen, A. McLellan, J. Manley, K. Vollman, N. J. Diaz, T. Ridge *et al.*, *Final report on the August 14, 2003 blackout in the United states and Canada: causes and recommendations*. US-Canada Power System Outage Task Force, 2004.

[4] 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.

[5] 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.

[6] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

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

[8] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with dc power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, 2015.

[9] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 396, pp. 204–211, 2014.

[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] Y. Zhu, J. Yan, Y. L. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274–3284, 2014.

[12] 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.

[13] 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.

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

[15] 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.