

## Smart power grid vulnerability analysis in composite system through power grid modelling

Shouvik Kumar Samanta, Chandan Kumar Chanda

Department of Electrical Engineering, Indian Institute of Engineering Science and Technology (IIEST), India

### Article Info

#### Article history:

Received Apr 22, 2019

Revised Feb 19, 2020

Accepted Apr 15, 2020

#### Keywords:

Complex network

Damage index

IEEE 39 bus

Network efficiency loss

Power model

Smart grid

Smart vulnerability index

Vulnerability analysis

### ABSTRACT

A though the number of traditional literature reviews most of the researchers in this area have concluded that modern intelligent electric network a referred standard new model which is considering for proposed power flow model analysis of smart power grid vulnerability through composite network. By the theorem of max-flow and complex power network theorems that are represented the advance vulnerability indices for pick out endangered lines of the smart grid network. In other hand, the power flow model and existing models simulation are examined on the IEEE 39-bus test model. The results of the simulation introduced that the proposed concept of grid model, estimation and the index application are more adequate in smart grid weakness power and efficiency analysis. In this paper briefly summarize the methods and probabilities of a vulnerability index which was explained in specific in references. Therefore, it is imperative to further implement new models and new tools so as to reach the novel state and moderate the huge or massive potential shutoff.

This is an open access article under the [CC BY-SA](#) license.



### Corresponding Author:

Shouvik Kumar Samanta

Department of Electrical Engineering

Indian Institute of Engineering Science and Technology, Shibpur

Howrah 711103, India

Email: samanta\_b007@yahoo.co.in, ckc\_math@yahoo.com

## 1. INTRODUCTION

In the competitive electricity market a new risk of cascaded events are rapidly rising of the whole power system scenario. Renewable energy resources and distributed generation, increase the stress in the system [1] network. After all, massive scale potential shutoff still occur all over the globe from time to time [2] because the regular growth of smart power grids. Complex networks theory have been surveyed intensively to solve empirical problems in large-scale complex power systems over the recent years. A power grid has worked out the most complex systems which is human-made. In consonance with recent study, it is to be illustrated as “small-world network” [3] that are highly accumulated. In the other hand, in spite of many nodes have not neighbours in the network. One node can be arrived from others by some few stepping’s [4, 5].

In power grid network, this architecture can bear a precise electrical distance between generators and loads although the grid size is enormous. Transmission capacity of large power grid network should be minimum when fault occur through these paths. Furthermore, power grid network demonstrate the “scale-free network” [6] properties. This is popularly known that “scale-free network” can be seen as resilient to random failure and weak at intended attacks [7]. Consequently, cascading grid failures and severe blackouts [8] would cause due to elimination of a few important lines and nodes in a grid. Moreover, a power grid system is vulnerable, when some foremost nodes of grid and lines are faulted. Thereafter, how precisely pointing out these lines and nodes are till as questionable. It has to pronounce that new implementation of

complex network field has contributed a novel regulation approach for power system vulnerability analysis [9]. Presently, most research is attentive on network topology architecture. Hence in references [10, 11] the topological and structural vulnerability methods of network for large-scale power outage in Italy as well as North American were surveyed. From these surveys, different techniques and indices, such as degree of allocation, shortest length path and radius are extensively used to examine the most effective lines of smart power grids. Such an example by references [12, 13] in methodology based on an American power grid is analysing to get fruitful result. Subject to these fundamental concepts, cascading failures in reference [14] of operational technique has been explained and efficiency depended cascading model failures were proposed. In view of this, the efficiency is explicated through edges efficiency by the harmonic composition.

Some fundamental modelling and conventional methodologies reviewed in reference [15] through structural vulnerability. In addition, two criteria depended on topology and load distributions pointing out the critical lines which are propounded at reference [16]. The consequences explain how can influence the network's capability by its link and location. Except conventional topology physical models, in reference [17] efficiency model of electrical topology is propounded, whereas depending upon the electrical topology [18] weighted graph is described on the power grid. Besides this, it is presumed in these models that the least resistance path is followed by the power flow. So therefore, weight lines of the power system are familiar with the admittance. In reference [19] netability which measures under normal operating states the performance of power system is contemplated. Hence in reference [20] is introduced cascading based model. Different critical system parameters of power grid are involved in reference [21]. Similarly power angle, Kirchhoff's Laws etc. can reach a closer approximation of real power grid. The problem is how much effective on network loss efficiency and damage efficiency in complex network to justified in higher combination of buses and generator module.

Most of the effort just analyses a power system but noted that did not finding centrally methodological smart control with several server security bounded problems considering the shortest path based algorithms or the efficiency model from the complex network (CN) theory [22, 23]. In these surveyed, a smart power grid model is illustrated through undirected weighted graph by shortest path model or efficiency model. Hence the power is controlled in a real power grid with the generation capacity, distribution of load probability, voltage and angles of rotor etc. So the power flows must have a direction. Besides, power cannot flow along with the shortest path or any efficient path. Truly, the power flows from the rich side of generation to the rich side of load determined by complex integration of all factors through parallel paths, which can be noted by analysis of power flow. By means of the flow features and its directions together cannot investigated with any prior techniques. Considering CN theory, the main focused of this paper is to establish a new improved model and analytically aim that approaching to analyse the smart vulnerability of a power grid system. At first, depended model on power flow is recommended. Therefore, it is a real power grid closest approximation. So, a novel characterization in smart vulnerability index is preceded to point out the set of vulnerable lines of smart power grid system. Higher vulnerability index of lines are treated as more damage in the power grid if they shut off.

## 2. NETWORK TOPOLOGY AND ELECTRICAL EFFICIENCY ANALYSIS MODELS

### 2.1. Elemental topology and structural analysis model

Power grids have a reliable number of buses with transmission lines connected to each other. Depending on the topological analysis of grid power, a graph  $S$  consist  $K$  edges and  $M$  nodes, where edges denote transmission lines and nodes denote buses respectively. The networked graph  $S$  [24] describes an adjacency matrix  $(M \times M)$ , which elements  $A_{ij}$  illustrate the physical integration in the network. From the adjacency matrix the key physical properties of the network can have acquired. In the network integration is mainly elucidated by clustering coefficients and the nodal degrees. Intimation of structural vulnerability analysis could give by analysing these properties in the power grid.

### 2.2. Electrical topological efficiency model

The electrical topological model can illustrated connections and the substantial structure of the power system. However, a complex network structure describe through the power grid. There are different electrical properties such as current and voltage which can influence the execution of the total network. Therefore, an advanced electrical efficiency model was initiated depending on the physical topology. In the long and distinct period of history model of electrical efficiency, the network of a power grid  $S$  is an admittance matrix  $(M \times M)$ , where  $Y_{ij}$  denoted by the electrical efficiency of the edge of grid. In the admittance approach, the network voltage-current characteristics equation can be described as:

$$\bar{I}_B = \bar{Y}_B \bar{V}_B \quad (1)$$

where  $I_B$  is the bus currents injection vector and  $V_B$  is the bus voltages vector relative to the slack bus and  $Y_B$  is bus admittance matrix, illustrated in (1).

$$\begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ \vdots \\ I_n \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & \dots & \dots & Y_{1n} \\ Y_{21} & Y_{22} & \dots & \dots & Y_{2n} \\ Y_{31} & Y_{32} & \dots & \dots & Y_{3n} \\ \vdots & \vdots & \dots & \dots & \vdots \\ Y_{n1} & Y_{n2} & \dots & \dots & Y_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ \vdots \\ V_n \end{bmatrix} \quad (2)$$

where:

$$Y_{ij} = \begin{cases} -(G_{ij} + jB_{ij}), & i = j \\ \sum_{i \neq j} (G_{ij} + jB_{ij}), & i \neq j \end{cases} \quad (3)$$

The parameters  $G_{ij}$  and  $B_{ij}$  shows as conductance and susceptance in between  $i$  and  $j$  node respectively. The bus matrix definition employed here captures together i.e. the real sections and imaginary sections in admittances of line. For pairing node  $i$  and node  $j$  which do not take part of a direct substantial connection, i.e.  $Y_{ij}=0$ . Furthermore  $Y_{ij}$  is the line admittance among the  $i$  and  $j$  node. The IEEE 9 bus electrical model shown in Figure 1 through simulation modelling for analysing the efficiency. The IEEE 9 bus electrical model is an example for this test system shown in Figure 2. An undirected graph is considered as the electrical model. Edge weight is denoted by electrical efficiency.

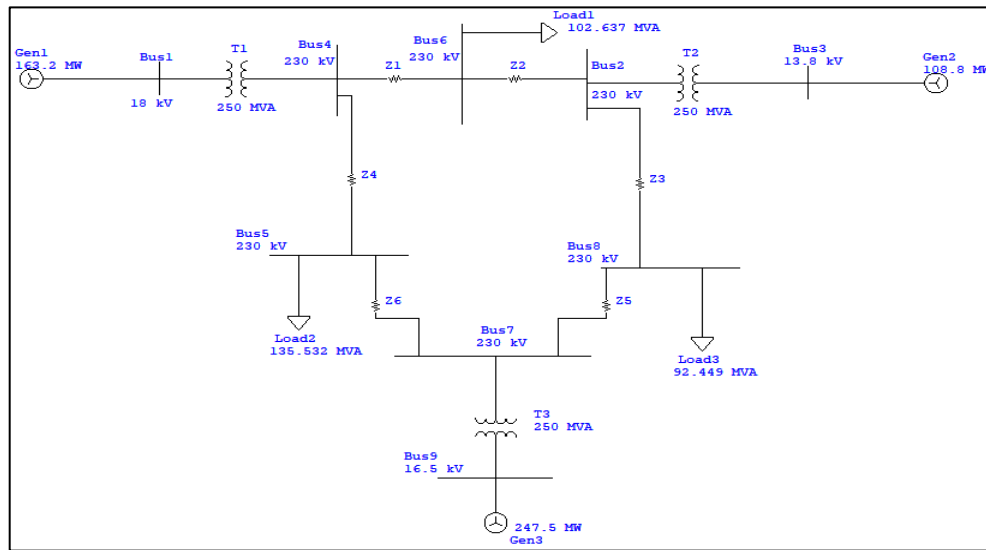


Figure 1. IEEE 9 bus electrical model

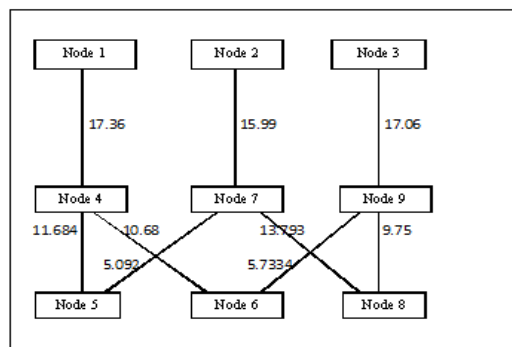


Figure 2. IEEE 9 bus system model for electrical efficiency

For this model, the electrical efficiency of edge between nodes  $i$  &  $j$  means power transmission level between the two nodes. Assuming transmitted power pursue through least resistance track in a circuit. In other words, the edge with higher  $Y_{ij}$  can transmit extra power in the system. As such based on performance, the average network efficiency  $E$  is engrossed, which is defined as:

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} Y_{ij} \quad (4)$$

In the cascading process events, if the each line efficiency changes, the average network efficiency  $E$  also change. The network loss efficiency [25] during collapses is illustrated as the damaged efficiency of network  $E_d$  is given by:

$$E_d = \frac{E_0 - E_f}{E_0} \quad (5)$$

where the fundamental network average efficiency is  $E_0$  and after cascading faults final network average efficiency is  $E_f$ . Therefore, it can be observed network sensibility of a power system by estimating  $E_d$  for collapse [26] on various transmission lines. If the most damage line which removes from network, biggest  $E_D$  is picked up as the most sensitive line in the power grid. So IEEE 9 bus system model analysis through transmission efficiency shown in Figure 3 and power flow based analysis are shown in Figure 4.

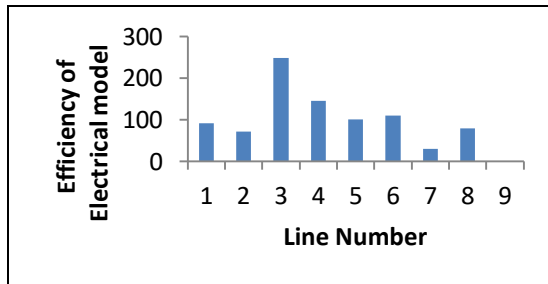


Figure 3. IEEE 9 bus system for electrical transmission efficiency

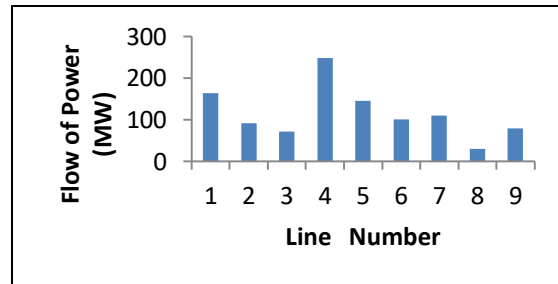


Figure 4. IEEE 9 bus system power flows on transmission

Hence the admittance of transmission lines of a power system acknowledges by the electrical efficiency model. So it may be used to identify the critical lines [27] as well as physical structure vulnerability. A comparison model between electrical efficiency and topological is exposed in reference. The comparative results show that the model of electrical efficiency has a superior performance. It identifies the vulnerability of power grids than the topological structure model.

### 3. ELECTRICAL POWER FLOW BASED PROPOSED MODEL

It is shown that electrical power flow based proposed model of IEEE 9 bus system in Figure 5. So, overcome this issues, weighted directed network is proposed for power flow network model and the following assumptions are made by:

- Transmission lines and buses of network model are identified to edges and nodes. Each node has completely steady and each edge is two stages i.e. working or faulted.
- The elemental network is self-loops free and connected.
- Each edge direction has the transmission line power flow direction. By steady state power flow [28] each edge is weighted.
- Besides the source nodes and sink nodes, the degrees of all nodes are 2.

In the model nodes have no the same functions in a directed graph. For this flow of power model, nodes are ordered as four various types. The input of a node is denoted as  $P_i$  and the output power flow is  $P_o$ . By  $L_n$  load is denoted and the generation node is denoted by  $S_n$ . Each type of node of power flow maintains the following criteria:

At Source nodes:  $P_i=0$ : it represents grid generator buses. Thus, in this case no flows of input.

At Sink nodes:  $P_o=0$ : load buses represent which mean flows of input. Sink nodes have no outputs.

Kirchhoff's Law always obey by Transmission nodes i.e.  $P_i = P_o$ . The incoming flow equal to the outgoing flow for the case of any intermediate node. Transmission load or generator nodes should satisfy:  $P_i = P_o + L_n - S_n$ . Commonly, in a real system grid there are more than single generator and load. Thus the advance model has multiple nodes of source and multiple nodes of sink. This will instigate the procedure of dealing with the multi-sources and multi-sinks problem in the later part. This model is designed on a directed graph and power flow is designed as weighted. Figure 5 shows an electrical power flow model of IEEE 9 bus system model. Flowchart shown in Figure 6.

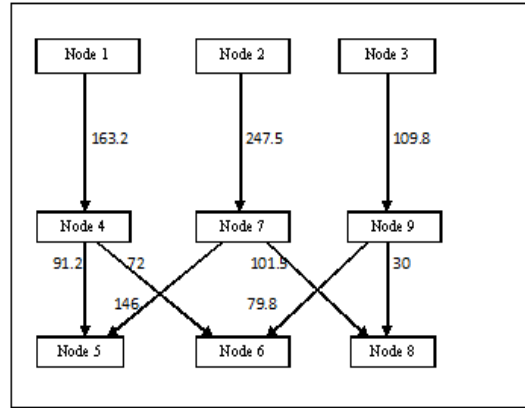


Figure 5. IEEE 9 bus system model for electrical power flow

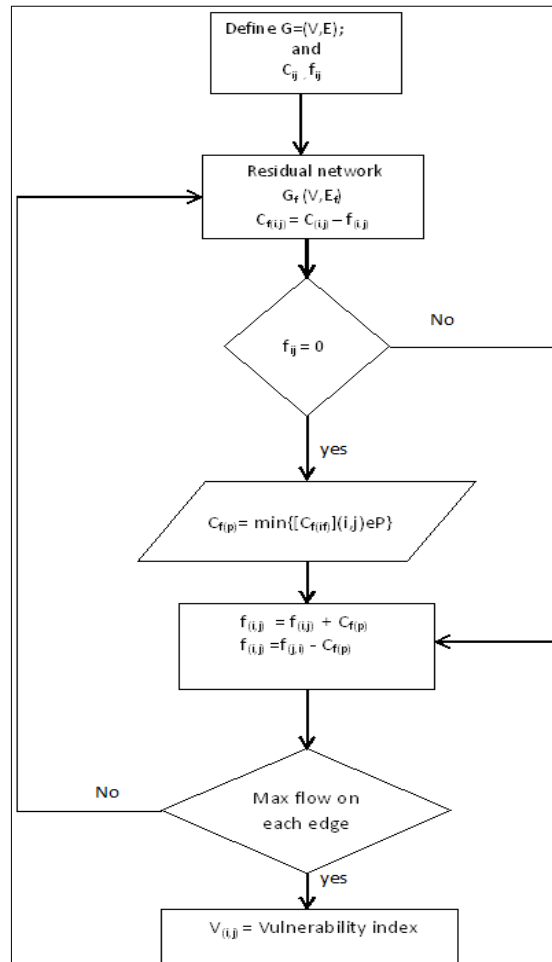


Figure 6. Flowchart of the vulnerability index and power flow

If a network has represented  $m$  no of sources and  $n$  no of sinks, since let flow of maximum power is  $S_{MAX}^{uv}$  from node  $u$  source to the node  $v$  sink and let  $S_{ij}^{uv}$  be the part of the flow pass through the edge  $E_{ij}$  of the network. Thus we define the Smart vulnerability of edge  $E_{ij}$  to be:

$$V_{ij(Smart)} = \frac{\sum_{u=1}^m \sum_{v=1}^n S_{ij(t)}^{uv}}{\sum_{u=1}^m \sum_{v=1}^n S_{MAX(t)}^{uv}} \quad (6)$$

Thus, using (6), the lines can be ranked with the smart vulnerability index depended on the smart power flow. Higher values of index lines are drawn as a high ranked in these analyses. Then smart ranking index method can be given as:

- Establish network model connection in power grid system.
- Examines steady state power grid flow and collects data.
- From previous readings edge Weight in network model gained power flow and helps to identify the flow directions.
- For each combination of source-sink in network at particular time is to determine the maximum flow.
- Compute smart vulnerability index  $V_{ij(smart)}$  with the Sum up of flow values with time.
- As stated in vulnerability index based values lines are ranked.

The IEEE 9 model bus system is examined with the comparative between model of electrical efficiency and proposed model. A sample is shown here. The V-index distribution of the IEEE 9 model bus system is shown in Figure 7.

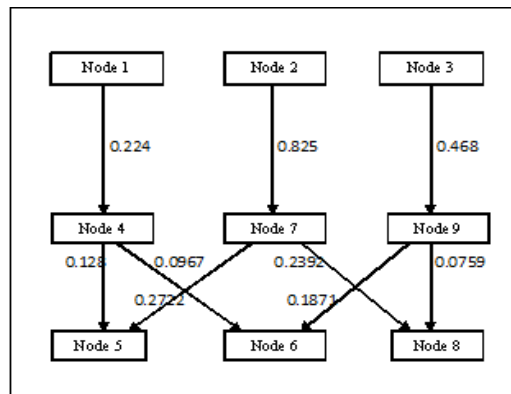


Figure 7. Distribution of V-index for IEEE 9 bus system model

The edges are ranking by vulnerability index and efficiency respectively. The maximum amount of load capacity is  $L$  examined here as the network performance measure. The line damage index of the system model network is illustrated as:

$$D_i = \frac{L_0 - L_f}{L_0} \quad (7)$$

where  $L_0$  is the initial load capacity and after removing the line from the system network final load capacity is  $L_f$ . The efficiency of damaged index also represents the line load loss in time of fault. Please note that in these system lines 3, 2 and 10 are the bus lines are connected to the generator bus directly. The power flow of this system is not converging when these lines are removed from the system. The generators are shutdown from the system directly when the elimination of important lines [29] respectively with generators, those lines have excessively higher smart vulnerability index shown in Figure 7. From Table 1 we are seen that comparative ranking between the two models are shown. According to the electrical efficiency ranking order is 3, 4, 6, 5, 1, 8, 2, 7 and 9, which are not meeting the practical outcome. Therefore, for the sake of the practical damage order ranking is 2, 7, 3, 9, 5, 8, 1, 4 and 6, realistically the practical damaged value of data is shown on table. The outcome shows that grid model power flow have a better ranking presentation to identify the important lines.

Table 1. The damage based on vulnerability ranking in IEEE 9 bus system model

Sl. No	Data according to line number	Ranking								
		1	2	3	4	5	6	7	8	9
1	Electrical efficiency model Ranking	3	4	6	5	1	8	2	7	9
2	Power flow model Ranking	4	1	5	7	6	2	9	3	8
3	Practical damaged ranking	2	7	3	9	5	8	1	4	6

#### 4. THE MODEL ANALYSIS AND CASE STUDY

The previous methodology is carried out and explained for smart vulnerability analysis in the before section. So the New England or IEEE 39 bus system are calculated and examined depended on previous methods. The smart vulnerability index and electrical efficiency of each edge in the grid system are strategic and standardize upon their mean value respectively. The standardized values distribution on the lines shows in Figure 8.

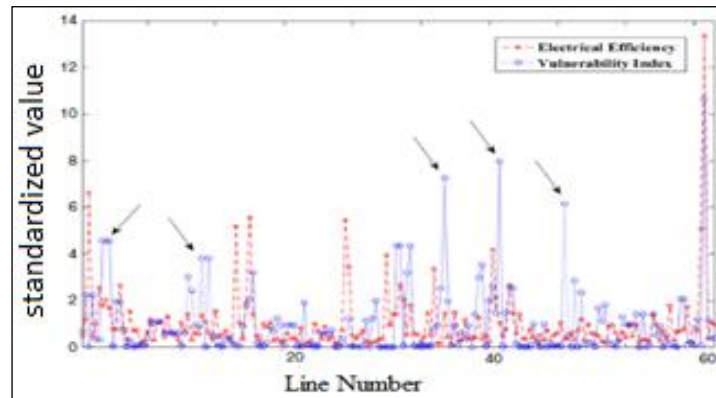


Figure 8. Standardized electrical efficiency and smart vulnerability distribution index of New England bus system

Electrical efficiency is low in some lines. It is less important in conventional model. These lines are critical in the entire system when these are literally with high smart vulnerability index. From Figure 8, the outcomes are distinctly different. Vulnerability index distribution value versus the lines number characteristics is shown in the Figure 9. It distinctly said that smart vulnerability index of most lines of New England test bed have low values. Approximately 85% lines of grid have low vulnerability index i.e. 0.045. Furthermore, the remaining 15% lines have high smart vulnerability indices. These are more critical in the proposed test system. So the proposed index in vulnerability analysis on simulation platform is illustrates the performance. As stated in the vulnerability index ranking random attacks and targeted attacks are set on 10. The set results are applied on simulation. Random attacks are applied on randomly selected failure lines and targeted attacks are applied on critical failure lines which are high smart vulnerability index.

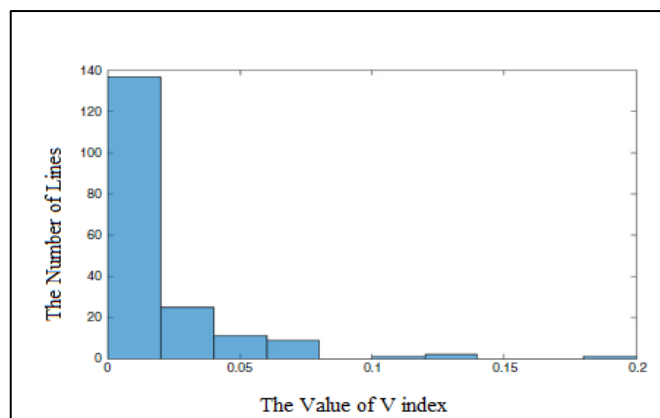


Figure 9. New England bus system value v-index distribution and the number of lines

The random and targeted attacks characteristics are shown in Figure 10. According to different attacks power grid load capacity are different. The capability of the network drops down to 75% after 10 intended attacks. Now the random attacks the capability comes down to about 98%. If the index values of lines are higher, it is more critically vulnerable to the grid system. This simulation result shows in complex network theory scale-free networks characteristics are similar with the results. Particularly, the grid system is resilient to random attacks and fragile to intended attacks. Furthermore, the simulations have been implemented for the analyse [30] of power flow and electrical efficiency performance which is model for vulnerability index. So therefore we execute the analysis of 10 targeted attacks. The targeted attacks lines are omitted the top 10 ranked lines. Load shifting is checked by the different types of models and is identified by the critical lines. The highest power flows occur in generator heavy area and there is not considerable amount affected by the attacks. On the other hand, the outcome is meaningful or notable when the power flow models points out higher ranker attacked lines. The grid system created a substantial load shifting in the network due to the overcritical lines mostly dropped down. There are detailed data also shown in the load shifting.

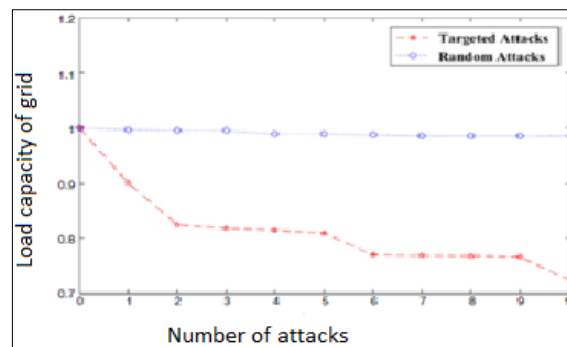


Figure 10. Different targeted and random attacks on the load capacity of grid system

In Figure 11, after attacks there are demonstrated in transmission lines the change of power flow variation [31]. In the above figure, a positive value of power shift occur in the graphical scenario that means despatcher line bears more power than the starting value. When the negative amount of power shift during the attacks shows that line losses power. From Figure 11, a small changed occur when the power flow distribution designed by electrical efficiency model with before and after the attacking stage. Most of the power gaps are less than 75 MW. Load shift occur over 100 MW in two or three lines. Larger amount of power shifts does not occur if the lines in the model are stroked or vulnerable most. Moreover, in power flow depended model power flow increase or decrease, it can be depend on an attack or fault in those lines. Load shift occur at line number 28. It had over 75 MW. This implies that here is a noteworthy shift of power in between nodes of the lines. Each necessary effected line removes against the transmission model to maintain power balance in the network. And so some of the lines carry more power due to exceed power match. Further failures occurred due to overloaded lines and result in large scale blackout.

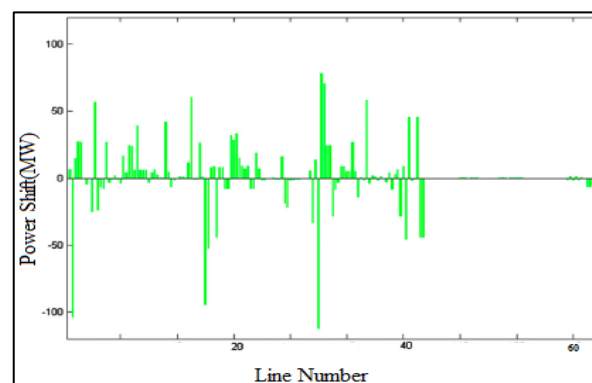


Figure 11. Efficiency model develops by change of power flow variations



## 5. CONCLUSION

This analysis proposes to implement a new power flow model based on smart vulnerability index. With the analytical approach possible vulnerable behaviour are identified in power model networks. These system models have a unique practical estimation of analytical grid system. Centrally control smart grid helps to identify critical lines and accurately remove particular vulnerable node from the network. A smart vulnerability index is established for quicker solution of critical lines or zone failure. Fortunately, critical lines are identified in strongly and accurately with the help of smart vulnerability index. The analysis finds out the cascading failures of network for predicting. It also powerfully supports to model redesign and implement arrangement.

Hence the grid of power system has an energetic and complex model. The main benefit of the proposed technique is cost effective. All factors are not considered in one model. Weight of the edges and steady state power flow are reviewed in those analyses of the network. The amount of power flow can alter with time. Generation of power and loads are changed due to demand shifting and change of seasons. Basically, smart grid is an intermutually complex network. Thus, researchers have an opportunity to model the constraint criteria and integrated networks. There are try to imply and extend approaches of analyzing new smart vulnerabilities indices. The implement of these factors will be acknowledged in future in a better way with consideration of many objectives and constraint criteria concurrently in the dynamic model.

## REFERENCES

- [1] K. Morison, Lei Wang and P. Kundur, "Power system security assessment," in *IEEE Power and Energy Magazine*, vol. 2, no. 5, pp. 30-39, 2004.
- [2] A. Atputharajah and T. K. Saha, "Power system blackouts-literature review," *2009 International Conference on Industrial and Information Systems (ICIIS)*, Sri Lanka, pp. 460-465, 2009.
- [3] D. J. Watts and S.H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440-442, 1998.
- [4] Xiao Fan Wang and Guanrong Chen, "Complex networks: small-world, scale-free and beyond," in *IEEE Circuits and Systems Magazine*, vol. 3, no. 1, pp. 6-20, 2003.
- [5] P. Chen, S. Cheng and K. Chen, "Smart attacks in smart grid communication networks," in *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24-29, 2012.
- [6] A. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509-512, 1999.
- [7] M. J. Eppstein and P. D. H. Hines, "A 'Random Chemistry' Algorithm for Identifying Collections of Multiple Contingencies That Initiate Cascading Failure," in *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698-1705, 2012.
- [8] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025-1028, 2010.
- [9] Q. Chen and L. Mili, "Composite Power System Vulnerability Evaluation to Cascading Failures Using Importance Sampling and Antithetic Variates," in *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2321-2330, 2013.
- [10] E. Bompard, R. Napoli and Fei Xue, "Analysis of structural vulnerabilities in power transmission grids," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1-2, pp. 5-12, 2009.
- [11] 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. 1-2, pp. 92-97, 2004.
- [12] R. Albert, I. Albert and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Phys. Rev. E*, vol. 69, no. 025103, 2004.
- [13] Jian-Wei Wang and Li-Li Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, pp. 1332-1336, 2009.
- [14] M. Ding and P. Han, "Reliability assessment to large-scale power grid based on small-world topological model," *2006 International Conference on Power System Technology*, Chongqing, pp. 1-5, 2006.
- [15] Lu Zongxiang, Meng Zhongwei and Zhou Shuangxi, "Cascading failure analysis of bulk power system using small-world network model," *2004 International Conference on Probabilistic Methods Applied to Power Systems*, Ames, IA, 2004, pp. 635-640.
- [16] D. Witthaut, M. Rohden, X. Zhang, S. Hallerberg, M. Timme, "Critical links and nonlocal rerouting in complex supply networks," *Physical Review Letters*, vol. 116, no. 13, pp. 138701, 2016.
- [17] A. Delgadillo, J. M. Arroyo and N. Alguacil, "Analysis of Electric Grid Interdiction With Line Switching," in *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 633-641, 2010.
- [18] G. Chen, Z.Y. Dong, D.J. Hill and G.H. Zhang, "An improved model for structural vulnerability analysis of power networks," *Phys. Stat. Mech. Appl.*, vol. 388, no. 19, pp. 4259-4266, 2009.
- [19] T. Chowdhury, G. K. Rout and C. K. Chanda, "Netability analysis of critical lines of power grid based on betweenness approach," *2015 International Conference on Energy, Power and Environment: Towards Sustainable Growth (ICEPE)*, Shillong, pp. 1-6, 2015.
- [20] J. Yan, Y. Tang, H. He and Y. Sun, "Cascading Failure Analysis With DC Power Flow Model and Transient Stability Analysis," in *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285-297, 2015.
- [21] D. T. Nguyen, Y. Shen and M. T. Thai, "Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment," in *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151-159, 2013.

- [22] A. Dwivedi and X. Yu, "A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 81-88, 2013.
- [23] R. Albert, H. Jeong and A. L. Barabasi, "Error and Attack tolerance of complex networks," *Nature*, vol. 406, pp. 378-382, 2000.
- [24] M. He and J. Zhang, "A Dependency Graph Approach for Fault Detection and Localization Towards Secure Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 342-351, 2011.
- [25] H. Zhu and G. B. Giannakis, "Sparse Overcomplete Representations for Efficient Identification of Power Line Outages," in *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 2215-2224, 2012.
- [26] R. Azami, A. mansori, Nosrat Allah M. Baigi, A. Omidian, and E. Mohammadian, "Transmission Loss Allocation Based on Lines Current Flow," *International Journal of Applied Power Engineering (IJAPE)*, vol. 1, no. 2, pp. 65-74, August 2012.
- [27] S. Bhongade and B. Tyagi, "Participation of Renewable Energy Sources in Restructured Power System," *International Journal of Applied Power Engineering (IJAPE)*, vol. 2, no. 1, pp. 1-14, April 2013.
- [28] Radita Arindya, "Load Flow Analysis for Process-Tank Loading Power Generation Networks Interconnection," *International Journal of Applied Power Engineering (IJAPE)*, vol. 3, no. 1, pp. 9-14, April 2014.
- [29] Syifaul Fuada, "Proposed An Intelligent System for Electricity Theft Detector at Smart City Scenarios," *International Journal of Applied Power Engineering (IJAPE)*, vol. 5, no. 1, pp. 51-58, April 2016.
- [30] S. S. Dhillon, J. S. Lather and S. Marwaha, "Steady State and Transient Analysis of Grid Connected Doubly Fed Induction Generator Under Different Operating Conditions," *International Journal of Applied Power Engineering (IJAPE)*, vol. 6, no. 3, pp. 171-192, December 2017.
- [31] Manoj Hans and Vivekkant Jogi, "Peak load scheduling in smart grid using cloud computing," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 8, no. 4, pp. 1525-1530, December 2019.

## BIOGRAPHIES OF AUTHORS



**Shouvik Kumar Samanta** was born in Bardhaman, West Bengal, India on August 2, 1983. He graduated in electrical engineering from the College of Engineering & Management, Kolaghat and master degree from Applied Physics, Calcutta University and pursuing doctoral research from IEST, Shibpur. His employment experience as lecturer in RVS College Engineering & Technology at Jamshedpur. He currently works as assistant professor in Seacom Engineering College. His special fields of interest on smart grid, distributed generation, power system stability.



**Chandan Kumar Chanda** received honorary degrees from institutions of higher learning including Columbia University, Yale. He graduated in electrical engineering from the Regional Engineering College, Durgapur (presently known as NIT, Durgapur) and master degree from IIT, Bombay and doctoral studied from BESU, Shibpur (Presently IEST, Shibpur). His special fields of interest on Distributed Generation, Power System Stability, Smart Grid. He is a professor of Electrical Engineering Department at Indian Institute of Engineering Science and Technology, Shibpur, Howrah (West Bengal). He is a fellow of Institute of Engineers (India) and life member of the Indian Society of Technical Education. He has about 5 years of industrial (SAIL) and 26 years of teaching and research experiences. Dr. Chanda has published/presented more than 135 research papers in national and international journals/conferences. He has received the best paper award in International conference held in Changsha, China in 2001 and also received the Tata Rao Prize in 2014 for best paper in electrical engineering from Institute of Engineers (India). He has authored/co-authored several successful leading books, including basic electrical engineering, electrical machines laboratory manuals, and digital fundamentals and applications.