Research on Importance Evaluation Method of Power Communication Network Node Based on Node Damage Resistance

WANG Ying \(^1\), SHI Zhan \(^1\), KANG Zhongmiao \(^1\), LI Xingnan \(^1\)

\(^1\) Power Dispatching Control Center, Guangdong Power Grid, Guangzhou, China, 510600

Abstract: In this study, the invulnerability performance of power communication network is elaborated in detail firstly, which is considered to be measured by two parameters of robustness and network efficiency. Then, the actual power communication data network model and power communication transmission network model are constructed. On this basis, different attack modes are selected, and the invulnerability performance of power communication network is analyzed through simulation experiments. Finally, experiments show that the impact on network invulnerability caused by selective attacks on important nodes is far greater than that of random attacks, and parameters of robustness and network efficiency can be used to measure the invulnerability of power communication network. In addition, the research results show that the node's invulnerability can be measured by the degree of network efficiency decline, and the greater the network efficiency decline, the better the node's invulnerability, corresponding to more important nodes in the whole network.

1. Introduction

With the rapid development of communication technology, the types of business under the power communication network are becoming more and more abundant and the scale is gradually increasing, which requires strengthening the management and maintenance of all important nodes in the network to provide a good environment for network operation [1]. In this paper, the importance of each node in the complex network is firstly described, and then the complex network is applied to practice by means of the characteristic topology parameter synthesis method, that is, the importance of each node in the power network is evaluated in detail through practice.

In general, the graph's invulnerability is mainly described by various invariants, such as integrity, discrete number, algebra, tenacity, connectivity, etc., while the description of power invulnerability in this study is mainly achieved by means of two kinds of performance, namely robustness and network efficiency. The essence of invulnerability is the ability of the network to withstand failures and attacks, which has nothing to do with the manner of attacks. From another point of view, it can be understood that invulnerability is actually the reliability of describing network topology, not the reliability of its nodes or edges [2], which can be directly equivalent to the difficulty of trying to destroy the whole system. Currently, there are two common destruction methods, namely, point removal and edge removal, and there are also two kinds of attack manner of random attack and selective attack. Besides, one of the issues that must be considered in evaluating the invulnerability is the invulnerability measure [3].
2. Invulnerability Index
If the network node is deleted, there will be two results that the network connectivity is destroyed; or the performance is significantly reduced and cannot meet the business requirements at all. In measuring the network's anti-corruption performance, two parameters of robustness and network efficiency are adopted, and the former is used to measure the change of robustness under different attack modes and the latter is used to evaluate the degradation of network performance.

2.1 Network Robustness
Robustness index is mainly used to measure the average influence of other nodes on their ability to maintain connectivity after nodes are deleted, which is defined as the average value of the ratio of the number of connected nodes to the total number of nodes in the network after any nodes are removed. Defining $G^*$ as the set of remaining network nodes after nodes are deleted, and the following representation can be obtained:

$$\eta_r = \frac{1}{n(n+1)} \sum_{i \neq j} l_{ij}$$

(1)

Where $l_{ij}$ represents the connection parameter between node $i$ and node $j$, and if the two nodes are connected by edges, the value of $l_{ij}$ is 1 or else the value is 0. Robustness is mainly used to describe the connectivity of the network itself after the nodes are deleted, that is, the condition that the network is actually segmented. Usually, the value of $\eta_r$ is between 0 and 1, and the lower value means the higher the number of unconnected nodes, which means that the network is in obvious segmented state.

2.2 Network Efficiency
The network efficiency is defined as the average value of the sum of the reciprocal of the shortest distance between two node pairs [4], which can be used to understand the performance of the network after attacks and can be formulated as follows:

$$E = \frac{1}{N(N+1)} \sum_{i=1}^{N} \frac{1}{d_{ij}}$$

(2)

Where $N$ represents the total number of nodes in the network; $d_{ij}$ represents the average path length between node pairs $V_i$ and $V_j$. Based on definition about the invulnerability of network nodes [5], the invulnerability of network nodes can be calculated as follows:

$$V_i = \frac{E - E_i}{E}$$

(3)

Where $E$ represents the initial network global efficiency; $E_i$ represents the global efficiency in the case that $V_i$ and other nodes are already in a failure state after the $V_i$ node is deleted.

If the network topology shows a fully connected state, the value of $E$ is the largest and equals to 1; once all nodes are isolated, the $E$ value is 0, and the value of $E$ directly indicates the situation of data transmission in the network. Generally, the short path means that the time required to complete the transmission of information is relatively short and the corresponding efficiency is high. Similarly, high efficiency is directly equivalent to short transmission time of data in the whole network, indicating that nodes have strong anti-corruption performance. In general, the larger the $E_i$, the smaller the difference between $E$ and $E_i$, and the smaller the $V_i$, which means that the nodes have higher invulnerability. Once a node fails, the efficiency of the network will decrease.

3. Power Communication Data Network and Transmission Network Model Construction

3.1 Power Communication Data Network Model Construction
In practice, the network topology of power communication data network is more or less different from each other, but the hierarchical design idea is always same, which includes core layer, convergence layer and connection layer [6]. Based on the actual power communication network, the topology is constructed in this paper of as Figure 1 shows, wherein the core layer comprises nodes 1 and 2; the
convergence layer has a total of 18 nodes, including 220 kV substations; and there are 35 nodes in the access layer. The networking modes of core layer and convergence layer 1 are semi-mesh, while the access layer is single link mode.

3.2 Power Communication Transmission Network Model Construction

Based on the actual situation, the power communication transmission network model is constructed as shown in Fig.2, including three major links presented as follows:

Ring 1: V1 - V2 - V3 - V4 - V5 - V6 - V7 - V8 - V9 - V10 - V11 - V12 - V1;
Ring 2: V13 - V14 - V15 - V16 - V19 - V18 - V21 - V22 - V23 - V24 - V13
Ring 3: V28 - V27 - V26 - V29 - V28.
V1 - V25 - V26. The connection between ring 2 and ring 3 is completed by 10G optical channel of V19 - V29.

The aforementioned three independent backbones are connected by hand-in-hand means, based on which double channels and routes have been established to ensure the safety and reliability of the network.

4. Power Communication Network Invulnerability Analysis

Based on the research on communication networks, the anti-damage performance of communication networks mainly refers to the capability of maintaining original service in the event of electronic warfare, physical damage or other threats [7]. There are also researchers believing that in order to achieve the minimum number of nodes or links that need to be removed to interrupt the communication between some nodes, there are generally two commonly used measurement metrics, of cohesion and connectivity. For the power system, its invulnerability mainly refers to the acceptable range of power communication network in order to maintain and restore the performance and efficiency in the power system. In other words, it is the ability of the system to save services when a network node or link encounters a failure [8]. For complex networks, there are two common attack modes, namely randomness and selectivity. In practice, the power communication network model constructed in Fig. 1 can be used to evaluate the invulnerability of the power communication network, which are measured by two parameters of network efficiency and robustness.

4.1 Random Attacks

In this section, the power communication network established in Figs. 1 and 2 are used for random attack testing. In this study, the random attack mainly refers to random attacks on points in the network in the case of gradually increasing the number of attacked nodes, and specific experimental analysis results are shown in Fig. 3 (PCDN is Power Communication Data Network; PCTN is Power Communication Transmission Network).

From Fig.3, it can be concluded that under the condition of random attack, the more nodes are deleted, the overall robustness and efficiency of the network will decrease. The reason for this phenomenon is that the more nodes deleted, the fewer nodes remaining in the network, resulting in that the connectivity of the entire network will be greatly reduced, and the corresponding robustness will tend to be 0. Meanwhile, with the increasing number of deleted nodes, the network efficiency is also gradually decreasing and eventually becoming zero.
4.2 Selective Attacks

Selective attack means the attack on nodes in network is selective. The starting point of a general attack is the maximum metric, and then the attack is launched in the order of the node degree decreasing. According to the analysis in the previous section, the nodes with higher degrees are V_6, V_15 and V_18 in the power communication network, and the attack order is from large degree to small degree, based on which the invulnerability variation of important nodes compared with that of random attack can be obtained as Fig. 4 shows.

As can be seen from Fig. 4, the more nodes deleted, the less robust and efficient the network is. By comparing two attack modes, it can be found that the decline extent of selective attack mode is relatively large. The reason for this phenomenon is that the nodes with high degree are firstly selected in this attack mode, in other words, the impact on network important nodes is more obvious than that of ordinary nodes, and therefore the robustness decreases greatly.

From Fig. 5(a), when the number of deleted nodes reaches 20, the robustness can be basically reduced to 0. A separate analysis of the degree values shows that the 20 nodes rank in the front in the sequence of degree values are all concentrated in the convergence layer, and if these 20 nodes are deleted, the basic connectivity of the network will drop sharply, because once these 20 nodes are deleted, most of the remaining nodes will be edge nodes, resulting in a serious drop in network connectivity. When the number of deleted nodes reaches 30, the network will be completely out of circulation.
5. Nodes Invulnerability Evaluation Importance Based on Power Communication Network

From the above test results, it can be found that the two indexes of network efficiency and robustness can reflect the overall invulnerability of the network regardless of the attack mode, based on which these indexes can be used to analyze the invulnerability of the power communication network has been proved. If the degree of selective attack nodes is large, the change of network invulnerability is pretty obvious. According to the invulnerability of node \( V_i \) defined by Eq.(3), the power communication data network presented in Fig. 1 is tested and the final results are shown in Fig.5 and Tab 1, where NN represents node serial number and NS represents node invulnerability:

![Fig.5](image)

**Tab.1 Comprehensive Evaluation Results of Power Communication Data Network Nodes Invulnerability**

| NN  | Unweighted NS | Weighted NS | Unweighted NS | Weighted NS |
|-----|---------------|-------------|---------------|-------------|
| 1   | 0.0434        | 0.0292      | 0.1301        | 0.0166      |
| 2   | 0.0557        | 0.0303      | 0.1337        | 0.0167      |
| 3   | 0.1004        | 0.0352      | 0.1078        | 0.0172      |
| 4   | 0.0663        | 0.0352      | 0.0990        | 0.0172      |
| 5   | 0.1365        | 0.0283      | 0.1148        | 0.0162      |
| 6   | 0.1577        | 0.0294      | 0.1364        | 0.0165      |
| 7   | 0.0663        | 0.0294      | 0.0742        | 0.0165      |
| 8   | 0.0750        | 0.0339      | 0.0762        | 0.0173      |
| 9   | 0.0636        | 0.0339      | 0.0762        | 0.0173      |
| 10  | 0.1130        | 0.0320      | 0.0997        | 0.0169      |
| 11  | 0.0450        | 0.0320      | 0.0653        | 0.0169      |
| 12  | 0.1412        | 0.0320      | 0.1297        | 0.0169      |
| 13  | 0.1377        | 0.0645      | 0.1160        | 0.0282      |
| 14  | 0.1426        | 0.0285      | 0.1475        | 0.0111      |
| 15  | 0.1487        | 0.0350      | 0.1163        | 0.0175      |
From Fig. 5 and Tab. 1, it can be concluded that the node invulnerability mainly reflects the efficiency of the whole network. In the unweighted network, the efficiency of $V_6$, $V_{18}$, and $V_{14}$ decreases largely, which rank in front in node invulnerability and therefore these nodes occupy an important position in the whole network.

As can be seen from Fig. 5 (a), the nodes after node $V_{20}$ in the access layer have relatively small invulnerability, and the corresponding network efficiency is also low. In other words, if these nodes fail, the overall network will not be affected greatly, and the network invulnerability is relatively better. Therefore, it can be inferred that the larger the node's invulnerability value, the smaller the corresponding network's invulnerability, which also means that such node plays a very important role in the entire network.

From Tab 1, the basic situation of the importance ranking of nodes under the analytic hierarchy process can be obtained. The top 20 nodes are basically the same in invulnerability and importance, and relatively important nodes can be found accurately in the network. The reason for the ranking is due to the difference in emphasis, and to evaluate the importance of a node in the network, the node invulnerability can be evaluated instead. The greater invulnerability means that more important position occupied in the network. However, the 20 nodes in convergence layer are all ranked in the top 20, of which invulnerability and importance rank are basically the same.

Based on the aforementioned analysis results, the node importance evaluation method proposed in this paper is demonstrated to be efficient in general, and the comparison results of node importance and invulnerability are presented as Tab 2 shows.

| Unweighted | Weighted |
|------------|----------|
| Importance | Invulnerability | Importance | Invulnerability |
| 14 | 6 | 2 | 14 |
| 15 | 15 | 1 | 6 |
| 2 | 18 | 14 | 18 |
| 1 | 14 | 15 | 2 |
6. Conclusion

The invulnerability performance of power communication network is described in detail, which are is considered to be measured by two parameters of robustness and network efficiency.

Based on the experimental results, the impact of different attack methods on the invulnerability performance of the network are demonstrated to be different, and selective attacks on important nodes have a far greater impact on network invulnerability than that of random attacks. In addition, it is found that the two parameters of robustness and network efficiency can also be used to measure the invulnerability of power communication network, which can be reflected by the decrease extent of network efficiency, and the greater decrease of network efficiency corresponds to the better node's invulnerability, which means that the more important position that the node occupies in the whole network.

On the whole, the importance of nodes is evaluated by ranking their invulnerability in this study, and the node importance evaluation method based on the hierarchical analysis method is demonstrated to be effective and significant through experimental results analysis.

References

[1] Kong J T, Huang J G, Li J X, et al. Evaluation methods of node importance in undirected weighted networks based on complex network dynamics models[J]. Acta Physica Sinica, 2018.

[2] Yu W, Guo J L, School B. Evaluation method of node importance in directed-weighted complex network based on multiple influence matrix[J]. Acta Physica Sinica, 2017.

[3] Fan W, Ping H, Liu Z. Multi-attribute node importance evaluation method based on Gini-coefficient in complex power grids[J]. Iet Generation Transmission & Distribution, 2016, 10(9):2027-2034.

[4] Zhong N, He Z W, Kuang J M, et al. Research on the Performance Evaluation Technique for Communication Network[J]. IEEE, 2009:1 - 5.
[5] Zhou X, Zhang F M, Li K W, et al. Finding vital node by node importance evaluation matrix in complex networks[J]. Acta Physica Sinica, 2012, 61(5):485-485.
[6] Zhang C, Lin Z, Wen F, et al. Two-stage power network reconfiguration strategy considering node importance and restored generation capacity[J]. Iet Generation Transmission & Distribution, 2014, 8(1):91-103.
[7] Zabludowski A. A recursive method for network reliability measures evaluation[J]. Microelectronics Reliability, 1984, 24(3):445-451.
[8] Chiasserini C F, Gaeta R, Garetto M, et al. Fluid models for large-scale wireless sensor networks[J]. Performance Evaluation, 2007, 64(7–8):715-736.