*Journal of Information Hiding and Multimedia Signal Processing* ©2018 ISSN 2073-4212
**Ubiquitous International** Volume **9**, Number **6**, November **2018**

# The Structural Vulnerability Analysis of Power Grids Based on Laplacian Centrality

Chao Chen[1], Xin-Ling Guo[2], Wen-Hua Ren[1] and Zhe-Ming Lu[2]*

[1]Department of Computer and Information Technology
Zhejiang Police College
Hangzhou, 310053, P. R. China
{chenchaocn;renwenhua999}@163.com

[2]School of Aeronautics and Astronautics
Zhejiang University
Hangzhou, 310027, P. R. China
zheminglu@zju.edu.cn

Received August 2017; revised July 2018

Abstract. *The power grid is one of the most important real-world networks nowadays and has been widely studied as a kind of complex network. It has been developed for more than one century and becomes an extremely huge and seemingly robust system. But it becomes extremely fragile as well because some unexpected minimal failures may lead to sudden and massive blackouts. Many works have been carried out to investigate the structural vulnerability of power grids from the topological point of view based on the complex network theory. This paper focuses on the structural vulnerability of the power grid under the effect of selective node removal. We test the effectiveness of the Laplacian centrality in guiding the node removal based on several IEEE power grids. Simulation results show that, compared with other node centralities such as degree centrality (DC), betweenness centrality (BC) and closeness centrality (CC), Laplacian centrality (LAPC) is effective to guide the node removal and can destroy the power grid in less steps.*
**Keywords:** Power grids, Complex networks, Vulnerability, Centrality, Laplacian Centrality.

1. **Introduction.** Outages of power systems affect a country severely in many respects, and the catastrophic consequences of blackouts may remind terrorists to mount attacks by exploiting the vulnerabilities of power systems. Many scholars have been interested in this topic and carried out lots of works in this area [1, 2]. Unfortunately, these works are mostly based on classical and detailed physical models which need complete information including system operation data. In fact, neither attackers nor defenders can predict the exact system operating states before the attacks are really preformed. Therefore, the problem of malicious threat should be analyzed from statistical and general perspective by a new theory.

In the past two decades, complex networks have received considerable attention, especially since the small-world [3] and scale-free [4] properties were discovered in many real networks. Since power grids have been widely thought of as a typical type of complex network, many works have utilized complex network concepts and properties to analyze the structural vulnerabilities [5] or cascading failure mechanisms [6] of power grids. For most real complex networks, they are considerably resilient against random removal or failure of individual units. However, when the highly connected elements are the target

of the removal, they may be very fragile. Such guided attacks have dramatic structural effects, typically leading to network fragmentation for many small-world networks with skewed power-law degree distributions [7, 8]. Power grids, having less skewed exponential degree distributions and often without small-world topology, display similar patterns of response to node loss [9].

From a topological viewpoint, various measures of the importance of a network element (link or node), i.e. the relevance of its location in the network with respect to a given network performance, can be introduced to guide the node removal. Typically, different node centralities [10, 11, 12, 13], such as degree centrality (DC), betweenness centrality (BC) and closeness centrality (CC), can be used to guide the node removal. In this paper, we present using Laplacian centrality to guide the node removal. This centrality will be compared with some existing centralities, as well as the random removal scheme, in attacking several IEEE power grids.

## 2. Node Centralities.

### 2.1. Traditional Centralities.

In this paper, we model a power grid as an undirected and unweighted network. For a power grid with $N$ nodes and $M$ transmission lines, we can describe it as a complex network $G(V, E)$, where $V$ is the set of nodes and $E$ is the set of links with $|V| = N$ and $|E| = M$. Centrality measures are used to rank the relative importance of nodes or links in a complex network. There are various centrality measures for a node. Here, we introduce the definitions of three kinds of widely used centralities, i.e., degree centrality (DC), betweenness centrality (BC), and closeness centrality (CC).

The simplest centrality for a node is its degree. This centrality represents the connectivity of a node to the rest of the network and reflects the immediate chance for a node to exert its influences to the rest of the network. For a power grid with $N$ nodes, the degree of Node $\mathtt{v}_i (1 \leq i \leq N)$, denoted as $k_i$, is defined as the number of links connected to it. Then, the degree centrality of Node $\mathtt{v}_i$ , which is a normalized value, can be defined as follows:

$$C_i^D = \frac{k_i}{N-1} \tag{1}$$

Node betweenness is one of the most widely used centrality measure. This measure reflects the influence of a node over the flow of information between other nodes, especially in cases where the information flow over a network primarily follows the shortest available path. Given an undirected graph $G(V, E)$, the betweenness of Node $\mathtt{v}_i$, denoted as $B_i$, is defined as the number of times the node $\mathtt{v}_i$ acts as a bridge along the shortest path between two other nodes:

$$B_i = \sum_{all j,k, j \neq k \neq i} \frac{\sigma_{jk}(\mathtt{v}_i)}{\sigma_{jk}} \tag{2}$$

where $\sigma_{jk}$ denotes the number of shortest paths from Node $\mathtt{v}_j$ to Node $\mathtt{v}_k$ and $\sigma_{jk}(\mathtt{v}_i)$ is the number of those paths that pass through Node $\mathtt{v}_i$. Then, the betweenness centrality of Node $\mathtt{v}_i$, i.e., the normalized value of $B_i$, can be defined as follows:

$$C_i^B = \frac{B_i}{(N-1)(N-2)/2} \tag{3}$$

The closeness centrality of Node $\mathtt{v}_i$ describes the level at which Node $\mathtt{v}_i$ can on average reach all other nodes in the network. It is the mean geodesic distance (i.e., the shortest path length in hops) between Node $\mathtt{v}_i$ and all the other nodes reachable from it:

$$C_i^C = \frac{\sum_{\mathtt{v}_j \in V, j \neq i} d_{ij}}{(N-1)} \tag{4}$$

TABLE 1. The time complexity of four centralities

| **Centrality** | **DC** | **BC** | **CC** | **LAPC** |
|---|---|---|---|---|
| **Time Complexity** | $O(n)$ | $O(n^3)$ | $O(n^3)$ | $O(m)$ |

where $d_{ij}$ is the shortest path distance between Node $\mathtt{v}_i$ and Node $\mathtt{v}_j$.

2.2. **Laplacian Centrality.** Although the degree centrality is easy to calculate, using the degree centrality to identify the node importance is incomplete because it only considers the direct connections to a target node. That is, the degree centrality is hard to characterize the global feature of the network. The betweenness centrality and closeness centrality are effective, but they are computationally intensive for large-scale networks. It may be more reasonable to use the information of a node itself and its neighbors to better characterize the centrality. Thus, we propose a new kind of centrality called overall information centrality, which can be described as follows.

Qi et al. [14] introduced Laplacian matrix and Laplacian energy for a graph and defined the Laplacian centrality for a vertex. In particular, the Laplacian centrality of a vertex is defined as the relative drop of Laplacian energy in the network caused by the deactivation of this vertex from the network. Let $G$ be an undirected simple (without graph loops or multiple edges) graph, consisting of a set of $n$ vertices $V(G) = \{\mathtt{v}_1, \mathtt{v}_2, \ldots, \mathtt{v}_n\}$ and a set of $m$ edges $E(G) = \{\mathtt{e}_1, \mathtt{e}_2, \ldots, \mathtt{e}_m\}$. The number of edges that are incident to a vertex is called the degree of the vertex. Let $\mathtt{A}(G) = (a_{i,j})_{n\times n}$ be the adjacency matrix of the graph $G$ where the element $a_{i,j}$ equals 1 if there is an edge between vertices $i$ and $j$ , and 0 if there is not. And diagonal matrix is shown as follows

$$\mathtt{D}(G) = diag(d_1, d_2, \ldots, d_n) \tag{5}$$

where $d_i$ is the degree of node $i$. Then the Laplacian matrix of the graph $G$ is

$$\mathtt{L}(G) = \mathtt{D}(G) - \mathtt{A}(G) \tag{6}$$

Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of its Laplacian matrix $\mathtt{L}(G)$. The Laplacian energy of $G$ is defined as the following invariant:

$$E_L(G) = \sum_{i=1}^{n} \lambda_i^2 \tag{7}$$

$$E_L(G) = \sum_{i=1}^{n} \{d_i^2 + d_i\} \tag{8}$$

$H$ is the graph obtained by removing vertex from $G$ and the Laplacian centrality (LAPC) $C_i^L$ of vertex $i$ is defined as

$$C_i^L = (\Delta E)_i = E_L(G) - E_L(H) \tag{9}$$

The time complexity of above centralities is shown in Table 1. From Table 1, we can see that the Laplacian centrality offers substantial advantages to the other measures when examining large scale networks. We admit that the degree centrality runs faster than the Laplacian centrality, but it only supplies us very local information for each vertex, which is less reliable. While the Laplacian centrality not only takes the local environment around it into account but also the larger environment around its neighbors, making it an intermediate between the global and local characterizations of the position of a vertex in a network.

3. **Structural Vulnerability Analysis of Power Grids Guided by Centralities.** The basic idea for analysis of structural vulnerabilities of power grids based on complex network theory is to compare the network performance before and after the attacks or failures of some components. Thus, we need at least two indices, one is for the guidance of element removal from the power grid, the other is to characterize the network completeness of the remained graph after each step of attacking. In this paper, we call the former index as the guidance index, while the latter as the vulnerability index. That is to say, the centralities presented in Section 2 are used as guidance indices. For vulnerability indices, several metrics have been proposed to evaluate the completeness of the network in the literatures, the frequently used ones including the relative size of giant component, efficiency, and the average geodesic distance [15, 16]. In this paper, we use the relative size of giant component to measure the vulnerability of power grids. The relative size of giant component $R'$ indicates the ratio of the size of the largest connected sub-graph $R_t$ to the size of the whole network $R_0$ as follows:

$$R' = \frac{R_t}{R_0} \tag{10}$$

where $R_0$ is the size of giant component of the initial network (i.e., $R_0 = N$ if the original network is connected), $R_t$ is the size of giant component of the remained network after the $t$-th step of node removal guided by the guidance index. The detailed process can be described as follows:

Step 1: Calculate the centralities $C_i(1 \leq i \leq N)$ of all the nodes in the original graph $G(V, E)$, and sort them in descending order with $C_1 \geq C_2 \geq \ldots \geq C_N$. Set $t = 0$ and $f = 0$, where $t$ denotes the number of iterations performed while $f$ means the fraction of nodes removed. Set $R_0 = N$ for the connected network $G(V, E)$.

Step 2: Let $t = t + 1$, remove Node $\mathtt{v}_t$ from the network (also all the links connected to it), obtaining the resulting graph $G_t(V, E)$.

Step 3. Calculate the size of giant component of $G_t(V, E)$ denoted as $R_t$, let $f = t/N$, and then calculate the corresponding relative size of the giant component $R'$ based on Eq. (10). Record the pair $(f, R')$ in the resulting data list.

Step 4. Repeat Steps 2 and 3 for at most $N - 1$ times until $R_t = 1$.

Step 5. Finally, based on the recorded data list, we draw the resulting chart to reflect the relationship between $f$ and $R'$.

4. **Experimental Results.** In this Section, we adopt five IEEE power grids as well as the US power grid to test the effectiveness of the Laplacian centrality in analyzing the structural vulnerability of power grids. These six power grids are with 14, 30, 39, 145, 162 and 4941 nodes respectively. Firstly, we show some basic topological features of these power grids in Table 1, including the number of nodes $N$, the number of links $M$, the average degree $< k >$, the clustering coefficient $C$, the diameter $D$ and the average path length $L$ and the degreeCdegree correlation coefficient $r_d$, aiming at discover the relationship between the Laplacian centrality and rd. From Table 2, we can see that IEEE145 and IEEE162 are both assortative while other power grids are disassortative or neutral, while in the reality normal power grid networks would be disassortative or neutral. We also show the degree distributions of these power grids in Fig.1. From Fig.1, we can see that the IEEE145 power grid obviously exhibits the small-world property because its clustering coefficient is large and its average path length is short. From Fig.1, we can see that for all power grids, the degree value 2 has the maximal occurrence probability, if we remove the point of degree 1, all degree distributions are close to power-law distribution, so these six power grids tend to be scale-free.

TABLE 2. The topological features of six IEEE power grids

| **Network** | $N$ | $M$ | $< k >$ | $C$ | $D$ | $L$ | $r_d$ |
|---|---|---|---|---|---|---|---|
| IEEE14 | 14 | 20 | 2.857 | 0.367 | 5 | 2.374 | −0.074 |
| IEEE30 | 30 | 41 | 2.733 | 0.235 | 6 | 3.306 | −0.087 |
| IEEE39 | 39 | 46 | 2.359 | 0.038 | 10 | 4.749 | −0.276 |
| IEEE145 | 145 | 453 | 6.251 | 0.543 | 11 | 4.391 | 0.192 |
| IEEE162 | 162 | 284 | 3.517 | 0.099 | 12 | 5.657 | 0.371 |
| USPower | 4941 | 6594 | 2.669 | 0.103 | 46 | 18.99 | 0.003 |

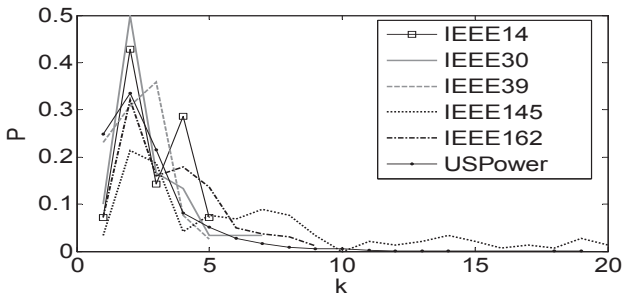


FIGURE 1. Degree distributions of six power grids.

In order to show the superiority of the Laplacian centrality in guiding the network attack, we compare Laplacian centrality (LAPC) with four schemes, i.e., random remove (RR), degree centrality (DC) based, betweenness centrality (BC) based and closeness centrality (CC) based schemes. The comparison results are shown in Fig. 2, where the abscissa axis f means the fraction of removed nodes and the longitudinal axis R' denotes the relative size of giant component.

From Fig.2, we can see that, for all power grids, the random remove scheme is the worst scheme to attack the power grid. For most power grids, LAPC can best guide the node remove process to fragmentize the network as soon as possible. However, for the IEEE145 power grid, the BC centrality is better than the Laplacian centrality at the beginning. This may be related to the average degree, because the descending order of the average degree is IEEE145>IEEE162>IEEE14>IEEE30>USPower>IEEE39, while the performance is just opposite. That is, the less the average degree is, the more important the mutual information tends to be, and thus the more effective the Laplacian centrality is. Fortunately, nearly for all power grids, most nodes has the degree value 2, which makes the Laplacian centrality more effective.

5. **Conclusions.** This paper investigates the structural vulnerability of power grids based on centralities. According to our simulation tests, we find that some power grids are small-world networks with relatively high coefficient and small average path length. And power grids have a nearly power-law degree distribution, showing scale-free properties. Laplacian centrality not only takes the local environment around it into account but also the larger environment around its neighbors, making it an intermediate between the global and local characterizations of the position of a vertex in a network. From the simulation results, we can conclude that the attack based on Laplacian centrality causes a great damage at the beginning of attacking process for power grids are disassortative or neutral while in the reality normal power grid networks would be disassortative or neutral. So, Laplacian centrality could be introduced to the research of power grids.

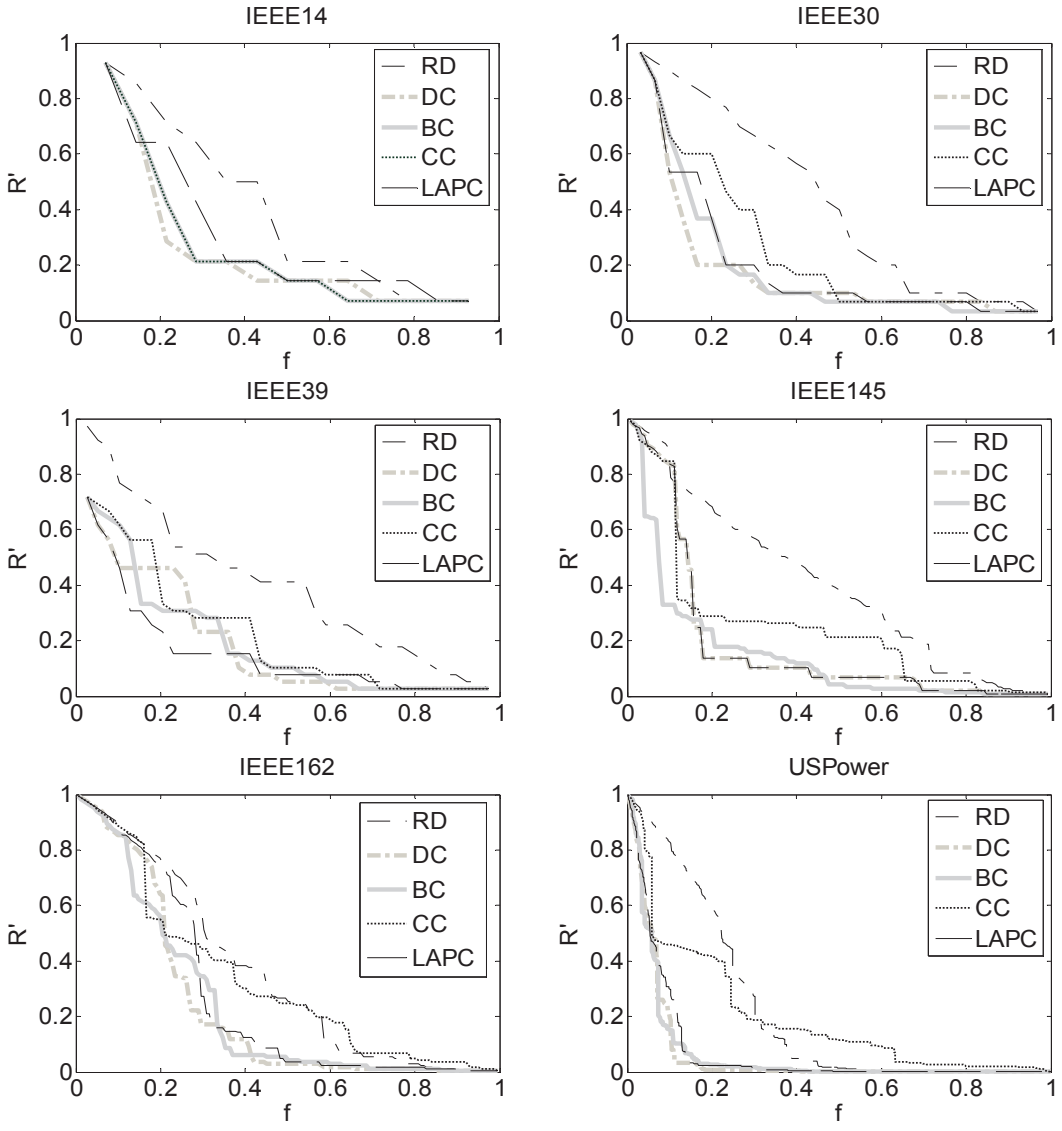


FIGURE 2. Performance comparisons among different attacking strategies.

**Acknowledgements.** This work was partly supported by the Zhejiang Provincial Natural Science Foundation of China under Grants LY17F030008. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

## REFERENCES

[1] P. F. Schewe, The Grid, Joseph Henry Press, Washington, D.C., 2007.
[2] J. Makansi, Lights Out: The Electricity Crisis, the Global Economy, and What It Means to You, John Wiley & Sons, New York, 2007.
[3] D. J. Watts and S. H. Strogatz, Collective dynamics of 'small-world' networks, *Nature*, vol. 393, pp. 440-442, 1998.
[4] A. L. Barabśi and R. Albert, Emergence of Scaling in Random Networks, *Science*, vol. 286, pp. 509-512, 1999.
[5] R. Albert, I. Albert, and G. L. Nakarado, Structural vulnerability of the North American power grid, *Physical Review E*, vol. 69, no.1, pp. 025103, 2004.
[6] D. P. Chassin, and C. Posse, Evaluating North American electric grid reliability using the Barabasi-Albert network model, *Physica A*, vol. 355, no. 2-4, pp. 667-677, 2005.

[7] R. Albert, H. Jeong, and A. L. Barabśi, Error and attack tolerance of complex networks, *Nature*, vol. 406, no. 2-4, pp. 378C677, 2000.
[8] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, Error and attack tolerance of complex networks, *Physica A*, vol. 340, no.1-3, pp.388-394, 2004.
[9] M. Rosas-Casals, S. Valverde, and R. V. Sol,Topological vulnerability of the European power grid under errors and attacks, *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 17, no.7, pp. 2465-2475, 2007.
[10] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, Attack robustness and centrality of complex networks, *PloS One*, vol. 8, no. 4, pp. 8-11, 2013.
[11] J. Hadidjojo and S. A. Cheong, Equal graph partitioning on estimated infection network as an effective epidemic mitigation measure, *PloS One*, vol. 6, no. 7, p. e22124, 2011.
[12] Y. Chen, G. Paul, S. Havlin, F. Liljeros, and H. Stanley, Finding a Better Immunization Strategy, *Physical Review Letters*, vol. 101, no. 5, pp. 2 C 5, 2008.
[13] C. M. Schneider, T. Mihaljev, and H. J. Herrmann, Inverse targetingAn effective immunization strategy, *Europhysics Letters*, vol. 98, no. 4, p. 46002, 2012.
[14] X. Q. Qi, R. D. Duval, and K. Christensen, Terrorist Networks, Network Energy and Node Removal: A New Measure of Centrality Based on Laplacian Energy, *Social Networking*, vol. 2, no. 1, p. 19-31, 2013.
[15] P. Holme, B. Kim, C. Yoon, and S. Han, Attack vulnerability of complex networks, *Physical Review E*, vol. 65, no.5, pp.056109, 2002.
[16] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, Efficiency of scale-free networks: error and attack tolerance, *Physica A*, vol. 320, no. 15, pp. 622-642, 2003.