*Journal of Network Intelligence* ©2024 ISSN 2414-8105 (Online)
**Taiwan Ubiquitous Information** Volume **9**, Number **2**, May **2024**

# Research on Structural Vulnerability Based Power Grid Link Isolation

Han-Qing Gu

School of Aeronautics and Astronautics
Zhejiang University
Hangzhou, 310027, China
nampl@zju.edu.cn

Zhe-Ming Lu*

School of Aeronautics and Astronautics
Zhejiang University
Hangzhou, 310027, China
zheminglu@zju.edu.cn

*Corresponding author: Zhe-Ming Lu

Received October 1, 2023, revised January 9, 2024, accepted March 21, 2024.

Abstract. *Vulnerable links or parts are the root causes of large-scale blackouts in power systems. How to forecast the vulnerable links accurately and disconnect the links that can cause fault propagation is invaluable for strangling large-scale cascading failures. Therefore, this paper proposes a link isolation algorithm in power network based on joint vulnerability index based on the link vulnerability ranking. Extensive simulation analysis verify the accuracy of the algorithm. The fragile links could be isolated effectively. Moreover the structure optimization of the power network could be guided through the algorithm, which could prevent the blackout failure.*

**Keywords:** Power network, Complex network, Link isolation, Vulnerability.

1. **Introduction.** The recent analysis indicate that the most large-scale outages [1] begin only with a few components, but the faults spread and lead to a wider range of cascading failure instantly owing to the vulnerable links [2, 3]. Therefore, the vulnerability analysis of power networks [4-8] is especially critical and could bring forward guidance on the construction and optimization of power systems.

Nowadays, vulnerability analysis methods can be classified into structure based schemes and state based schemes. To keep the security of power systems, many researchers adopt complex network theory to analyze the structure vulnerability from a topological perspective [9]. Pure complex network theory based schemes find out risk links or nodes through certain metrics, such as centrality. After several decades, people have successively put forward many centralities [10], such as degree, betweenness, and closeness, and so on. Most of these schemes perform random and intentional attacks on complex networks to measure system vulnerability [11]. Actually, these schemes ignore different node types in the power system, including generation nodes, transmission nodes, and load nodes. Furthermore, these schemes also ignore that transmission lines have different materials with different line parameters and voltage levels. In addition, the power flow should follow Kirchhoff's law. In a word, these metrics do not take into the physical characteristics and operational constraints of the power system into account [12]. Considering this point, some extended electrical centralities [13] based on branch impedance, branch power limitation, and source or load capacity have been proposed to further enhance vulnerability analysis. However, all of these schemes do not consider the physical characteristics of power system.

State based schemes consider utilizing DC or AC power flow equations to analyze vulnerability, including the constraints of power flow equations, total reserve capacity constraints, active and reactive power flow limitations of generators, current carrying capacity of transmission lines, and node voltage levels [14]. However, because of the rapid development of high-voltage interconnected power grids, state based schemes should solve AC power flow equations with a huge computational burden. Thus, the maximum flow method is applied to power grid planning and introduced into the vulnerability of the power system. This is because the maximum flow method can approximately consider operational constraints like AC or DC equations, such as transmission line capacity, node voltage level, generator output, and so on. Reference [15] improved the maximum flow method to identify the fragile line in western Denmark. As a further extension of the power system vulnerability analysis based on complex network theory, there are numerous methods for analyzing the vulnerability of power systems that consider component dependencies. In contrast, these methods can fully consider the dynamic characteristics of post fault power transfer and transmission capacity conversion. Reference [16] respectively use the improved structural pore theory and the depth of k-shell decomposition method to identify fragile lines. In reference [17], a fast screening method based on Page Rank was derived to identify fragile lines by considering directed weighted graphs. Reference [18] evaluated this vulnerability by using cascading fault maps. Key components are identified through a state fault network formed by cascading fault chains and loss data [19].

Link isolation control is an effective means to avoid the spread of power grid faults [20-22]. There are few technical achievements related to link isolation in current researches. Most of them adopt artificial isolation or isolation through management area. Other automatic isolation schemes still have no effective technical means. The traditional approach is to carry out splitting method when a fault occurs, then the entire grid would be isolated into several parts of independent operation. Broadly defined, the splitting solution could be divided into two categories: passive and active. Currently, the criteria for passive splitting mainly include current-based, impedance-based, voltage-based, and phase-based. The defects of passive splitting are obvious. In the case of forced splitting, the internal power will be unbalanced in some power islands. Then the generator or load have to be shed, which cause a great impact on the load. Therefore, the active splitting method has gradually become a research hotspot recently [23-25]. Reference [23] proposed a method of searching splitting sections based on scheduling partitions, dividing the system into several sub-regions, and only needed to search connecting lines of instability regions and the rest to obtain feasible solution space. Reference [24] searched weakly connected lines as candidate space based on slow coherency theory. Reference [25] pointed out that commonly used splitting control strategy based on slow coherency or oscillation center positioning can achieve better results only in system with significant coherency grouping or relatively fixed oscillation center. It was proposed that for a system where coherency grouping is not obvious, maintaining the power supply for important load can be implemented as a control target, and an adaptive splitting framework was proposed. However, real-time fault information is usually not considered during prescreening, so the pre-selected sections may not match actual grids response. It seems that most of the current active splitting methods demand a high computational complexity owing to the power angle characteristics of the generator set. It cannot meet the timeliness requirements, so that the majority of scholars gradually begin to explore new thoughts [26-28].

In view of the above situation, this paper proposes a link isolation method based on vulnerability analysis, which abandons the power angle characteristics of the generator and fully utilizes the complex network vulnerability analysis results. The calculation process becomes very brief. Simulation results show the effectiveness of the proposed algorithm.

## 2. **Basic Vulnerability Indicators for Power Grids.**

A grid with $N$ nodes and $M$ transmission lines could be described as a complex network $G(V, E)$, where $V$ is the set of nodes, $E$ is the set of links, $|V| = N$ and $|E| = M$.

### 2.1. **Second-order centrality index.**

Kermarrec et al. proposed a distributed second-order centrality based on a single random walk on the network [29], where each node only needs to know its immediate neighborhood without any global information. The node hosting the random walk selects the neighbors randomly and, and transmits the random walk to the selected neighbors depending on the degree of the two nodes. When a random walk is received on the node $v_i$, the neighbor $v_j$ would be randomly and uniformly selected from $\Gamma_i$ (the set of adjacent nodes of $v_i$). The degree value $d_j$ of the node $v_j$ could be calculated out, and the random number $p \in [0, 1]$ is generated uniformly. If $p \leq d_i/d_j$, the random walk would be forwarded to $v_j$, otherwise the random walk still remains at $v_i$. If it is the first visit to the random walk of $v_i$, the array $\Xi_i$ would be created, otherwise the return time $r$ since the last access would be calculated out and added to $\Xi_i$. If $|\Xi_i| \geq 3$, the standard deviation $\sigma_i(K)$ could be calculated as:

$$\sigma_i(K) = \sqrt{\frac{1}{K-1}\sum_{k=1}^{K}\Xi_i(k)^2 - [\frac{1}{K-1}\sum_{k=1}^{K}\Xi_i(k)]^2} \tag{1}$$

In practice, the second-order centrality calculation proposed by distributed computing is fast and accurate to identify key nodes. The change in the frequency of the random walk access node could be acquired through above algorithm. After the third recorded return time, node vi will calculate the standard deviation of the $K$ values in $\Xi_i$. These return times are independent, we have a strong law of large numbers: $\lim_{K\to\infty}\sigma_i(K) = \sigma_i$. Once the random walk has been run on the graph for a sufficient amount of time, according to the detailed analysis given in [29], the standard deviation $\sigma_i$ based on unbiased random walk can be easily calculated by:

$$\sigma_i = \sqrt{2\Sigma_{j\in V}T(j,i) - |V|(|V|-1)} \tag{2}$$

Where $T(j, i)$ is the entry of the expected time matrix $T$ of size $N \times N$, $T(j, j)$ represents the expected time between two consecutive accesses to node $j$, and for $j \neq i$, $T(j, i)$ represents the expected time from node $j$ to node $i$ for the first time, and $V$ is a set of nodes with $|V| = N$. Thus, the value of $\sigma_i$ can represent the relative importance of the nodes in the graph: the lower the value, the higher the importance of the node. Therefore, the Second-order Centrality (SOC) can be finally defined as:

$$C_i^{(SOC)} = \frac{\min_{1\leq j\leq N}\{\sigma_i\}}{\sigma_i} \tag{3}$$

2.2. **Traditional link betweenness indicators.** The betweenness index is mainly to characterize the role of nodes in the information flow, and its value combines the proportion of the paths with node $v_i$ in all the shortest paths between pairs of nodes. The betweenness of $v_i$ could be calculated as follows:

$$C_b(v_i) = \Sigma_{s<t} \frac{g_{st}}{n_{st}} \tag{4}$$

Where $g_{st}(v_i)$ represents the number of the shortest path from $v_s$ via $v_i$ to $v_t$, and $n_{st}$ represents the total number of all the shortest paths from $v_s$ to $v_t$. For normalization, the maximum possible value of the betweenness must be calculated, which corresponds to the most extreme case, that is, any two other nodes are selected as the starting point and the ending point, and the shortest paths are all passed by a fixed node. Thus the maximum value could be acquired as $(N-1) \times (N-2)/2$. The index could be normalized as follows:

$$C_B(v_i) = \frac{2C_b(v_i)}{(N-1)(N-2)} \tag{5}$$

## 3. **Comprehensive State Vulnerability Index.**

On behalf of take both the structural and state vulnerability of the power network into account, this paper proposes a comprehensive vulnerability index, which utilizes the normalized link betweenness as structural vulnerable degree, and the link load level as the state vulnerable degree. The proposed comprehensive vulnerability index can be defined as the average of the link normalized betweenness and load level. The specific formula is as follows:

$$F(e_{ij}) = 0.5[C_b(e_{ij}) + L(e_{ij})] \tag{6}$$

Where the link betweenness $C_b(e_{ij})$ and the load level $L(e_{ij})$ could respectively indicate the structural and state vulnerability. The link betweenness is defined as the proportion of the link $e_{ij}$ which must be passed among all the shortest paths in order to evaluate the incidence of the link on the structure. The betweenness of link $e_{ij}$ can be expressed as Equation (5). The load level of the link is defined as the ratio of the link active power flow to the maximum link active power flow:

$$L(e_{ij}) = \frac{P(e_{ij})}{P_{\max}} \tag{7}$$

In the above formula, the larger $L$ is, the larger the load is. Actually the load level may be outage ($L = 0$), light, normal, heavy or full ($L = 1$) load. $L$ should be calculated based on actual operating parameters. However, owing to the limited response time, the proposed algorithm ignores the load change caused by the outage of other links when performing fault isolation.

Here, the second-order centrality of each node (shown as Equation (3)) could be only utilized as an auxiliary means to reconfirm the vulnerable link.

## 4. **Link Isolation Algorithm Based on Grid Vulnerability.**

The proposed link isolation algorithm combines the comprehensive state vulnerability index with the node second-order centrality index and the traditional link betweeness index. Firstly, the link is selected as the object of vulnerability assessment. The vulnerable link set would be constructed to identify link vulnerability through comprehensive state vulnerability, link betweeness and node second-order centrality. Secondly, the link isolation algorithm is utilized to isolate the link for preventing the accident from spreading over a large area when a fault occurs at the link belonging to the estimated vulnerable link set. Since the state and structure are considered simultaneously, the comprehensive index proposed is closely related to the operating state at each moment. Therefore, the comprehensive index must be updated in the whole operating period of the power system, also the vulnerable link set would be updated at different instants.

The specific isolation procedures are as follows:

Step 1: Calculate the comprehensive vulnerability of each link and the second-order centrality of each node

Step 2: Generate the vulnerable link set The main idea of this step is to utilize the calculated comprehensive index and the second-order centrality of each node to evaluate the vulnerability of the power network links, and place the link that may cause cascading fault into the vulnerable link set. The vulnerable link set is detected and updated at any time. When the operating state of the power network changes, the link set may change.

The set generation process is as follows:

1) Build complex network based on the topological relationship of power network;

2) Sort respectively the links based on the calculation of the comprehensive vulnerability index as Equation (6) and sort respectively the nodes based on the calculation of the second-order centrality as Equation (3);

3) Attack each link in sequence according to the link rankings until the connectivity of the network (the ratio of the number of normal working links to the total number of links) falls to the preset threshold $T_1$, and then classify the attacked links into the temporary link set, and restore the power network.

4) Remove each node in sequence according to the node rankings until the connectivity of the network (the relative size of the largest connected branch) drops to the preset threshold $T_2 (T_2 > T_1)$, and classify the attacked node into the temporary node set.

5) Eliminate those links in the temporary link set whose starting and ending nodes are not present in the temporary node set, and finally form the vulnerable link set.

Step 3: Check whether the fault link is in the vulnerable link set.

If the fault link does not belong to the vulnerable link set, this illustrates that this fault could hardly cause a cascading failure, thus link isolation isn't required. If the fault link belongs to the vulnerable link set, the following link isolation operation would be performed.

Step 4: Detect the connectivity of links in the vulnerable link set.

This step is to minimize the isolation scope. If several links in the vulnerable link set could constitute a connected set, the isolated area would be quite large, otherwise the fault would be spread to the area where is vulnerable, and the consequences would be uncontrollable. To this end, the proposed solution is: when the links in the vulnerable link set could constitute a connected set, all these links need to be isolated; when they are not fully connected, check respectively whether it leads to cascading faults through simulative isolation of the links. If not, the link would be disconnected and disposed as one of the perimeter link set $C_2$. Otherwise, the link should not be separate, and the node of the link should be placed in set $C_1$.

Step 5: Generate a preliminary fault area node set $C_1$ and perimeter link set $C_2$.

The number of elements in $C_1$ obtained in the previous step is denoted by l (that is, the number of parent nodes). Here, the link in the vulnerable link set is sorted based on the comprehensive vulnerability indicator. The detailed process is that when the links are attacked in turn, the vulnerability indicator $F$ of the attacked link is recorded at this time if the ratio of the number of running links to the number of unattacked links is less than a given threshold. Then the nodes in $C_1$ would be traversed, and sequentially be estimated whether the vulnerability index of each link connected to the current node is less than $F$, and if so, the link would be inserted into $C_2$, otherwise the connected node would be inserted into $C_3$. Since the number of parent nodes in $C_1$ before failure isolation is l, this step is based on exhaustive search. For the current parent node, if the number

Table 1. Comparison of the attacking results based on single index and combined index when the first 9 lines are attacked for IEEE 118 power grid

| Attacked links | Link betweenness | Load level | Comprehensive indicator | Random |
|---|---|---|---|---|
| 1 | 97.8 | 98.4 | 97.9 | 98.4 |
| 2 | 84.4 | 97.9 | 96.8 | 97.9 |
| 3 | 80.7 | 97.3 | 94.6 | 97.3 |
| 4 | 79.6 | 97.3 | 89.8 | 96.8 |
| 5 | 79.0 | 96.8 | 81.7 | 96.2 |
| 6 | 75.3 | 95.2 | 59.7 | 95.7 |
| 7 | 74.2 | 27.4 | 41.9 | 95.2 |
| 8 | 67.2 | 18.3 | 41.4 | 94.6 |
| 9 | 61.8 | 18.3 | 38.2 | 94.1 |

of subnodes in $C_3$ is $m$, then the subordinate subnodes of any node in the set would be searched out respectively to estimate that whether the vulnerability index of the link connecting the two nodes is less than $F$. If so, the link would be placed in $C_2$. Otherwise, the subordinate subnode would be classified into $C_4$, and then $C_3$ is updated with $C_4$ and $C_4$ is cleared. Until $C_3$ becomes an empty set, the parent node traversal operation would terminate.

Step 6: Generate a set of nodes outside the failure zone $C_5$.

By taking the perimeter node as the root node, the exhaustive operation is adopted to generate the out-of-failure node set $C_5$ on condition of the adjacency matrix generated by the link indicator, and also to operate separately the isolated nodes, the full load parts or the full power generation parts. For the out-of-failure nodes in the perimeter link set, the frequency of occurrence in the perimeter would be check out: If the frequency is equal to the node degree, it is known that an isolated point appears, which would be classified into the fault node set, and the relevant link would also be deleted from the perimeter link set. If some of the nodes belong to the generator node set or none of them belongs to the generator node set, these nodes would be set into the fault node set, and the relevant perimeter link would be deleted.

Step 7: Check the power difference between the isolated parts and then perform appropriate fine-tuning on isolation area.

The power difference inside each isolation zone would be calculated. If the difference can reach the basic balance within each isolation zone, the isolation algorithm terminates, otherwise appropriate changes must be considered.

## 5. **Simulation Analysis.** The IEEE118 power system is adopted as the simulation model, and its topology is shown in Figure 1. The network consists of 118 nodes, 186 lines, 19 generator sets, total power generation of 4377.4 MW, and total load of 4242 MW.

### 5.1. **Effect of comprehensive vulnerability indicator.** The link attack simulation is carried out by utilizing the traditional single index and the comprehensive index proposed in this paper. The results in Table 1 compares the remaining connectivity of the single indicators and the comprehensive indicators under the condition that the links in the top ranking of the indicators are attacked, and compares it with the result of random links.

Obviously if the number of attack links increases to 4.8% of the total links, the remaining connectivity is reduced to about 62% after the link with large betweenness is attacked, while the remaining connectivity after random attacks on the link is only reduced to about 91%. Therefore, the link betweenness could be effectively utilized to estimate the

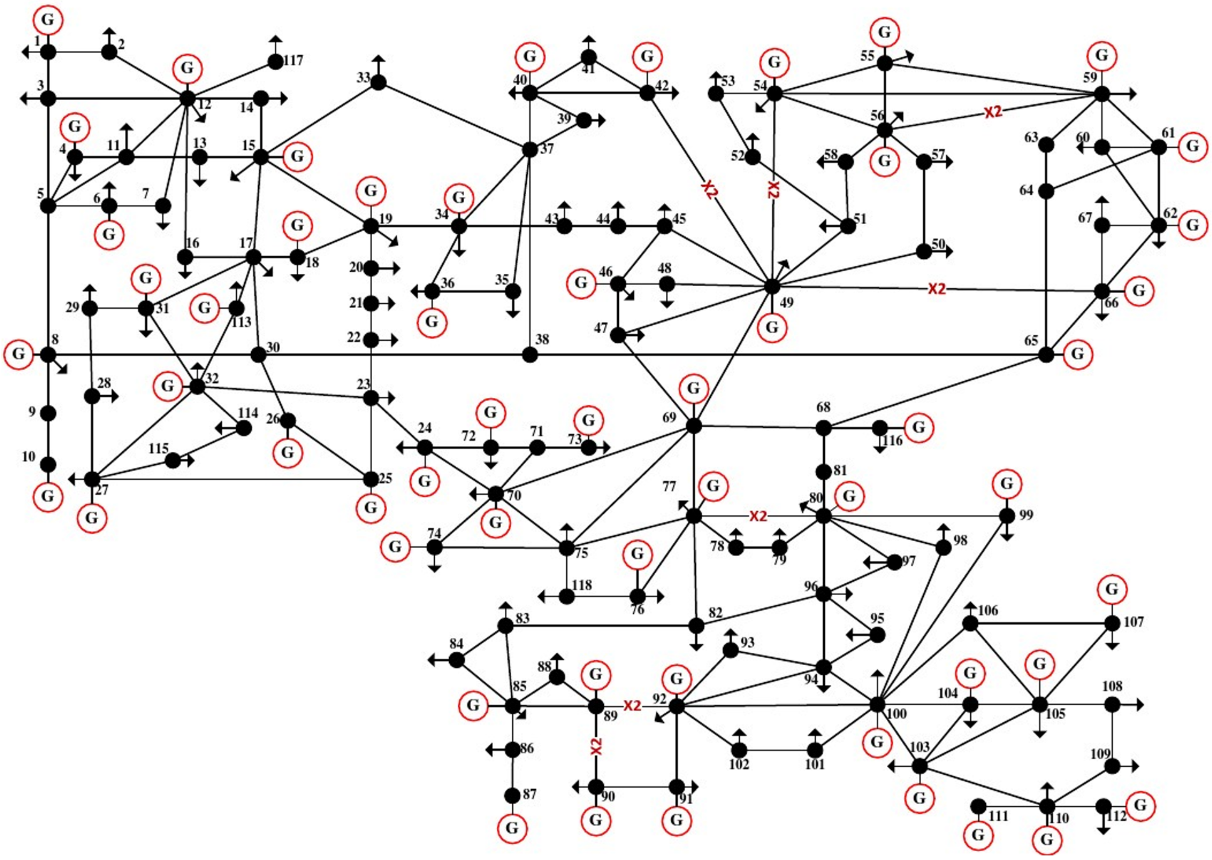

FIGURE 1. The topological structure of IEEE 118 power grid

link vulnerability; however, when attacking the link with different betweenness, it does not indicate that the link with larger betweenness has greater influence on the power grid, hence only the link betweenness cannot distinguish the critical links that could induce cascading failure. For the attack degree based on load level, only when the link ranking in the first 1-7 is attacked, the remaining connectivity is quickly reduced, but the reduction is rapidly reduced after the 7th link fails, the fault of the first six links has not yet led to a large reduction in connectivity. Therefore, the load level can be utilized to detect which link is with large vulnerability, but the identification of the subsequent link is not good. For the comprehensive index, the recognition effect works well. If the number of attacked links increases to 4.8%, the remaining connectivity is reduced to about 40% when attacking the previous nine links ranking by comprehensive index.

It can be seen that the link with greater comprehensive index will produce greater impact on the power grid. Therefore, the comprehensive indicator proposed in this paper can identify the key links that will lead to cascading failure, which means that the indicators can be utilized to estimate the vulnerable links. Due to the small probability of large-scale power outages, there are fewer components that can generate large-area accidents. The conclusions of the above-mentioned vulnerability analysis are basically consistent with the reality. Excluding those links that are prone to generate large-scale power outages, the remaining links still own different effects on power system connectivity. It shows that the comprehensive vulnerability can not only find out the vulnerable links but also distinguish other links. Therefore, the comprehensive indicator is utilized as the isolation indicator. Through the above described algorithm, we can set $T_1 = 0.3$ and $T_2 = 0.4$, and finally the vulnerable link set is acquired as e38-65, e30-38, e8-5, e65-68, e8-9, e9-10.

5.2. **The effect of the isolation algorithm.** After acquisition of the vulnerable link set, the link e8-9 and link e30-38 failure in the set are taken as examples to carry out the link isolation simulation test.

1) If link e8-9 fails

When link e8-9 fails, e38-65, e65-68 are connected to e30-38, and e8-5, e8-9,e9-10 are connected, also the two sets of links are connected via link e8-30.If the link e8-30 is separated, the split of e8-30 does not cause other links to fail. Therefore, the link e8-30 needs to be split. After carrying out a series of processing on the system with the algorithm described above, the isolation results are shown in Figure 2.

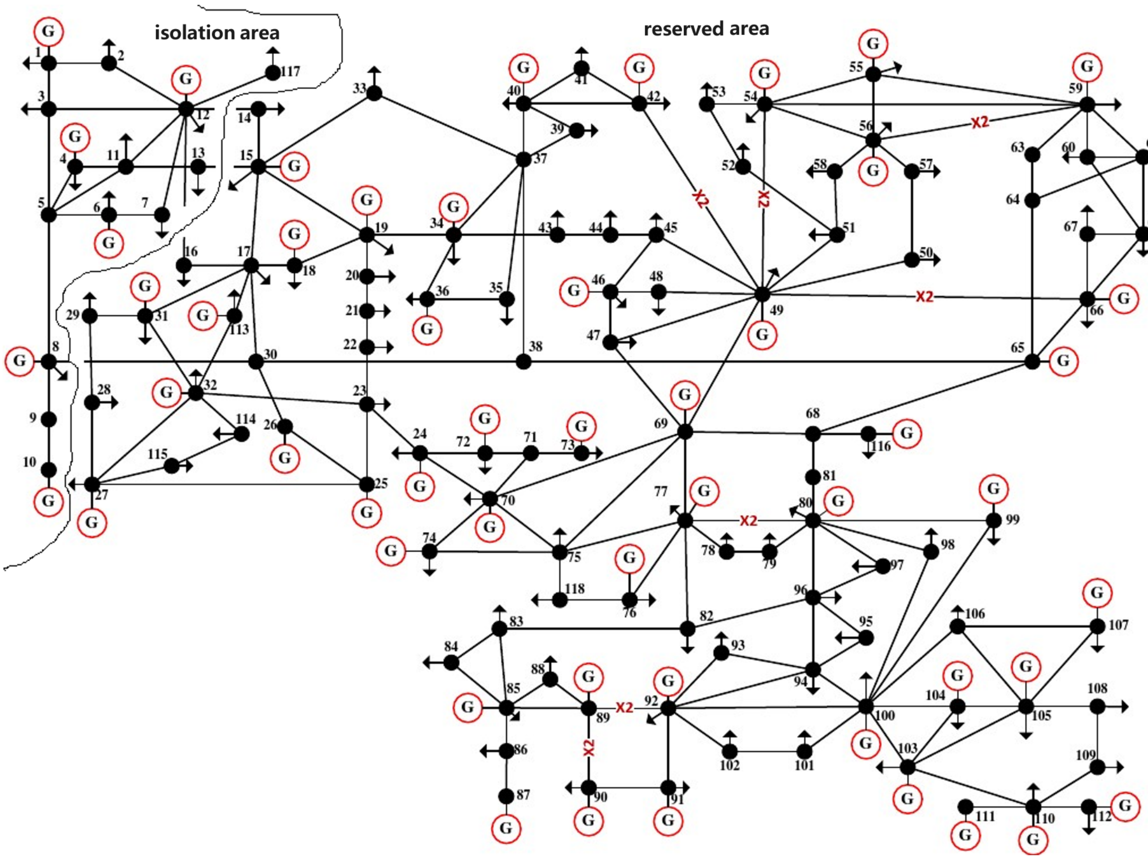

Figure 2. The isolation results when the line e8-9 failed in the IEEE 118 power grid

From Figure 2, the split link set is e8-30, e12-14; e12-16; e13-15, and the power difference of each part is shown in Table 2. The failed link is isolated in the upper left corner. Without considering the network loss, Table 2 shows that the power generation is 3842.4 MW, the load is 3823 MW, and the unbalance rate is only 0.44% in the reserved area. It is basically in equilibrium and can operate independently without optimization measures. Moreover, there are only four links in the split link set, therefore the network recovery after the failure is relatively simple.

2) If the link e30-38 fails

When the link e30-38 fails, the link e8-30 is connected to the e38-65, e65-68, e30-38, and e8-5, e8-9, e9-10 links. After the link e8-30 is split, it is found that the split e8-30 still does not cause other links to fail, so the link e8-30 needs to be split. By performing a series of processing on the system described above, the isolation result can be finally obtained as shown in Figure 3.

Table 2. The power difference of various parts after isolation when the line e8-9 failed

| area | Power generation | Load | Power difference | unbalance rate |
|---|---|---|---|---|
| | MW | MW | MW | % |
| isolation area | 535 | 419 | 116 | 2.65 |
| reserved area | 3842.4 | 3823 | 19.4 | 0.44 |
| total | 4377.4 | 4242 | - | |

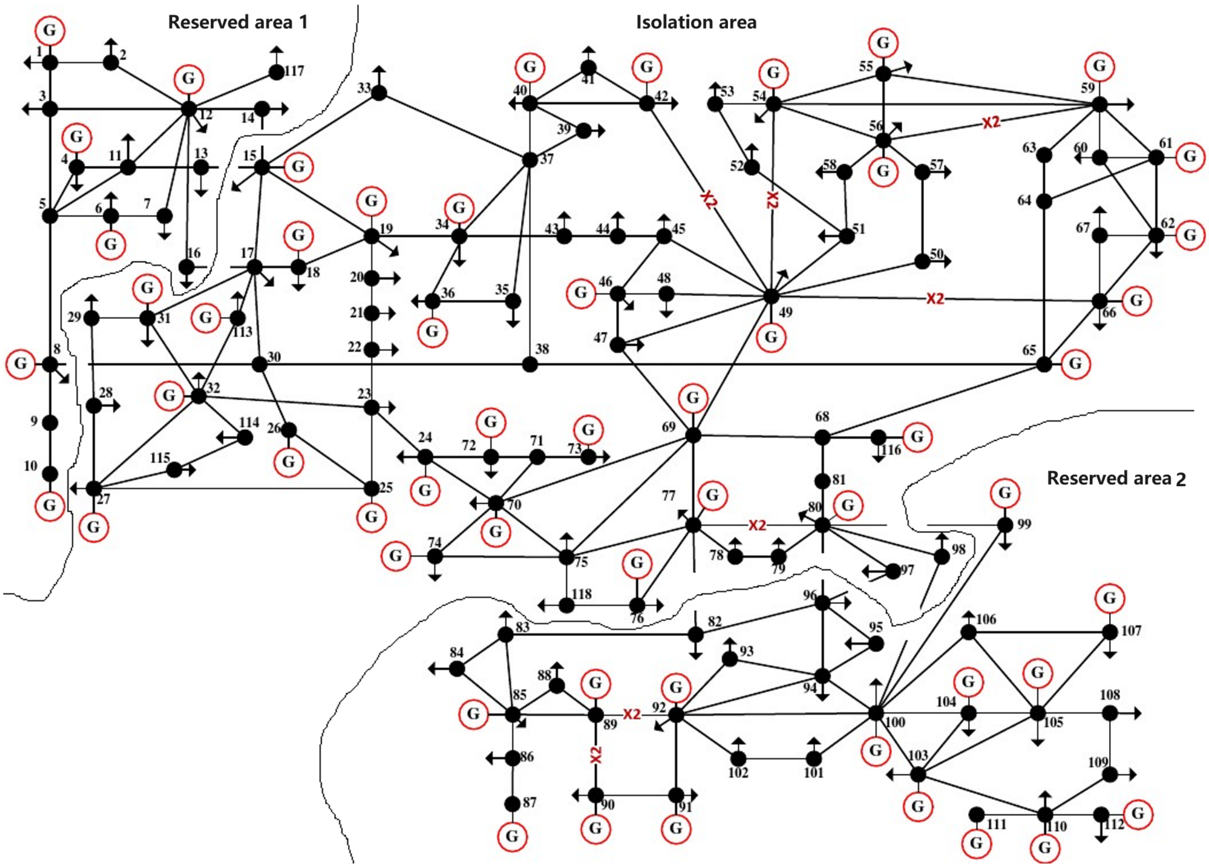

Figure 3. The isolation results when the line e30-38 failed in the IEEE 118 power grid

From Figure 3, the split link set is e30-8, e17-16, e15-13, e15-14, e77-82, e80-96, e80-99, e97-96, e98-100, and the power difference of each part is shown in Table 3. In Figure 3, the failed link is located in the middle zone, and the upper left corner section and the lower right corner section are reserved areas without failure. As shown in Table 3, the unbalance rate of the reserved area 1 and the isolated area are respectively 1.76% and 1.49%. The parts are basically balanced and no optimization is required. However, the amount of electricity generated in the reserve area 2 is slightly lower than the load, therefore a small number of small load components need to be cut so that the three parts can continue to operate separately during the fault operation. In addition, there are only 9 links in the split link set, which is only 4.84% of the IEEE 118 system owning 186 links, so the network recovery after the failure is relatively simple.

Table 3. The power difference of various parts after isolation when the line e30-38 failed

| area | Power generation | Load | Power difference | unbalance rate |
|---|---|---|---|---|
| | MW | MW | MW | % |
| reserved area 1 | 535 | 458 | 77 | 1.76 |
| reserved area 2 | 939 | 946 | -7 | -0.16 |
| isolation area | 2903.4 | 2838 | 65.4 | 1.49 |
| total | 4377.4 | 4242 | - | - |

The analysis of the above two examples shows that the comprehensive index and the corresponding link isolation algorithm proposed in this paper are effective.

6. **Conclusions.** In this paper, for the application of vulnerability analysis, the link is selected as the vulnerability assessment object. Comprehensive state vulnerability, link interface and node second-order centrality constitute indicators together to identify link vulnerability and construct the vulnerable link set. Secondly, the link isolation algorithm is utilized to isolate the fault link in vulnerable link set to prevent the accident from spreading over a large area. The simulation experiment is carried out in IEEE118 power system. The results show that the comprehensive vulnerability is more effective in identifying vulnerable links. Then, the link isolation process is simulated based on the vulnerable link set generated by comprehensive vulnerability. The proposed isolation algorithm could not only isolate the failed part, but also ensure the power balance of each part. Hence the algorithm is effective and feasible, and can effectively assist to prevent the power outage accident in power grid.

**Acknowledgment.** The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

## REFERENCES

[1] J. Xiao, W. Zhang, M. Huang, Y. Lu, W. R. Lawrence, Z. Lin, M. Primeau, G. Dong, T. Liu, W. Tan, W. Ma, X. Meng, and S. Lin, "Increased risk of multiple pregnancy complications following large-scale power outages during Hurricane Sandy in New York State," *Science of The Total Environment*, vol. 770, no. 6, 145359, 2021.

[2] M. Chen, L. Jin, X. Gong, X. Wang, and W. Sun, "Analysis of the spatial cascading effect in networks," *International Journal of Modern Physics*, vol. 31, no. 4, 2050055, 2020.

[3] A. J. Flueck, I. Dobson, Z. Huang, N. E. Wu, R. Yao, and G. Zweigle, "Dynamics and protection in cascading outages," in *Power and Energy Society General Meeting (PESGM)*, IEEE, 2020, pp. 1–5.

[4] W. -L. Fan, X. -F. He, Y. -Q. Xiao, and Q. -Y. Li, "Vulnerability analysis of power system by modified H-index method on cascading failure state transition graph," *Electric Power Systems Research*, vol. 209, 107986, 2022.

[5] K. Chen, N. Zheng, Q. Cai, Y. Li, C. Lin, and Y. Li, "Cyber-physical power system vulnerability analysis based on complex network theory," in *Sixth Asia Conference on Power and Electrical Engineering (ACPEE)*, IEEE, 2021, pp. 482–486.

[6] H. Yuan, G. Zhu, J. Xu, L. Dong, D. Dai, and L. Zheng, "Research on power system line vulnerability analysis and quantitative assessment under blind attack," in *Thirteen International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, IEEE, 2021, pp. 244–250.

[7] J. Peng, W. Jiang, H. Jiang, H. Ge, P. Gong, and L. Luo, "Stochastic vulnerability analysis methodology for power transmission network considering wind generation," in *2022 Power System and Green Energy Conference (PSGEC)*, IEEE, 2022, pp. 85–90.

[8] D. Chen, Z. Chen, J. Li, and J. Liu, "Vulnerability analysis of Cyber-physical power system based on Analytic Hierarchy Process," in *Tenth Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, IEEE, 2022, pp. 2024–2028.

[9] E. Bompard, W. Di, and X. Fei, “Structural vulnerability of power systems: a topological approach,” *Electric Power System Research*, vol. 81, no. 7, pp. 1334—1340, 2011.

[10] F. Gutierrez, E. Barocio, F. Uribe, and P. Zuniga, “Vulnerability analysis of power grids using modified centrality measures,” *Discrete Dynamics in Nature and Society*, vol. 2013, pp. 1—11, 2013.

[11] G. J. Correa, and J. M. Yusta, “Grid vulnerability analysis based on scale-free graphs versus power flow models,” *Electric Power System Research*, vol. 101, pp. 71-–79, 2013.

[12] E. Bompard, R. Napoli, and F. Xue, “Analysis of structural vulnerabilities in power transmission grids,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1-2, pp. 5—12, 2009.

[13] H. Ai, and S. Miao, “Hybrid flow betweenness approach for identification of vulnerable line in power system,” *IET Generation Transmission and Distribution*, vol. 9, no. 12, pp. 1324-–1331, 2015.

[14] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, S. Mei, W. Wei, and L. Ding, “Risk assessment of multi-timescale cascading outages based on markovian tree search,” *IEEE Transactions on Power System*, vol. 32, no. 4, pp. 2887-–2900, 2017.

[15] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, “Power system structural vulnerability assessment based on an improved maximum flow approach,” *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 777–785, 2018.

[16] W. L. Fan, X. M. Zhang, and S. W. Mei, “Vulnerable transmission lines identification considering depth of K-shell decomposition in complex grids,” *IET Generation Transmission and Distribution*, vol. 12, no. 5, pp. 1137—1144, 2018.

[17] Z. Y. Ma, C. Shen, F. Liu, and S. Mei, “Fast screening of vulnerable transmission lines in power grids: a PageRank-based approach,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1982-–1991, 2017.

[18] X. G. Wei, S. B. Gao, T. Huang, E. Bompard, R. Pi, and T. Wang, “Complex network-based cascading faults graph for the analysis of transmission network vulnerability,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1265-–1276, 2018.

[19] L. Z. Li, H. Wu, Y. H. Song, and Y. Liu, “A state-failure–network method to identify critical components in power systems,” *Electric Power System Research*, vol. 181, 106192, 2020.

[20] Y. Liu, L. Li, Y. Yang, S. Wu, Z. Yu, Y. Zhu, R. Zhang, and J. Liu, “An improved active section splitting method for multi-machine power systems based on multilayer graph segmentation algorithm,” in *IEEE Sustainable Power and Energy Conference (iSPEC)*, IEEE, 2022, pp. 1–5.

[21] R. Bian, J. Li, X. Wu, W. Sun, and J. Sun, “A review on active splitting control of power systems,” in *Fifth Asia Conference on Power and Electrical Engineering (ACPEE)*, IEEE, 2020, pp. 555–559.

[22] M. Qing, F. Tang, M. Qing, W. Liang, C. Xiao, W. Jian, D. Liu, and Q. Zhao, “A two-steps splitting strategy based on Laplacian eigenmap algorothm for large power grid with power wind connected,” in *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, IEEE, 2019, pp. 308–312.

[23] Y. Liu, and Y. Liu, “An islanding cutset searching approach based on dispatching area,” *Automation of Electric Power Systems*, vol. 32, pp. 20–24, 2008.

[24] Y. Qiao, C. Shen, and Q. Lu, “Islanding decision space minimization and quick search in case of large-scale grids,” *Proceedings of the CSEE*, vol. 28, pp. 23–28, 2008.

[25] D. Ma, K. Tang, H. Qiao, and C. Shen, “Adaptive islanding control method applied to ac/dc power systems aiming at maintaining the power supply of crucial loads,” *Proceedings of the CSEE*, vol. 39, pp. 3149–3159, 2019.

[26] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, N. A. Al-Nabhan, “An enhanced pairing-based authentication scheme for smart grid communications,” *Journal of Ambient Intelligence and Humanized Computing*, 2021. [Online]. Available: https://doi.org/10.1007/s12652-020-02740-2

[27] C.-M. Chen, L. Chen, Y. Huang, S. Kumar, J. M.-T. Wu, “Lightweight authentication protocol in edge-based smart grid environment,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, 68, 2021.

[28] K. Wang, Z. Chen, X. Dang, X. Fan, X. Han, C.-M. Chen, W. Ding, S.-M. Yiu, J. Weng, “Uncovering hidden vulnerabilities in convolutional neural networks through graph-based adversarial robustness evaluation,” *Pattern Recognition*, vol. 143, 109745, 2023.

[29] A. M. Kermarrec, E. L. Merrer, B. Sericola, G. Tredan, “Second order centrality: Distributed assessment of nodes criticity in complex networks,” *Computer Communications*, vol. 34, no.5, pp. 619–628, 2011.