IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

European Journal of Electrical Engineering
Vol. 21, No. 1, February, 2019, pp. 11-17
Journal homepage: http://iieta.org/Journals/ejee

A Novel Invulnerability Index for Invulnerability Assessment of Complex Power Network

Shuai Huang[1], Hua Cheng[1*], Zhidong Li[2], Hongzhen Zhang[1], Jiulin Li[3], Jianyong Guo[1,4]

[1] Dept. of Petroleum Supply Engineering, Army Logistics University of PLA, Chongqing 401311, China
[2] Academy of Military Science, Beijing 100091, China
[3] Air Defence Force Academy, Shenyang 110000, China
[4] 32150 troops of PLA, Xinxiang 453002, China

Corresponding Author Email: chwjct@163.com

https://doi.org/10.18280/ejee.210103

Received: 5 May 2018
Accepted: 6 January 2019

Keywords:
complex power network, invulnerability assessment, invulnerability value, source-load pair, complex network theory

ABSTRACT

Based on complex network theory and electrical analysis methods, this paper puts forward a novel Invulnerability index to improve invulnerability assessment of complex power network. The index was constructed based on concepts like line invulnerability value, invulnerability value of source-source-load pair, influence value and influence penalty. The invulnerability assessment effect of the index was compared with that of other indices under random, comprehensive static and comprehensive dynamic attacks. It was verified that the proposed invulnerability index outperformed other indices in the assessment of power network invulnerability. The research findings shed new light on the analysis of power network invulnerability.

1. INTRODUCTION

Power networks are the cornerstone of modern society. The stable operation of power network is an important guarantee of social stability. In recent years, the structure of power networks has become increasingly complex, in order to cover a wider area and provide a greater capacity. Against this backdrop, it is of great significance to ensure the invulnerability of complex power networks.

The existing studies on power network invulnerability are either based on analytic method [1, 2] or inspired by complex network theory [5, 6]. The former can fully reflect the functional features of the increasingly complex power networks, but is too complex to be applied widely or computed easily [3, 4]. The latter approach supports rapid analysis of large networks, but has difficulty in analysing functional features. What is worse, its conclusions cannot be directly applied to other types of power networks [7, 8]. In fact, the complexity theory is only starting to be employed for network analysis [9]. The theoretical results on network topology are far from enough to satisfy specific cases.

Recently, some scholars have attempted to integrate the two complementary approaches. The integration is usually carried out in three steps, namely, model setup, mechanism analysis and index synthesis. Most of the available integrated methods still have many defects. On model setup, the edge number in complex network theory is often replaced with line impedance, pipe, route or route length, depending on the different properties of a network, yet the replacement is not conducive to the assessment of overall invulnerability [10-13]. On mechanism analysis, the complex network indices are designed for largescale computation, rather than specific networks [14-19]. On index synthesis, it is difficult to sort out the relationship between the macro-topological indices from complex network theory and the state quantity indices from analytic method. In many cases, the two types of indices can only be examined separately [20, 21].

To solve the above problems, this paper designs a novel invulnerability index that characterizes the structural and functional features of power networks, and put forward an innovative index system integrating electrical analysis with complex network invulnerability theory. To verify the proposed method, various attack strategies were adopted to test the variation in invulnerability with the redundancy, structure of the power network, as well as the source and load locations. The verification fully demonstrates the superiority of the invulnerability index.

2. THEORETICAL BASES

2.1 Power network modelling

A power network differs greatly from a general network in functional and physical properties. The topology of a typical power network is presented in Figure 1 below.

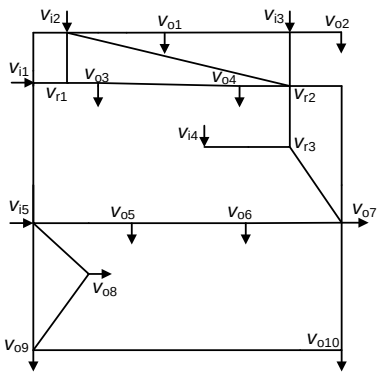

Figure 1. The topology of IEEE14-node power grid

The network topology can be modelled as:

$$\begin{cases} G = < V, E > \\ V = V_{in} \cup V_{out} \cup V_{relay} \\ V_{in} = \{v_{i1}, v_{i2}, ..., v_{in_{in}}\} & n_{in} > 0 \\ V_{out} = \{v_{o1}, v_{o2}, ..., v_{on_{out}}\} & n_{out} > 0 \\ V_{relay} = \{v_{r1}, v_{r2}, ..., v_{rn_{realy}}\} & n_{relay} \geq 0 \\ V_{in} \cap V_{out} = V_{out} \cap V_{relay} = V_{in} \cap V_{relay} = \varnothing \end{cases} \quad (1)$$

where, G is the power network topology consisting of the node set V and the edge set E; V_{in}, V_{out} and V_{relay} are the set of n_{in} input nodes, the set of n_{out} output nodes, and the set of n_{relay} relay nodes, respectively.

During a transmission task, each node remains in its class and the medium always moves from an input node to an output node. However, the transmission load or direction on each edge is not only determined by the total task load, but also by the scheduling strategy. In addition, the path structure is assumed as constant in the short term, for the routes and nodes in the network all correspond to real-world objects like cables, pipes, roads and websites.

2.2 Complex network invulnerability theory

The complex network invulnerability theory measures the invulnerability of network topology with the number of closed routes [22, 24]. Let n_k be the number of closed routes with the length of k. The length of a closed route is positively correlated with the number of repetitive statistics on the edges, and negatively with the contribution to invulnerability [25]. Thus, a weighted penalty should be assigned according to the length of the closed route. The number of closed routes S_3 after weighting correction can be expressed as:

$$S_3 = \sum_{k=0}^{\infty} \frac{n_k}{k!} \quad (2)$$

To sum up, a proper penalty should be assigned to the elements of the repetitive statistics, such that the network redundancy and structural features can be obtained accurately through invulnerability assessment.

3. INVULNERABILITY INDEX SYSTEM

3.1 Definition and application of the line invulnerability value

To simplify the feature analysis on the power network, the power grid G_E was taken as an example of power network G in the following analysis. In this network, each input node is viewed as a power source, each output node as a load and each edge as a power line. The network invulnerability was evaluated like the way of computing equivalent resistance in electrical analysis. Firstly, the line value was adopted to characterize the effect of each edge on network invulnerability. Note that the line value is about how much the network functionality is inhibited when the network connectivity is affected by attacks on the corresponding edges. The larger the edge value, the greater the impact on connectivity, the poorer the network invulnerability, and the higher the line value.

Considering the negative correlation between line value and invulnerability, the author proposed the concept of invulnerability value. The invulnerability value of each edge can be calculated as: $R=\{r_1, r_2, \ldots, r_k, \ldots, r_m\}$ ($r_k>0$, $1\leq k\leq m$), where m is the number of edges in the network. In the initial state, all edges have the same invulnerability value, that is, $r_1= r_2= \ldots= r_m=1$.

Since the network nodes are only effective when connected to the edges, the failure of a node can be considered as equivalent to the failure of its adjacent edges, eliminating the need of separate discussion of the failure of node.

3.2 Invulnerability value of source-load pair

In the power grid G_E, the power sources and loads form $n_{pair}= n_{in}n_{out}$ source-load pairs. Each pair can be regarded as a linear resistor single-port network with an independent power supply. According to Thevenin's theorem, this network can be simplified as a circuit with the voltage source connected to an equivalent value in series. Despite the difference from invulnerability value of the source-load pair network to its resistance in electrical analysis, the invulnerability value of the source-load pair network can be roughly obtained by computing the equivalent values of the source-load pairs in the network $R^0_{pair}=\{r^0_{p1}, r^0_{p2}, \ldots, r^0_{pnpair}\}$. After acquiring the equivalent values, it is possible to determine the difficulty for each source to power each load when the network is under attack.

3.3 Influence value and influence penalty

Pertaining to linear circuits, the power grid G_E can be analysed by the superposition theorem. This theorem holds that the currents on the edges between source-load pairs can be superimposed to compute the flow distribution of the entire power grid. Hence, the edges can be used repeatedly in different source-load pairs during the calculation of network invulnerability value.

According to complex network invulnerability theory, the repetitive calculations of the edges must be penalized to ensure the evaluation accuracy. In addition, an edge affects network invulnerability value differently in different source-node pairs. Therefore, the edges that greatly affect the network were selected from each source-load pair to receive penalty. The impact of each edge was measured by an index called the influence value.

For source-load pair $v_i \rightarrow v_j$ ($i\leq n_{in}$, $j\leq n_{out}$), the relative strength of the impact of each edge can be measured by the magnitude of the current on that edge. The greater the current, the more important the edge is to the electricity flow along $v_i \rightarrow v_j$, and the larger the impact of the edge on the invulnerability value of $v_i \rightarrow v_j$. The magnitude of current on each edge $I_{ij}=\{i_1, i_2, \ldots i_m\}$ can be determined by Newton's method. Then, the influence value Im_{ij} of each edge connecting $v_i \rightarrow v_j$ can be calculated from the maximum current i_{max} on that edge: $\{i_1/ i_{max}, i_2/ i_{max}, \ldots, i_m/ i_{max}\}$. Let i_{th} be the influence threshold. Then, any edge with $i_k/ i_{max} > i_{th}$ ($1\leq k\leq m$) must have a significant impact on the invulnerability value of $v_i \rightarrow v_j$ and be penalized accordingly.

The proper influence penalty is imposed in the following steps: (1) Initialize the influence penalty of each edge as $P_{Im}=\{p_1=0, p_2=0, \ldots, p_m=0\}$; (2) Obtain the Im_{ij} of $v_i \rightarrow v_j$ though current calculation, and increase the influence penalty p_k of edge k by 1 if $i_k/ i_{max} > i_{th}$; (3) Repeat the above two steps for

each source-load pair until the influence penalties of all edges in the network $P_{Im}=\{p_1, p_2,\ldots, p_m\}$ are obtained; (4) Adjust the invulnerability value of each edge based on P_{Im}, and obtain a new invulnerability value for each edge $R'=\{ r_1', r_2', \ldots, r_k',\ldots r_m'\}$ ($r_k'>0$, $1\le k\le m$).

$$r_k'' = ar_k + bp_k (1 \le k \le m) \tag{3}$$

where, a and b are two penalty factors, r_k'' can be calculated as the invulnerability value of line k modified by p_k. The total invulnerability value of all edges must remain constant, for the network is under the same external attacks. To ensure that $\sum_{l=1}^{m} r_l = \sum_{l=1}^{m} r_l'$, the adjusted values in equation (3) can be normalized by:

$$r_k' = \frac{r_k'' \sum_{l=1}^{m} r_l}{\sum_{l=1}^{m} r_l''} \tag{4}$$

With the aim to minimize $\sum_{l=1}^{m} p_l\ (p_l \in P_{Im})$, the basic operation rules of the power grid were taken as the constraints, the initial values of a, b and R were inputted, and then a single objective intelligent optimization algorithm [26, 27] was adopted to iteratively optimize the penalty factors a and b and find the optimal solution $R_{opt}=\{r_{opt\_1}, r_{opt\_2},\ldots, r_{opt\_m}\}$ through the above steps.

In this way, the impact of repetitive statistical factors on invulnerability assessment can be minimized, and the invulnerability of each source-load pair can be accurately derived from R_{opt}. Based on the equivalent value of each network node, the invulnerability value of each source-load pair in the network can be obtaine for R_{pair}.

$$R_{pair} = \begin{bmatrix} r_{p1} & r_{p2} & \cdots & r_{pn_{out}} \\ r_{p(n_{out}+1)} & r_{p(n_{out}+2)} & \cdots & r_{p(n_{out}+n_{out})} \\ \vdots & \vdots & & \vdots \\ r_{p((n_{in}-1)n_{out}+1)} & r_{p((n_{in}-1)n_{out}+2)} & \cdots & r_{pn_{pair}} \end{bmatrix} \tag{5}$$

Let $L=\{l_1, l_2,\ldots l_{nout}\}$ be the difficulty for powering each load when the network is under attack. For R_{pair}, the difficulty is equivalent to the invulnerability value. If all sources in the network belong to the same state, then the invulnerability value of load j can be defined as:

$$l_j = \frac{\sum_{i=1}^{n_{in}} r_{p((i-1)n_{out}+j)}}{n_{in}} (1 \le j \le n_{out}) \tag{6}$$

3.4 Invulnerability value of power network

The invulnerability value of a power network depends on many factors, ranging from the network topology, design function to task demand [28]. Since the capacity is not our research focus, the following assumptions were made: (1) The input range of source node V_{in} is [0, +∞), while the output range of load node V_{out} is equal to or greater than zero; (2) The probability of being attacked differs from line to line, and depends on the line capacity and the importance of the surrounding facilities, but the effect of the probability difference is negligible for the time being.

Then, the task demand was designed as ensuring the output of each member in the set of n_s load nodes is greater than d (d>0). Since the normal operation of the power network hinges on the state of the most vulnerable load node, the invulnerability value R_{supply} of the power network can be calculated as:

$$R_{supply} = \max\{l_1'', l_2'', \ldots l_{n_s}''\} \tag{7}$$

where, $\{l_1'', l_2'',\ldots, l_{ns}''\}$ is the set of the invulnerability values of the n_s load nodes.

4. CASE STUDY

The proposed invulnerability value R_{supply} was verified through the application in an IEEE 300-node power grid. Specifically, the relay circuits were attacked continuously by a strategy St until the power grid could no longer operate normally and the number of attacks was recorded as a_1^{St}. This process was repeated t times. Then, the mean number of attacks $\overline{a^{St}} = \frac{\sum_{u=1}^{t} a_u^{St}}{t}$ was computed to reflect the invulnerability of the power grid to the attack strategy St.

The attack strategy is an integration of a random attack S_0, a comprehensive static attack S_1, and a comprehensive dynamic attack S_2. Note that S_1 was designed from three types of static attacks, while S_2 from three types of dynamic attacks. Under the comprehensive static attack S_1, the circuits in the initial network were attacked in descending order of the edge degree, edge betweenness and edge clustering coefficient, and the attack method with the minimum $\overline{a^{St}}$ was selected for verification. Under the comprehensive dynamic attack S_2, each attack is on the circuits with the maximum edge degree, edge betweenness or edge clustering coefficient of the residual network, and the attack method with the minimum $\overline{a^{St}}$ was also selected for verification.

The relevant parameters were set as i_{th}=0.03, d=1 and t=500. According to the source and load information in the IEEE 300-node power grid, the number of sources and that of loads were respectively set to n_{in}=20 and n_s=50. The locations of the sources and loads were kept unchanged in section 4.1 and 4.2.

The common way to assess power grid invulnerability combines the complex network theory with such parameters as the number of sources, the number of loads, the source capacity and the load capacity [15, 19, 28]. All these parameters remained constant in the present paper, exerting not impact on the assessment result. Hence, the power grid invulnerability is usually evaluated directly by natural connectivity NC, network structure entropy NSE, network efficiency NE, network diameter ND, and average route length AL, all of which are commonly used in complex network theory.

For convenience, R_{supply}, ND and AL are inverted in the figures and tables below, because they are, by definition, negatively correlated with invulnerability. Whereas the number of sources and loads remain the same, the invulnerability of the power network is affected by network redundancy, network structure, as well as source and load

locations. Thus, the effectiveness of R_{supply} was discussed in the following three cases.

4.1 Changing network redundancy

The IEEE 300-node power grid was modified 25 times, creating 25 power grids. Each time, 3~5 circuits were added randomly. The invulnerability indices were computed and verified for each of the 25 power grids. The results are displayed in Figure 2 and Table 1 below. The correlation between the invulnerability indices and the simulation results was measured by Pearson correlation coefficient, Spearman's rank correlation coefficient and Kendall rank correlation coefficient, respectively.

It can be seen from Figure 2 and Table 1 that all the indices demonstrated the network invulnerability well despite the variation in redundancy under S_0, S_1 and S_2. The Pearson correlation coefficients show some differences between the invulnerability indices, while Spearman's and Kendall rank correlation coefficients indicate that the invulnerability results estimated by different indices were similar, except for that estimated by *NSE*. Overall, the indices could be ranked as R_{supply}>*NC*>*NE*>*ND*>*AL*>*NSE* in descending order of the estimated invulnerability.

Comapred with other indices, R_{supply} is featured by a long assessment time. The mean duration of R_{supply} -based assessment of the 25 times was 143.6s, while that of any other index was below 1s under the same conditions. The high time consumption is attributable to the electric analysis and optimization for R_{supply} computation. Obviously, R_{supply} is more suitable if high accuracy is required and a long time is allowed.

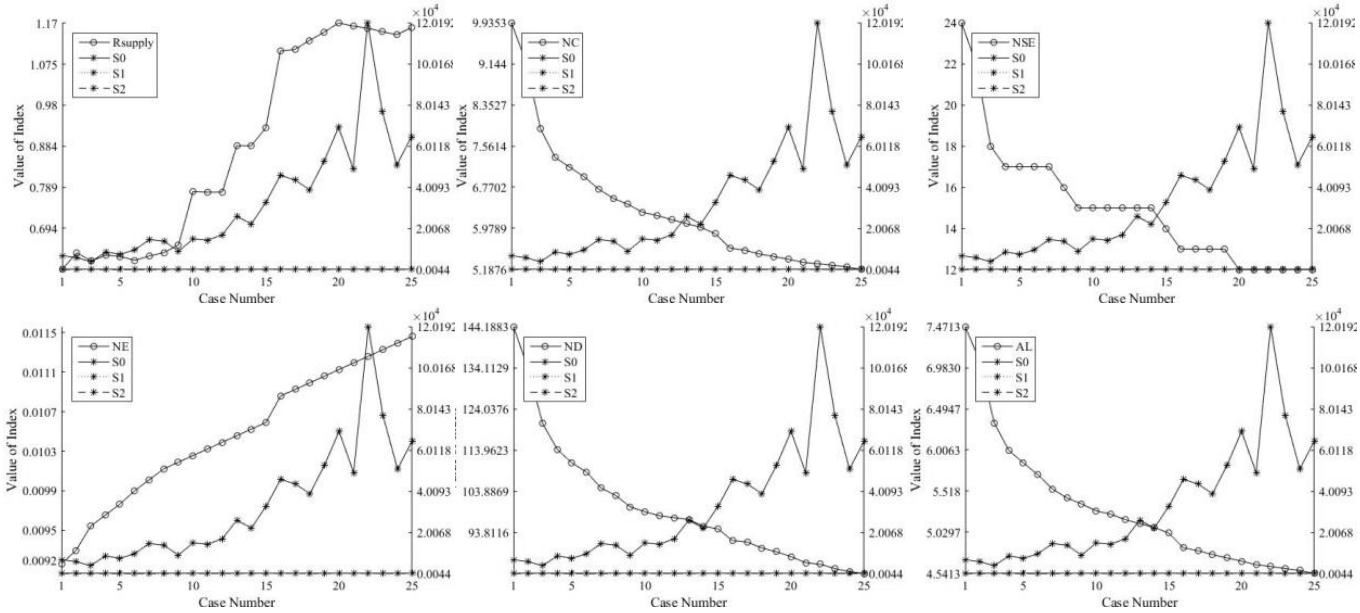

Figure 2. Index values and simulation results with changing network redundancy

Table 1. Correlation coefficients of index values and simulation results with changing network redundancy

Indices	Pearson				Spearman				Kendall			
	S0	S1	S2	Mean1	S0	S1	S2	Mean2	S0	S1	S2	Mean3
R_{supply}	0.9164	0.8593	0.7409	0.8389	0.9638	0.7268	0.7296	0.8068	0.8400	0.5659	0.5246	0.6435
NC	0.9254	0.8260	0.6800	0.8105	0.9631	0.7458	0.7296	0.8128	0.8400	0.5797	0.5246	0.6481
NSE	0.8183	0.4909	0.7511	0.6868	0.6977	0.4017	0.7967	0.6320	0.5000	0.2553	0.5787	0.4447
NE	0.8811	0.8164	0.6398	0.7791	0.9631	0.7458	0.7296	0.8128	0.8400	0.5797	0.5246	0.6481
ND	0.8202	0.7485	0.6219	0.7302	0.9528	0.7098	0.7585	0.8070	0.8555	0.5618	0.5657	0.6610
AL	0.7991	0.7792	0.5768	0.7184	0.9631	0.7458	0.7296	0.8128	0.8400	0.5797	0.5246	0.6481

4.2 Changing network structure

Under constant number of edges and enough connectivity, the edges of the IEEE 300-node power grid were connected in different means, producing 25 different power grids with the same redundancy. Then, the invulnerability indices were computed and verified for each of these power systems. The results are presented in Figure 3 and Table 2 below.

Figure 3 and Table 2 show obvious differences between the invulnerability indices inferred to changes in network structure. The invulnerability results estimated by *NE*, *ND* and *AL* were basically uncorrelated to simulation results under S_0, and slightly correlated under S_1 and S_2. It can be seen that the three indices can reflect the slight changes in invulnerability under the deliberate attack of structural change, but cannot fully assess the invulnerability to random attacks. Overall, the invulnerability results estimated by *NC* and *NSE* had a certain degree of relevance under S_0, S_1 and S_2, revealing the invulnerability variation under different attacks on structure. However, the invulnerability assessed by *NC* was not desirable under deliberate static attacks. R_{supply} achieved better assessment effect than the other indices, and made balanced response to different attack strategies.

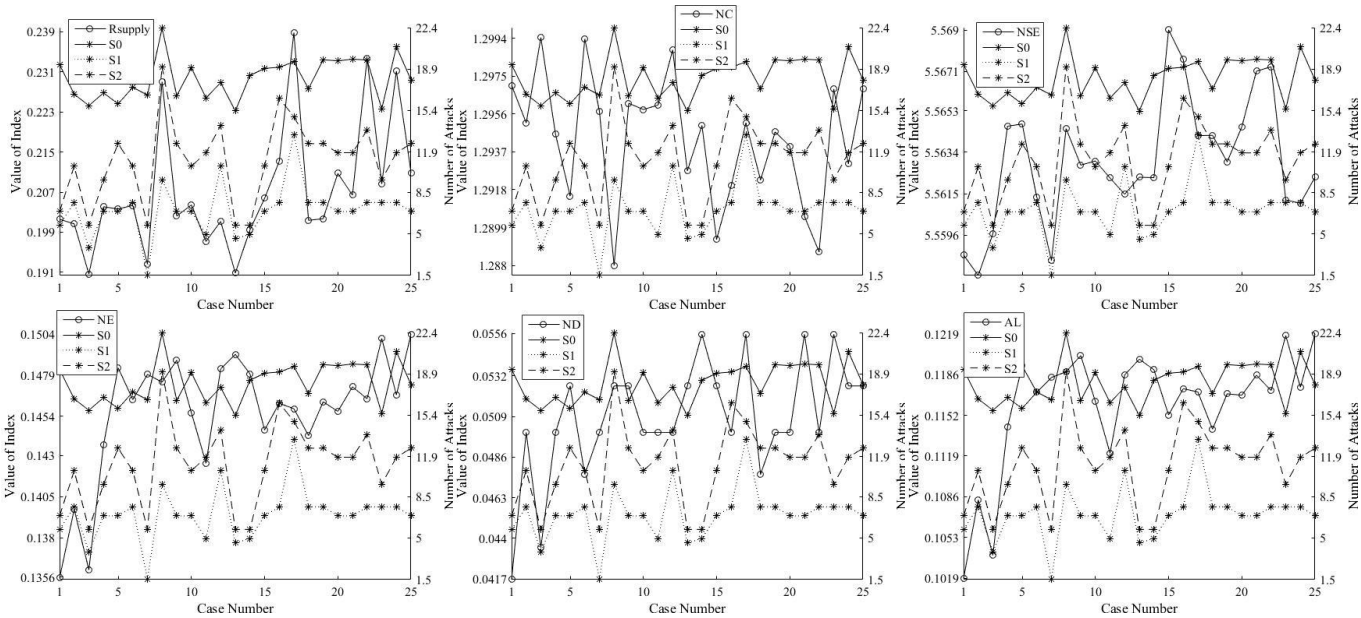

Figure 3. Index values and simulation results with changing network structure

Table 2. Correlation coefficients of index values and simulation results with changing network structure

Indices	Pearson				Spearman				Kendall			
	S0	S1	S2	Mean1	S0	S1	S2	Mean2	S0	S1	S2	Mean3
R_{supply}	0.7081	0.6993	0.6858	0.6977	0.6577	0.6086	0.5974	0.6212	0.4933	0.5000	0.4594	0.4843
NC	0.4921	0.1394	0.4346	0.3553	0.4238	0.1826	0.3418	0.3161	0.3333	0.1370	0.2490	0.2398
NSE	0.3840	0.3205	0.5235	0.4093	0.3693	0.2083	0.5099	0.3625	0.2437	0.1707	0.3724	0.2623
NE	0.0362	0.1920	0.2987	0.1757	0.1262	0.0764	0.1655	0.0386	0.0133	0.0778	0.1508	0.0718
ND	0.1091	0.3046	0.2937	0.2358	0.0975	0.1073	0.1315	0.1121	0.0651	0.0766	0.1089	0.0835
AL	0.0841	0.2355	0.3561	0.2252	0.0838	0.0951	0.2144	0.0752	0.0067	0.0926	0.1999	0.0997

4.3 Changing source and load locations

Without changing the redundancy and structure, 20 sources and 50 loads were selected randomly from the IEEE 300-node power grid. The selection was performed unrepetitively 25 times, forming 25 power grids. The invulnerability of each grid was computed and recorded in Figure 4 and Table 3.

Figure 4 and Table 3 show that R_{supply} was the only index capable of assessing the network invulnerability, despite the changing source and load locations. The good performance was consistently observed under S_0, S_1 and S_2. Therefore, it can be concluded that R_{supply} can reflect the effect of source and load locations on network invulnerability.

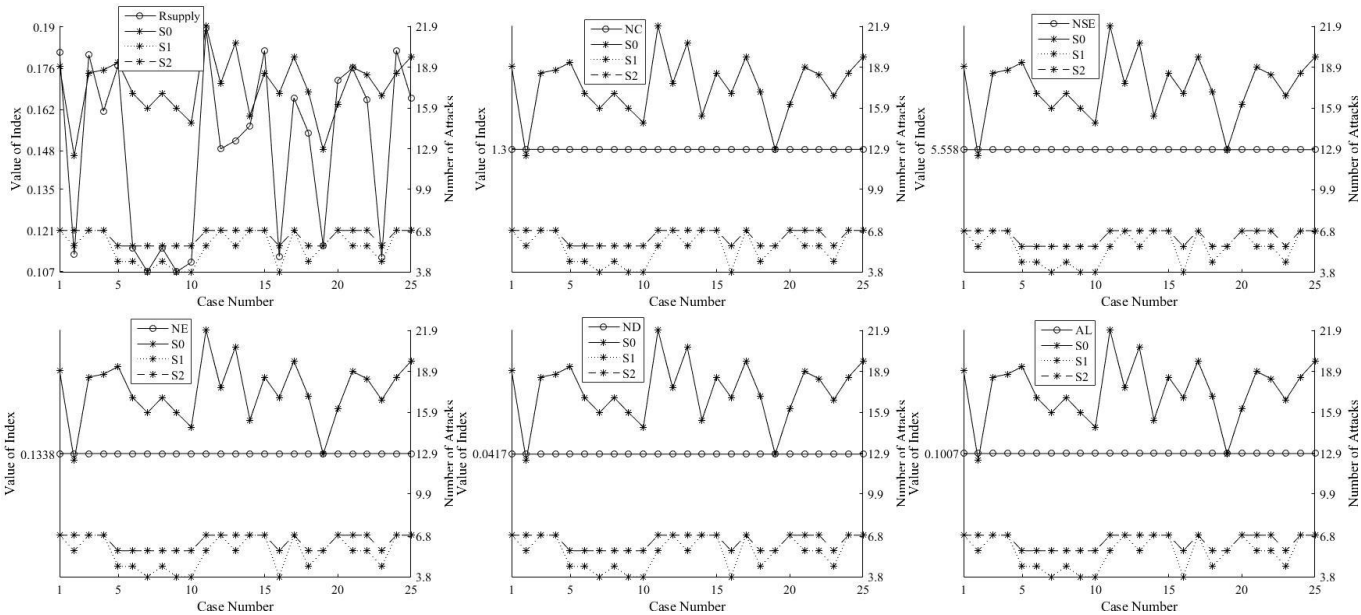

Figure 4. Index values and simulation results with changing source and load locations

Table 3. Correlation coefficients of index values and simulation results with changing source and load locations

Indices	Pearson				Spearman				Kendall			
	S0	S1	S2	Mean1	S0	S1	S2	Mean2	S0	S1	S2	Mean3
R_{supply}	0.6978	0.7536	0.7432	0.7316	0.7027	0.7023	0.6686	0.6912	0.5102	0.5748	0.5600	0.5483
NC	0	0	0	0	0	0	0	0	0	0	0	0
NSE	0	0	0	0	0	0	0	0	0	0	0	0
NE	0	0	0	0	0	0	0	0	0	0	0	0
ND	0	0	0	0	0	0	0	0	0	0	0	0
AL	0	0	0	0	0	0	0	0	0	0	0	0

5. CONCLUSIONS

With unique structure and functionality, power network requires specially designed methods to assess their invulnerability. Some assessment methods have been developed, coupling the analytic method with complex network invulnerability theory. However, these approaches fail to accurately measure the invulnerability of power grids.

In this paper, the power network is transformed into a self-defined power grid without sacrificing the structural and functional features, and the concept of invulnerability value is proposed for invulnerability assessment. To mitigate the impact of repetitive statistics, several theoretical tools, namely, Thevenin's theorem, Newton's method, superposition theorem and complex network invulnerability theory, were combined to compute the influence penalty of each edge, and to adjust the invulnerability value of each edge. Finally, the invulnerability value of power network that leads to the optimal assessment accuracy was derived. It was verified that the proposed invulnerability index outperformed other indices in the assessment of power network invulnerability under various attack strategies (e.g. changing redundancy, structure, and source and load locations.

The invulnerability index will be further refined in the future research. For example, the effect of influence penalty on invulnerability will be put under control, the impact of the number and capacity of source and load nodes on invulnerability will be investigated, and the invulnerability indicator will be formulated specific to each attack strategy.

REFERENCES

[1] Fang J, Su C, Chen Z, Sun HS, Lund P. (2016). Power system structural vulnerability assessment based on an improved maximum flow approach. IEEE Transactions on Smart Grid 9(2): 777-785. http://dx.doi.org/10.1109/TSG.2016.2565619

[2] Kim T, Wright SJ, Bienstock D, Harnett S. (2016). Analyzing vulnerability of power systems with continuous optimization formulations. IEEE Transactions on Network Science & Engineering 3(3): 132-146. http://dx.doi.org/10.1109/TNSE.2016.2587484

[3] Wang Z, Chen G, Hill DJ, Dong ZY. (2016). A power flow based model for the analysis of vulnerability in power networks. Physica A Statistical Mechanics & Its Applications 460: 105-115. http://dx.doi.org/10.1016/j.physa.2016.05.001

[4] Sanz FA, Ramírez JM, Correa RE. (2015). Experimental design for a large power system vulnerability estimation. Electric Power Systems Research 121: 20-27. https://doi.org/10.1016/j.epsr.2014.11.026

[5] Rout GK, Chowdhury T, Chanda CK. (2016). Betweenness as a tool of vulnerability analysis of power system. Journal of the Institution of Engineers 97(4): 463-468. https://doi.org/10.1007/s40031-016-0222-z

[6] Luo L, Han B, Rosas-Casals M. (2016). Network hierarchy evolution and system vulnerability in power grids. IEEE Systems Journal 12(3): 2721-2728. https://doi.org/10.1109/JSYST.2016.2628410

[7] Efrain ETR, Yoshihara T, Ohara S. (2016). Correlations of topological measures with power systems vulnerability and identification of potential locations to install voltage control devices. IEEE/PES Transmission & Distribution Conference & Exposition, Dallas, USA, pp. 1-5. http://dx.doi.org/10.1109/TDC.2016.7520060

[8] Xu T, Chen J, He Y, He DR. (2012). Complex network properites of Chinese power grid. International Journal of Modern Physics B 18(17-19): 2599-2603. http://dx.doi.org/10.1142/S0217979204025749

[9] Zio E. (2007). From complexity science to reliability efficiency: A new way of looking at complex network systems and critical infrastructures. International Journal of Critical Infrastructures 3(3): 488-508.

[10] Liu CX, Xu Q, Chen Z, Bak CL. (2012). Vulnerability evaluation of power system integrated with large-scale distributed generation based on complex network theory. Universities Power Engineering Conference, London, UK, 1-5. https://doi.org/10.1109/UPEC.2012.6398605

[11] Konstantinos Z. (2012). The vulnerability of the petroleum supply chain. Imperial College London Press, London.

[12] Liu S, Liao Z, Feng Y, Rong G. (2010). Topological properties of refinery system: A complex network approach. IEEE International Conference on Control and Automation, Xiamen, China, 345-349. https://doi.org/10.1109/ICCA.2010.5524377

[13] Xia Y, Hill DJ. (2008). Attack vulnerability of complex communication networks. IEEE Transactions on Circuits & Systems II Express Briefs 55(1): 65-69. http://dx.doi.org/10.1109/TCSII.2007.908954

[14] Fan W, Ping H, Liu Z. (2016). Multi-attribute node importance evaluation method based on Gini-coefficient in complex power grids. IET Generation Transmission & Distribution 10(9): 2027-2034. https://doi.org/10.1049/iet-gtd.2015.0803

[15] Dwivedi A, Yu X. (2013). A maximum-flow-based complex network approach for power system vulnerability analysis. IEEE Transactions on Industrial Informatics 9(1): 81-88. http://dx.doi.org/10.1109/TII.2011.2173944

[16] Adjetey-Bahun K, Planchet JL, Birregah B, Chatelet E. (2016). Railway transportation system's resilience: Integration of operating conditions into topological

indicators. NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, IEEE Press, London, 1163-1168. https://doi.org/10.1109/NOMS.2016.7502981

[17] Tanguy M, Napoli A. (2015). A methodology to improve the assessment of vulnerability on the maritime supply chain of energy. Oceans, Washington, USA, pp. 1-7. https://doi.org/10.23919/OCEANS.2015.7404414

[18] Zhao Y, Zhuang B, Zhou G, Zhao XH. (2010). Study on hydraulic vulnerability and risk assessment of water distribution system. International Conference on Environmental Science and Information Application Technology, Bangkok, Thailand, pp. 576-579. https://doi.org/10.1109/ESIAT.2010.5568865

[19] Chowdhury T, Chakrabarti A, Chanda CK. (2016). Analysis of Vulnerability indices of power grid integrated DG units based on Complex Network theory. India Conference, Anjrudh Krishna, India, pp. 1-5.

[20] Wang W, Liu J, Jiang X. (2009). A Multi-agent model for optimizing train formation plan. International Conference on Information and Computing Science, Manchester, UK, pp. 256-259. https://doi.org/10.1109/ICIC.2009.375

[21] Pan Z, Zhang Y. (2015). Index system and method for structure strength assessment of urban power network. Proceedings of the Csee 35(16): 3999-4005. http://dx.doi.org/10.13334/j.0258-8013.pcsee.2015.16.001

[22] Wu J, Barahona M, Tan YJ, Deng HZ. (2011). Spectral measure of structural robustness in complex networks. IEEE Transactions on Systems Man & Cybernetics Part A Systems & Humans 41(6): 1244-1252. https://doi.org/10.1109/TSMCA.2011.2116117

[23] Tan SY, Wu J, Li MJ, Liu X. (2016). Approximating natural connectivity of scale-free networks based on largest eigenvalue. Europhysics Letters 114(5): 58002. https://doi.org/10.1209/0295-5075/114/58002

[24] Estrada E, Rodríguez-Velázquez JA. (2005). Subgraph centrality in complex networks. Physical Review E Statistical Nonlinear & Soft Matter Physics 71(2): 056103. https://doi.org/10.1103/PhysRevE.71.056103

[25] Estrada E, Rodríguez-Velázquez JA. (2005). Spectral measures of bipartivity in complex networks. Physical Review E Statistical Nonlinear & Soft Matter Physics 72(2): 046105. https://doi.org/10.1103/PhysRevE.72.046105

[26] Chao OY, Ansari R. (2017). Applying a hybrid particle swarm optimization tabu search algorithm to a facility location case in Jakarta. Journal of Industrial and Production Engineering 34(3): 1-14. http://dx.doi.org/10.1080/21681015.2016.1243167

[27] Huang S, Long Y, Zhao HW, Feng P, Wang HL. (2016). Preliminary study on stand-alone microgrid invulnerability planning in important areas. Transactions of China Electrotechnical Society 31(5): 77-84.

[28] Poroseva S. (2013). Designing power system topologies of enhanced survivability. Aiaa/asme/asce/ahs/asc Structures, Structural Dynamics, and Materials Conference, Boston, USA, pp. 1-8. https://doi.org/10.2514/6.2010-2572