Complex Networks Theory Based Vulnerability Analysis of Power Grid with Distributed Generation

Yougang Zhang
School of Electrical Engineering,
Southwest Jiaotong University,
Chengdu, China,
e-mail: zhangyougang1@163.com

Shunjin Chen
School of Electrical Engineering,
Southwest Jiaotong University,
Chengdu, China,
e-mail: cshunj@126.com

***Abstract*—Vulnerability of power grids with distributed generation (DG) is investigated in this paper. Some vulnerability assessment indices suitable for assessment of vulnerability of complex power grids with DG are given and some special attack strategies are designed to facilitate the investigation. Simulation results show that the adding of DG can not only improve the power supplying ability of power grids, it can also enhance the reliability.**

Keywords-Complex Networks*; *Distributed Generation*; *Vulnerability

I. Introduction

The vulnerability analysis of complex power grids [1-7] has been a hot topic in last decades because of the frequently occurrences of blackouts, especially those happened in North America recently, which brought about tremendous damages [7]. However in most of the papers DG is not considered for vulnerability analysis of power grids. Actually in many existed power grids, some load nodes are far away in distance from the generators, so it is very difficult for these nodes to acquire enough supplying of power. In this case the adoption of distribution generation (DG) technology will be a good choice [8-10]. DG can reduce long-distance transmission and balance the power flow, thus make the power grid more reliable. In addition, DG can also reduce the energy consumption and the invest cost, and enhance both reliability and flexibility of power grids.

Of course, failure of some part of the power grid with DG can also make the power grid become vulnerable, so the vulnerability assessment of power grid with DG is also very important. In this paper, complex networks theory is utilized and some vulnerability indices are given to analyze the vulnerability of power grids with DG. Especially, some special attack strategies are designed to analyze the vulnerability of IEEE-57 nodes system and the simulation results demonstrate the effectiveness of them.

II. Vulnerability measures for power grids

In this paper, the power grid is simplified as an undirected and weightless network G=g (V, L), where V= {v}, L= {l} are set of nodes and of links, respectively. There are 3 kinds of nodes in set V, namely, load nodes V_D, generator nodes V_G, and transmitting nodes V_C. And the numbers for these 3 kinds of nodes are n_D、 n_G and n_C , respectively.

A general measure for Vulnerability assessment of power grid is the so called efficiency index [11], and it can be used to describe the transmitting efficiency of the power grid. The transmitting efficiency of the link connecting nodes i and j is denoted by e_{ij}, and the initial transmitting efficiency is 1 for every link in the network. The efficiency of a path between nodes i and j is the harmonic mean of efficiencies of all the links the path passed by [11]. In all of the paths connecting nodes i and j, the one with the maximal efficiency is called the most efficient path, and its efficiency is denoted as ε_{ij}, which belongs to [0,1]. If there's no path between two nodes i and j, we have ε_{ij} =0.

Correspondingly we can define the global efficiency E of the power grid as the average of the maximal path efficiencies between all of the generators and load nodes:

$$E=\frac{1}{n_D n_G}\sum_{i\in V_D}\sum_{j\in V_G}\varepsilon_{ij} \tag{1}$$

The global efficiency index E can express the ability of the power grid to transmit power and we can assess the vulnerability of the power grid according to the amount of the decrease of E after the cascading failure occurs.

For weightless networks, ε_{ij} in (1) can be the reciprocal of the length of the shortest path between generator nodes and load nodes, so we have

$$E=\frac{1}{n_D n_G}\sum_{i\in V_D}\sum_{j\in V_G}\frac{1}{d_{ij}} \tag{2}$$

where d_{ij} is the shortest path length between generator node j and load node i. It is obvious that the bigger E is, the smaller the shortest path length between generator nodes and load nodes will be, so transmitting efficiency will be higher.

However it is easy to understand that, while the power grid is supplied with DG, the vulnerability indices proposed just now may not be applicable. The main difference of power grids with DG from that of without DG is the local power supplying characteristic of DG. In addition, generally the capacity of DG is small and it is often mounted for remote load nodes that can not get enough power supply, so it contributes very little to the load nodes which are far away from it. The power supplying ability of it will decrease dramatically with the increase of distances between it and the load nodes. So the efficiency index will not be directly applicable for vulnerability assessment of power grid with DG. In view of this, in [8] a new index considering the local supplying characteristic of DG is proposed:

Published by Atlantis Press, Paris, France.

$$e_i = \frac{1}{P_{Di} n_G} \sum_{j\in V_G} \frac{P_{Gj}}{2^{d_{ij}-1}} \tag{3}$$

Where e_i denotes the power supplying efficiency of the entire network to load node i, P_{Di} is the active load of node i, P_{Gj} is the active capacity of generation node j, and d_{ij} is the length of the shortest path between generation node j and load node i. It is easy to understand that the bigger e_i is, the higher the power supplying efficiency of node i will be.

Similarly we have the following global average power supplying efficiency index:

$$e = \frac{1}{n_D}\sum_{i\in V_D} e_i = \frac{1}{n_D n_G}\sum_{i\in V_D, j\in V_G} \frac{P_{Gj}}{2^{d_{ij}-1} P_{Di}} \tag{4}$$

About formula (3) and (4) we have the following demonstrations.

1) If the active load P_{Di} of node i is big, then to some extent node i will not be safe.

2) Generally the capacities P_{Gj}'s of distributed generation nodes are small, so their power supplying capabilities are weak.

3) The exponential function $1/2^{d_{ij}-1}$ describes the characteristic of power supplying efficiency to decrease dramatically with the increase of the transmitting distance.

In addition, we can assess the vulnerability of the network according to the decrease of e, for this we have the following index

$$e' = \frac{e_0 - e}{e_0} \times 100\% \tag{5}$$

Where, e_0 and e are the power supplying efficiency before and after the occurrence of failures, respectively. From (5) we can see that the bigger e' is, the more dramatic the performance of the network will decrease, and so the related failure node or link will be more vulnerable.

III. STRUCTURE OF IEEE-57 NODES SYSTEM WITH DG

In the following sections, we will take the IEEE-57 nodes system as an example to demonstrate the effectiveness of the above-mentioned indices. The IEEE-57 nodes system has 57 nodes and 78 links, and the numbering of its nodes is shown in figure 1. Among the 57 nodes, 7 are generators, 35 are load nodes and 15 are transmitting nodes.

In order to determine the locations to mount DG, we need to know the power supplying efficiency of every load node. For this we should calculate the shortest path lengths between all of the generators and load nodes. Then from formula (3) we can get the power supplying efficiencies of the 35 load nodes. We found the 10 nodes with the lowest power supplying efficiencies are the nodes numbered as 31，33，30，25，32，35，47，54，53，27, whose efficiencies are 0.1, 0.12, 0.32, 0.36, 0.55, 0.59, 0.63, 0.77, 0.79, 1.09, respectively. Among them we choose 5 nodes with the lowest power supplying efficiencies, whose numbers are 31，33，25，47，54 for which the DG is mounted. The capacity for each DG is 10MW. For these new generation nodes, we numbered them from 58~62. And we name the new network with 62 nodes as IEEE-57 nodes system with DG. Among the 62 nodes, 12 are generation nodes, 35 are load nodes and 15 are transmitting nodes.

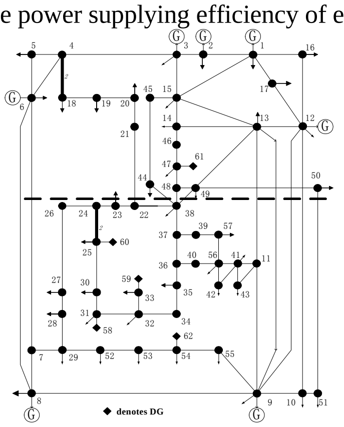

Fig.1 IEEE-57 nodes system with DG

From Fig.1 we can see that the new network can be divided into two parts roughly [8]. The part above the dash line has many generators and very few load nodes, so it can be seen as the primary power supplying area. The other part below the dash line has very few generators and many load nodes, so it can be seen as the primary load area. In addition we found that except node 47, all of the other load nodes with low power supplying efficiencies lie in the primary load area. Namely most of the load nodes with low efficiencies are in the primary load area. And this is in accordance with the real power grids. It also demonstrates the effectiveness of index e_i in assessing power supplying efficiency of load nodes. Another important thing is that it can provide us a reliable criterion to mount the DG to avoid mounting them randomly. And that is also the reason to choose them to be mounted with DG.

IV. ATTACK STRATEGIES

For comparison of power grid vulnerability before and after the mounting of DG, the conditions or parameters for them should be similar so the results could be reliable. But the randomness of the selection of nodes or links of random attack strategies means they are not reliable, at least to some extent. Because after the mounting of DG, the structure and size of the power grid has been changed. So the random selections of nodes or links are not based on the same network, which means the comparability is weak.

In view of this, in this paper the following two attack strategies are considered:

1) Comparison under the same targeted attack strategy

In such attack strategy, the same standard for the two power grids is adopted to compare the performance of them. For example, we can select the same percentage of the most important nodes [12], the same percentage of the nodes with largest degree, or the same percentage of nodes or links with the largest betweenness.

But by simulations we found that for assessing of vulnerability, node importance index and node betweenness index are more effective than node degree index. So we will not consider the case of removing the nodes with largest degree in this paper.

2) Comparison under global attack strategies of nodes or links

We can assess the performance of the two power grids by removing all the nodes or links alternately, and by so doing we can compare the performance difference before and after the mounting of DG globally.

V. Comparison analysis of IEEE-57 nodes system under targeted attacks

Assuming that altogether 20% of the nodes and links will be removed in the simulations and the simulation results are shown in figure 2.

From Fig.2 we found that with the strategy of removal of the most important nodes, the curve for the power grid with DG decays slower than that without DG. This shows that under the same condition of removal of the most important nodes, the power supplying efficiency of the power grid with DG decreases slower than the one without DG. So it means that the power supplying efficiency of the power grid is improved with the mounting of DG. Similarly, for attacks on links with the largest betweenness, we found the same phenomenon. It also demonstrates the improvement of power supplying efficiency and the strengthening of ability to resist targeted attacks.

VI. Comparison under global attack

In order for the convenience of investigation in this section, we adopt another vulnerability index e' in (5). e' expresses the decreasing proportion of power supplying efficiency. So the bigger e' is, the more dramatic the power supplying efficiency of the power grid will decrease, the related node or link will be more vulnerable. Under global attack strategies, all the nodes or links will be removed once. And while we remove the next node or link, we need to remove from the whole original power grid, or remove after the restoration from removal of the last node or link.

For brevity we only give the simulation results for the case of removing nodes (Actually we got similar conclusions for the case of removing links). In such removal each node will be removed in turn. And in every removal the shortest path length between all generators and load nodes will be calculated. And then e and e' can be obtained, as shown in figure 3 and figure 4.

From Fig.3 and Fig.4 we can see that, the influence of failures from most of the nodes is not so large, and only the failure from one of the nodes 8, 12,9,1,11,13 will make the decrease of power supplying ability be more than 10%. And among the 6 nodes the nodes numbered as 8, 12, 9, 1 are generators. Moreover, the nodes numbered as 8,12,1 have a rather large capacity and they will provide the majority part of the power supplying. So any failure of these nodes will have a dramatic influence on the power supplying ability. Furthermore, although node 9 is not a node with large capacity, it is the node with largest degree and the most important node. And it is also one of the nodes with the largest betweenness. So of course its failure will increase the length of power transmitting path dramatically.

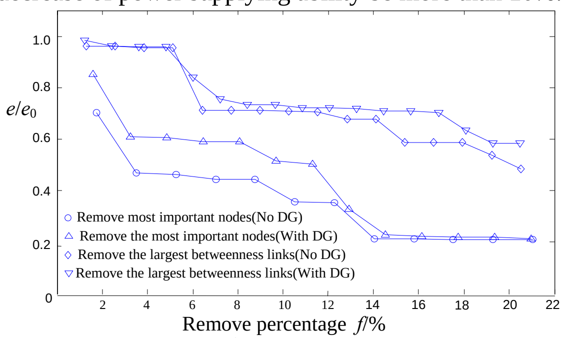

Fig.2 Comparison analysis of IEEE-57 nodes system under targeted attacks

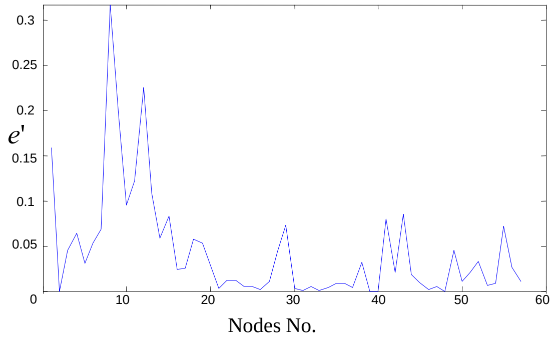

Fig.3 Vulnerability under global attacks on nodes (without DG)

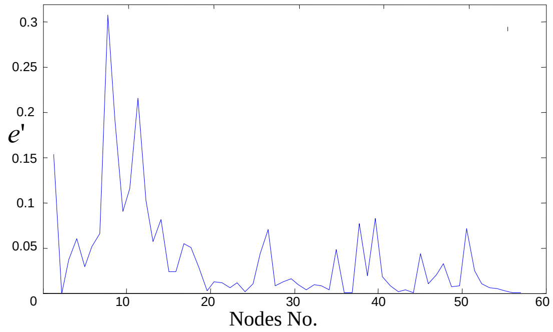

Fig.4 Vulnerability under global attacks on nodes (with DG)

From Fig.3 and Fig.4 we can find the 10 nodes with the largest e' value, as listed in Table 1 and Table 2. In Tab.2 we also listed 5 newly added DG. From Tab.1 and Tab.2 we can see that the generators with large capacity are generally very vulnerable. And some other nodes, although without large capacity, may still be key nodes in the network, such as node 11. The removal of node 11 will weaken the connection between the primary power supplying area and the primary

Table 1 Vulnerability of some nodes of the IEEE 57-nodes systems without DG under attacks on nodes

Node	e'	Node	e'
8(G)	0.3168	13	0.1090
12(G)	0.2263	10	0.0953
9(G)	0.1983	43	0.0855
1(G)	0.1590	15	0.0830
11	0.1222	41	0.0796

Table 2 Vulnerability of some nodes of the IEEE 57-nodes systems with DG under attacks on nodes

Node	e'	Node	e'	Node	e'
8(G)	0.3090	13	0.1028	58(DG)	0.0060
12(G)	0.2165	10	0.0913	59(DG)	0.0050
9(G)	0.1933	43	0.0831	60(DG)	0.0033
1(G)	0.1545	15	0.0824	61(DG)	0.0006
11	0.1166	41	0.0775	62(DG)	0.0003

load area. Accordingly this will change the power transmitting path remarkably. Another example is node 13, which is also a very important node with high degree and betweenness, just like node 9. The removal of node 13 will increase dramatically the length of the average shortest path between generators and load nodes, and this will have an influence on power transmitting efficiency. So, by attack vulnerability indices we can identify rather accurately the vulnerable nodes in power grids.

In Tab.2 we also listed the vulnerability of the 5 newly added generators of the IEEE 57 nodes system. And we can see that any one of them is not vulnerable. The influence on power supplying of removal from any one of them is less than 1%. Especially the decrease from the removal of node 62 is only 0.03%, and this is in accordance with the realistic requirements of power grids design with DG. The fact that the removal of a small scale DG has very little influence on the whole power grid, demonstrates the effectiveness of determining the positions for mounting of DG based on our power supplying efficiency indices. In addition, the newly added DG is specially designed for the 5 load nodes with low power supplying efficiency. From Tab.2 we can also see that, the weaker the power supplying efficiency the load node is, then the more vulnerable the generator added to it will be, which is also in accordance with the real power grids.

From Tab.1 and Tab.2, after the adding of DG, all the nodes of the power grid are less vulnerable. This shows that the ability of the power grid to resist attacks is strengthened. In order to demonstrate this further, we can calculate the maximum value and average value of the vulnerability of the IEEE 57-system before and after the mounting of DG under the attacks on nodes, as shown in table 3.

From table 3 we can see that the maximum value and average value of the vulnerabilities of all the nodes have decreased 2.46%, and 5.83%, respectively, which further shows the effectiveness of the mounting of DG to improve power transmitting ability and resilience to failures of nodes.

From the above simulation results, we can see that the targeted attack strategies on nodes and links have shown that the mounting of DG can improve the ability of the power grid to resist nodes failure and links failure, respectively. Similarly, the global attack modes on nodes and links have shown that the mounting of DG can improve the ability to resist nodes failure and links failure, respectively. Namely, whatever attack strategy we adopt, all of them arrived at a common conclusion: DG can effectively improve the power supplying efficiency and the ability to resist failures. Meanwhile, the simulations of global attacks on nodes or links demonstrate that the attack vulnerability index can identify effectively the vulnerable nodes and vulnerable links, which can be helpful for specialized guarding of power grid.

VII. CONCLUSIONS

In this paper, we tested the effectiveness of power supply efficiency index e and vulnerability index e' to assess the vulnerability of the IEEE-57 nodes system. By simulations we can see that these indices not only are applicable for vulnerability analysis of power grid with DG, they are also applicable for analyzing the vulnerability of power grid without DG. In addition, some special attack strategies are designed specially to compare the performance between the power grids with and without DG. The simulation results demonstrated that the mounting of DG can improve both the power transmitting ability and vulnerability to attacks on nodes or links.

Table 3 Comparison of vulnerability under attacks on nodes

e'	Without DG	With DG	improvement
Maximum	0.3168	0.3090	2.46%
Average value	0.0429	0.0404	5.83%

ACKNOWLEDGMENT

The authors would like to thank the supports of the State Key Program of National Natural Science of China (Grant No.61134001) and the Fundamental Research Funds for the Central Universities (Grant No.SWJTU09CX028, SWJTU11ZT06).

REFERENCES

[1] A. Motter, Y. Lai, “Cascade-based attacks on complex networks”, Physical Review E, vol.62, 2002 (065102)

[2] A. Motter, “Cascade control and defense in complex networks”, Phys. Rev. Lett, vol.93, 2004(098701)

[3] J. Wang, L. Rong, “Robustness of the western United States power grid under edge attack strategies due to cascading failures”, Safety Science, vol.49, 2011, pp.807-811

[4] E. Zio, L. Golea, “Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements”, Reliability Engineering and System Safety,vol.101, 2012, pp.67-74

[5] Z. Bao, Y. Cao, G. Wang, L. Ding, “Analysis of cascading failure in electric grid based on power flow entropy”, Physics Letters A,vol.373, 2009, pp.3032-3040

[6] I. Dobson, B. Carreras, V. Lynch, D. Newman, “Complex systems analysis of series of blackouts Cascading failure, critical points, and self-organization”, CHAOS, vol.17, 2007(026103)

[7] R. Kinney, P. Crucitti, R. Albert,a, V. Latora, “Modeling cascading failures in the North American power grid”, The European Physical Journal B,vol.46, 2005, pp.101-107

[8] Y. Wang, S. Mei, Y. Mao, F. Liu, “Vulnerability Assessment of Power Grid with Distributed Generation Based on Complex Network Theory”, J. Sys. Sci. & Math. Scis., vol.30, 2010，pp.859-868(in Chinese)

[9] R. Zhang, L. Zhang; Y. Li, L. Lv, “Distribution Network Reliability Considering Weather and Distribution Generation”, Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific, pp.1-6

[10] Y. Mao, F. Liu, S. Mei, “On the Topological Characteristics of Power Grids with Distributed Generation”, Proceedings of the 29th Chinese Control Conference, 2010, Beijing, pp. 4714-4720

[11] M. Ding, P. Han, “Small-world topological model based vulnerability assessment algorithm for large-scale power grid”, Automation of Electric Power Systems，vol.30, 2006, pp.7-10 (in Chinese)

[12] Y. Liu, X. Gu, “Skeleton-network reconfiguration based on topological characteristics of scale-free networks and discrete particle swarm optimization”, IEEE Trans. On Power Systems, vol.22, 2007, pp.1267-1274