IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 July 2023, accepted 17 August 2023, date of publication 28 August 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3309188

METHODS

A TOPSIS-Based Vulnerability Assessment Method of Distribution Network Considering Network Topology and Operation Status

JUAN WEN, SIYU LIN, XING QU, AND QIANKANG XIAO
School of Electrical Engineering, University of South China, Hengyang 421000, China

Corresponding author: Siyu Lin (2656390720@qq.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62003157, in part by the Research Foundation of Education Bureau of Hunan Province under Grant 21B0434, and in part by the Technology Planning Project of Hunan Province under Grant 2020JJ5498.

ABSTRACT Vulnerability assessment is one of the effective ways to prevent cascading failures of a distribution network (DN). Considering topological structure and operation status, a comprehensive assessment method based on the technique for order preference by similarity to ideal solution (TOPSIS) is proposed to accurately identify the vulnerable parts of the DN. In the method, the improved structural vulnerability indices based on complex network theory are defined, such as degree and network efficiency. And the electrical betweenness and power flow transfer entropy are established to evaluate the state vulnerability of a DN. Combining the analytic hierarchy process (AHP) and the entropy weight method, a comprehensive weight matrix of each vulnerability index is obtained. Based on the weighted vulnerability indices, the TOPSIS method is proposed to calculate the comprehensive vulnerability of each node and line in the DN. Moreover, the obtained comprehensive vulnerability results are corrected by the grey correlation degree to accurately identify vulnerable parts in the DN. In addition, the system transmission efficiency index is established to describe the degree of system performance degradation of the DN under different attack strategies. The simulation results of IEEE 33-bus test case show that the proposed method can effectively identify vulnerable nodes and lines in the DN.

INDEX TERMS Distribution network, vulnerability assessment, TOPSIS method, complex network theory, attack strategy.

I. INTRODUCTION

The stable operation of the DN is crucial to the reliability of the power system and the daily of users because it is the bond connecting the power system and users [1]. The complexity of DNs has increased significantly with the penetration of distributed generation and the growth of the network scale [2], [3]. Although the change in the scale of the DN can improve the robustness of the system, it will also increase the vulnerability of the network [4]. Due to the uncertainty of power flow and the interaction between nodes, the vulnerability of distribution systems is a key factor affecting the safe operation of the power system [5], [6]. Effective vulnerability assessment of DNs is beneficial for the safe and stable operation of the power system [7].

The complex network theory studies systems in the form of a network avoiding complex dynamic analysis [8], [9]. It has been widely used in analyzing cascading failures [10], [11] and identifying vulnerable nodes in power systems [12], [13]. Many scholars have carried out a lot of research work in vulnerability assessment. But the existing researches have mainly focused on transmission networks. The complex network theory was used to analyze the topological structure of power networks. The research results reveal the scale-free properties of power networks and indicate the system is more vulnerable to deliberate attacks than random failures [14]. To improve the robustness of the system and accurately address potential threats, some topological structure indices

The associate editor coordinating the review of this manuscript and approving it for publication was Tariq Masood.

and overall information centrality have been applied to identify vulnerability nodes in the power networks [15], [16], [17]. However, the pure topological metrics fail to take into account the physical characteristics of the power system. The vulnerability indices with electrical characteristics were proposed [18], [19], [20]. In [18], the electrical distance of electrical parameter of transmission network is used to extend pure topological metrics in complex network theory. The maximum-flow method was proposed to identify vulnerable lines in power systems according to the power flow from generator to load [19]. Reference [20] extended the traditional betweenness index to the hybrid flow betweenness based on the actual path and transmission capacity of the system. Although the improved vulnerability indices considered the operational characteristics of transmission networks, the propagation mechanism of failures is not revealed. For this reason, the influence graph [21], cascading fault graph [22], and adjacent graph [23] were proposed. The mechanism of failure propagation and the adjacent relationships among lines are revealed by analyzing the structural, physical, and operational characteristics of transmission networks. The power system presents an increasingly complex situation with access to wind energy, photovoltaic and electric vehicles and the increase of the demand of users for electricity. Thus, the researchers propose a vulnerability identification model of the power system considering the volatility of distributed generation and the uncertainty of load demand [24], [25], [26]. Moreover, reference [27] explored the impact of extreme weather on the vulnerability of transmission networks.

Due to the difference in topological structure, the research results obtained in transmission networks cannot be directly applied to DNs. Therefore, it is necessary to identify the vulnerable parts according to the unique topological structure and power flow characteristics of distribution systems. Reference [28] found that spatial properties and geographical constraints significantly affect the performance of DNs. In [29], the structural indices of degree and cohesion have been applied to evaluate the vulnerability of nodes in DNs. Reference [30] constructed a comprehensive assessment model based on the network structure and load shock to evaluate the vulnerability of lines in DNs. Although the above methods analyze the vulnerability of distribution systems from the perspective of a complex network, none of them improve the evaluation indices according to the radial topology of DNs. Considering the topological structure sparse of DNs, reference [31] improved the node degree index and the line flow entropy index to evaluate the vulnerability of nodes and lines in DNs.

To sum up, the current vulnerability researches mainly focus on the transmission network. The specific and reliable evaluation indices are still lacking in the vulnerability assessment of the distribution system. Therefore, we present the important theories of the vulnerability assessment method for DNs [32]. Based on the theory in [32], we propose vulnerability assessment indices of the distribution system from different perspectives. Considering the radial topology of the DN, the extended node degree index and line degree index are proposed based on complex network theory. By analyzing the impact on network efficiency after removing a node or line, the node efficiency index and line efficiency index are proposed. Based on the network structure and system power flow, the state indices are proposed, such as electrical betweenness. And the AHP and the entropy weight method are combined to construct a comprehensive weights matrix. The weights of each evaluation index are determined using the weighted vulnerability matrix. The TOPSIS method is presented to obtain the comprehensive vulnerability of nodes and lines in the DN. The obtained results are corrected by the grey correlation degree [33]. Finally, we have established random attack and deliberate attack models based on the attack strategies. The system transmission efficiency index is constructed to describe the degree of system performance degradation of the DN under different attack strategies. Different attack methods are tested on IEEE 33-bus system to simulate the change in system transmission efficiency before and after the system attacks. Using the proposed method, the results show that the attack makes the transmission efficiency of the system decrease the most. It is proved that the comprehensive multi-index TOPSIS method can effectively identify the vulnerable nodes and lines in the DN. The key contributions of this paper are as follows:

1) Some structural vulnerability indices considering the radial topology of the distribution system are proposed. By analyzing the power flow change of the DN after removing a node or line, some state vulnerability indices are proposed. Each index can describe the vulnerability of DN from different aspects.

2) A TOPSIS method improved by the grey correlation degree is presented to calculate the comprehensive vulnerability of nodes and lines in the DN. This method integrates multiple assessment indices to identify vulnerable nodes and lines in the DN, which overcomes the deficiency of a single indicator.

3) An attack model is established, including deliberate attack and random attack strategies. Moreover, an efficiency index is presented to describe the degree of system performance degradation of the DN under different attack strategies.

The rest of this paper is organized as follows: Section II gives vulnerability assessment indices of node and line, including structural indices and state indices. Section III provides the TOPSIS method to identify vulnerable nodes and lines by integrating multiple indices. Section IV presents the system transmission efficiency index and the attack model. Section V presents the simulation results of an IEEE 33-bus system. Finally, section VI outlines conclusions.

II. VULNERABILITY ASSESSMENT INDICES

A. STRUCTURAL VULNERABILITY INDICES

According to complex network theory, the DN can be simplified as an undirected weighted network without

self-loops $G = (V, L, W)$, where $V = \{v_1, v_2, \ldots, v_N\}$ is the node set composed of generator nodes, load nodes and transmission nodes in the system, $L = \{l_1, l_2, \ldots, l_m\}$ is the set of transmission lines between nodes, and $W = \{w_{l1}, w_{l2}, \ldots, w_{lm}\}$ is the set of weights of each line. Considering that the longer the line in the same type of line, the greater the impedance, we set the weight of each line as the modulus value of the line impedance, so $w_{lm} = |Z_{lm}|$.

1) EXTENDED NODE DEGREE

The degree is defined as the number of edges connected to a node. Due to the radial topology of the DN, many nodes with the same degree. To distinguish the importance of these nodes, we will make improvements to the traditional degree metrics.

Considering that a network consists of nodes and edges, the importance of nodes is not only related to the edges but also affected by adjacent nodes [34]. Moreover, since the degree only reflects the local characteristic and cannot describe the global importance of the node, the definition of closeness centrality is introduced. The closeness centrality of i node is:

$$C_i = \frac{1}{\frac{1}{n-1}\sum_{j=1}^{n} d_{ij}} \tag{1}$$

where n is the number of nodes in the network, d_{ij} is the weighted shortest distance between i and j nodes.

The closeness centrality can measure the degree to which a node is located in the center of the network. The greater the closeness centrality of a node, the more critical its global position in the network is.

In summary, by considering the contribution of adjacent nodes and the degree of nodes approaching the network center, the extended degree of i node is defined as:

$$ND_i = C_i \frac{D_i}{k^2} \sum_{j \in V_{ad}} C_j D_j \tag{2}$$

where D_i is the traditional degree of i node, k is the average degree of all nodes, V_{ad} represents the set of all nodes adjacent to i node.

2) LINE DEGREE

The degree is usually used to describe the importance of nodes. We introduce the degree to the evaluation of line vulnerability. The higher the degree of nodes connected at the beginning and end of the line, the more critical the line is. Therefore, the degree of line l is defined as:

$$LD_l = \frac{1}{\bar{D}_N} \sqrt{D_{l1} D_{l2}} \tag{3}$$

where $\bar{D}_N$ is the average value of newly defined degrees of all nodes, D_{l1} and D_{l2} are the newly defined degrees of the first and last nodes of line l respectively.

3) NODE EFFICIENCY

In (2), the degree index identifies vulnerable nodes from a static point of view. For a dynamically changing network, the identification of vulnerable nodes needs to consider the changes in the network topology after nodes are removed due to failure.

Therefore, we introduce the node deletion method to evaluate the vulnerability of nodes by analyzing the change in network efficiency of DN before and after node deletion. The network efficiency is defined as:

$$E = \frac{2}{n(n-1)} \sum_{i \neq j \in N} \frac{1}{d_{ij}} \tag{4}$$

where N is the set of nodes in the network.

Considering the characteristics of closed-loop design and open-loop operation of DN, the corresponding tie switches can be closed to reconnect the network when a node is removed. Therefore, we will close the corresponding tie switches to make the network reconnect after deleting a node. The node efficiency index of i node is defined as:

$$NE_i = \frac{E - E^*}{E} \tag{5}$$

where E and E^* are network efficiency before and after i node deletion respectively.

4) LINE EFFICIENCY

Refer to the method of calculating the node efficiency by using the node deletion method. The line efficiency index evaluates line vulnerability by the change of network efficiency after the line is deleted. Similarly, considering the special structure of the DN, it is necessary to close the corresponding tie switches to make the network reconnect after deleting a line.

Therefore, the line efficiency index of l line is defined as:

$$LE_l = \frac{E' - E'^*}{E'} \tag{6}$$

where E' and E'^* are network efficiency before and after l line deletion respectively.

B. STATE VULNERABILITY INDICES

1) LINE ELECTRICAL BETWEENNESS

The betweenness is the number of times the shortest path passes an edge between all pairs of nodes in the network. Reference [35] points out that the power is not only transmitted along the shortest path between generator and load. According to the characteristics of power flow propagation and combined with the basic ideas of existing models, the electrical betweenness of the line (m, n) can be defined as follows:

$$B_e(m, n) = \sum_{i \in G, j \in F} \sqrt{W_i W_j} |I_{ij}(m, n)| \tag{7}$$

where $I_{ij}(m, n)$ represents the current induced on the line (m, n) after adding a unit injection current source between

the generator and the load node pair $(i,\ j)$, W_i is the weight of generator node i, which takes the rated capacity or actual output of the generator, W_j is the weight of load node j, which is the actual or peak load, G and F are sets of generator nodes and load nodes, respectively.

In the above electrical betweenness, current will be generated on all lines in the system when a current source is injected between generator i and load j. However, this is inconsistent with the actual situation in the power system that the transmission from the generator to the load is only along some lines.

In this paper, the factors not considered in the above-mentioned electrical betweenness are improved. The electrical betweenness of l line is defined as:

$$LB_l = \left| \sum_{i \in G, j \in F} w_{ij} \frac{p_{ij}(l)}{p_{ij}} \right| \tag{8}$$

where $w_{ij} = \min(S_{Gi}, S_{Fj})$, S_{Gi} represents the rated generating capacity of the generator node i, S_{Fj} represents the maximum load demand of the load node j, P_{ij} is the power transmitted from generator node i to load node j, $P_{ij}(l)$ is the component of the power transmitted from generator node i to load node j on line l.

The line electrical betweenness overcomes the deficiency of the traditional betweenness assumption that the power flow between buses flows along the shortest path. It not only considers the topological structure of the DN and the power flow distribution of the system, but also reflects the utilization of the line by the power flow between the ''generation-load'' node pairs and the direction of actual power transmission.

2) NODE ELECTRICAL BETWEENNESS

There are three types of nodes in DNs: generation nodes, load nodes and transmission nodes. According to Kirchhoff's law, the absolute value of the inflow power to any node is equal to the absolute value of the outflow power; that is, the power passing through the node is equal to half of the sum of the absolute value of the inflow and outflow power. Therefore, the importance of a node is related to its type and the line connected to the node. According to the electrical betweenness mapping relationship between lines and nodes in the DN, the electrical betweenness corresponding to the three types of nodes is [36]:

$$NB_i = \begin{cases} \frac{1}{2}(\sum_{l \in F(i)} LB_l + \sum_{j \in L} w_{ij}), & i \in G \\ \frac{1}{2}(\sum_{l \in F(i)} LB_l + \sum_{j \in G} w_{ji}), & i \in L \\ \frac{1}{2} \sum_{l \in F(i)} LB_l, & i \notin G, \quad i \notin L \end{cases} \tag{9}$$

where LB_l is the line electrical betweenness of l line, $F(i)$ represents the set of lines connected to i node, G and L are sets of generator nodes and load nodes, respectively.

3) LINE POWER FLOW TRANSFER ENTROPY

Entropy can reflect the degree of chaos in the system. Therefore, it can be used as an indicator to measure the order and disorder of the system. The entropy is defined as:

$$H_i = -C \sum_{i=1}^{M} \gamma(W_i) \ln \gamma(W_i) \tag{10}$$

where W_i is the i state, γ is the probability of W_i, C is a constant, M is the number of states.

The power system is a complex nonlinear system. The entropy can be used as an indicator to characterize its state during operation. Reference [37] proposed the power flow transfer entropy of the transmission network based on the entropy theory, which is used to quantitatively describe the balance degree of residual power flow distribution in the system after a fault line is disconnected.

Considering the radial structure characteristics of the DN, subsequent nodes will not be able to supply power when a line is disconnected. Therefore, when a line is out of operation due to failure, we will close the tie switch of the ring network where the line is located. Then, the disconnected lode nodes can reconnect to the system.

When the line l in the DN is disconnected due to failure, the power flow variation ΔP_{kl} of line k is:

$$\Delta P_{kl} = |P_{kl} - P_{k0}| \tag{11}$$

where P_{k0} is the initial power of line k, P_{kl} is the power of line k after line l is disconnected.

Then, after line l is disconnected, the power flow impact ratio η_{kl} borne by line k is:

$$\eta_{kl} = \frac{\Delta P_{kl}}{\sum_{k=1}^{K} \Delta P_{kl}} \tag{12}$$

where K is the number of lines in the system.

Given a constant sequence $U = [U_1, U_2, U_e, \ldots, U_n]$, we take $U = [0, 0.02, 0.04, \ldots, 1]$ in this paper. Using $Z_{e(l)}$ to represent the number of lines whose power flow impact ratio is in the interval $\eta_{kl} \in (U_e, U_{e+1}]$ after the line l is disconnected, it can be known that the probability of any line load rate in $\eta_{kl} \in (U_e, U_{e+1}]$ is:

$$p_{e(l)} = \frac{Z_{e(l)}}{\sum_{e=1}^{n-1} Z_{e(l)}} \tag{13}$$

Based on the traditional entropy model, we define the power flow transfer entropy of line l as:

$$LT_l = -C \sum_{e=1}^{n-1} p_{e(l)} \ln p_{e(l)} \tag{14}$$

where C takes in $\ln 2$.

In (14), the power flow transfer entropy index LT_l reflects the uniformity of the transfer power flow distribution after the lines in the DN are out of operation. When the value of LT_l is large, it indicates that the impact of the transfer power flow on the system after the line l is disconnected is large.

4) NODE-INJECTED POWER

The node-injected power can reflect the ability of the node to transmit power in the system. If nodes with the same injected power are located in different positions of the distribution system, their impacts due to failures are also different. Therefore, based on the radial structure of the DN, we assign different grades to nodes in different branches and use it as a weight factor to multiply the node injection power. The weighted node injection power ratio is proposed as:

$$NP_i = \omega_i \frac{P_i}{S_b} \tag{15}$$

where ω_i represents the level of distribution node i, P_i is the injected power of i node, S_b is the base capacity of the system.

The node hierarchical search step includes: in the initial situation, let all nodes of the DN be one-level. Search downward along the feeder from the bus node. If the next node is not a branch node, continue to search down while keeping the node level unchanged. If a branch node is encountered, the level of this node and all nodes before the node will be increased by one. Continue to search along the line in this way until all nodes in the DN are traversed.

The IEEE 33-bus system in Fig. 2 is taken as an example to analyze. After adopting this hierarchical method, nodes 1 and 2 are four-level nodes, node 3 is a three-level node, nodes 4, 5 and 6 are second-level nodes, and other nodes are first-level nodes.

III. VULNERABILITY ASSESSMENT METHOD

A. TOPSIS METHOD

Taking nodes or lines in the DN as a scheme and the vulnerability indices defined in Section II as attributes. Then, the vulnerability assessment of nodes and lines can be transformed into a multi-attribute decision-making problem. We propose the TOPSIS method to solve this problem. However, when the Euclidean distances of the two schemes are the same, the TOPSIS method cannot be effectively evaluated. Therefore, we use the grey correlation degree to adjust the results obtained by the TOPSIS and construct a relative closeness to evaluate each scheme. The detailed implementation process of the TOPSIS is as follows [33].

Step 1: The vulnerability assessment indices of the node and line in the DN were calculated according to the definition in Section II. Let the number of nodes be n, the number of lines be n', and the number of corresponding indices be m and m'. Take nodes and lines as row vectors and evaluation indices as column vectors to construct decision matrices $\boldsymbol{X} = (x_{ij})_{n\times m}$ and $\boldsymbol{X'} = (x'_{ij})_{n'\times m'}$. The row and column vectors can be viewed as alternatives and attributes, respectively. The vulnerability identification of nodes and lines is carried out independently, and the subsequent steps take node vulnerability identification as an example.

$$\boldsymbol{X} = \begin{array}{c} \\ \text{node } 1 \\ \vdots \\ \text{node } n \end{array} \begin{array}{c} \begin{array}{ccc} \text{index } 1 & \dots & \text{index } m \end{array} \\ \begin{bmatrix} x_{11} & \dots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \dots & x_{nm} \end{bmatrix} \end{array} \tag{16}$$

Step 2: Calculates the normalized decision matrix $\boldsymbol{R} = (r_{ij})_{n\times m}$. Perform vector normalization processing on each element in $\boldsymbol{X} = (x_{ij})_{n\times m}$. In this way, the difference in dimension and meaning of each index can be eliminated. Then, the unified calculation of the index can be realized.

$$r_{ij} = x_{ij} / \sqrt{\sum_{i=1}^{n} x_{ij}^2} \tag{17}$$

Step 3: Calculates the weight normalized decision matrix $\boldsymbol{Z} = (z_{ij})_{n\times m}$. Set the weight $\boldsymbol{W} = (\omega_1, \omega_2, \dots, \omega_m)$ for each evaluation index, and calculate each element in the weight normalization matrix as:

$$z_{ij} = \omega_j r_{ij} \tag{18}$$

Step 4: Determine the positive ideal solution and negative ideal solution of the evaluation object as $\boldsymbol{Z}^+$ and $\boldsymbol{Z}^-$ respectively.

$$\begin{cases} \boldsymbol{Z}^+ = (z_{i1}^+, z_{i2}^+, \dots, z_{ij}^+) = (\max\limits_i z_{i1}, \max\limits_i z_{i2}, \dots, \max\limits_i z_{ij}) \\ \boldsymbol{Z}^- = (z_{i1}^-, z_{i2}^-, \dots, z_{ij}^-) = (\min\limits_i z_{i1}, \min\limits_i z_{i2}, \dots, \min\limits_i z_{ij}) \end{cases} \tag{19}$$

Step 5: Calculate the Euclidean distance for each scenario:

$$\begin{cases} \boldsymbol{M}_i^+ = \sqrt{\sum_{j=1}^{m} (\boldsymbol{Z}_j^+ - \boldsymbol{Z}_{ij})^2} \\ \boldsymbol{M}_i^- = \sqrt{\sum_{j=1}^{m} (\boldsymbol{Z}_j^- - \boldsymbol{Z}_{ij})^2} \end{cases} \tag{20}$$

Step 6: Calculate the grey correlation coefficient matrix of each alternative scheme and the ideal scheme as $\boldsymbol{U}^+ = (u_{ij}^+)_{n\times m}$, $\boldsymbol{U}^- = (u_{ij}^-)_{n\times m}$. where:

$$\begin{cases} u_{ij}^+ = \dfrac{\min\limits_i \min\limits_j |\boldsymbol{Z}_j^+ - \boldsymbol{Z}_{ij}| + 0.5 \max\limits_i \max\limits_j |\boldsymbol{Z}_j^+ - \boldsymbol{Z}_{ij}|}{|\boldsymbol{Z}_j^+ - \boldsymbol{Z}_{ij}| + 0.5 \max\limits_i \max\limits_j |\boldsymbol{Z}_j^+ - \boldsymbol{Z}_{ij}|} \\ u_{ij}^- = \dfrac{\min\limits_i \min\limits_j |\boldsymbol{Z}_j^- - \boldsymbol{Z}_{ij}| + 0.5 \max\limits_i \max\limits_j |\boldsymbol{Z}_j^- - \boldsymbol{Z}_{ij}|}{|\boldsymbol{Z}_j^- - \boldsymbol{Z}_{ij}| + 0.5 \max\limits_i \max\limits_j |\boldsymbol{Z}_j^- - \boldsymbol{Z}_{ij}|} \end{cases} \tag{21}$$

The grey correlation degree calculated according to the grey correlation degree matrix is:

$$\begin{cases} \boldsymbol{N}_i^+ = \dfrac{1}{m} \sum\limits_{j=1}^{m} u_{ij}^+ \\ \boldsymbol{N}_i^- = \dfrac{1}{m} \sum\limits_{j=1}^{m} u_{ij}^- \end{cases} \tag{22}$$

Step 7: Calculate close distance $\boldsymbol{L}_i^+$ and $\boldsymbol{L}_i^-$. Normalize $\boldsymbol{M}_i^+, \boldsymbol{N}_i^+, \boldsymbol{M}_i^-$ and $\boldsymbol{N}_i^-$ respectively.

$$\begin{cases} \boldsymbol{L}_i^+ = \alpha M_i^- + \beta N_i^+ \\ \boldsymbol{L}_i^- = \alpha M_i^- + \beta N_i^- \end{cases} \tag{23}$$

where α and β represent the closeness coefficients of the alternative and the positive ideal scheme in terms of position and shape, respectively, satisfying $\alpha + \beta = 1$. We believe that the Euclidean distance and the grey correlation degree are equally important and are taken as 0.5.

Step 8: Calculate the relative closeness $\boldsymbol{D}$.

$$\boldsymbol{D}_i = \frac{\boldsymbol{L}_i^+}{(\boldsymbol{L}_i^+ + \boldsymbol{L}_i^-)} \tag{24}$$

The positive ideal scheme can reflect the maximum vulnerability of nodes that may exist in the DN. The relative closeness can be used to measure the closeness of the node's vulnerability to the maximum vulnerability. Therefore, the relative closeness can be used as a measure of the comprehensive vulnerability of each node in the DN.

B. COMPREHENSIVE WEIGHT

We adopt the AHP and the entropy weight method to weight each index from both subjective and objective perspectives. Entropy can be used to measure the disorder of a system. The more obvious the difference in the state of each parameter in the system is, the more unstable the system is. Thus, entropy can be used to measure the role of indices in describing the vulnerability of nodes and lines. Define the entropy value of index j as:

$$E_j = -\sum_{i=1}^{n} h_{ij} \ln h_{ij}, \quad (j = 1, 2, \ldots, m) \tag{25}$$

where h_{ij} is obtained after standardizing the decision matrix in (16), then $h_{ij} = x_{ij} / \sum_{i=1}^{n} x_{ij}$.

The larger the entropy, the more stable the system, and the smaller the role of indices in evaluation. Therefore, the entropy of index j is processed as follows, and its objective weight ε_{1j} is obtained as:

$$\varepsilon_{1j} = \frac{1 - E_j}{m - \sum_{j=1}^{m} E_j}, \quad (j = 1, 2, \ldots, m) \tag{26}$$

The entropy weight method assigns weight to each index from an objective perspective, but it cannot fully describe the importance of indices. Therefore, we combine AHP and entropy weight method to construct a comprehensive weight.

The AHP can combine qualitative analysis with quantitative analysis. Commonly used scaling methods in AHP include three-scale, nine-scale, and exponential scales. Considering that multiple indices are required for vulnerability assessment, we choose the scale of $e^{0/5} \sim e^{8/5}$ to construct a judgment matrix and calculate the subjective weight of each index. The judgment scale is shown in Table 1.

The maximum eigenvalue and eigenvector of the judgment matrix are calculated. After the judgment matrix passes the consistency test, the subjective weight vector ε_{2j} is calculated. The description of the importance of indices should combine the effects of both objective and subjective weights. Therefore, the comprehensive weight calculation formula is as follows:

$$\varepsilon_j = \frac{\sqrt{\varepsilon_{1j}\varepsilon_{2j}}}{\sum_{j=1}^{m} \sqrt{\varepsilon_{1j}\varepsilon_{2j}}}, \quad (j = 1, 2, \ldots, m) \tag{27}$$

TABLE 1. Judge rules.

Evaluation	Scale value
Equally important	$e^{0/5}$
Minor importance	$e^{1/5}$
Slightly important	$e^{2/5}$
More important	$e^{3/5}$
Obviously important	$e^{4/5}$
Very important	$e^{5/5}$
Strongly important	$e^{6/5}$
More strongly important	$e^{7/5}$
Extremely important	$e^{8/5}$

IV. ATTACK MODEL

A. SYSTEM TRANSMISSION EFFICIENCY

Most of the existing studies use the maximally connected subgraph index to analyze the impact of the removal of nodes and lines on the system. However, the essence of the power system is power flow transmission. Reference [38] proposed a network efficiency index by analyzing the system topological structure. The relative efficiency R is used to evaluate the decline degree of system performance after the system is attacked.

$$E = \frac{2}{n(n-1)} \sum_{i \neq j \in N} \frac{1}{d_{ij}} \tag{28}$$

$$R = \frac{E}{E_0} \tag{29}$$

where E_0 is the network efficiency of the initial network, E is the network efficiency after the system is attacked.

Considering the actual characteristics of the power network, we propose the transmission efficiency index TE based on the network efficiency.

$$TE = \frac{1}{N_G N_L} \sum_{i \in G} \sum_{j \in L} \frac{\min(P_i, P_j)}{Z_{ij}} \tag{30}$$

where N_G and N_L are the number of generator nodes and load nodes in the network, $\min(P_i, P_j)$ is the maximum transmission power between the generator-load node pair, Z_{ij} is the electrical distance between nodes i and j.

To describe the ability of the system to maintain power transmission after being attacked, we add the active power survival rate PS to the evaluation index.

$$PS = \frac{\sum_{j \in L} P_j}{P_{sum}} \tag{31}$$

where $\sum_{j\in L} P_j$ is the sum of active power remaining after the system is attacked, P_{sum} is the initial total active power of the system. Therefore, we propose the system transmission efficiency index as follows:

$$STE = TE \times PS = \left(\frac{1}{N_G N_L}\sum_{i\in G}\sum_{j\in L}\frac{\min(P_i, P_j)}{Z_{ij}}\right) \times \left(\frac{\sum_{j\in L} P_j}{P_{sum}}\right) \quad (32)$$

B. ATTACK STRATEGY

Two attack strategies of random attack and deliberate attack are used. The attack process is to continuously remove nodes or lines in the system and calculate the variation of *STE*. Random attacks simulate the generation of random failures, removing nodes or lines at random. Deliberate attacks are based on the ranking results of the vulnerability of nodes or lines. The nodes or lines with high vulnerability in the system are removed in turn. Considering that the DN has the characteristics of closed-loop design and open-loop operation, the normal operation of the system can be maintained by closing the tie switch when a node or line is attacked. Therefore, the corresponding tie switches are closed to reconnect the disconnected load nodes after each attack. Taking node attack as an example, the attack flow chart is shown in Fig. 1.

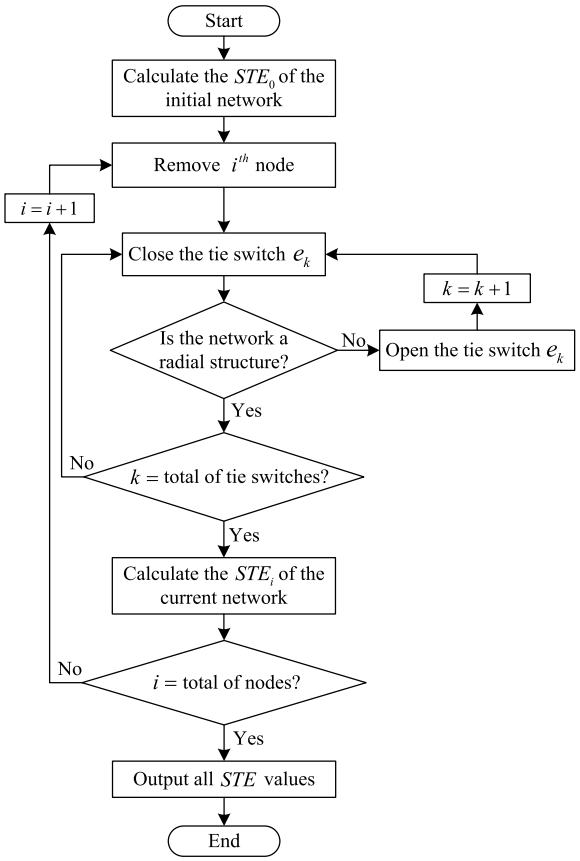

FIGURE 1. The flow chart of the node attack.

V. CASE STUDY AND RESULTS

In this work, the proposed comprehensive assessment method and attack strategy are tested on an IEEE 33-bus system, presented in Fig. 2. The system has five loops which the tie-branches are e34-e37.

A. NODE VULNERABILITY ANALYSIS

1) VULNERABLE NODE IDENTIFICATION

The IEEE 33-bus system is modeled as a weighted network in Python following the procedure in Section II. The line weights are impedance values. Based on the network model, the *ND* and *NE* values of each node are calculated according to equations (1), (2), (4), and (5). It can be seen from Fig. 2 that when nodes 1 and 2 are removed, adding tie switches cannot keep the network connected to the generator node 1. Therefore, nodes 1 and 2 are considered important and assigned the maximum value of *NE* in the calculation. The power flow model of this system is built in MATLAB. Based on the power flow model, the *NB* and *NP* values of each node are calculated according to equations (9) and (15). The calculated results are shown in Fig. 3 after normalization.

From Fig. 3, it can be observed that the *ND* and *NE* values of each node are quite different. For instance, the *ND* value of node 4 is 0.4723, while the *NE* value is 0.9878. The reason for this difference is that the *ND* index and the *NE* index identify the vulnerable nodes of the network topology from different perspectives. The *ND* index reflects the degree to which a node is close to the center of the network topology and the importance of its neighbor nodes. In Fig. 2, nodes 3 and 6 are the convergence centers of the branches in the network. When these nodes are attacked, it will cause great damage to the network structure. Therefore, the vulnerability values of nodes 6 and 3 obtained by the *ND* index are 1.0 and 0.8917, respectively. The *NE* index identifies vulnerable nodes by describing the degree of damage to the network topology after removing a node. In Fig. 2, nodes 3, 4, 5, and 6 are located at the key positions of power transmission in the system. When these nodes are attacked, the network efficiency of the system will drop significantly. Therefore, the vulnerability values of nodes 3, 4, 5, and 6 obtained through the *NE* index are 0.9397, 0.9878, 0.8916, and 1.0, respectively.

In Fig. 3, the calculation results of the *NP* and *NB* indices of each node in the system are similar. The reason for this phenomenon is that both *NP* and *NB* indices describe the role of nodes in transmitting energy in the system. When the active power passing through a certain node is greater, the vulnerability of the node calculated by *NP* and *NB* indices is greater, such as nodes 1, 2, 3, 4, 5, and 6.

To distinguish the importance of each index in the vulnerability assessment, a comprehensive weight is established to weight the indices from a subjective and objective perspective. Calculate the subjective weight of each index through AHP according to the steps in Section III. According to the definition of each index in Section II, we believe that

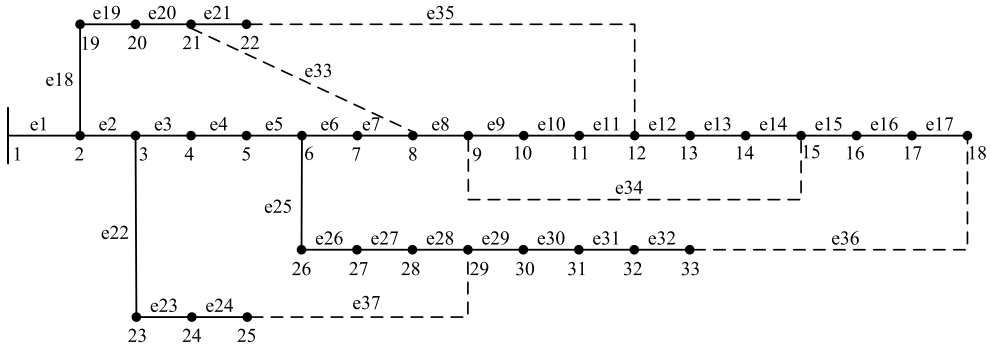

FIGURE 2. IEEE 33-bus system topology.

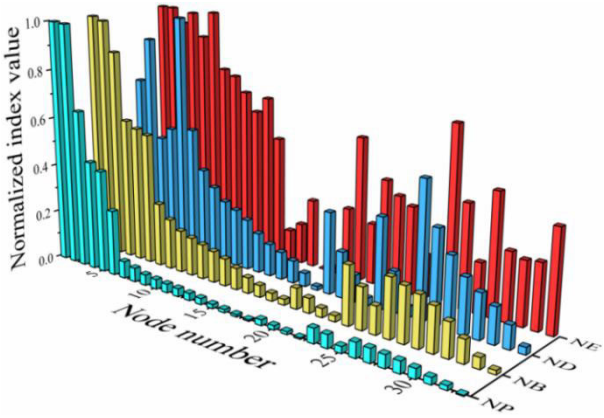

FIGURE 3. Calculation results of node vulnerability indices.

TABLE 2. The comparison matrix of node indices.

Indexes	ND_i	NE_i	NB_i	NP_i
ND_i	$e^{0/5}$	$e^{0/5}$	$e^{-1/5}$	$e^{1/5}$
NE_i	$e^{0/5}$	$e^{0/5}$	$e^{-1/5}$	$e^{1/5}$
NB_i	$e^{1/5}$	$e^{1/5}$	$e^{0/5}$	$e^{2/5}$
NP_i	$e^{-1/5}$	$e^{-1/5}$	$e^{-2/5}$	$e^{0/5}$

the *NB* index is the most important, followed by the *ND* and *NE* indices, and the *NP* index is the least important. Based on the above judgments and the assignment rules in Table 1, the comparison matrix is constructed as shown in Table 2.

The subjective weight is calculated according to the comparison matrix. According to the calculation results of each index in Fig. 3 and equations (25) and (26), the objective weights are calculated. According to the equation (27), the comprehensive weight results of each index are obtained by combining the subjective and objective weights, as shown in Table 3.

The calculation results and weight information of each index are substituted into the TOPSIS method. Then, the comprehensive vulnerability of each node in the system is calculated following the steps in Section III, as shown in Fig. 4.

The top ten nodes are 2, 3, 1, 6, 4, 5, 7, 26, 8, and 9. In Fig. 4, it is worth noting that the vulnerability values of

TABLE 3. Weight results of each node index.

Indexes	ND_i	NE_i	NB_i	NP_i
Subjective weight	0.2475	0.2475	0.3023	0.2026
Objective weight	0.1625	0.0891	0.2549	0.4935
Comprehensive weight	0.2127	0.1575	0.2944	0.3354

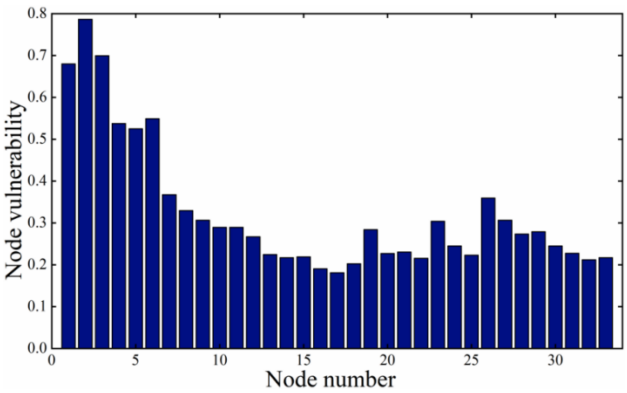

FIGURE 4. Calculation results of node comprehensive vulnerability.

nodes 1, 2, 3, 4, 5, and 6 are much larger than other nodes. From Fig. 2, it can be observed that node 1 is a generator node. Moreover, nodes 2, 3, 4, 5, and 6 are located at key positions where the generator node transmits active power to other nodes. The results show that the vulnerable nodes identified by the proposed method are in line with the actual situation.

2) NODE ATTACK ANALYSIS

To justify the effectiveness of the proposed method, the former methods such as single-index methods, and methods in [7] and [31] are compared to our method. The results are shown in Table 4.

As seen in Table 4, the ranking results of node vulnerability obtained by each single index are not the same. Every single index only evaluates the vulnerable nodes in the DN from a specific aspect. The results obtained by this assessment method have limitations. The proposed method takes into account the complementarity among the indices,

TABLE 4. Comparison of node vulnerability ranking by different methods.

Rank	Single index				[7]	[31]	Method in this paper	
	ND_i	NE_i	NB_i	NP_i	node	node	node	vulnerability
1	6	1	1	1	1	2	2	0.783
2	3	2	2	2	2	1	3	0.701
3	2	6	3	3	3	3	1	0.670
4	26	4	4	4	4	4	6	0.556
5	7	3	5	5	5	6	4	0.537
6	5	5	6	6	6	5	5	0.526
7	4	7	7	7	7	23	7	0.373
8	27	8	23	26	8	7	26	0.365
9	8	26	26	23	26	26	8	0.333
10	23	9	27	8	9	24	27	0.310

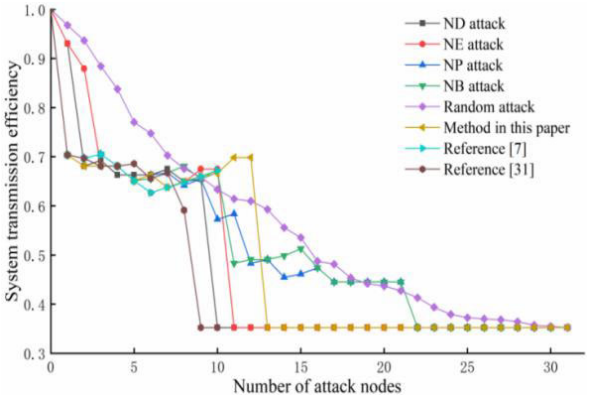

FIGURE 5. Node attack results under different methods.

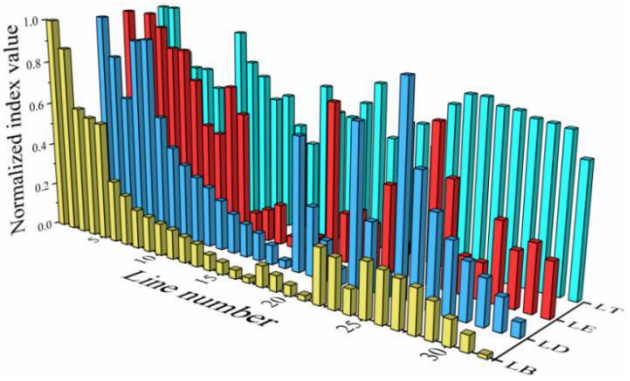

FIGURE 6. Calculation results of line vulnerability indices.

and the results obtained are more convincing. In addition, the assessment results obtained by the proposed method are in good agreement with the results of references [7] and [31]. The results obtained by the three methods show that high-vulnerability nodes are 1, 2, 3, 4, 5, 6, 7, and 26 respectively. It proves that the comprehensive multi-index TOPSIS method can reliably assess the vulnerability of the system.

To justify the superiority of the proposed method, the attack strategy proposed in Section IV is tested on the IEEE 33-bus system. From Fig. 2, once nodes 1 or 2 are attacked, other nodes will not be able to connect to the generator node again by closing the tie switch. Therefore, the protection level of nodes 1 and 2 is extremely high and they will not be removed during the attack on the system. Two attack models of random attack and deliberate attack are established in MATLAB. The deliberate attack results include the results obtained with four single indices, the TOPSIS method, and references [7] and [31]. According to different attack methods, the change curve of the system transmission efficiency index is shown in Fig. 5. The data of the first ten attacks are shown in Table 5.

Compared with the random attack, Fig. 5 shows that deliberate attacks make the transmission efficiency of the system significantly lower under the first three attacks. Among them, the NE attack, the proposed method, reference [31] reduces the system efficiency by 31.93%, the ND attack reduces the system efficiency by 30.74%, the NB attack, the NP attack, reference [7] reduces the system efficiency by 29.48%, random attack reduces the system efficiency by 11.57%. It indicates that the damaging effects of attacks on high-vulnerability nodes in the system are much higher than those of ordinary nodes.

In Table 5, the 4th to 7th deliberate attacks only slightly reduce the transmission efficiency of the system. Among them, reference [7] makes the system efficiency decrease the most, which is 6.76%. The distribution system was compromised into a more sparse network after the first three attacks. Some high-vulnerability nodes became unimportant nodes. For this reason, subsequent attacks only cause minor damage to the system. In Fig. 5, according to reference [31], ND attack, NE attack and the proposed method, the transmission efficiency of the system drops sharply after the 9th, 10th, 11th and 13th deliberate attacks respectively. After the first eight attacks, the five tie switches of the IEEE 33-bus system have all been closed. Once the subsequent attack is close to the power node, there will be no tie switch to reconnect the disconnected part. At this point, massive loads will exit the system.

According to Table 5, the proposed method reduces the system efficiency by 29.66% after the first attack, which

TABLE 5. Comparison of the first ten node attack results of different attack methods.

Number of attacks	STE drop ratio/%							
	ND attack	NE attack	NP attack	NB attack	Random attack	Proposed method	Reference [7]	Reference [31]
1	6.93	6.93	29.65	29.65	3.21	29.65	29.65	29.65
2	31.93	12.08	30.32	30.32	6.33	31.93	30.32	30.32
3	30.74	31.93	29.48	29.48	11.57	31.93	29.48	31.93
4	33.70	31.93	31.93	31.93	16.22	31.93	31.93	31.93
5	33.70	34.88	34.88	34.88	22.97	34.88	34.88	31.42
6	33.70	37.33	33.70	34.46	25.25	33.70	37.33	34.46
7	32.52	36.23	33.28	33.28	29.73	36.23	36.23	33.28
8	35.05	35.22	35.81	31.93	32.43	35.05	35.22	40.88
9	34.54	32.52	34.54	34.54	34.12	33.95	33.95	64.78
10	64.78	32.52	42.74	33.19	36.66	33.36	32.77	64.78

TABLE 6. The comparison matrix of line indices.

Indexes	LD_l	LE_l	LB_l	LT_l
LD_l	$e^{0/5}$	$e^{0/5}$	$e^{1/5}$	$e^{-1/5}$
LE_l	$e^{0/5}$	$e^{0/5}$	$e^{1/5}$	$e^{-1/5}$
LB_l	$e^{-1/5}$	$e^{-1/5}$	$e^{0/5}$	$e^{-2/5}$
LT_l	$e^{1/5}$	$e^{1/5}$	$e^{2/5}$	$e^{0/5}$

TABLE 7. Weight results of each line index.

Indexes	LD_l	LE_l	LB_l	LT_l
Subjective weight	0.2475	0.2475	0.2026	0.3023
Objective weight	0.2614	0.2199	0.4111	0.1077
Comprehensive weight	0.2659	0.2438	0.3017	0.1886

is higher than 6.93% of the ND attack and the NE attack. After the second attack, the proposed method reduces the system efficiency by 31.93%, which is higher than 6.93% of the NE attack and 30.32% of references [7] and [31]. It turns out that the multi-index TOPSIS method is superior to the single-index method and the methods proposed in [7] and [31].

B. LINE VULNERABILITY ANALYSIS

1) VULNERABLE LINE IDENTIFICATION

Similar to the process of calculating the vulnerability index results of each node in Section V. Based on the weighted network model, the *LD* and *LE* values of each line are calculated according to equations (3) and (6). In Fig. 2, e1 is the only line connected to the generator node in the system. Once the line e1 is disconnected, the generator node cannot be connected to the system by closing the tie switch. Therefore, when calculating the *LE* value of line e1, the maximum *LE* value of other lines will be assigned to e1. Based on the power flow model, the *LB* and *LT* values of each line are calculated according to equations (7)-(8) and (11)-(14). Similarly, when calculating the *LT* value of line e1, the maximum *LT* value among other lines will be assigned to e1. The calculated results are shown in Fig. 6 after normalization.

From Fig. 3 and Fig. 6, there is a corresponding relationship between the calculation results of the *ND* value and the *LD* value. For instance, the *ND* value of nodes 6 and 26 are large, and the *LD* value of line e25 connecting nodes 6 and 26 is also large, which is 0.9331. Similarly, there is a corresponding relationship between the calculation results of the *LB* value and the *NB* value. The lines e1, e2, e3, e4, and e5 connecting nodes 1, 2, 3, 4, 5, and 6 are the top five lines in the *LB* index. The above analysis shows that the results in Fig. 3 and Fig. 6 are consistent with the definitions of these four indices in Section II. Both the *LE* index and the *LT* index calculate the vulnerability of the line by describing the state change of the system after a line is disconnected. In Fig. 2, when lines e2, e3, e4, and e5 are disconnected, the tie switch needs to be closed to connect e33 to the network. At this time, the distance between each node in the network will become larger. The network efficiency will also decrease accordingly. Therefore, lines e2, e3, e4, and e5 have larger *LT* values, which are 0.8612, 1.0, 0.9401, and 0.8460, respectively. The power flow fluctuation of the system caused by disconnecting a line is small, so the difference of *LE* value of each line is small. Among them, the lines with larger *LT* values are e2 and e8, which are 1.0 and 0.9169 respectively.

According to the definition of each index in Section II, we believe that the *LT* index is the most important, followed by the *LD* and *LE* indices, and the *LB* index is the least important. Based on the above judgments, the comparison matrix is constructed as shown in Table 6.

The subjective weight is calculated according to the comparison matrix. The objective weights are calculated based on the calculation results in Fig. 6. The comprehensive weight results of each index are obtained by combining the subjective and objective weights, as shown in Table 7.

TABLE 8. Comparison of line vulnerability ranking by different methods.

Rank	Single index				[31]	[39]	Method in this paper	
	LD_l	LE_l	LB_l	LT_l	line	line	line	vulnerability
1	e2	e1	e1	e1	e5	e2	e2	0.772
2	e25	e3	e2	e2	e3	e5	e1	0.694
3	e6	e4	e3	e8	e1	e3	e3	0.657
4	e5	e2	e4	e25	e4	e1	e5	0.634
5	e3	e5	e5	e26	e25	e4	e4	0.608
6	e22	e6	e6	e3	e27	e27	e6	0.548
7	e4	e18	e22	e9	e26	e7	e25	0.530
8	e18	e25	e25	e19	e22	e6	e7	0.453
9	e26	e7	e7	e27	e8	e8	e22	0.450
10	e7	e10	e26	e28	e9	e9	e26	0.437

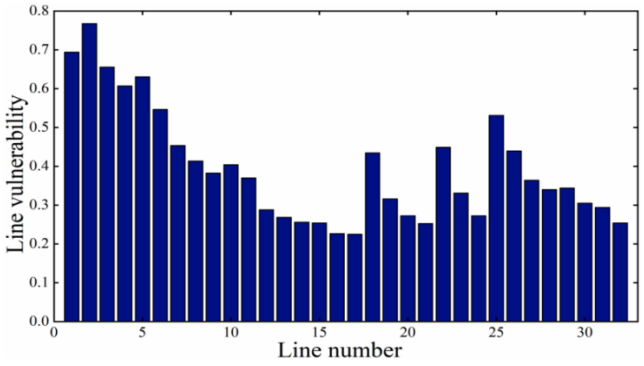

FIGURE 7. Calculation results of line comprehensive vulnerability.

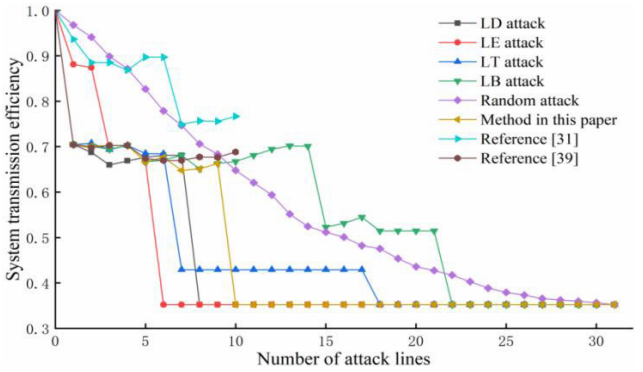

FIGURE 8. Line attack results under different methods.

The calculation results and weight information of each index are substituted into the TOPSIS method. Then, the comprehensive vulnerability of each line in the system is calculated following the steps in Section III, as shown in Fig. 7.

In Fig. 7, the top ten lines are e2, e1, e2, e5, e4, e6, e25, e7, e22, and e26. From Fig. 7, the vulnerability values of lines e1, e2, e3, e4, and e5 are much larger than other lines. In Fig. 2, the lines e1, e2, e3, e4, and e5 are located at key positions where the generator node transmits energy to other nodes. Therefore, the vulnerable lines identified by the proposed method are in line with the actual situation.

2) LINE ATTACK ANALYSIS

To illustrate the effectiveness of the proposed method, the former methods such as single-index methods, and methods in [31] and [39] are compared to our method. The results are shown in Table 8.

As seen in Table 8, the ranking results of line vulnerability obtained by each single index are not the same. In Table 8, every single index describes the vulnerability of each line in the system from a certain perspective. The proposed method combines all indices to identify vulnerable lines in the system. Moreover, the evaluation results obtained by the proposed method are in good agreement with the results of references [31] and [39]. The results obtained by the three methods show that high-vulnerability lines are e1, e2, e3, e4, e7, and e26, respectively. It proves that the results of the proposed method can identify effectively vulnerable lines.

To illustrate the superiority of the proposed method, two attack models of random attack and deliberate attack are established in MATLAB. Fig. 8 shows the deliberate attack results including the results obtained with four single indices, the TOPSIS method, and references [31] and [39]. From Fig. 2, once line e1 is attacked, the generator node cannot be connected to the system again by closing the tie switch. Therefore, the protection level of line e1 is extremely high and it will not be removed during the attack on the system. The data of the first ten attacks are shown in Table 9.

Compared with random attacks, Fig. 8 shows that deliberate attacks cause greater damage to the system except for reference [31] under the first five attacks. Among them, the LE attack, the LB attack, the proposed method reduces the system efficiency by 33.36%, reference [39] reduces the system efficiency by 32.6%, the LD attack reduces the system efficiency by 32.35%, the LT attack reduces the system efficiency by 31.50%, the reference [31] reduces the system efficiency by 10.3%, random attack reduces the system efficiency by 17.31%. According to Table 9, the proposed method reduces the system efficiency by 29.56% after the first attack, which is higher than 11.91% of the LE attack and 6.33% of the reference [31]. After the second attack, the proposed method

TABLE 9. Comparison of the first ten line attack results of different attack methods.

Number of attacks	STE drop ratio/%							
	LD attack	LE attack	LT attack	LB attack	Random attack	Proposed method	Reference [31]	Reference [39]
1	29.56	11.91	29.56	29.56	3.21	29.56	6.33	29.56
2	31.25	12.58	29.22	29.90	5.91	29.90	11.49	30.24
3	34.04	30.57	30.66	30.57	10.14	29.73	11.49	29.73
4	33.11	29.73	29.73	29.73	12.84	29.73	13.18	29.73
5	32.35	33.36	31.50	33.36	17.31	33.36	10.30	32.60
6	31.93	64.78	31.59	32.94	22.13	32.35	10.30	33.02
7	31.93	64.78	57.10	31.93	25.34	35.22	25.08	33.02
8	64.78	64.78	57.10	34.88	29.39	34.88	24.32	32.26
9	64.78	64.78	57.10	33.70	31.67	33.70	24.41	32.35
10	64.78	64.78	57.10	33.28	35.22	64.78	23.31	31.17

reduces the system efficiency by 29.9%, which is higher than 12.58% of the LE attack and 11.48% of the reference [31]. Thus, the proposed method is superior to the single-index method and the methods proposed in [31] and [39].

VI. CONCLUSION

In this paper, a successful vulnerability assessment method of DN integrating multiple indices considering topological structure and operation state has been presented. The proposed assessment method provides a new idea for operators to identify vulnerable nodes and lines.

1) The proposed evaluation indices not only consider the structure and state characteristics of the DN, but also analyze the impact on the system after the removal of nodes or lines. The case study demonstrates that these indices can identify the key nodes and lines of the DN. Moreover, the nodes and lines that have a greater impact on the system after being attacked can be determined.

2) Compared with other assessment methods, the TOPSIS method based on comprehensive weight adjustment reflects the effective information contained in the objective data and the difference in the contribution of each indicator based on actual operating experience.

3) The proposed attack model considering the characteristics of the closed-loop design and open-loop operation of the DN is presented. The attack results on the IEEE 33-bus system demonstrate that the network transmission efficiency drops the most after attacking five times by the proposed method.

With the development of the smart grid and the access to distributed generation, the scale of DN is gradually increasing and its electrical characteristics are becoming more complex. The DN model with distributed generation and defining the corresponding node and line vulnerability assessment indices will be the focus of follow-up research.

ACKNOWLEDGMENT

The authors would like to acknowledge the 2023 8th Asia Conference on Power and Electrical Engineering where the main idea of this was presented.

REFERENCES

[1] T. Fu, D. Wang, X. Fan, and Q. Huang, "Component importance and interdependence analysis for transmission, distribution and communication systems," *CSEE J. Power Energy Syst.*, vol. 8, no. 2, pp. 488–498, Mar. 2022.

[2] I. T. Papaioannou, A. Purvins, and E. Tzimas, "Demand shifting analysis at high penetration of distributed generation in low voltage grids," *Int. J. Electr. Power Energy Syst.*, vol. 44, no. 1, pp. 540–546, Jan. 2013.

[3] J. Goop, M. Odenberger, and F. Johnsson, "Distributed solar and wind power—Impact on distribution losses," *Energy*, vol. 112, pp. 273–284, Oct. 2016.

[4] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *Int. J. Bifurcation Chaos*, vol. 17, no. 7, pp. 2465–2475, Jul. 2007.

[5] B. A. Carreras, D. E. Newman, and I. Dobson, "North American blackout time series statistics and implications for blackout risk," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4406–4414, Nov. 2016.

[6] V. Rampurkar, P. Pentayya, H. A. Mangalvedekar, and F. Kazi, "Cascading failure analysis for Indian power grid," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1951–1960, Jul. 2016.

[7] J. M. Zhang, C. B. Li, M. F. Peng, and Z. W. Peng, "Vulnerable links analysis based on integrated active power betweenness in active distribution network," *Power Syst. Protect. Control.*, vol. 46, no. 18, pp. 41–48, Sep. 2018.

[8] M. Saleh, E. Yusef, and M. Ahmed, "Applications of complex network analysis in electric power systems," *Energies*, vol. 11, no. 6, p. 1381, May 2018.

[9] D. Bose, C. K. Chanda, and A. Chakrabarti, "Vulnerability assessment of a power transmission network employing complex network theory in a resilience framework," *Microsyst. Technol.*, vol. 26, no. 8, pp. 2443–2451, Feb. 2020.

[10] F. Wenli, L. Zhigang, H. Ping, and M. Shengwei, "Cascading failure model in power grids using the complex network theory," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 15, pp. 3940–3949, Nov. 2016.

[11] J. Wu, Z. Chen, Y. Zhang, Y. Xia, and X. Chen, "Sequential recovery of complex networks suffering from cascading failure blackouts," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2997–3007, Oct. 2020.

[12] L. Luo, B. Han, and M. Rosas-Casals, "Network hierarchy evolution and system vulnerability in power grids," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2721–2728, Sep. 2018.

[13] X. Wei, S. Gao, T. Huang, T. Wang, and T. Zang, "Electrical network operational vulnerability evaluation based on small-world and scale-free properties," *IEEE Access*, vol. 7, pp. 181072–181082, 2019.

[14] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Anal.*, vol. 26, no. 4, pp. 955–969, Aug. 2006.

[15] A. Shahpari, M. Khansari, and A. Moeini, "Vulnerability analysis of power grid with the network science approach based on actual grid characteristics: A case study in Iran," *Phys. A, Statist. Mech. Appl.*, vol. 513, pp. 14–21, Jan. 2019.

[16] P. Panigrahi and S. Maity, "Structural vulnerability analysis in small-world power grid networks based on weighted topological model," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 7, pp. 1–18, Jul. 2020.
[17] Y.-J. Zhang, Z.-J. Kang, X.-L. Guo, and Z.-M. Lu, "The structural vulnerability analysis of power grids based on overall information centrality," *IEICE Trans. Inf. Syst.*, vol. E99.D, no. 3, pp. 769–772, 2016.
[18] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012.
[19] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 81–88, Feb. 2013.
[20] H. Bai and S. Miao, "Hybrid flow betweenness approach for identification of vulnerable line in power system," *IET Gener., Transmiss. Distrib.*, vol. 9, no. 12, pp. 1324–1331, Sep. 2015.
[21] P. D. H. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 958–967, Mar. 2017.
[22] X. Wei, S. Gao, T. Huang, E. Bompard, R. Pi, and T. Wang, "Complex network-based cascading faults graph for the analysis of transmission network vulnerability," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1265–1276, Mar. 2019.
[23] T. Zang, S. Gao, T. Huang, X. Wei, and T. Wang, "Complex network-based transmission network vulnerability assessment using adjacent graphs," *IEEE Syst. J.*, vol. 14, no. 1, pp. 572–581, Mar. 2020.
[24] X. Zhan, T. Xiang, and H. Chen, "The application of weighted entropy theory in vulnerability assessment and on-line reconfiguration implementation of microgrids," *Entropy*, vol. 16, no. 2, pp. 1070–1088, Feb. 2014.
[25] A. M. L. da Silva, J. L. Jardim, L. R. de Lima, and Z. S. Machado, "A method for ranking critical nodes in power networks including load uncertainties," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1341–1349, Mar. 2016.
[26] N. Liu, X. Hu, L. Ma, and X. Yu, "Vulnerability assessment for coupled network consisting of power grid and EV traffic network," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 589–598, Jan. 2022.
[27] B. H. Xie, X. G. Tian, L. L. Kong, and W. M. Chen, "The vulnerability of the power grid structure: A system analysis based on complex network theory," *Sensors*, vol. 21, no. 21, p. 7097, Oct. 2021.
[28] L. Luo, G. A. Pagani, and M. Rosas-Casals, "Spatial and performance optimality in power distribution networks," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2557–2565, Sep. 2018.
[29] S. Wang, X. Y. Xu, X. R. Kong, and Z. Yan, "Multi-stage optimal PMU configuration in distribution network considering bus vulnerability," *Proc. CSU-EPSA*, vol. 31, no. 7, pp. 8–14, Jul. 2019.
[30] S. X. Sun, X. M. Li, F. B. Zhang, W. C. Shi, and C. C. Hao, "Identification of vulnerable lines in the distribution network based on network structure importance and potential hazard vulnerability," *Power Syst. Protect. Control*, vol. 46, no. 14, pp. 107–113, Jul. 2018.
[31] 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," *Proc. CSU-EPSA*, vol. 30, no. 12, pp. 125–131, Dec. 2018.
[32] S. Lin and J. Wen, "A comprehensive assessment method of distribution network vulnerability considering topological structure and operation status," in *Proc. Asia Conf. Power Electr. Eng. (ACPEE)*, May 2023, pp. 1–6.
[33] S. S. Bai, Y. K. Zhang, L. J. Li, N. Shan, and X. Y. Chen, "Effective link prediction in multiplex networks: A TOPSIS method," *Expert Syst. Appl.*, vol. 177, pp. 1–16, Sep. 2021.
[34] Z. X. Wang, S. H. Miao, S. Y. Guo, J. Han, H. R. Yin, and W. D. Mao, "Node vulnerability evaluation of distribution network considering randomness characteristic of distributed generation output," *Electr. Power Automat. Equip.*, vol. 41, no. 8, pp. 33–40, Aug. 2021.
[35] 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," *Phys. A, Stat. Mech. Appl.*, vol. 390, nos. 23–24, pp. 4692–4701, Nov. 2011.
[36] Y. Xu and J. Zhi, "Identification of key nodes in power grid based on improved node electric betweenness," *Proc. CSU-EPSA*, vol. 29, no. 9, pp. 107–113, Sep. 2017.
[37] Y. Xu, X. S. Lei, B. Qin, H. Yang, K. Luo, and L. Liu, "Method based on comprehensive importance for critical line identification in a power grid," *Electr. Power Construct.*, vol. 40, no. 7, pp. 85–90, Jul. 2019.
[38] C. C. Ji, P. Yu, and W. J. Li, "Comprehensive vulnerability assessment and optimisation method of power communication network," *Int. J. Embedded Syst.*, vol. 11, no. 3, pp. 315–324, 2019.
[39] X. L. Wang, C. C. Hao, X. M. Li, S. X. Sun, and W. C. Shi, "The vulnerability analysis of distribution network with distributed generation," *Electr. Meas. Instrum.*, vol. 16, no. 6, pp. 38–43, Mar. 2019.

JUAN WEN received the B.Eng. degree in electrical engineering, the M.Eng. degree in electrical theory and new technology, and the Ph.D. degree in electrical engineering from Hunan University, Changsha, China, in 2007, 2010, and 2018, respectively. Since 2018, she has been with the School of Electrical Engineering, University of South China, where she is currently a Lecturer. Her research interests include power system operation analysis and power network modeling.

SIYU LIN received the B.Eng. degree in electrical engineering and automation from the University of South China, Hengyang, China, in 2021, where he is currently pursuing the M.Eng. degree in electronic information. His research interest includes vulnerability analysis of distribution networks.

XING QU received the B.Eng. degree in electrical engineering from the University of South China, Hengyang, the M.Eng. degree in electronic science and technology from the Guilin University of Electronic Technology, Guilin, and the Ph.D. degree in electrical engineering from Hunan University, Changsha, China. Since 2018, he has been with the School of Electrical Engineering, University of South China, where he is currently a Lecturer. His research interest includes power system load modeling.

QIANKANG XIAO received the B.Eng. degree in automation from the University of South China, Hengyang, China, in 2019, where he is currently pursuing the M.Eng. degree in electronic information. His research interest includes power system fault diagnosis.