Identification of two vulnerability features: A new framework for electrical networks based on the load redistribution mechanism of complex networks

Hindawi
Complexity
Volume 2019, Article ID 3531209, 14 pages
https://doi.org/10.1155/2019/3531209

Research Article

Identification of Two Vulnerability Features: A New Framework for Electrical Networks Based on the Load Redistribution Mechanism of Complex Networks

Xiaoguang Wei,[1] Shibin Gao,[1] Tao Huang,[2] Tao Wang,[3] and Wenli Fan[1]

[1]*School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China*
[2]*Department of Energy, Politecnico di Torino, Torino 10129, Italy*
[3]*School of Electrical Engineering and Electronic Information, Xihua University, Chengdu 610039, China*

Correspondence should be addressed to Shibin Gao; 1514754029@qq.com and Tao Huang; tao.huang@polito.it

Received 24 September 2018; Accepted 25 October 2018; Published 16 January 2019

Guest Editor: Seyedmohsen Hosseini

This paper proposes a new framework to analyze two vulnerability features, impactability and susceptibility, in electrical networks under deliberate attacks based on complex network theory: these two features are overlooked but vital in vulnerability analyses. To analyze these features, metrics are proposed based on correlation graphs constructed via critical paths, which replace the original physical network. Moreover, we analyze the relationship between the proposed metrics according to degree from the perspective of load redistribution mechanisms by adjusting parameters associated with the metrics, which can change the load redistribution rules. Finally, IEEE 118- and 300-bus systems and a realistic large-scale French grid are used to validate the effectiveness of the proposed metrics.

1. Introduction

Critical component identification is an important part of security analyses for electrical networks [1–3]. The main idea is to rank the weakness of the equipment in an electrical network via a set of metrics.

As an artificial network, electrical grids have topological similarities to other general networks. They also exhibit several typical features of complex networks, such as small-world properties [4–6]. Therefore, complex network theory (CNT) is a popular method to assess the vulnerability of electrical networks[3, 4, 7–13]. The construction of structural metrics is an important branch of vulnerability evaluations [14] based on CNT. CNT uses the connectivity information abstracted from the network to create indices based on statistics and, sometimes, physical features of the network are added to improve the effectiveness of the indices [10, 11].

However, there are still several problems with this method. Compared to general networks (or systems), an electrical network has its own characteristics that limit the wide application of CNT. First, analyzing the topological structures of electrical networks without considering their operational status does not disclose the real features of the systems [10, 11]. Secondly, in most general networks, when a vertex (or an edge) of a network fails, the direct neighbors are the first to be affected or have the largest impact based on CNT. However, this is not generally true for electrical networks [15]. Moreover, the structural metrics are static indices [12, 13, 16] that only consider the normal operational status of the network. To overcome the above problems, statistical graphs [17, 18] are employed to analyze the vulnerability or cascading failures of electrical networks. For example, [19, 20] proposed a sequential attack graph (SAG) to identify critical nodes while [21] proposed a correlation matrix. In addition, [22] proposed influence graphs to analyze cascading failures. Statistical graphs have also provided promising options for security, because they comprehensively consider the topological, physical, and operational characteristics of a system.

In addition, another problem in which features of vertices (edges)(For clarity, hereinafter the terms "network, branch and node" are used only for electric systems and "graph,

edge and vertex" only for complex networks.) in complex network vulnerability detection, especially in electrical networks, should be distinguished, is often overlooked. For example, some vertices can easily spread faults leading to a high probability of a network failure event. Conversely, some vertices are easily affected by propagated faults. Therefore, it is necessary to devise a method to identify these two features of vertices and to better reveal the vulnerabilities of networks.

In summary, our main contributions are as follows.

First, we propose a new framework that employs statistical graphs to represent the useful information for analyzing the network vulnerability from the original physical grid, using CNT, compared to a traditional framework that employs the original topological structure of the gird.

Secondly, inspired by [19–24], we propose a correlation graph (CG) generated via critical paths to analyze the electrical network vulnerability.

Thirdly, using benchmarks, we analyze the topological properties of the CGs based on CNT via the cumulative distributions of the vertex degrees. According to the analysis, the CGs are scale-free graphs, which verifies that electrical networks have scale-free properties under deliberate attacks, as opposed to traditional complex network methods, which verify the properties by correlating the drop in the network demand (or efficiency) with the attacked branches.

Finally, we define two vulnerability features from the perspective of CNT and then map the features onto electrical networks. Further, we employ the scale-free structures of the CGs to construct vulnerability metrics for the first time to differentiate the two features from the perspective of the load redistribution mechanism of CNT. The features of the metrics are explained in detail, including their relationship with the degree.

In addition, note that, even though dynamic models analyzed by real-time simulation platforms[25] are more comprehensive for security analyses in the real world, they require much longer simulation times and result in an immense computational burden, which makes it difficult to analyze a large-scale network. Meanwhile, as a media connecting equipment in the power system, the transmission network has notably fast dynamics/transients, compared to rotating devices. In other words, the transmission network *per se* can usually be considered to be a static component. Therefore, static models from the perspective of the load redistribution are widely employed to analyze the network vulnerability in existing literature [10–24]. Based on above, we focus on understanding the nature of the transmission network using static models by the load redistribution from the entire network.

2. Correlation Graph

We constructed a CG to incorporate both the structural features and the operational status of power systems, using critical paths from the point of view of *load redistribution mechanism* (LRM). The constructed graph considers both the topological structures and the operational features under fault operation of the system. For example, branches of an electrical network can be transformed into vertices in a new graph while edges are formed to reflect the adjacent relationships between branches.

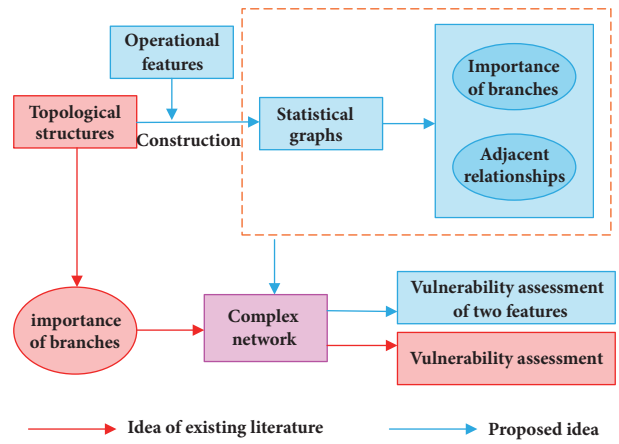

Figure 1: Comparison between proposed idea and existing literatures based on CNT.

2.1. Vulnerability Assessment: A New Framework. To overcome the limitations of structural vulnerability identification methods by applying CNT to the electrical network vulnerability assessment, we need to consider the following two aspects: (1) the importance of a vertex and (2) the adjacent relationships between vertices. To assess the importance of a vertex, there are many indices (e.g., degree and betweenness) that can be used to qualify it from the perspective of LRM. Comparatively, there are few indices for quantifying the importance of branches because it is difficult to assess edges under LRM. In addition, in most general networks, when a vertex (or an edge) of a network fails, the adjacent relationship between vertices usually imply that the immediate neighbors are the first to be affected or suffer the largest impact based on CNT. However, this is not generally true for electrical networks; sometimes, nonadjacent branches are the first to be affected due to the physical laws of electric circuits and the physical and operational constraints [15]. Therefore only using the information of the structure of an electrical network cannot effectively identify the critical branches.

In summary, it is spatially insufficient to analyze the network vulnerability using only the topological structures of the girds. Therefore, we propose a new framework that employs statistical graphs [19–24] to represent information useful for analyzing the network vulnerability from the original physical grid, using CNT, as shown in Figure 1. In the existing methods, the topological structures are employed to assess the electrical network vulnerability based on the CNT on the original physical networks. Its main idea is to focus on the importance of branches by constructing statistical metrics without the evolvement of the operational feature of the system. However, we construct statistical graphs comprehensively considering topological, physical and operational features of power systems, and further based on the constructed statistical graphs which can reveal not

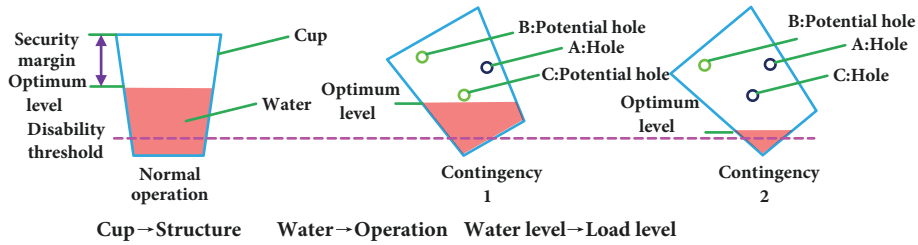

Figure 2: An example to explain the electrical vulnerability.

only importance of branches but also adjacent relationships among branches we assess the vulnerability with two features by replacing the original electrical networks.

2.2. Correlation Graph. Although many statistical graphs are proposed in references [19–21], there are still many limitations in the construction of statistical graphs to identify critical branches. In references [19, 20], a SAG was constructed by investigating different node combinations under sequential attacks. However, a SAG cannot be used to identify the critical branches of a large-scale electrical network because the different branch combinations will increase exponentially with increasing network scales. In reference [21], a correlation matrix was constructed under N-1, but an N-k contingency was not considered and the proposed method was not verified on a large-scale grid. Meanwhile, the above statistical graphs are only analyzed from the perspective of static statistical indices (e.g., degree).

Therefore, it is necessary to construct a new statistical graph to apply to the identification of vulnerable branches of large-scale networks under the N-k contingency and the corresponding properties should be analyzed in depth. To explain the rationale of the construction of a statistical graph, we use a cup of water as an example. The cup represents the topological structure of an electrical network and the water in the cup represents the operational status, as shown in Figure 2. Under normal operation, the system operator decides on an optimal/appropriate operational point, considering different constraints, including the necessary security margin. The optimal/appropriate point corresponds to a certain electric load level in the electrical network, represented by the water level in the cup. When a hole "A" in the cup is created, for example, by a contingency 1 due to structural damage, the optimal level for the water will change. Therefore "A" decides the optimal/appropriate water level, analogous to the electric load level, which can be viewed as the importance of the elements inside the contingency 1. Further, we assume that there are two potential holes, i.e., "B" and "C," which can only be revealed after contingency 1, and that "C" is more decisive for the appropriate water level than "B." This infers that the adjacent relationship "A"⟶"C" is more important than that of "A"⟶"B." Therefore, the adjacent relationship "A"⟶"C" and the properties of "C" decide the appropriate water level. Accordingly, "A"⟶"C" can be viewed as the adjacent relationship between two branches during fault propagation.

Note that, in every step, we only need to pick the most decisive "hole" in the cup, which is nearest to the optimal level of the water.

To trace the adjacent relationships between branches, we need to consider different combinations. Now, the computational burden becomes an issue. For example, if we consider the N-k criterion, for an electrical network with N_L branches, we need to calculate N^k contingencies. For a French grid with 2596 branches, we need to calculate 17.5 billion contingencies for N-3.

Therefore, to simplify the calculation, we constructed critical paths [17, 18] to trace the adjacent relationships. We employed a *Branch loading assessment index* (BLAI) introduced in our precious work [17, 18, 26] to select an attacked branch, having the largest impact on the electrical network, as the next contingency. In addition, a commonly used termination condition, i.e. the blackout size, was used to mark the end of the critical paths [20].

To select a branch, the BLAI is employed to reflect the loading burden and its possibility of failure under the current contingency from the perspective of the load redistribution. The index can be calculated as

$$\alpha_j = \frac{f_j^x - f_j^0}{f_j^M} \exp\left(\frac{f_j^x - f_j^M}{f_j^M}\right) \tag{1}$$

The *blackout size* is adopted to mark the end of the critical paths and is viewed as a measure of the gravity of a critical path. The blackout size is defined as

$$\delta_z^x = 1 - \frac{\sum_{d\in B_z} P_d^x}{\sum_{d\in B_z} P_d^{(x-1)}} \tag{2}$$

$$\Lambda = \sum_{x=1}^{N_S-1} \sum_{z=1}^{Z^x} \delta_z^x \tag{3}$$

and when $\Lambda \geq \Delta$, we terminate the process.

Based on the above-mentioned considerations, we employ the structural features and the operational status of the electrical network to construct a CG to reveal the adjacent relationships between the branches. Using the CG, the spatial association network between branches was translated into a CG. However, before introducing the CG, we define the vulnerability relationship to describe the relationship between the two branches.

Vulnerability Relationship. We denote two adjacent links on a critical path as having a vulnerability relationship.

Critical Path Generation Method. To explore the vulnerability relationship, we use the critical paths of a network to construct a CG. For a network with N branches, we treat every branch as a triggering fault. We can obtain N paths of a critical path. Note that some paths may contain only one vertex. DC-OPF (optimal power flow) is employed to optimize the operation status in different topological structures. The critical path is generated as follows.

Step 1. Input the electrical network information. Initialize $\mathsf{S} = \phi$ and Δ. Select a branch as a triggering fault.

Step 2. Remove the selected branch from the electrical network and add it to S.

Step 3 (island detection and partition). Calculate the DC power flow [27–29] of every island. Employ (1) to calculate α for every branch.

Step 4. Take (2) as the objective function. Calculate the minimum δ of every island using the DC-OPF algorithm [1, 28]. Employ (3) to calculate Λ.

Step 5. If $\Lambda \geq \Delta$, end the critical path generation process; otherwise select the branch whose α is the maximum of all the branches as the candidate branch under next contingency scenario and go to Step 2.

Step 6. Output S.

By above process, we can simply and quickly develop critical paths and efficiently reduce the computational burden.

CG Generation Method. To map a critical path $\mathsf{S}^i = \{L_1^{i\prime}, L_2^{i\prime}, \ldots, L_{N_S}^{i\prime}\}$ onto a graph G^i, let the branches in S^i be the vertices of G^i, i.e., $\mathsf{V}^i = \{v_j \mid v_j = L_j^{i\prime},\ j = 1, 2, \ldots, N_{N_S}^i\}$. Then the edges can be defined as $\mathsf{E}^i = \{e_q^i \mid e_q^i = L_j^{i\prime} L_{j+1}^{i\prime},\ j = 1, 2, \ldots, N_{N_S}^i - 1\}$. By merging corresponding N_L graphs, we can obtain the CG, i.e., $\mathsf{G} = \mathsf{G}^1 \cup \mathsf{G}^2 \cup \ldots \cup \mathsf{G}^{N_L}$. Finally the CG is represented as

$$\mathsf{G} = \left\{(\mathsf{V}, \mathsf{E}) \mid \mathsf{V} = \mathsf{V}^1 \cup \mathsf{V}^2 \cup \cdots \cup \mathsf{V}^{N_L}, \mathsf{E} = \mathsf{E}^1 \cup \mathsf{E}^2 \cup \cdots \cup \mathsf{E}^{N_S}\right\}. \tag{4}$$

Obviously, the CG is an undirected and unweighted graph.

CG Topological Features. To analyze the topological features of the CG, we employ four benchmark systems (described in Table 1). We set the threshold $\Delta = 20\%$ [20]. The CG of the IEEE 14-bus system, shown in Figure 3, manifests the adjacent vulnerability relationship between the branches. Using the CG, the spatial association network between the branches in the electrical network can be translated into a statistical graph.

The cumulative distributions of the vertex degree [29] $P(K > k) = \sum_{K>k} P(k)$ in CGs are all power laws whose r and R^2 are given in Table 2, except for the CG of the IEEE 14-bus system because its vertices are too few to allow statistical conclusions to be drawn. Table 2 indicates that CGs are scale-free graphs (i.e., $P(K > k) \sim x^{-r}$), which have high robustness under random vertex attacks, but low robustness under intentional attacks. In addition, we can employ the CGs to verify the scale-free properties of electrical networks under deliberate attack, and compared them to traditional complex network methods which verify the properties by correlating the drop in the network demand (or efficiency) to the attacked branches. Due to its scale-free features, its statistics of under faults operation and its vulnerability relationships between branches, we can indirectly assess the electrical network vulnerability using the CG.

Table 1: Description of test benchmarks.

Test benchmarks	N_B	N_W	N_L
IEEE 14-bus system	14	5	20
IEEE 118-bus system	118	54	186
IEEE 300-bus system	300	69	411
French Grid	1951	391	2596

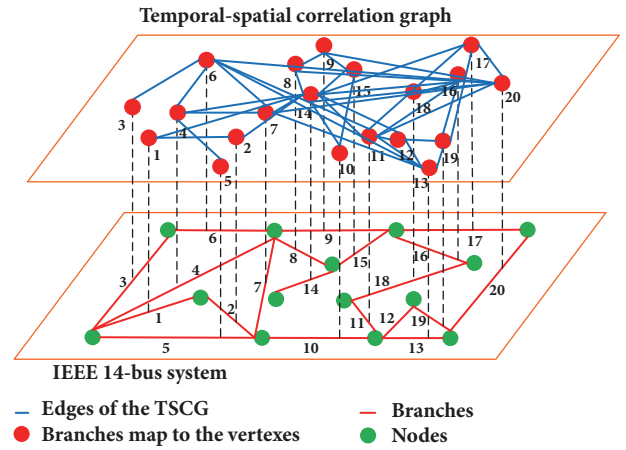

Figure 3: Mapping between IEEE 14-bus system and CG.

Table 2: Parameters r and R^2 of cumulative distributions of the vertex degree in three CGs. Generally, $R^2 \geq 80\%$ has a satisfactory fitting effect.

Test benchmarks	r	R^2
IEEE 14- bus system	0.8880	0.7254
IEEE 118-bus system	1.3023	0.9338
IEEE 300-bus system	1.3500	0.9166
French grid	1.2180	0.9497

3. CG Based Vulnerable Indices with Two Vulnerability Features Using CNT

In this section, we define the two vulnerability features. Then we propose CG based metrics to differentiate the two features to assess the electrical network vulnerability from the perspective of LRM. Before defining the two vulnerability

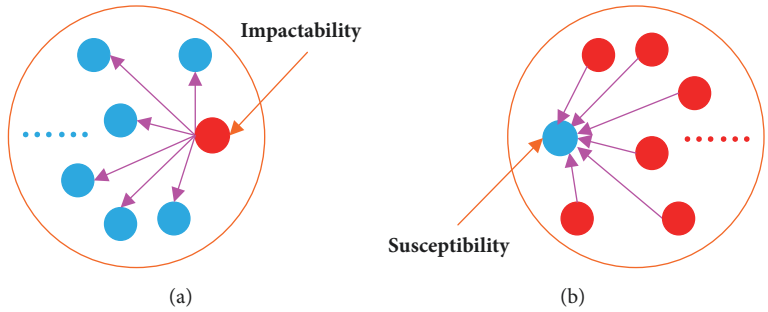

Figure 4: The diagram to explain impactability and susceptibility.

features, we briefly introduce the taxonomy from CNT used in this paper.

Flow is a tangible or intangible substance that exists in a specific network. For example, in physical networks, such as water networks, the water flow is the flow. In social networks, the flow is the communication between people.

Load is defined as the quantity of a flow that a vertex owns for a certain status of the network [30].

Load capacity is the maximum load that a vertex can withstand [31]. Once the load of a vertex is beyond the load capacity, the vertex is then in *overload*.

Load redistribution is the process where, when a vertex fails or is removed, its corresponding load needs to be reallocated or transferred to other vertices following certain rules. In particular, when the corresponding load is reallocated to the adjacent vertices that are directly connected to the fault vertex, the redistribution rule is called *neighbor distribution rule (NDR)*[32]; meanwhile when the load is reallocated to all the other vertices, the redistribution rule is called the *global distribution rule (GDR)* [31]. When the corresponding load is evenly reallocated to selected vertices, the redistribution rule is called a *uniformity distribution rule*.

In this paper, we analyze the vulnerability from the angle of LRM of CNT [33, 34]. That is, we assess the vulnerability of the network by the changes due to load redistributions when a vertex fails.

3.1. Two Vulnerability Features. At present, a popular vulnerability analysis is to identify the critical vertices (or edges) of an electrical network, which easily leads to a network failure event under deliberate attacks [1]. Such approaches only identify critical branches that can easily affect the network when they fail, as shown in Figure 4(a). However, they ignore the other feature of critical branches which are easily affected by faults of other branches, as shown in Figure 4(b). Therefore it is necessary to differentiate the two vulnerability features and we call *impactability* and *susceptibility*.

When a branch fails (is attacked), it causes obvious or serious changes in the original status of the network in one or more aspects, such as the topological structure and the function, and in such a case, the branch is called an *impactable vertex*.

When one or more network branches fail, if a branch is easily affected by the faults, leading to changes in the original status of this branch, such as the load increasing (even overload), branch failure, then the branch is called a *susceptible vertex*.

The impactability of a branch in an electrical network describes how the failure of that branch can cause a considerable load increase in other branches, leading to serious system changes. The susceptibility of a branch in an electrical network describes, when other branches fail, the branch, and how easily the branch is affected by a fault, leading to a severe load increase or failure.

The differentiation of these two features of branches has practical implications. First, it provides useful lists of critical branches corresponding to different operation states for power dispatchers to monitor. For example, under normal operation, dispatchers need to give priority to impactable branches because they can easily spread faults when they are attacked. Conversely, under fault operation, dispatchers should also pay attention to susceptible branches because they can easily be affected by other faults. Secondly, analyzing the impactability of branches provides suggestions to offenders about how to cause significantly large disturbances to a system and to defenders about how to protect the safe operation of a system at the lowest cost. By analyzing the susceptibility of branches, it can reduce or avoid further deterioration of the system under a deliberate attack. In summary, the differentiation of the two features can improve the management of system security.

3.2. Proposed Vulnerability Metrics with the Two Features. Previous studies of the load in LRM in complex networks have primarily focused on the load model (e.g., the initial load) and the load redistribution strategy. For example, the betweenness or degree is generally employed to define the initial load of a vertex [32, 33, 35–37]. Similarly, we employ the degree to define the load of a vertex because the degree can reflect its importance in the propagation process. For the load redistribution strategy, [33, 36] investigated NDR while [37] proposed stochastic probability redistribution models. However, the redistribution rule they proposed is not adjustable. References [32, 34] first considered the adjustable redistribution rules for the load. To define the vulnerability metrics by means of LRM, we adopted the adjustable load redistribution strategy to study LRM. Before defining the metrics, we introduce some new concepts based on CNT as follows.

The vulnerability flow is a virtual substance that reflects the vulnerability relationship between the branches. For example, we can define the flow that exists in the CG as the vulnerability flow. The vertices of the CG carry a certain proportion of the vulnerability flow called the *load*. The edges of the CG reveal the paths of transmitted load. When a branch of an electrical network fails, it causes changes in other branches in terms of their loads. If we map a contingency onto the CG, it describes the corresponding vertex failures, causing the reallocation of the load onto other vertices (i.e., load redistribution) via the edges.

Initial Load. In a CG, a higher degree vertex plays a more important role in the fault propagation process; therefore we employ the degree of the vertices to quantify the amount of the initial load [34]. The initial load of vertex v_j is expressed as

$$\rho_j = \frac{D_j^{\tau}}{\sum_{j=1}^{N_L} D_j^{\tau}} \tag{5}$$

Distance. In a CG, there may be more than one path between any two vertices. Therefore, to quantitatively depict the distance between any two vertices, we use the minimum path between them [32, 34] to quantify their vulnerability relationship.

In an electrical network, the failure of a branch will cause the redistribution of the initial power flow in the fault branch to other branches, leading to an increase in the transmitted power over other branches. Correspondingly, when we map a contingency onto the CG, the relevant fault vertex will lead to the redistribution of its initial load to other vertices. Therefore we use the increase in the vulnerability flow at other vertices to quantify the impact of the corresponding fault branch on the electrical network.

The load redistribution $\Delta\rho_{j\longrightarrow k}$ from vertex v_j to vertex v_k in the set of affected vertices Q_j ($v_k \in \mathrm{Q}_j$) is defined as

$$\Delta\rho_{j\longrightarrow k} = \begin{cases} \dfrac{l_{jk}^{-\lambda}}{\sum_{\gamma\in \mathrm{Q}_j} l_{j\gamma}^{-\lambda}}\rho_j, & k \in \mathrm{Q}_j \\ 0, & k \notin \mathrm{Q}_j \end{cases} \tag{6}$$

$$\mathrm{Q}_j = \left\{ k \left| \frac{l_{jk}^{-\lambda}}{\sum_{\gamma=1}^{N_L} l_{j\gamma}^{-\lambda}} > \eta,\ 0 < \eta \le \frac{1}{N_L - 1} \right. \right\} \tag{7}$$

Obviously, the load redistribution is proportion to the distance between v_j and v_k. λ controls the portion of the load that v_j reallocates to v_k, and η is used to define the set Q_j. Equation (6) reflects not only the importance of a vertex but also the vulnerability relationships between that vertex and others. We employ the parameters τ and λ to adjust the proportion between the *importance of a vertex* and its *vulnerability relationships*.

Impactability Metric (IM). To describe the impactability of a fault vertex v_j in a CG, we introduce the entropy

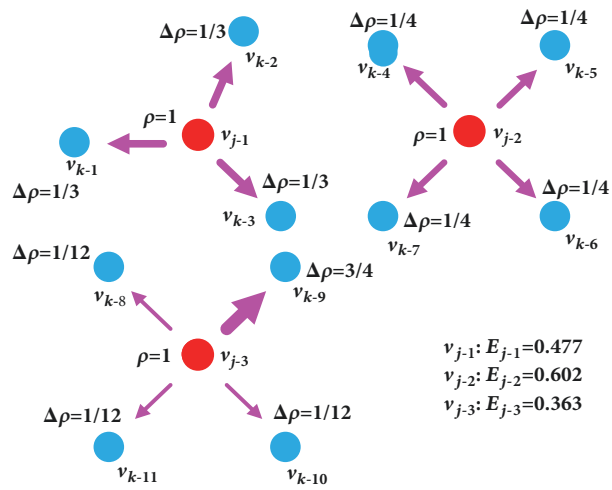

Figure 5: An example to understand (8).

expressed in the following to measure the load change in the graph.

$$E_j = -\sum_{k\in \mathrm{Q}_j} \Delta\rho_{j\longrightarrow k} \ln \Delta\rho_{j\longrightarrow k} \tag{8}$$

Eq. (8) considers the severity of the fault in terms of the affected number of vertices and measures the uniformity of the load redistribution. Further, E_j is larger for more severe faults and/or more even load redistributions between affected vertices. To illustrate the two aspects we mentioned for Equation (8), we use 3 vertexes depicted in Figure 5. Assuming under even load redistribution strategy, the E_{j-2} of v_{j-2} is greater than $E_{j-1}$of v_{j-1} solely because v_{j-2} affects more vertexes. In contrast, with the same number of affected vertexes, E_{j-2} of v_{j-2} is greater than E_{j-3} of v_{j-3} due to a more uniform load redistribution.

However, note that some vertices may exist whose entropy is greater than that of others, due to more even load redistributions between larger affected number of vertices, yet cause small load increases for other vertices, resulting in a small overall impact. To exclude these vertices, we further refine

$$IV_j = \frac{1}{N_Q} E_j = -\frac{1}{N_Q} \sum_{k\in \mathrm{Q}_j} \Delta\rho_{j\longrightarrow k} \ln \Delta\rho_{j\longrightarrow k} = -\frac{1}{N_Q} \cdot \sum_{k\in \mathrm{Q}_j} \frac{l_{jk}^{-\lambda}}{\sum_{r\in \mathrm{Q}} l_{j\gamma}^{-\lambda}} \left(\frac{D_j^{\tau}}{\sum_{j=1}^{N_L} D_j^{\tau}} \right) \cdot \ln \frac{l_{jk}^{-\lambda}}{\sum_{\gamma\in \mathrm{Q}_j} l_{j\gamma}^{-\lambda}} \left(\frac{D_j^{\tau}}{\sum_{j=1}^{N_L} D_j^{\tau}} \right) \tag{9}$$

We define $0 \ln 0 = 0$.

Susceptibility Metric (SM). To describe the susceptibility of an affected vertex v_k in a CG, we use the average incremental

load redistribution from all other fault vertices into that vertex:

$$SV_k = \frac{1}{\sum_{j=1}^{N_L} \sigma\left(\Delta\rho_{j\longrightarrow k}\right)} \sum_{j=1}^{N_L} \Delta\rho_{j\longrightarrow k} \quad \forall v_j \in \mathsf{G},\ j \neq k \tag{10}$$

$$\sigma\left(\Delta\rho_{j\longrightarrow k}\right) = \begin{cases} 1, & \Delta\rho_{j\longrightarrow k} > 0 \\ 0, & \Delta\rho_{j\longrightarrow k} \leq 0 \end{cases} \tag{11}$$

3.3. Load Redistribution Rules for IM and SM. In this subsection, we discuss two rules for the load redistribution: NDR and GDR which explore the relationship between the two metrics and the degree.

Neighborhood Distribution Rule. When $\lambda = +\infty$, the load redistribution rule is NDR.

(1) For IM, (9) is simplified as

$$IV_j = -\frac{{D_j}^{\tau-1}}{\sum_{j=1}^{N_L} {D_j}^{\tau}} \ln \frac{{D_j}^{\tau-1}}{\sum_{j=1}^{N_L} {D_j}^{\tau}} \tag{12}$$

When $0 < \tau < 1$, IV_j is inversely proportional to D_j. When $\tau = 1$, IV_j is constant, i.e., $IV_1 = IV_2 = \cdots = IV_{N_L}$. Clearly, IV_j is invalid in terms of identifying the impactability for IM under NDR. When $\tau > 1$, IV_j is proportional to D_j.

(2) For SM, (10) is simplified as

$$SV_k = \frac{1}{D_k} \sum_{j=1}^{D_k} \frac{{D_j}^{\tau-1}}{\sum_{j=1}^{N_L} {D_j}^{\tau}} \tag{13}$$

When $\tau = 1$, SV_k is a constant and $SV_1 = SV_2 = \cdots = SV_{N_L}$. When $\tau \neq 1$, SV_k is determined by D_j and D_k. If for two existing vertices $D_{k1} = D_{k2}$ and $\sum_{j=1}^{D_{k1}} D_j^{\tau-1} > \sum_{j=1}^{D_{k2}} D_j^{\tau-1}$, then $SV_{k1} > SV_{k2}$. This indicates that a vertex is more susceptible to its high vertex degree neighbors.

Global Distribution Rule. When $\lambda = 0$, then the load redistribution rule is the GDR.

(1) For IM, (9) is simplified as

$$IV_j = -\frac{1}{N_L - 1}\left(\frac{{D_j}^{\tau}}{\sum_{j=1}^{N_L} {D_j}^{\tau}}\right) \ln \frac{1}{N_L - 1}\left(\frac{{D_j}^{\tau}}{\sum_{j=1}^{N_L} {D_j}^{\tau}}\right) \tag{14}$$

(2) For SM, (10) is simplified as

$$SV_k = \frac{1}{\left(N_L - 1\right)^2}\left(1 - \frac{{D_k}^{\tau}}{\sum_{j=1}^{N_L} {D_j}^{\tau}}\right) \tag{15}$$

Equations (14) and (15) show that IV_j is proportional to the degree D_j, while SV_k is inversely proportional to the degree D_k.

The analysis shows that when τ has different values; the impactability and susceptibility of the branches are different under the same redistribution rule. In addition, one can infer that compared with all other topologies, the central vertex in a star graph has the largest impactability and susceptibility (refer to the proof in the appendix).

4. Simulation and Analysis

The simulations were performed for the IEEE 118-bus system, the IEEE 300-bus system, and a French gird and were implemented in MATLAB to verify the validity of the proposed method by sequentially attacking branches to calculate the total amount of affected loads and the relevant load decreasing speeds. For all the simulations conducted below, we set the parameter $\eta = 5.40\times10^{-3}$, 2.43×10^{-3}, and 3.85×10^{-4} in the IEEE 118- and 300- bus systems and the French gird, respectively.

4.1. Relationship between the Two Metrics and the Degree under Different Load Redistribution Rules. To visualize the relationships under different rules, we employ the TSCG of French grid and change the values of λ ($\lambda = 0, +\infty, 0.5$) and τ ($\tau = 0.1, 1, 1.5$).

(1) $\lambda = +\infty$ (NDR). It can be seen from Figure 6 that when $\tau = 1$, both IM and SM are constant and do not change with the degree of vertexes. When $\tau = 0.1$ and $\tau = 1.5$, the values of the IM of a vertex are inverse and direct power law functions of the vertex's own degree, respectively. In contrast, the values of the SM of a vertex are not closely related to the vertex's own degree. In other words, the degree is invalid to identify the vulnerability of the vertexes. However, in this case, our proposed SM is still valid to identify the vulnerable vertexes.

(2) $\lambda = 0$ (GDR). Figure 7 shows that the IM and SM of a vertex are inverse and direct proportional to the vertex's own degree, respectively. It demonstrates that, under the GDR, the metrics of a vertex are only dependent on its own degree.

(3) $\lambda = 0.5$ (an example of some value in $(0, +\infty)$). When $\lambda \in (0, +\infty)$, the corresponding redistribution rule can be regarded as somewhere in between the GDR and the NDR. For example, in Figure 8(a), when $\tau = 0.1$, the IM of a vertex is not obviously in proportional relationship with its own degree. It indicates that the distance plays a more important role in (12) in this case. On the contrary, when $\tau = 1$ or $\tau = 1.5$, the values are approximately of power law with respect to a vertex's own degree. By simulations performed on different systems for many times, the authors find that when λ takes any fixed value in $(0, +\infty)$, with the increase of τ, the degree have more impact on the IM than the distance. In Figure 8(b), the SM is decided jointly by both the distance and degree, and when λ takes any fixed value in $(0, +\infty)$, the SM increases with the growth of τ.

Further, we analyze the changes of metrics with λ when τ is fixed. Figures 9(a) and 9(b) display the changes of two randomly chosen branches: the IM of branch 513 and the SM of branch 2372, respectively. When λ changes from 0.1

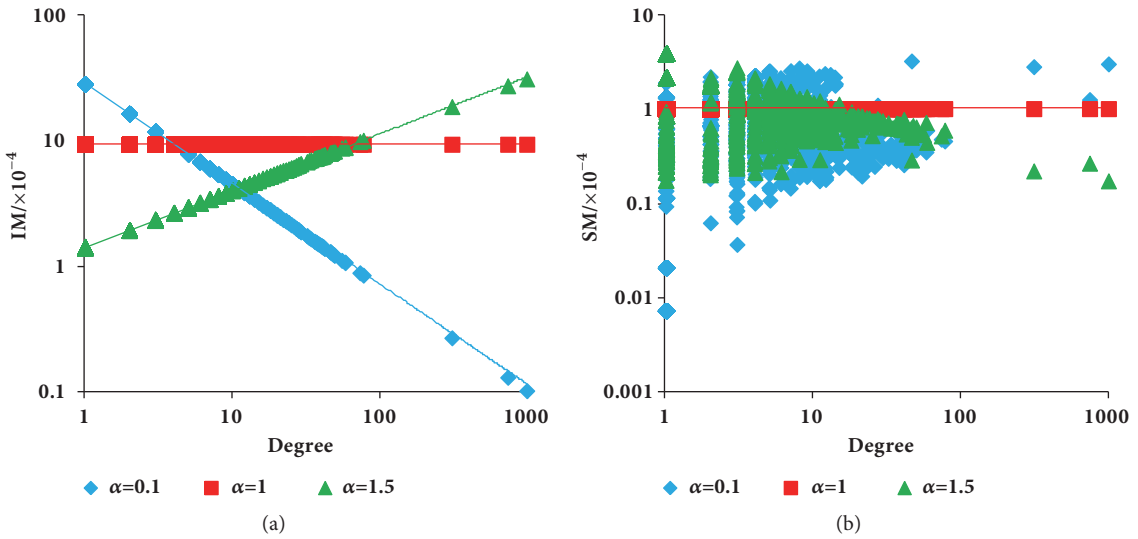

Figure 6: The relationship between metrics and degree in NDR. (a)IM and (b)SM.

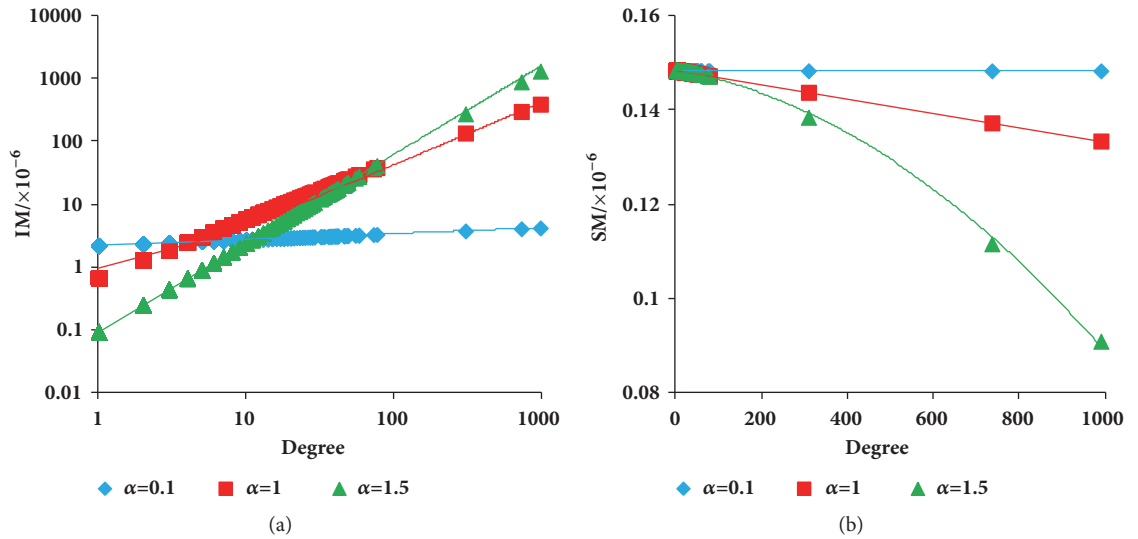

Figure 7: The relationship between metrics and degree in GDR. (a)IM and (b)SM.

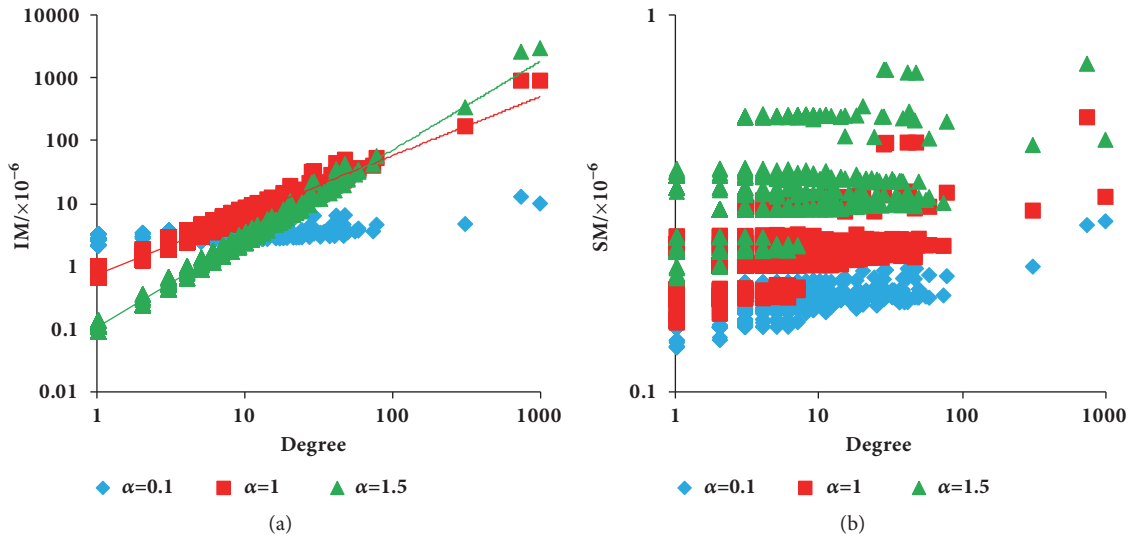

Figure 8: The relationship between metrics and degree in between. (a)IM and (b)SM.

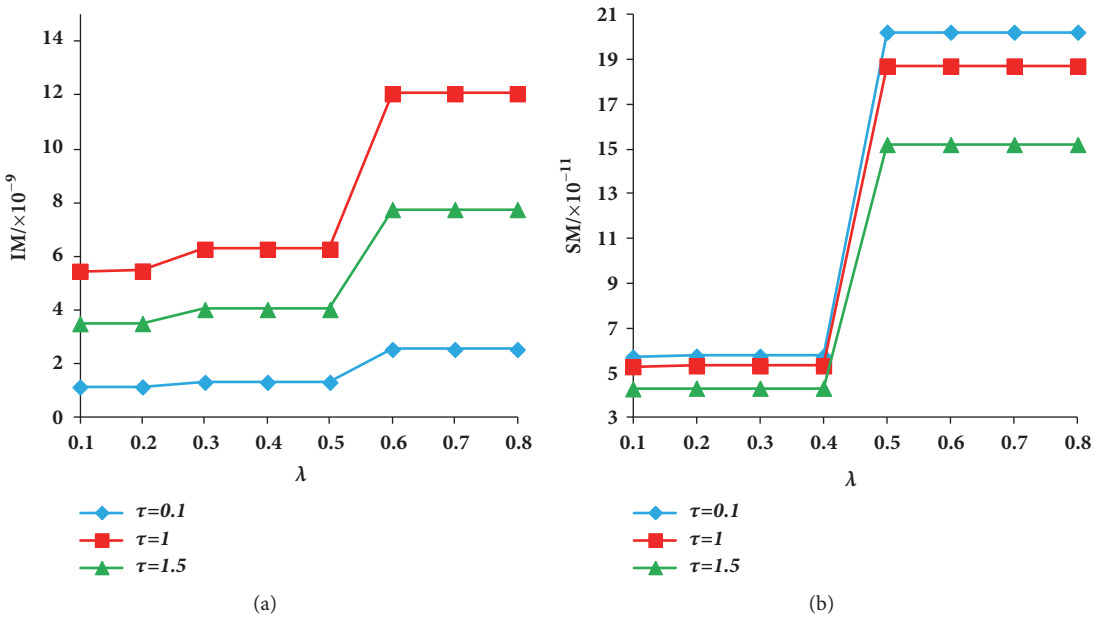

FIGURE 9: The trend of the change of metrics with λ increasing. Here, (a) IM of branch 513 and (b) SM of branch 2372.

to 0.8 with an interval of 0.1, both the IM and the SM exhibit stepwise features, which indicates that there exists points that divide λ into different segments, and the values of the IM and SM are insensitive to λ in each segment. In practice, in order to enlarge the discriminative ability of the proposed metrics, a larger λ is recommended.

In summary, our proposed metrics can identify the vulnerability when degree fails. The λ is vital in the two metrics as it defines the elements in Q_j, which further affects the relationship between the metrics and degree. The proposed metrics can be applied to both neighborhood and global redistribution rules by simply adjust λ and τ.

4.2. Vulnerability Analysis of Electric Networks. To verify the validity of the proposed method, we sequentially attack the 20, 40 and 140 critical branches in the IEEE 118- and 300-bus systems and the French gird, respectively, as identified by IM and SM, and evaluated the remaining load and rate of load decrease. For all the attacks, after removing an identified branch, DC-OPF was used to redispatch the network, with the objective of minimizing the load shedding.

The *remaining load* was used to evaluate the gravity of the attack, and is obtained at the end of the simulation.

The *rate of load decrease* was adopted to reflect the speed at which the load decrease reached important vertices. We calculated the slope between the adjacent samples and then the average slope was used to represent the rate of load decrease, as shown in

$$\kappa = \frac{1}{Y}\sum_{y=2}^{Y}\left(\psi_y - \psi_{y-1}\right) \tag{16}$$

In our simulations, λ varied from 0 to 2 with an interval of 0.2 and τ varied from 0 to 2 with an interval of 0.2. In addition, to consider NDR, we also set $\lambda = +\infty$. With all these combinations, for the IM and SM, we can obtain $12 \times 11 = 132$ sets of critical branches.

TABLE 3: Performances of the metrics by remaining load.

Test benchmarks	ψ	IM	SM
IEEE 118-bus system	>80%	**52.81%**	80.32%
	>90%	**23.87%**	58.74%
IEEE 300-bus system	>80%	**35.09%**	74.67%
	>90%	**16.02%**	43.32%
French grid	>80%	100%	100%
	>90%	**52.46%**	100%

TABLE 4: Comparisons between the IM & SM using remaining load.

Test benchmarks	$\psi_{IM} < \psi_{SM}$	$\psi_{IM} > \psi_{SM}$
IEEE 118-bus system	96.28%	3.72%
IEEE 300-bus system	94.29%	5.71%
French grid	94.47%	5.53%

TABLE 5: Comparisons of the metrics by the rate of load decrease.

Test benchmarks	$\kappa_{IM} < \kappa_{SM}$	$\kappa_{IM} > \kappa_{SM}$
IEEE 118-bus system	76.37%	23.63%
IEEE 300-bus system	79.21%	20.79%
French grid	67.19%	32.81%

The simulation results are given in Tables 3–5. Table 3 gives the statistical results of the 132 attacks. IM is better at identifying critical branches than SM. For example, removing branches according to the IM can cause the grid to lose more than 10% of its load in approximately half of the simulations of the French grid, compared to SM.

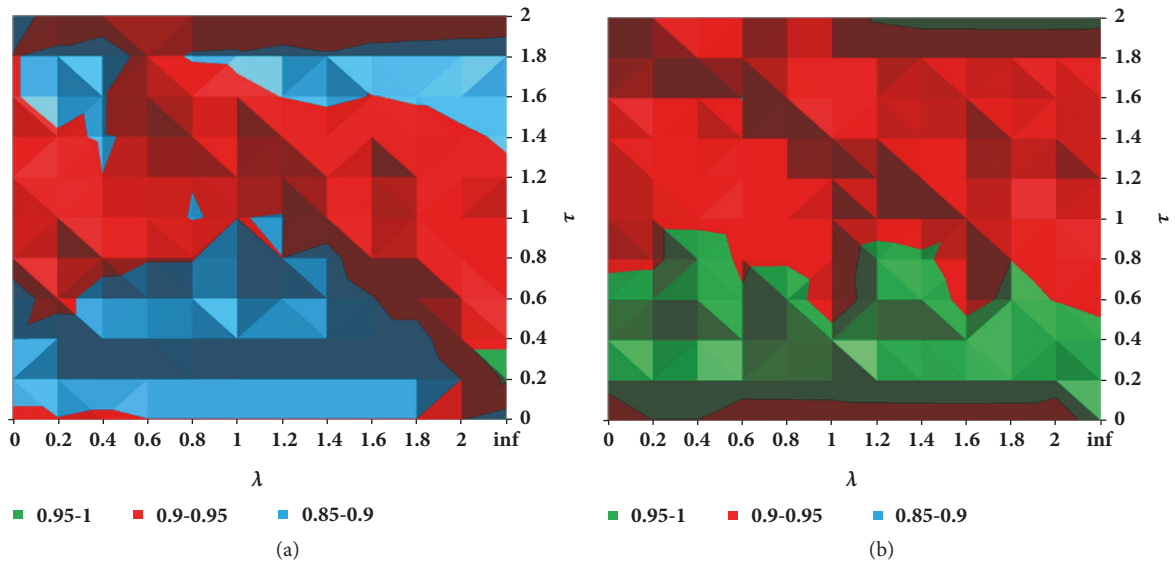

Figure 10: Distribution of removing load under different parametric combinations on the French grid. (a)IM and (b)SM.

To be more quantitative, Table 4 shows the performance difference of the two metrics according to the residual load of the systems under the same λ and τ. The second to the third columns list the percentage of the two metrics in which (1) IM is better than SM and (2) SM is better than IM. It is clear that a load associated with a fault can easily be redistributed to many other branches; therefore, the branches can distinctively exhibit one of the two features, i.e., impactability or susceptibility.

In addition to the percentage of the remaining load, we compared the performance of the metrics according to the speed of the load decrease, as shown in Table 5. Similarly, in the majority of the simulations, the speed of the load loss after an attack following IM is faster than that after SM in the three benchmarks. The speed signifies the intensity of the attack. The faster the load decreases the more difficult it is for the system operator to apply control strategies to stop cascades.

Combining the results from Tables 3–5, we can infer that the identification of the two features becomes increasingly important, becasue they reveal different features in terms of the fault propagation. In general, both from the perspective of a power grid and a general graph, the branches with high impactability more easily spread faults; therefore, they decide the speed of the consequences (in the power system cases used in this paper, this is the loss of the load) and the affected area. Conversely, when branches with high susceptibility are attacked, the fault propagation is slow and load loss is small. This is because the susceptible vertices do not propagate faults as easy as impactable vertices do; they usually work as propagation sinks. So they define the consequences of a cascade.

Accordingly, in practice, with the distinction of the two features of the branches, a system operator can deploy better defense strategies resorting to the most relevant features under different operation states. Protecting impactable branches can effectively avoid triggering failures. However, during a cascading process, particularly under deliberate attacks or fault propagation, susceptible branches can be easily affected by a fault, which can deteriorate the network functionality due to the enhanced consequences from them. Therefore susceptible branches also need to be protected and considered as well.

Furthermore, we investigated the distribution of removed load for different parametric combinations. Due to space limitations, we offer only the French grid (Figure 10) as an example. In Figure 10, when there are different combinations of λ and τ, the load removed from the system is different, which demonstrates the importance of the branches and the adjacent relationships between vertices on determining the vulnerability of a system. In addition, the distribution of the removed load is relatively centralized. For example, the removed load is less when λ and τ are 0-1.8 and 0-0.8, respectively. Meanwhile, note that to obtain the optimum of parametric combination, which is analogous to the parameter selection of deep-learning algorithms, some optimization algorithms, such as genetic algorithms, can be employed.

4.3. Comparison with Existing Methods. Compared to susceptible branches, because impactable branches can easily spread faults, which cause the gird to collapse faster, impactable branches will be primary targets for deliberate attacks. To verify this, we compared the proposed impactable branches to the critical branches as ranked by the degrees of the CGs, betweenness, electrical betweenness, network efficiency [11] and network ability [19] of system structures on the French grid, and the IEEE 118- and 300- bus systems.

In the three benchmarks, when (1) $\lambda = 0.6$ and $\tau = 2$, (2) $\lambda = 0.6$ and $\tau = 1.4$, and (3) $\lambda = 0.6$ and $\tau = 1$, the rankings of the impactable branches had the optimum values, respectively. Figure 11 shows that the remaining load after the removal of the branches ranked by IM of the branches is generally smaller than the degree of the CG. This

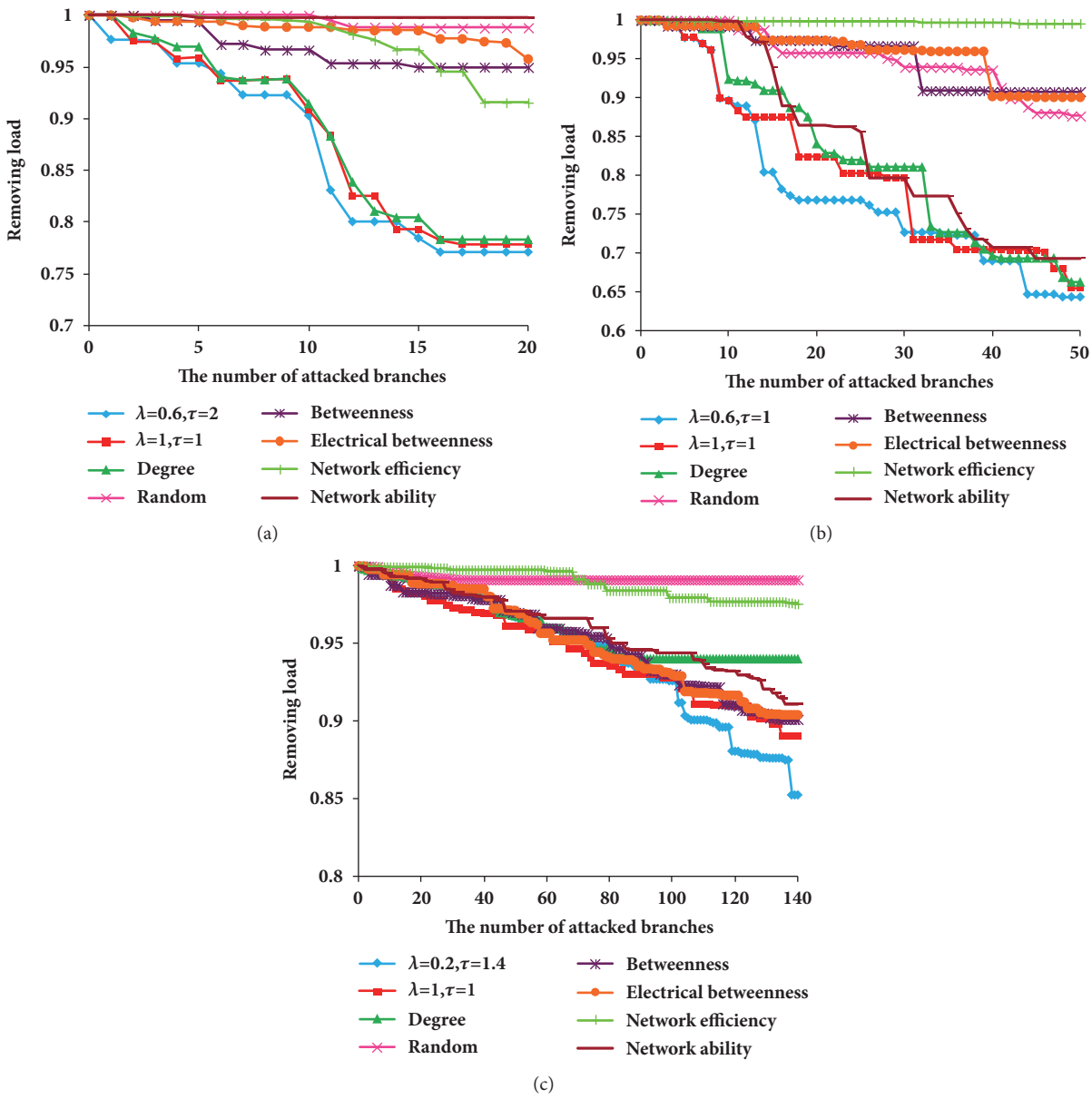

Figure 11: The remaining load with the number of the critical branches increasing. (a) IEEE 118-bus system; (b) IEEE 300-bus system; (c) French grid.

indicates that the vulnerability of branches is related not only to the importance of the branches but also to the adjacent relationships between the vertices. Therefore, considering the relationships to construct indices is necessary to improve the accuracy of vulnerability assessments.

Further, we compared our proposed method to other indices and random attacks for the three benchmarks. For random attacks, some branches are randomly selected and successively removed from benchmarks. Figure 11 shows that the remaining load after the removal of the branches identified by our model is smaller, which indicates that our proposed method has better accuracy when identifying vulnerable branches. In addition, in the three benchmarks, when $\lambda = 1$ and $\tau = 1$, our results have also the relatively better accuracy than other indices even if we did not set the adjustable parameters (τ and λ).

5. Conclusions

In this paper, we employed structural, physical, and operational features to construct a CG to analyze the electrical network vulnerability. On this basis, IM and SM are built to distinguish these two vulnerability features. Adjusting the parameters associated with the metrics can dynamically change the load redistribution rules. Simulations based on benchmarks systems proved the validity of the proposed method. Both IM and SM can identify critical branches of a system; however, IM is more effective than SM in most cases.

Thanks to the general features of the proposed method, i.e., from the perspective of the LRM of the CNT, the IM and SM can also be applied to identify the impactable and susceptible vertices of other networks, e.g., water networks and transportation networks. Similarly to the application we conduct in this paper for electric network, the IM and SM are also expected to not only identify the vulnerability in these networks but also reveal their roles in it.

However, there are still some existing problems to overcome. First, it is important to reduce the time complexity so that our proposed method can be applied to an online assessment of large scale electrical networks. Parallel or distributed computing such as PC clusters and, cloud computing may help to combat the time complexity issue. Secondly, even though adjusting the associated parameters of the two metrics can dynamically change the redistribution rules, there is currently no guidance available as to how to choose them.

Appendix

Proof of the Maximum of the IM and SM

We are interested to find when the IM and SM reach their maximum, regardless of the values of λ and τ. For the IM, supposing that N_Q and ${D_j}^{\tau}$ are fixed, if (9) reaches its maximum, (A.1) needs to be satisfied by the maximum principle of the entropy. Obviously, the necessary and sufficient condition for (A.1) is (A.2).

$$\frac{l_{j1}^{-\lambda}}{\sum_{r\in \mathsf{Q}} l_{jr}^{-\lambda}} = \frac{l_{j2}^{-\lambda}}{\sum_{r\in \mathsf{Q}} l_{jr}^{-\lambda}} = \cdots = \frac{l_{jN_Q}^{-\lambda}}{\sum_{r\in \mathsf{Q}} l_{jr}^{-\lambda}} \tag{A.1}$$

$$l_{j1} = l_{j2} = \cdots = l_{jN_Q} = 1 \tag{A.2}$$

From (A.4), it is manifested that if and only if the other vertexes are all neighbors of the vertex v_j, which means v_j is located at the central position in a star graph, IV_j reaches its maximum expressed in (12).

For the SM, supposing N_Q is fixed, we firstly focus on one of the vertexes affecting the vertex v_k, say vertex v_j. If and only if (A.3) and (A.4) are satisfied, $\Delta\rho_{j\longrightarrow k}$ takes the maximum value, which indicates that only degree of v_j can be greater than or equal to 1 and the degree of other vertexes including v_k must be equal to 1. Further, we analyze the impact of N_Q vertexes on v_k. When $\Delta\rho_{1\longrightarrow k}, \Delta\rho_{2\longrightarrow k}, \ldots, \Delta\rho_{N_Q\longrightarrow k}$ simultaneously reaches their maximum values, i.e., (A.3) and (A.4) are satisfied at the same time, SV_k arrives the maximum. To simultaneously satisfy (A.3) and (A.4) for all $\Delta\rho_{j\longrightarrow k}$ ($j = 1, 2, \ldots, N_Q$), if and only if $D_j = 1$ ($j = 1, 2, \ldots, N_Q$) and $D_k = N_Q$, i.e., v_k is located at the central position in a star graph, SV_k reaches its maximum value expressed in (13).

$$l_{jk}^{-\lambda} = 1 \tag{A.3}$$

$$D_r = \begin{cases} D_j, & r = j \\ 1, & r \neq j \wedge r \neq k \end{cases} \tag{A.4}$$

Symbols

Electrical Network

L: Set of branches (i.e., lines, transformers) in a transmission network, $= \{\cdots, L_j, \cdots\}$, $\dim\{\mathsf{L}\} = N_L$
B: Set of nodes (i.e., buses) in a transmission network, $\dim\{\mathsf{B}\} = N_B$
S: Critical path. $\mathsf{S} = \{\cdots, L_j', \cdots\}$, $\mathsf{S} \subseteq \mathsf{L}$, $\dim\{\mathsf{S}\} = N_S$
α_j: Loading assessment index of the branch j, $L_j \in \mathsf{L}$
f_j^0: Power flow of the branch j under normal operation, $L_j \in \mathsf{L}$
f_j^x: Power flow of the branch j during the contingency x, $L_j \in \mathsf{L}$
f_j^M: Flow limit of the branch j, $L_j \in \mathsf{L}$
P_d^x: Active load during the contingency x, $d \in \mathsf{B}$
δ_z^x: Load shedding percentage in the zth island during contingency x
Z^x: Number of islands during the contingency x
Λ: Normalized total load shedding percentage ($0 \leq \Lambda \leq 1$)
Δ: Threshold for total load shedding percentage

Correlation Graph

V: Set of vertices in a graph, $\dim\{\mathsf{V}\} = N_L$
E: Set of edges in a graph, $\dim\{\mathsf{E}\} = N_q$
G: A correlation graph, $\mathsf{G} = \{\mathsf{V}, \mathsf{E}\}$
V^i: Set of vertices in critical path i, $\mathsf{V}^i = \{\cdots, v_j, \cdots\}$, $v_j = L_j^{i\,\prime}$, $\mathsf{V}^i = \mathsf{S}^i$, $\dim\{\mathsf{V}^i\} = N_S^i$
E^i: Set of edges in critical path i, $\mathsf{E}^i = \{\cdots, e_q^i, \cdots\}$, $e_q^i = L_j^{i\,\prime} L_{j+1}^{i\,\prime}$, $q = j$, $\dim\{\mathsf{E}^i\} = N_S^i - 1$
G^i: Graphic representation of critical path i, $\mathsf{G}^i = \{\mathsf{V}^i, \mathsf{E}^i\}$
r: Power exponent of cumulative distributions
R^2: Fitting effect of the power law
ρ_j: Initial load of the vertex v_j
D_j: Degree of the vertex v_j
τ: Scale factor for initial load, $\tau > 0$
Q_j: Set of vertices affected by vertex v_j. $\mathsf{Q}_j = \{\cdots, v_k, \cdots\}$, $\mathsf{Q} \subseteq \mathsf{V}$, $\dim\{\mathsf{Q}_j\} = N_Q$
$\Delta\rho_{j\longrightarrow k}$: Load variation of vertex v_k due to failure of vertex v_j
l_{jk}: Distance between the vertices v_j and v_k
λ: Portion control factor for load redistribution, $\lambda \geq 0$
η: Threshold for selection of vertices into Q_j
E_j: Entropy of the vertex v_j

IV_j: Impactability of the vertex v_j
SV_k: Susceptibility of the vertex v_k
$\sigma(\cdot)$: Impulse response function
ψ_y: Percentage of remaining load when attacking y branches
κ: Descent rate
Y: Number of adjacent samples.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

All authors declare that they have no conflicts of interest.

Acknowledgments

This research was partially funded by grants from the Key Projects of National Natural Science Foundation of China (U1734202), National Key Research and Development Plan of China (2017YFB1200802-12), and the National Natural Science Foundation of China (61703345, 51877181).

References

[1] 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 Transactions on Power Systems*, vol. 31, no. 2, pp. 1341–1349, 2016.

[2] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading Failure Analysis With DC Power Flow Model and Transient Stability Analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, 2015.

[3] E. I. Bilis, W. Kröger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

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

[5] P. Cructti, V. Latora, and M. Marchiori, "Topological analysis of the Italian electric power grid," *Phyica A*, vol. 338, pp. 92–97, 2004.

[6] V. Rosato, S. Bologna, and F. Tiriticco, "Topological properties of high-voltage electrical transmission networks," *Electric Power Systems Research*, vol. 77, no. 2, pp. 99–105, 2007.

[7] J. Yan, H. He, and Y. Sun, "Integrated Security Analysis on Cascading Failure in Complex Networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, 2014.

[8] Y. Cai, Y. 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, 2016.

[9] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the North American electric power infrastructure," *IEEE Systems Journal*, vol. 6, no. 4, pp. 616–626, 2012.

[10] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET Generation, Transmission & Distribution*, vol. 4, no. 6, pp. 716–724, 2010.

[11] 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, 2012.

[12] A. Dwivedi and X. 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, 2013.

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

[14] Y. Wang, X. Li, J. Li, Z. Huang, and R. Xiao, "Impact of Rapid Urbanization on Vulnerability of Land System from Complex Networks View: A Methodological Approach," *Complexity*, vol. 2018, Article ID 8561675, 18 pages, 2018.

[15] T. Huang, S. L. Voronca, A. A. Purcarea, A. Estebsari, and E. Bompard, "Analysis of chain of events in major historic power outages," *Advances in Electrical and Computer Engineering*, vol. 14, no. 3, pp. 63–70, 2014.

[16] S. Blumsack, E. Bompard, A. Carbone et al., "Power grids vulnerability: a complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, Article ID 013119, 2009.

[17] 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 Transactions on Industrial Informatics*, 2018.

[18] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A Novel Cascading Faults Graph Based Transmission Network Vulnerability Assessment Method," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2995–3000, 2018.

[19] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274–3284, 2014.

[20] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, 2014.

[21] F. Wenli, Z. Xuemin, M. Shengwei, H. Shaowei, W. Wei, and D. Lijie, "Vulnerable transmission line identification using ISH theory in power grids," *IET Generation, Transmission & Distribution*, vol. 12, no. 4, pp. 1014–1020, 2018.

[22] 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 Transactions on Power Systems*, vol. 32, no. 2, pp. 958–967, 2017.

[23] J. Qi, K. Sun, and S. Mei, "An interaction model for simulation and mitigation of cascading failures," *IEEE Transactions on Power Systems*, vol. 30, no. 2, pp. 804–819, 2015.

[24] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 20, no. 3, Article ID 033122, 2010.

[25] E. Bompard, A. Monti, A. Tenconi et al., "A multi-site real-time co-simulation platform for the testing of control strategies of distributed storage and V2G in distribution networks," in

Proceedings of the 2016 18th European Conference on Power Electronics and Applications (EPE'16 ECCE Europe), pp. 1–9, Karlsruhe, September 2016.

[26] X. Wei, S. Gao, and D. Li, "Cascading fault graph for the analysis of transmission network vulnerability under different attacks," *Proceedings of the Chinese Society for Electrical Engineering*, vol. 38, no. 2, pp. 465–474, 2018.

[27] B. Stott, J. Jardim, and O. Alsaç, "DC power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.

[28] B. Stott, O. Alsac, and F. Alvarado, "Analytical and computational improvements in performance-index ranking algorithms for networks," *International Journal of Electrical Power & Energy Systems*, vol. 7, no. 3, pp. 154–160, 1985.

[29] L. Guo and X. Cai, "Degree and weighted properties of the directed China Railway Network," *International Journal of Modern Physics C*, vol. 19, no. 12, pp. 1909–1918, 2008.

[30] L. Kencl and J. Le Boudec, "Adaptive load sharing for network processors," in *Proceedings of the IEEE Information Communications Conference (INFOCOM 2002)*, pp. 545–554, New York, NY, USA, 2002.

[31] H. Wang, K. Liu, and P. Ao, "Magnetic field and specific axial load capacity of hybrid magnetic bearing," *IEEE Transactions on Magnetics*, vol. 49, no. 8, pp. 4911–4917, 2013.

[32] D. Duan, J. Wu, H. Deng et al., "Cascading failure model of complex networks based on tunable load redistribution," *Systems Engineering-Theory & Practice*, vol. 33, no. 1, 2013.

[33] W. X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 77, no. 2, Article ID 026101, 2008.

[34] D. Duan and R. Zhan, "Evolution mechanism of node importance based on the information about cascading failures in complex networks," *Acta Physica Sinica*, vol. 63, no. 6, Article ID 068902, 2014.

[35] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 70, no. 3, Article ID 035101, 2004.

[36] D.-H. Kim, B. J. Kim, and H. Jeong, "Universality class of the fiber bundle model on complex networks," *Physical Review Letters*, vol. 94, no. 2, Article ID 025501, 2005.

[37] J. Lehmann and J. Bernasconi, "Stochastic load-redistribution model for cascading failure propagation," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 81, no. 3, Article ID 031129, 2010.