

# Vulnerable Point Identification Using Heterogeneous Interdependent Node Theory for Distribution Systems

Yu Zhang, Xiaohui Song, *Member, IEEE*, Liwei Xie, *Member, CSEE*, Hua Liu, *Member, CSEE*, and Yong Li, *Senior Member, IEEE, Member, CSEE*

**Abstract**—In order to reduce the occurrence or expansion of accidents and maintain safety in distribution networks, it is essential to find out the vulnerable points for the power system in time. In this paper, a vulnerable point identification method based on heterogeneous interdependent (HI) node theory and risk theory is proposed. Compared with the methods based on betweenness theory, the method based on HI nodes theory can deal with the shortcomings of the power flow shortest path, and consider the direct and indirect relationship of nodes. It is more suitable for identifying vulnerable points in a realistic power system. First, according to the analysis of heterogeneous interdependent networks, the HI nodes are defined and used to evaluate the utility coupling value of each node. Then an identification indicator, which combines the utility coupling value and the risk indicators, is utilized to evaluate the vulnerability of each node. Results show that the proposed method is a suitable one to find the vulnerable points and better than betweenness-based methods for a distribution network.

**Index Terms**—Distribution network, heterogeneous interdependent nodes, utility coupling, vulnerable point identification.

## I. INTRODUCTION

**D**ISTRIBUTION networks are more complex in their structures than transmission networks and connect directly to consumers [1], [2]. The operational risk of a distribution network is an essential factor affecting the quality and reliability of the power supply [3]. Once the vulnerable point is broken or subjected to great interference, it will lead to the successive failure and even cause a large-scale power outage [4]–[6]. Therefore, it is necessary to find the vulnerable point of the power system in a timely fashion. Vulnerable point identification can help the crew to take some defensive or improvement measures in advance, which can reduce the occurrence and effect of risk accidents.

At present, a lot of research has been done on vulnerable point identification for power systems, and can mainly be divided into two categories. In the first category, the cascaded failures are modelled as the migration of steady-states of the power system, then the critical events can be identified and prevented [7]. Based on the steady-state model, the critical contingencies can be determined. In [8], considering a potential cascading fault, the voltage over-limit and load losses, a set of comprehensive risk assessment index system is built to identify the vulnerable part of power system operation based on utility theory. References [9], [10] proposed an identification method of grid vulnerable point identification based on the utility entropy of risk. According to the current distribution clustering and uniformity, this is effective to identify the vulnerability of a power grid. In [11], a tracking analysis is used to obtain the “contribution value” of each component to the system reliability index. The greater the value, the more important is the corresponding component for system reliability. The component which has the greatest contribution value is the most vulnerable part in the system.

The second category adopts topological methods for vulnerability assessments [12], [13]. In recent years, complex network theory has been acknowledged a method of topological analysis power systems [14]. Considering the topology properties between power grids and a complex network, the application of complex network theory has been initiated to assess the power system’s vulnerability [15]. If some critical nodes or edges are removed in the power system, the network will collapse. Terms in complex network theory such as node degree, betweenness, clustering coefficient, etc. are used to identify the vulnerable nodes and buses in a power network [16]. In [17], the node degree is used to analyze the vulnerable nodes in the network. The node with highest node degree is most vulnerable. Some researchers [18]–[20] proposed the node betweenness indicator to evaluate critical nodes in the network. For each node, the authors accumulate the number of paths that pass through it. The larger the number, the more vulnerable the node. Compared with the node degree indicators, node betweenness is better at identifying vulnerable nodes for power systems [21]. However, the power flow does not always follow the node’s shortest path. The node betweenness is therefore not the best indicator to identify the node’s vulnerability in a power system network. In [22], an extended betweenness centrality is proposed to identify

Manuscript received September 25, 2019; revised February 11, 2020; accepted April 8, 2020. Date of online publication April 30, 2020; date of current version July 28, 2020. This work was supported in part by the Science and Technology Project of SGCC “Research on Key Technology of High Reliability Distribution Network in Xiongan New Area” (PDB17201800056).

Y. Zhang and X. H. Song are with China Electric Power Research Institute, Beijing 100192, China.

L. W. Xie, H. Liu and Y. Li (corresponding author, e-mail: yongli@hnu.edu.cn) are with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China.

DOI: 10.17775/CSEEJPES.2019.02310

the criticality of components in power grids. However, the shortcomings of shortest paths are still unsolved. In [23], the max-flow based approach is proposed to assess the vulnerable lines in the power systems with the novel centrality index. In [24] an electric betweenness method is used to identify vulnerable nodes.

These above researchers have conducted in-depth research on vulnerable point identification of large power grids, however, in their analysis models, they assumed that the power flow between each node follows the node's shortest path. In fact, the power flow is also related with the line parameters and load connected at the node. They ignored other possible transmission paths and directions and approaches are not consistent with the realistic power flow transmission characteristics.

To address the shortcomings of power flow shortest path, and analyze the direct and indirect relationships of nodes, we propose a node identification method based on HI theory and risk theory. It used utility coupling value as an indicator to evaluate the node importance weight in a distribution network. This indicator considers the line parameters, node load, power flow path and direction. Its physical background is more appropriate for real case power systems.

Compared with the node betweenness and electric betweenness indicator, the utility coupling value can reflect the influence of "power generation-load" node pairs and is better than the traditional methods in node vulnerability evaluation via simulation. Compared with voltage fluctuation influence tests of different nodes, the results show that the changing trends of node importance are similar to the testing results. Furthermore the utility coupling value is a good indicator of evaluate the node's degree of vulnerability in the distribution network.

In this paper, when a distribution network is given, HI node theory is utilized to define the HI nodes and calculate their utility coupling values. Then, considering the operation events, the utility coupling value and the risk severity degree are combined to establish an identification indicator based on risk theory. The node vulnerability is related to the identification indicator. The larger the indicator value is bigger, the more vulnerable the node. Finally, the node vulnerability weights are sorted from the maximum value to the minimum value according to the value of the identification indicators. The simulation results show that the proposed method can identify the vulnerable points and is better than the traditional method in node vulnerability evaluation.

This paper is organized as follows: Heterogenous interdependent (HI) network theory analysis is presented in Section II. Section III and IV describe the proposed method; first for utility coupling value of nodes, and then for the combination between HI theory and risk theory. Section V presents the simulation and followed by conclusion in the end.

## II. HETEROGENOUS INTERDEPENDENT NETWORK

From [25]–[27], the theory of HI nodes is generated by the existence of HI networks which are the form of evolution from heterogeneous networks. According to complex network theory, the heterogeneous networks consist of different attribute

elements, e.g., the association between multiple types of nodes or edges [28]. For a heterogeneous network  $G$ ,  $T_a$  and  $T_b$  are the set of elements, where  $T_a$  and  $T_b$  represent the set of nodes or links. The number of  $T_a$  and  $T_b$  are more than zero, and the intersection between them is an empty set in the network. If  $T_a$ 's original state  $f(T_a)$  is changed to an instability state  $f'(T_a)$ ,  $T_b$ 's state  $f(T_b)$  is also changed toward an instability or failure state  $f'(T_b)$ . In this time, the heterogeneous network can be defined as a HI network, i.e.,

$$\begin{cases} T_a \cap T_b = \emptyset \\ f(T_a) \rightarrow f'(T_a) \sim f'(T_b) \\ f'(T_b)_{\infty} \notin [\xi_{\min}, \xi_{\max}] \\ |T_a| > 0 \\ |T_b| > 0 \end{cases} \quad (1)$$

where  $f'(T_b)_{\infty}$  is final state of  $T_b$ ,  $\xi_{\min}$  and  $\xi_{\max}$  represent the threshold value with stable states,  $|T_a|$  and  $|T_b|$  are the element number of  $T_a$  and  $T_b$ .

In [27], the HI network is defined as several different structure types according to the research objectives. An electrical power grid network, which is not connected with information cyber, can be roughly classified as two categories. One category is a HI network under the hierarchical structure. As shown in Fig. 1, the entire power grid is stratified with the voltage level.

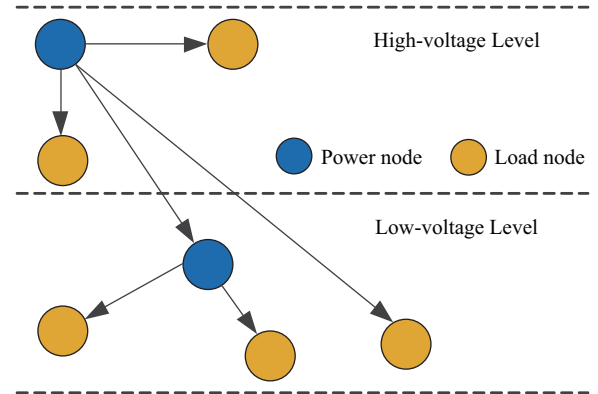


Fig. 1. HI power network based on different voltages.

In the upper layer, the heterogeneous network consists of the high-voltage power nodes and load nodes. In the other layer, the HI network is made of the low-voltage power nodes and load nodes. The power of low-voltage systems is supplied by the high-voltage system. When the upstream node fails, the nodes which are not supplied by other power node are also in a state of power loss. These heterogeneous nodes have interdependent relationships. Therefore, the whole network is a HI network with a two-layer heterogeneous network.

The other category is a HI network with a single-layer structure. The whole distribution network consists of power node, load nodes and DGs nodes in Fig. 2. Although, many load and DG nodes are not directly connected with the power node, they are powered by the power node and connected with a power flow. When the power node state is changed to an instability state, the load nodes are all affected. For example,

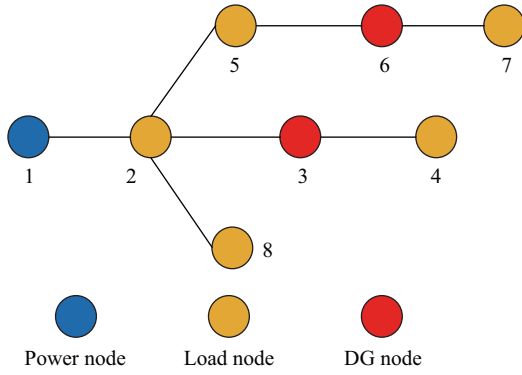


Fig. 2. HI power network based on different nodes.

because of the uncertainty of DG's output, it is difficult for DG nodes to supply power independently to the distribution network. Once the operation state of power node is changed, the output powers and state of DG nodes are also changed. Therefore, the distribution network can be defined as a HI network. In this paper, the IEEE 33 bus system is researched, and its HI nodes consist of one power node and 32 load nodes.

### III. UTILITY COUPLING VALUE OF NODES

In a distribution network, there are different types of nodes, e.g., power nodes, load nodes etc. Some load nodes have direct connection paths with power nodes, and others do not. Thus, the HI nodes are divided into two types: direct and indirect HI nodes in this paper. When each different type element has a directly connected path, these HI nodes are direct HI nodes. For two random HI nodes without a direct connection path, if one node's state is changed with the change of the other, they are defined as indirect HI nodes.

Therefore, in a distribution network, when a node state is changed, the state of direct HI nodes and indirect HI nodes are both changed. The utility coupling degree of nodes are used to evaluate the node failure impacts on operation stability.

As shown in Fig. 3, there is a single-layer distribution network with several nodes. The solid arrows express the direct connection path between nodes, and the dashed arrows are indirect connection path between nodes. For direct HI nodes, they are connected with solid arrows. For indirect HI nodes, they are connected with dashed arrows between each node. The arrow's orientation shows the in and out direction of

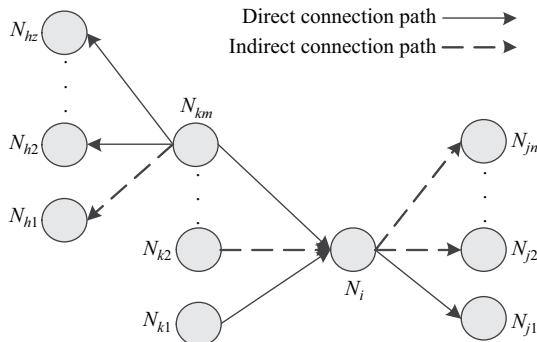


Fig. 3. HI network path between nodes.

power flow. Therefore, a node may have direct HI nodes or indirect nodes in two different directions. For instance, node  $N_i$  is a direct HI node for  $N_k$  where the power flow is from  $N_k$  to it, and is also an indirect node for  $N_j$  where the power flow is from it to  $N_j$ . The node utility value can be defined as

$$\gamma_i = \sum_{t=1}^n V_{kti} + \sum_{l=1}^m V_{ijl} \quad (2)$$

where  $V_{kti}$  is the utility degree between node  $i$  and its in-direction arrow nodes  $kt$ , and  $V_{ijl}$  is the utility degree between node  $i$  and its out-direction arrow nodes  $jl$ .  $n$  and  $m$  are the number of nodes  $N_k$  and  $N_j$  respectively.

In fact, a node may have several in or out direction nodes, e.g., node  $N_k$  is the out-direction node for nodes  $N_i$  and  $N_h$ . Considering the in and out direction weight between each node, the in-direction weight of node  $N_i$  can be expressed as

$$W_{kti} = \frac{V_{kti} / \sum_{p=1}^z V_{khp}}{\sum_{t=1}^n \left( V_{kti} / \sum_{p=1}^z V_{khp} \right)} \gamma_i \quad (3)$$

where  $V_{khp}$  is the utility degree between node  $k$  and its out-direction node  $h$ ,  $V_{ktp}$  is the utility degree between node  $k_t$  and its out-direction node  $h_p$ , and  $z$  is the number of nodes  $N_h$ .

The out-orientation weight of nodes  $N_i$  can be given as:

$$W_{ijl} = \frac{V_{ijl}}{\sum_{l=1}^m V_{ijl}} \gamma_i \quad (4)$$

where  $V_{ijl}$  denotes the utility degree between node  $i$  and its out-direction nodes  $il$ .

The entropy value method is an objective weighting method. It determines the weight of each indicator by the amount of actual data information. The entropy value also can be used to reflect the degree of chaos in the system, and its size is related to the degree of chaos in the system [29]. Compared with the method of experts using a grading and analytic hierarchy process, it is better [29].

In this paper, the entropy value is used to calculate the utility coupling value of nodes. From the previous analysis, the node  $N_i$ 's utility coupling value consists of its in-direction and out-direction utility coupling value.

$$T_i = T_i^{\text{in}} + T_i^{\text{out}} \quad (5)$$

where  $T_i^{\text{in}}$  and  $T_i^{\text{out}}$  are the in-direction and out-direction utility coupling value of  $N_i$ . They are expressed as

$$\begin{cases} T_i^{\text{in}} = \left( 1 - \sum_{t=1}^n \left( \frac{V_{kti}}{\sum_{t=1}^n V_{kti}} \ln \frac{V_{kti}}{\sum_{t=1}^n V_{kti}} \right) \right) \sum W_{kti} \\ T_i^{\text{out}} = \left( 1 - \sum_{l=1}^m \left( \frac{V_{ijl}}{\sum_{l=1}^m V_{ijl}} \ln \frac{V_{ijl}}{\sum_{l=1}^m V_{ijl}} \right) \right) \sum W_{ijl} \end{cases} \quad (6)$$

Because the vulnerable points are the relative results, the normalization of nodes does not affect the identification results of vulnerable nodes. In the normalization, the maximum value of each indicator is selected as the reference value, and the normalization value of  $T_i$  is  $T_i^*$ .

#### IV. VULNERABLE POINT IDENTIFICATION OF RISK

##### A. Risk Theory

Risk refers to the probability or the severity of a disaster [30]. Vulnerable point identification based on risk theory in a power system can help the crew to check the possible disasters according to the operational status of the system, and thus deal with these problems and take appropriate measures. Risk is generally defined as the product of the accident probability and severity degree. It is expressed as:

$$R = P \times S \quad (7)$$

where  $R$  represents the risk value,  $P$  is the probability of risk and  $S$  denotes the severity degree of the accident.

##### B. Risk Indicator of Voltage Over-limit

The traditional indicator of voltage over-limit risk usually uses a linear severity function to express the degree of voltage risk. In this paper, considering the volatility of load, the node voltage is changed with the oscillation of its load. The traditional voltage over-limit risk indicator of node  $N_i$  is:

$$S(N_i) = \begin{cases} e^{U_i - 1.05}, & U_i > 1.05 \\ e^{0.95 - U_i}, & U_i < 0.95 \\ 0, & 0.95 \leq U_i \leq 1.05 \end{cases} \quad (8)$$

where  $U_i$  represents the actual voltage standard value of the node. The utility coupling values of nodes are applied to the voltage over-limit risk indicator. Submitting  $T_i^*$  into (8), the novel indicator is obtained as:

$$F_{Ni} = T_i^* \times S(N_i) \quad (9)$$

Considering the relative nodes, the severity degree indicator  $F_{Ni}$  is normalized as  $F_{Ni}^*$ . The node risk indicator of is given by:

$$R(N_i) = F_{Ni}^* \times P(N_i) \quad (10)$$

where  $P(N_i)$  is the probability of voltage over-limit risk.

##### C. Identification of Vulnerable Point

As shown in Fig. 4, the process of identification can be summarized in the following seven steps.

*Step 1:* Based on the topology of the distribution network, calculate the utility value between each node. According to the impedance between nodes in [31],  $V$  can be expressed as

$$V_{ij} = \left| \frac{1}{Z_{ii} + Z_{jj} - 2Z_{ij}} \right| \quad (11)$$

where  $Z_{ii}$  and  $Z_{jj}$  are the self-impedance of node  $N_i$  and  $N_j$  respectively, and  $Z_{ij}$  is the trans-impedance of node  $N_i$  and  $N_j$ .

*Step 2:* Calculate the utility coupling value  $T$  of each node.

*Step 3:* Judge the conditions of topology for the distribution network. If the topology is changed, step 3 returns back to step 1. If the topology is unchanged, step 3 is followed by step 4.

*Step 4:* Calculate the probability of operation risk at each node according to the current topology of distribution network.

*Step 5:* Calculate the identification indicators of each node.

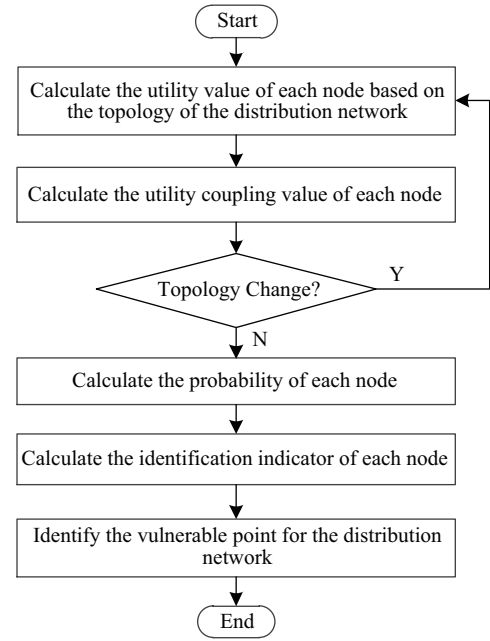


Fig. 4. Flow chart of vulnerable point identification.

*Step 6:* Arrange the node vulnerability in descending order according to value of node risk indicators.

*Step 7:* Identify the vulnerable point for the distribution network.

According to the above-mentioned risk assessment system, the value of a node risk indicator is used to evaluate the node's vulnerability, and the node which has the maximum value of risk indicator is the most vulnerable point.

#### V. TESTING AND SIMULATION

##### A. Node's Importance Evaluation Method Comparisons

In this part, a simple case is used to compare the difference between the traditional method and the proposed method in node importance evaluation. As shown in Fig. 5, there are two systems with one power node and two load nodes. The node evaluation results are shown in Tables I and II.

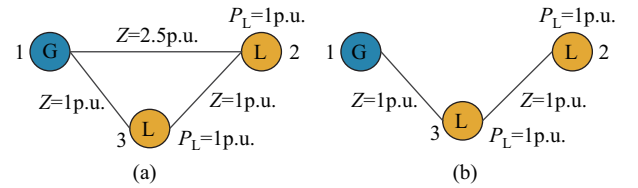


Fig. 5. Simple systems. (a) Line 1-2 closed. (b) Line 1-2 disconnected.

TABLE I  
RESULTS OF TRADITIONAL METHOD

| Node | Nodes 1, 3 connection importance weight (%) | Nodes 1, 3 disconnection importance weight (%) | Change rate (%) |
|------|---------------------------------------------|------------------------------------------------|-----------------|
| 1    | 40                                          | 40                                             | 0               |
| 2    | 20                                          | 20                                             | 0               |
| 3    | 40                                          | 40                                             | 0               |

In Fig. 5(a), node 2 and node 3 are directly connected to node 1. Node 2 and node 3 can receive the power from node

TABLE II  
RESULTS OF PROPOSED METHOD

| Node | Nodes 1, 3 connection importance weight (%) | Nodes 1, 3 disconnection importance weight (%) | Change rate (%) |
|------|---------------------------------------------|------------------------------------------------|-----------------|
| 1    | 38.23                                       | 38.27                                          | 0.1             |
| 2    | 37.49                                       | 23.46                                          | -37.4           |
| 3    | 24.28                                       | 38.27                                          | 57.6            |

1. However, in Fig. 5(b), the topology is changed, and the severity degree of each node will be changed. In Fig. 5(b), node 3 becomes the node which connect node 1 and node 2. Thus, node 3's importance weight will be increased.

From the results of Tables I and II, for the traditional method, the results of nodes 1, 2, and 3 remain unchanged at 40%, 20% and 40% respectively in two different conditions. For the proposed method, the results of nodes 1, 2, and 3 are changed, and especially, node 3's importance weight is increased by 57.6%, while node 2's importance weight is reduced by 37.4%. Thus, the HI method is better than the traditional method in node importance evaluation.

### B. Vulnerable Points Identification

In this part, an IEEE 33 bus system is used to validate the proposed method. As shown in Fig. 6, the system is a distribution network with 33 nodes, 37 branches, 5 contact switches respectively on the branches (33), (33), (34), (35), (36), (37). The types of loads are PQ type, and the reference voltage of power network is 12.66 kV. The contact switches are open under normal operation conditions.

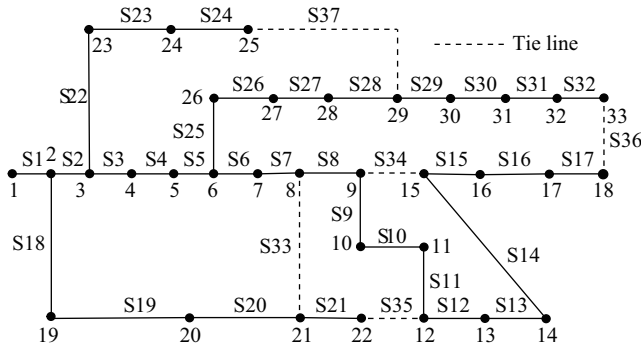


Fig. 6. Topology of the IEEE 33 bus system.

#### 1) Case 1: Normal Operation

As shown in Fig. 6, the distribution network is working with the normal topology. Regardless of the system's operation risk, the node utility coupling values are calculated and shown in Fig. 7, which is represented by the blue line.

In order to validate the utility coupling value, the influences of all the node voltage fluctuations are analyzed and shown in Fig. 7 by the orange line. In Fig. 7, the horizontal coordinate is the node number, the left vertical coordinate is the number of voltage over-limit nodes caused by the voltage fluctuations, and the right vertical coordinate is the utility coupling value. When the testing voltage of node is simulated, the reconstruction of the distribution network is not considered, where the voltage of each node exceeds 10% of its limit. In the simulation, the severity degree of voltage fluctuation is

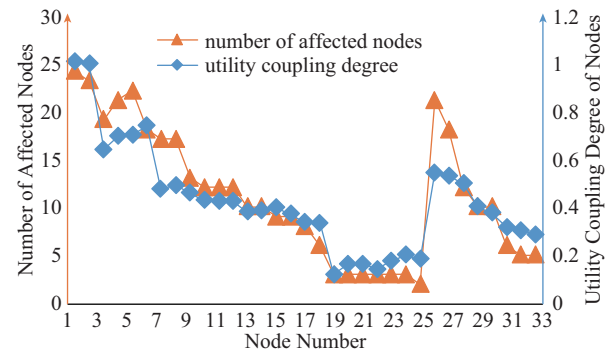


Fig. 7. Utility coupling degree and voltage fluctuation of the IEEE 33 node system.

related to the voltage level of the over-limit node. The node becomes important when the number of the affected nodes become large. Also the greater the node's utility coupling value, the more important is the node. From the results of Fig. 7, the two curves have similar trends and the node 1 is the most important node as shown by both methods. Therefore, according to the above comparison results, the utility coupling value is a good indicator in evaluating the node severity degree in a distribution network.

In order to verify the reliability of the vulnerable point identification method, the proposed method is compared with the node betweenness, electric betweenness and literature [21]. The results are arranged in descending order of vulnerability values in Table III. The rank of the first 15 nodes only are listed.

TABLE III  
IDENTIFICATION RESULTS OF THE VULNERABLE POINT

| No | Node Betweenness |       | Electric Betweenness |       | Reference [21] |       | Proposed Method |       |
|----|------------------|-------|----------------------|-------|----------------|-------|-----------------|-------|
|    | Node             | Value | Node                 | Value | Node           | Value | Node            | Value |
| 1  | 1                | 1     | 1                    | 1     | 2              | 1     | 3               | 1     |
| 2  | 2                | 1     | 2                    | 0.988 | 3              | 0.948 | 2               | 0.983 |
| 3  | 3                | 0.844 | 3                    | 0.88  | 1              | 0.824 | 4               | 0.980 |
| 4  | 4                | 0.719 | 4                    | 0.624 | 4              | 0.578 | 1               | 0.960 |
| 5  | 5                | 0.688 | 5                    | 0.601 | 6              | 0.567 | 5               | 0.951 |
| 6  | 6                | 0.656 | 6                    | 0.591 | 5              | 0.545 | 6               | 0.921 |
| 7  | 7                | 0.375 | 26                   | 0.304 | 26             | 0.299 | 8               | 0.731 |
| 8  | 8                | 0.344 | 27                   | 0.290 | 23             | 0.272 | 26              | 0.723 |
| 9  | 9                | 0.313 | 28                   | 0.277 | 27             | 0.268 | 7               | 0.678 |
| 10 | 10               | 0.281 | 29                   | 0.256 | 7              | 0.263 | 9               | 0.637 |
| 11 | 11               | 0.250 | 7                    | 0.252 | 28             | 0.252 | 27              | 0.630 |
| 12 | 26               | 0.250 | 23                   | 0.219 | 29             | 0.236 | 10              | 0.627 |
| 13 | 12               | 0.219 | 8                    | 0.201 | 8              | 0.206 | 28              | 0.610 |
| 14 | 27               | 0.219 | 30                   | 0.176 | 24             | 0.201 | 11              | 0.607 |
| 15 | 13               | 0.188 | 9                    | 0.168 | 30             | 0.199 | 13              | 0.563 |

From the Table III, in the top 15 nodes, the proposed method has 10 nodes, which also exist in node betweenness method, electric betweenness method and [21]. These nodes are nodes 1, 2, 3, 4, 5, 6, 7, 8, 26 and 27, respectively. The first 6 nodes are the same in four methods. Although their orders are not the same exactly, the area consisting of their locations may be critical in the distribution network.

In node betweenness and electric betweenness methods, node 1 is the most vulnerable node. However, the most vulnerable node in [21] and the proposed method are node 2 and node 3, respectively. This is because these methods



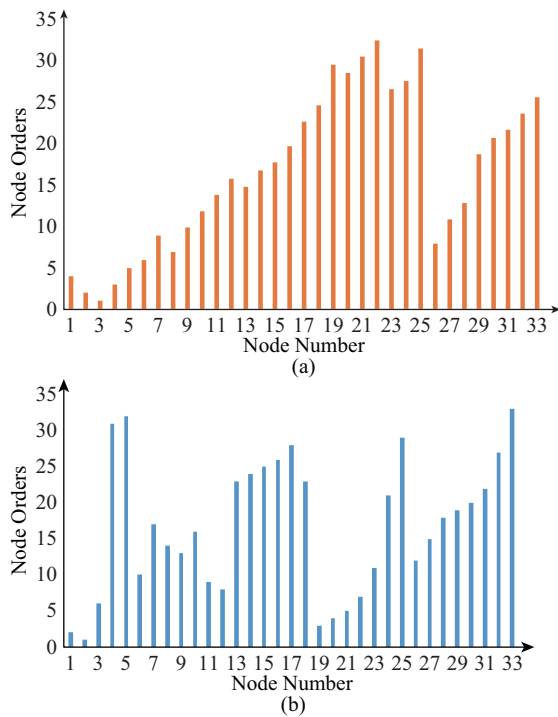


Fig. 9. Node rank of risk indicator. (a) Node rank of case 1. (b) Node rank of case 2.

method is more capable for identifying vulnerable points in a distribution network.

## VI. CONCLUSIONS

According to the characteristics of distribution network, a vulnerable point identification method is proposed based on the heterogeneous interdependent node theory and risk theory. It combines the utility coupling value and the severity degree concepts of risk theory to establish an identification indicator of for each node. The greater the node's indicator value, the more vulnerable is the node in this distribution network. Results show that the proposed method can also solve the problems of power flow path and direction. It is therefore superior to traditional methods and more suitable for an actual (real case) distribution network.

## REFERENCES

- [1] Y. W. Shang, S. X. Shi, B. Wang, X. Z. Dong, and J. Liu, "Operation risk assessment for distribution system with Photovoltaic Substation connections," in *Proceedings of the 12th IET International Conference on Developments in Power System Protection*, 2014, pp. 1–5.
- [2] V. B. Venkateswaran, D. K. Saini and M. Sharma, "Approaches for optimal planning of energy storage units in distribution network and their impacts on system resiliency," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 4, pp. 816–833, Dec. 2020.
- [3] L. Zhou, W. Sheng, W. Liu and Z. Ma, "An optimal expansion planning of electric distribution network incorporating health index and non-network solutions," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 3, pp. 681–692, Sep. 2020.
- [4] A. S. Wang, Y. Luo, G. Y. Tu, and P. Liu, "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory," *IEEE Transactions on Power System*, vol. 26, no. 1, pp. 442–450, Feb. 2011.
- [5] J. K. Fang, C. Su, Z. Chen, H. S. 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, Mar. 2018.
- [6] Y. Cai, Y. J. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.
- [7] X. B. Yu and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1811–1820, Nov. 2004.
- [8] W. N. Wu, J. Yang, W. P. Hu, Z. L. Zeng, T. K. Yu, and P. Liu, "Power grid risk assessment system considering characteristics of transmission line failure," *Electric Power Automation Equipment*, vol. 34, no. 6, pp. 129–134, Jun. 2014.
- [9] M. Ding, Y. Guo, and J. J. Zhang, "Vulnerability identification for cascading failures of complex power grid based on effect risk entropy," *Automation of Electric Power Systems*, vol. 37, no. 17, pp. 52–57, Sep. 2013.
- [10] M. Ding, Y. Guo, J. J. Zhang, Y. C. Qian, X. J. Qi, J. He, and J. Yi, "Node vulnerability assessment for complex power grids based on effect risk entropy-weighted fuzzy comprehensive evaluation," *Transactions of China Electrotechnical Society*, vol. 30, no. 3, pp. 214–223, Feb. 2015.
- [11] Y. Zheng, K. G. Xie, H. B. Li, Z. Y. Li, B. Hu, and Y. H. Ma, "Application of the weak part identification based on reliability tracking method to reliability improvement of provincial power network," *Electrical Measurement & Instrumentation*, vol. 52, no. 6, pp. 118–123, Mar. 2015.
- [12] D. T. Nguyen, Y. L. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, Mar. 2013.
- [13] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, Jul. 2011.
- [14] R. Albert, H. Jeong, and A. L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.
- [15] S. W. Mei, X. M. Zhang, and M. Cao, *Power Grid Complexity*. Berlin Heidelberg: Springer, 2011.
- [16] G. Chen, Z. Y. Dong, D. J. Hill, and G. H. Zhang, "An improved model for structural vulnerability analysis of power networks," *Physica A: statistical Mechanics and its Applications*, vol. 388, no. 19, pp. 4259–4266, Oct. 2009.
- [17] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.
- [18] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, no. 2, pp. 025103, Feb. 2004.
- [19] X. G. Chen, K. Sun, and Y. J. Cao, "Structural vulnerability analysis of large power grid based on complex network theory," *Transactions of China Electrotechnical Society*, vol. 22, no. 10, pp. 138–144, Oct. 2007.
- [20] M. Ding and P. P. Han, "Vulnerability assessment to small-world power grid based on weighted topological mode," *Proceedings of the CSEE*, vol. 28, no. 10, pp. 20–25, Apr. 2008.
- [21] W. C. Shi, X. M. Li, X. L. Wang, S. X. Sun, Y. X. Zhou, and C. C. Hao, "Vulnerability assessment method for distribution network," *Proceedings of the CSU-EPSA*, vol. 30, no. 12, pp. 125–131, Dec. 2018.
- [22] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, Sep. 2012.
- [23] A. Dwivedi and X. H. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 81–88, Feb. 2013.
- [24] R. W. Wang, Y. G. Zhang, Y. Yang, and J. Li, "Vulnerable line identification of complex power grid based on electrical betweenness," *Power System Protection and Control*, vol. 42, no. 20, pp. 1–6, Oct. 2014.
- [25] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.
- [26] J. X. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, Dec. 2012.
- [27] S. Y. Wu and G. Xu, "Degeneration characters of heterogeneous-interdependent network and key node Identification," *Acta Automatica Sinica*, vol. 44, no. 5, pp. 953–960, May 2018.
- [28] Y. Z. Sun, J. W. Han, X. F. Yan, P. S. Yu, and T. Y. Wu, "PathSim: Meta path-based top-k similarity search in heterogeneous information networks," in *Proceedings of the VLDB Endowment*, vol. 4, no. 11, pp. 992–1003, Aug. 2011.

- [29] W. Y. Liu, J. M. Wang, C. Xie, and W. Z. Wang, "Brittleness source identification model for cascading failure of complex power grid based on brittle risk entropy," *Proceedings of the CSEE*, vol. 32, no. 31, pp. 142–149, Nov. 2012.
- [30] F. Xiong, B. B. Dong, and G. F. Li, "Risk evaluation of distribution system with stochastic distributed generator," *Automation of Electric Power Systems*, vol. 40, no. 12, pp. 62–67, Jun. 2016.
- [31] K. Wang, B. H. Zhang, Z. Zhang, X. G. Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 23–24, pp. 4692–4701, Nov. 2011.



**Yu Zhang** received the B.S. degree in Electrical Engineering from North China Electric Power University, Baoding, China, in 2007 and the M.Sc. degree in Electrical Engineering from North China Electric Power University, Beijing, China, in 2010. She is currently a Senior Engineer in the China Electric Power Research Institute. Her main research interests include risk identification and assessment of distribution network and operation analysis of distribution network.



**Xiaohui Song** received the B.S. degree in Electrical Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1991 and the M.Sc. degree in Electrical Engineering from China Electric Power Research Institute, Beijing, China, in 2005. He is currently a Senior Engineer and a Registered Electrical Engineer in the China Electric Power Research Institute. His main research interests include operation analysis, protection and control of distribution network.

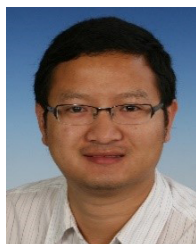


**Liwei Xie** received the B.Eng. degree and M.S. degree in Electrical Engineering from Changsha University of Science and Technology, Changsha, China, in 2015 and 2018, respectively. He is currently pursuing the Ph.D. degree at Hunan University, Changsha, China. His main research interests include self-healing control, power system protection and control.



distribution system.

**Hua Liu** received the B.Sc. degree in Electrical Engineering from the College of Information Engineering, Xi'an Polytechnic University, Xi'an, China, in 2013; and the M.Sc. degree in Electrical Engineering from the College of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China, in 2017. He is currently pursuing the Ph.D. degree at the College of Electrical and Information Engineering, Hunan University, Changsha, China. His research interests include the self-healing control and optimizing operation in power



and control of power quality, and HVDC and FACTS technologies. Dr. Li is a member of the Editorial Board of IET Generation, Transmission, and Distribution and the Associate Editor of IET Power Electronics.

**Yong Li** (S'09–M'12–SM'14) received the B.Sc. and Ph.D. degrees in Electrical Engineering from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2004 and 2011, respectively, and the second Ph.D. degree in Electrical Engineering from TU Dortmund University, Dortmund, Germany, in 2012. He is currently a Full Professor of Electrical Engineering with Hunan University. His research interests include power system stability analysis and control, AC/DC energy conversion systems and equipment, analysis