IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 26, 2019, accepted March 15, 2019, date of publication March 26, 2019, date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906286

Electrical Network Operational Vulnerability Evaluation Based on Small-World and Scale-Free Properties

XIAOGUANG WEI[1], **SHIBIN GAO**[1], **TAO HUANG**[2], **(Member, IEEE), TAO WANG**[3], **AND TIANLEI ZANG**[1,4]

[1]School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China
[2]Department of Energy, Politecnico di Torino, 10129 Turin, Italy
[3]Electrical Engineering and Electronic Information, Xihua University, Chengdu 610039, China
[4]Department of Electrical Engineering, Tsinghua University, Beijing 100000, China

Corresponding author: Shibin Gao (1514754029@qq.com) and Tao Huang (tao.huang@polito.it)

This work was supported by grants from the National Natural Science Foundation of China under Grant 51877181 and Grant 61703345, in part by the Key Projects of the National Natural Science Foundation of China under Grant U1734202, and in part by the National Key Research and Development Plan of China under Grant 2017YFB1200802-12.

ABSTRACT Assessment of electrical network vulnerability based on complex network theory (CNT) has attracted increasing attention. However, CNT focuses on analyzing the structural vulnerability and has significant limitations regarding operational vulnerability. To address the lack of a comprehensive CNT-based framework to assess operational vulnerability, a temporal-spatial correlation graph (TSCG) that considers the topological, physical, and operational characteristics of electrical networks is proposed. To better assess vulnerability, two metrics, i.e., impact ability and susceptibility of branches, based on symmetric entropy from the load redistribution mechanism of electrical networks and their corresponding TSCGs are proposed. Applications to IEEE 39-bus system, IEEE 118-bus system, and French grid demonstrate that the proposed TSCGs have distinctive features that can intuitively and simply reveal the features of impact ability and susceptibility in CNT.

INDEX TERMS Complex network theory, electrical network, vulnerability assessment, temporal-spatial correlation graph, impactability, susceptibility.

I. INTRODUCTION

Electrical network vulnerability assessment (ENVA), which is also called critical branch or bus identification, is an important approach to focus on identifying the most vulnerable elements of a transmission network which have great impacts on network function or structure mostly against deliberate attacks or other causes. Currently, complex network theory (CNT) is a popular method to evaluate ENV [1]–[4]. Based on CNT, various studies have proven that many electrical networks are small-world networks by investigating the average shortest path and average clustering coefficient of networks [5]–[7]. In addition, electrical networks have also been shown to exhibit scale-free features [8]–[10]. Such scale-free properties demonstrate that electrical networks are robust against random attacks; however, they are highly vulnerable if critical targets are attacked.

Due to the scale-free properties, it is necessary to identify critical branches to enhance security. From a CNT perspective, pure statistical metrics [11]–[15], such as degree [11] and betweenness [12], [13], have been widely employed in ENVA. However, such pure statistical metrics only consider the topology of an electrical network, thereby neglecting physical features. Thus, such metrics may not represent the real responses of power grids, which leads to inaccurate evaluation results. Therefore, extended statistical metrics [16]–[23], such as extended betweenness [19] and electric betweenness [21], which can capture and integrate the specific physical behaviors of power grids into CNT, have been proposed. For example, branch admittance is employed as an edge weight to define the electrical distance from generation nodes to load nodes [16]–[18].

However, although extended statistical metrics consider some physical features of electrical networks, they still focus on structural vulnerability analysis. In addition, the

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

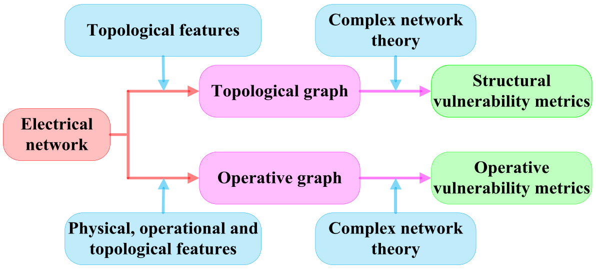


FIGURE 1. Operative vulnerability metrics.

topological and physical features cannot comprehensively reveal the operational states (especially fault operational states) of electrical networks. For example power transmission over branches involves both admittance properties and the network's operational rules. Therefore, applying CNT in consideration of topological, physical, and operational features to assess operational vulnerability is challenging.

In summary, to address the lack of a comprehensive framework for CNT-based operational assessment, we propose the use of topological, operational, and physical characteristics to abstract statistical features [24]–[27] as an operative graph to reveal the vulnerable features of an electrical network. Then, CNT is employed to analyze the operative graph to replace the original structure, as shown in Fig. 1. Based on the proposed process, we map an electrical network with spatial distribution to a graph that considers impactability and susceptibility with fault temporal information among branches. We call the graph a temporal-spatial correlation graph (TSCG). Our main contributions are summarized as follows.

- To classify each branch into impactable and susceptible features, we propose an index based on the symmetric entropy of the differences between the power flows over each branch before and after contingencies relative to the load redistribution mechanism of an entire network.
- Based on the impactable and susceptible features of branches, we propose an impactable TSCG (iTSCG) and susceptible TSCG (sTSCG) that consider the topological, physical, and opterational characteristics of electrical networks.
- CNT is applied to analyze the iTSCG and sTSCG properties to intuitively and simply reveal the vulnerable features of an electrical network. Furthermore, operational topological metrics are developed to evaluate the ENVA.

In addition, for the clarity, the terms ''network, branch (i.e., line, transformer), node (i.e., bus)'' are used only for electric networks and ''graph, edge, vertex'' only for iTSCGs(sTSCG).

The remainder of this paper is organized as follows. Section II describes symmetric entropy-based feature identification. Section III proposes a method to develop the iTSCG and sTSCG. In Section IV, the properties of the iTSCG and sTSCG are analyzed based on CNT. IEEE 39-bus and 118-bus systems are employed to verify the effectiveness of the proposed method. Conclusions are presented in Section V.

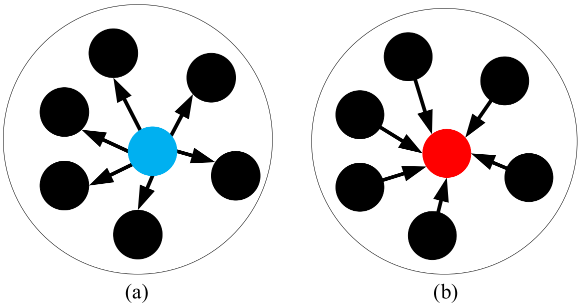


FIGURE 2. Diagrammatic representation of (a) impactability and (b) susceptibility.

II. FEATURES OF VULNERABLE BRANCHES AND VULNERABILITY METRICS

A. IMPACTABILITY AND SUSCEPTIBILITY

We classify vulnerable branches in an electrical network as highly impactable or highly susceptible. Highly impactable branches (Fig. 2(a)) can easily spread faults to other branches, which is likely to results in a blackout under deliberate attacks or other causes. Highly susceptible branches (Fig. 2(b)) are more easily affected by a fault. It should be noted that each branch has both impactable and susceptible features, but with different importance to the network. As our focus is to identify the ones with high importance, hereinafter, we simply call highly impactable or highly susceptible branches as impactable and susceptible branches for short.

By distinguishing these two features of vulnerable branches, better defense strategies can be devised relative to the most relevant feature under different operational states. For example, an electrical network is primarily affected when offenders attack impactable branches under normal operating conditions; thus, the TSO must focus on protecting impactable branches. Protecting impactable branches can reduce the likelihood of network failures. However, in fault operation, particularly under deliberate attacks or other causes, susceptible branches must also be protected because they can be easily affected by a propagated fault.

B. SYMMETRIC ENTROPY-BASED VULNERABILITY METRIC

System failure can lead to both system and branch state changes. Generally, the more harmful the changes to the system and branch states, the more critical the fault is, particularly when the system has been under stress. Thus, we propose symmetric entropy to measure the changes to construct a method to identify the two features from the perspective of a load redistribution mechanism. Note that we focus on the vulnerability of a transmission network from the perspective of a load redistribution mechanism; thus a static model is adopted with the following simplifications. 1) The dynamic/transient stability features of generators or load are not considered [28]. 2) Only static network behaviors are considered. 3) The protections and controllers of electronic devices or generators are ignored. 4) Only protections related to the transmission branch are modeled. The load redistribution is performed through a standard OPF.

1) SYMMETRIC ENTROPY

Assume two systems (or two different states of a system) $\mathbb{X} = \{X_1, X_2, \ldots, X_N\}$ and $\mathbb{Y} = \{Y_1, Y_2, \ldots, Y_N\}$, where X_i and Y_i represent the condition of the element i of the two systems (states) $\mathbb{X}$ and $\mathbb{Y}$, $0 \leq X_i \leq 1$ and $0 \leq Y_i \leq 1 (i = 1, 2, \ldots, N)$. Relative entropy $S(\mathbb{X}, \mathbb{Y})$ [29] can be employed to quantify the difference between $\mathbb{X}$ and $\mathbb{Y}$ as follows.

$$S(\mathbb{X}, \mathbb{Y}) = \sum_{i=1}^{N} \left[X_i \log \frac{X_i}{Y_i} + (1 - X_i) \log \frac{1 - X_i}{1 - Y_i} \right] \tag{1}$$

Obviously, greater $S(\mathbb{X}, \mathbb{Y})$ yields a greater difference between $\mathbb{X}$ and $\mathbb{Y}$. However, Equation (1) has the following disadvantages: 1) it is asymmetric, i.e., $S(\mathbb{X}, \mathbb{Y}) \neq S(\mathbb{Y}, \mathbb{X})$ leading to a non-uniqueness of difference value between $\mathbb{X}$ and $\mathbb{Y}$, and 2) it is unbounded, i.e., $\lim\limits_{Y_i \to 1 \vee 0} S(\mathbb{X}, \mathbb{Y}) \to \infty$, leading to no solution when the element $Y_i = 1 \vee 0$.

To overcome these problems, we propose and define symmetric entropy to measure the difference between $\mathbb{X}$ and $\mathbb{Y}$, which maintains the other properties of relative entropy. The symmetric entropy $S'(\mathbb{X}, \mathbb{Y})$ is defined as follows:

$$S'(\mathbb{X}, \mathbb{Y}) = \sum_{i-1}^{N} \left[\sqrt{X_i Y_i} \log \frac{2\sqrt{X_i Y_i}}{X_i + Y_i} + \left(1 - \sqrt{X_i Y_i}\right) \log \frac{2 - 2\sqrt{X_i Y_i}}{2 - (X_i + Y_i)} \right] \tag{2}$$

It can be proved that Equation (2) has the following properties:

(a) Non-negativity: $S'(\mathbb{X}, \mathbb{Y}) \geq 0$, $S'(\mathbb{X}, \mathbb{Y}) = 0 \Leftrightarrow \mathbb{X} = \mathbb{Y}$;

(b) Symmetry: $S'(\mathbb{X}, \mathbb{Y}) = S'(\mathbb{Y}, \mathbb{X})$;

(c) Boundedness: $S'(\mathbb{X}, \mathbb{Y}) \leq N$.

According to the non-negativity of the relative entropy, it is manifest that Equation (2) satisfies the non-negativity. Obviously, Equation (2) has a symmetric feature (proof can be done easily by swapping $\mathbb{X}$ & $\mathbb{Y}$). The proof of the boundedness is given in the appendix.

To apply symmetric entropy to power systems, we must select a physical quantity to be used in Equation (2). Here, we employ power flow over branches P_{no} and P_{fo} during normal and fault operation, respectively. To normalize the power flow over a branch, we use the maximum power limit of branch P_M to define A and B.

$$A = \left| \frac{P_{no}}{P_M} \right|, \quad B = \begin{cases} \left| \dfrac{P_{fo}}{P_M} \right| & \left| P_{fo} \right| < P_M \\ 1 & \left| P_{fo} \right| \geq P_M \end{cases} \tag{3}$$

From an engineering perspective, the definitions of A and B are extremely simple, i.e., the p.u. value of the power flow in the network under normal and emergency states. Note that when $\left| P_{fo} \right| \geq P_M$, Y is set to 1 to satisfy the requirement of Equation (2).

Based on the above definition, we can employ the symmetric entropy to identify impactable and susceptible branches from the load redistribution of the entire network or single branches. Note that we use the term ''selected physical quantity'' to describe impactable and susceptible branch identification.

2) IMPACTABLE BRANCH

We denote a selected physical quantity of branch i before and after branch j fails as A_i and B_i^j, respectively. Then, the corresponding normal and fault operation states of an electrical network can be expressed as $\mathbb{A}_I = \left\{A_1, A_2, \ldots, A_{N_L}\right\} \backslash A_j = \left\{A_1, A_2, \ldots, A_{j-1}, A_{j+1} \ldots, A_{N_L}\right\}$ and $\mathbb{B}_I^j = \left\{B_1^j, B_2^j, \ldots, B_{N_L}^j\right\} \backslash Bj^j = \{B_1^j, B_2^j, \ldots, B_{j-1}^j, B_{j+1}^j \ldots, B_{N_L}^j\}$, respectively, where $j \in \{1, 2, \ldots, N_L\}$ and N_L is the number of branches in the network. The $\mathbb{X}$ and $\mathbb{Y}$ in Equation (2) are then defined as $\mathbb{A}_I$ and $\mathbb{B}_I^j$, resectively. Using Equation (2), we employ the changes of the physical quantity before and after branch j fails to reflect impact on the network as follows.

$$S'\left(\mathbb{A}_I, \mathbb{B}_I^j\right) \tag{4}$$

3) SUSCEPTIBLE BRANCH

We denote a selected physical quantity of branch i before and after branch j fails as A_i and $\mathbb{B}_S^i = \left\{B_i^1, B_i^2, \ldots, B_i^{N_L}\right\} \backslash B_i^i = \left\{B_i^1, B_i^2, \ldots, B_i^{i-1}, B_i^{i+1}, \ldots, B_i^{N_L}\right\}$, respectively, where $i, j \in \{1, 2, \ldots, N_L\}$. The $\mathbb{X}$ and $\mathbb{Y}$ in Equation (2) are then defined as $A_i \cdot \mathbf{1}^T$ and $\mathbb{B}_S^i$, respectively. Using Equation (2), we employ the impact of all other branch failures on element i to quantify the susceptibility of i as follows.

$$S'\left(A_i \cdot \mathbf{1}^T, \mathbb{B}_S^i\right) \tag{5}$$

where $\mathbf{1}^T = \underbrace{(1, 1, \ldots, 1)}_{N_L - 1}$.

III. TSCG GENERATION

In Section II, although we construct vulnerable metrics for two features, we only consider a single network fault. To reflect the fault operation of an entire network, we employ the cascade concept to construct a directed statistical graph based on fault chain theory [30], [31] that considers the topological, physical, and operational characteristics of electrical networks from the perspective of operational vulnerability. This graph can reveal adjacent fault relationships among branches by transforming an electrical network with spatial information into a TSCG based on fault chain theory. In addition, the TSCG can be divided into an impactable TSCG (iTSCG) and susceptible TSCG (sTSCG).

A. FAULT CHAIN GENERATION

To better illustrate fault chain generation, we consider a cup with water (Fig. 3) as an example. The cup can be

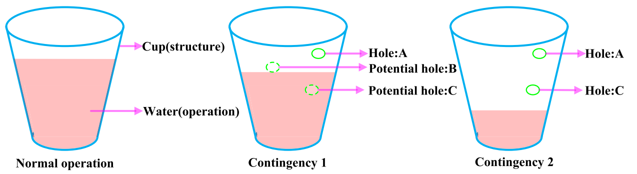


FIGURE 3. The relationships between cup (structure) and water (operation).

considered the topological structure of an electrical network, and the water can be considered as the operational status. If contingency 1 creates hole "A" in the cup, its ability to hold water will be reduced due to the structural damage. Therefore, "A" impacts the topological structure and can potentially limit operations, particularly the optimal operating point. Furthermore, structural damage "A" may also create other potential vulnerable points. Suppose two potential holes "B" and "C" are new vulnerable points created by "A" and both can be selected as contingency 2. To trace the potential vulnerable points, we need to consider different combinations. For example, if we consider N-k criterion, for an electrical network with N_L branches, we need to calculate $\prod_{i=1}^{k}(N_L - i + 1)$ contingencies. Therefore, for a large-scale network, the calculation burden becomes an issue.

To decrease calculation burden, we only choose the most influential vulnerable point. For example, if "C" has more serious impact on operation status than "B," i.e., "C" results in greater water loss, then "C" is selected. Note that even though only a single element is selected to evolve the fault, the potential consequences of other element failure are covered implicitly. Because at each step, we select the element which can cause the most severe consequence for the entire network; therefore, the gravity of the network-wise consequences of other potential elements failure would be lower than the selected one. In addition, it is obvious that our proposed method can greatly decrease the calculation burden. The larger the network is, the higher the decrease will be. Take the IEEE 39-bus system, IEEE 118-bus system and French grid as examples, the calculation burden is decreased 95.51%, 98.28% and 99.23%, respectively.

To reproduce the process, based on Equations (4) (i.e., impactability) and (5) (i.e., susceptibility), we define impactable and susceptible branch assessment indices (BAI), shown in Equations (6) and (7), respectively, to evaluate the fault possibility of each branch.

$$\alpha_x^i = S'\left(\mathbb{A}_{I(x-1)}, \mathbb{B}_{Ix^j}\right) \tag{6}$$

$$\beta_x^i = S'\left(A_{i(x-1)} \cdot \mathbf{1}^T, \mathbb{B}_{Sx^i}\right) \tag{7}$$

Here, x is the x-th contingency of the network. Thus, α_x^i and β_x^i quantify the impactability and susceptibility of branch L_i under two different contingencies. In this study, at each cascading stage, the contingency set contains a single branch, i.e., the selected next most possible fault branch according to Equations (6) or (7).

With Equations (6) and (7), we can develop impactable and susceptible fault chains for different contingencies. Here Algorithm 1 is employed to develop a fault chain. The main function of electrical networks is to continuously provide quality electricity to the final users. In addition, as the main focus is to assess the vulnerability of the network by Equations (6) and (7), thus the termination criterion for the fault chain is not the natural stop of a cascading failure [32], [33]. In other words, after the functional loss reaches a certain level, we do not differentiate the gravity of the impact any more.; therefore, like most other studies [23], [24], we employ the scale of blackout expressed as a percentage of total load shedding Λ to measure the consequence of the fault and mark the end of the fault chain via a threshold of load shedding Δ, i.e., if $\Lambda \geq \Delta$, the fault chain ends. It is noted that to generate the TSCG containing fault operation states initialized by all single branch failures, we successively select each branch as the first candidate branches to generate fault chains. Moreover, the fault chain is defined as a series of faults selected by an index which is deliberately designed to individualize a specific property of the transmission network with the consideration of the main operational features.

Algorithm 1 Impactable (or Susceptible) Fault Chain Generation

```
Input: Electrical network information
Output: Fault chain set $\mathbb{C}$ and $\alpha$ ($\beta$) of each branch in $\mathbb{C}$
Step1: Initialization: $\mathbb{C} = \emptyset$, $x = 0$ and the threshold of
       total load shedding $\Delta$ for fault chain termination.
Step2: Beginning point: Select a branch from the original
       network as the first candidate branch to begin and
       add it to $\mathbb{C}$; set $\alpha_0 = 0$ ($\beta_0 = 0$) for
       the first candidate branch;
Step3: WHILE $x = x + 1$
Step4: Power flow calculation: Employ DC power flow
       method to calculate power flow over each
       branch in the electrical network;
Step5: BAI calculation: Employ Equation (6) and (7) to
       calculate $\alpha_x^i(\beta_x^i)$ of branch $L_i$
       ($i = 1, 2, \ldots, N_L, L_i \notin \mathbb{C}$) in $x$th contingency;
Step6: Branch choice: choose the branch $L_t$ with the
       largest $\alpha_x^t(\beta_x^t)$ as the candidate branch
       in $x + 1$ th contingency, where $t :=$
       $\arg \max_{i=\{1,2,\ldots,N_L\}} \left(\alpha_x^i\right)$ ($t := \arg \max_{i=\{1,2,\ldots,N_L\}} \left(\beta_x^t\right)$);
Step7: Load shedding calculation: Employ DC OPF to
       calculate the minimum load shedding $\Lambda_x$ in
       $x$ th contingency;
Step8: IF $\sum \Lambda_x \geq \Delta$
Step9: Termination: Break;
Step10: ELSE IF
Step 11: Chain generation:Add the candidate branch $L_t$ to
        $\mathbb{C}$ and remove it from the electrical network; record
        $\alpha_x^t(\beta_x^t)$ of the candidate branch.
Step12: END IF
Step13: END WHILE
```

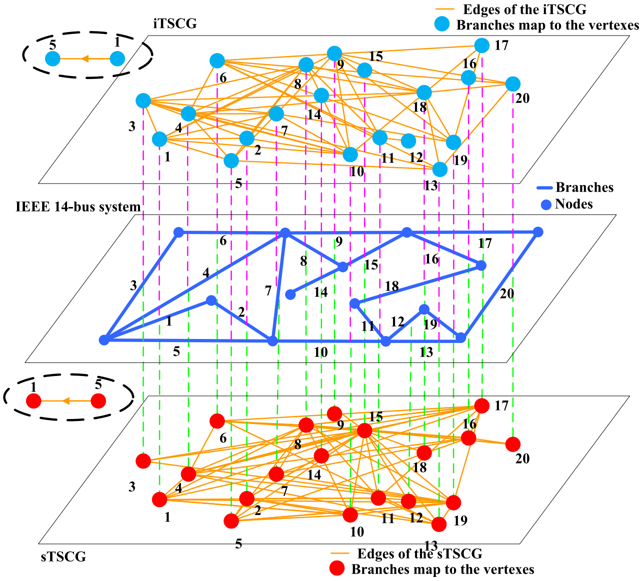


FIGURE 4. iTSCG and sTSCG of the IEEE 14-bus system.

In addition, although the power flow over network is complex power, the reactive power is a local problem and only active power is a network-wise problem. Meanwhile, considering that we focus on investigating the network vulnerability from the load redistribution of the entire network and the AC power flow and AC OPF can easily create the risk of divergence of power flow due to the reactive and voltage problem, DC power flow and DC OPF are an appropriate option to quantify the load distribution features from the perspective of the CNT.

B. TSCG GENERATION

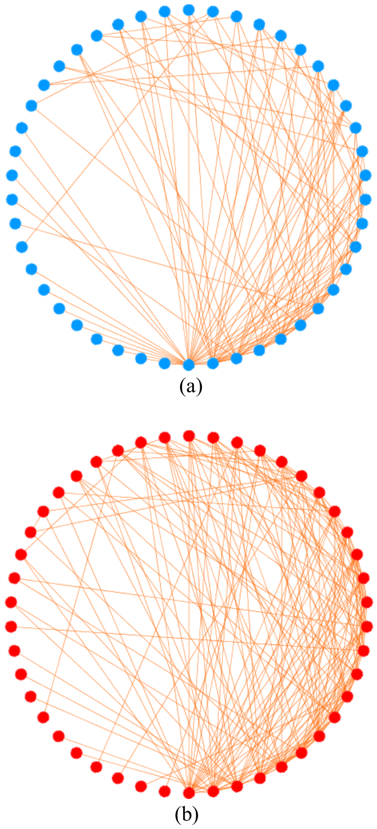
Assume an electrical network with N_L branches. We successively consider each branch as a beginning point to capture N_L impactable (susceptible) fault chain sets $\mathbb{C}1, \mathbb{C}2, \ldots, \mathbb{C}_{N_L}$ by algorithm 1. For an impactable (susceptible) fault chain set $\mathbb{C}_i$ of N_i branches $L_1, L_2, \ldots, L_{N_L}$, we map $\mathbb{C}_i$ to the impactable (susceptible) fault chain graph $\mathscr{g}_i = \{\mathrm{v}_i, e_i\}$, where vertex v_i and edge e_i are expressed as follows:

$$\mathrm{v}_i = \left\{v_j | v_j = L_j, j = 1, 2, \ldots, N_i\right\},$$
$$e_i = \left\{e_j | e_j = L_j L_{j+1}, j = 1, 2, \ldots, N_{i-1}\right\}.$$

It is noted that the connections among the vertices are generated by alogrithm1. Therefore, the iTSCG (sTSCG) $\mathbb{G}$ constructed using the N_L fault chain graph $\mathscr{g}_1, \mathscr{g}_2, \ldots, \mathscr{g}_{N_L}$ can be represented as follows.

$$\mathbb{G}=\left\{(\mathbb{V}, \mathbb{E})\,|\mathbb{V}=\mathrm{v}_1 \cup \mathrm{v}_2 \cdots \cup \mathrm{v}_{N_L}, \mathbb{E}=e_1 \cup e_2 \cdots \cup e_{N_L}\right\}$$

We demonstrate the iTSCG and sTSCG for the IEEE 14-bus system in Fig. 4 as an example. Note that the arrows of directed edges are omitted in Fig. 4 for clarity; however, each edge has an arrow to identify the direction between two adjacent vertexes, such as vertexes 1 and 5 (black dotted ellipse). Moreover, the arrows reveal the sequential relationships among branches w.r.t. fault propagations (evaluated by our contingency selection criterion) and always point to the next most impactable (susceptible) branch caused by current faulty branch. This sequential relationship is called adjacent relationships among branches.



(a)

(b)

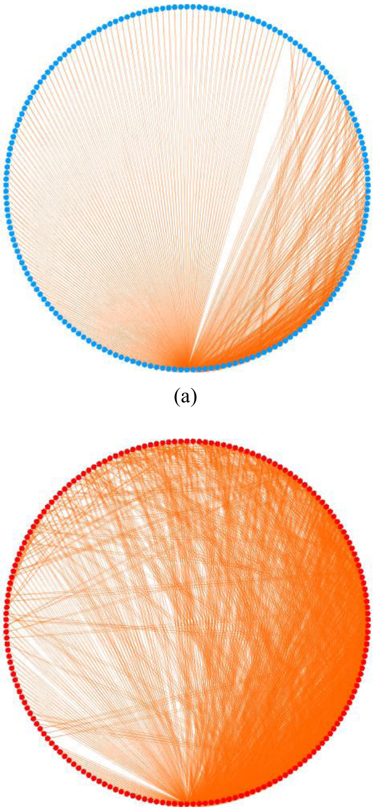
FIGURE 5. iTSCG and sTSCG of IEEE 39-bus system. (a) iTSCG, and (b) sTSCG.

As shown in Fig. 4, the iTSCG and sTSCG can transform electrical networks with spatial information into a directed graph with temporal-spatial information between branches through the load redistribution mechanism. The two TSCGs are statistical graphs that intuitively and simply reveal adjacent relationships among branches under fault operation.

IV. CASE ANALYSIS AND SIMULATION RESULTS

A. PROPERTIES OF iTSCGs AND sTSCGs

To study the properties of the two TSCGs, we constructed both the iTSCGs and sTSCGs of the IEEE 39-bus system, IEEE 118-bus system and French grid by setting $\Delta = 20\%$, which is a sufficiently sized blackout for an electrical network [34]. In three study cases, the French grid is a large-scale network with 2596 branches, 391 generators and 1951 buses. The TSCGs for the two IEEE systems are shown in Figs. 5 and 6. The TSCGs are drawn using CYTOSCAPE. Considering that the scales of TSCGs for the French grid are large and space is limited, the TSCGs are not given. As can be seen, the complexity of the iTSCGs differs compared to the sTSCGs. In addition, we analyzed the cumulative distribution of the vertexes degree of the iTSCGs, which is defined as $P(K > k) = \sum_{K>k} P(k)$. We found that the



(a)

(b)

FIGURE 6. iTSCG and sTSCG of IEEE 118-bus system. (a) iTSCG, and (b) sTSCG.

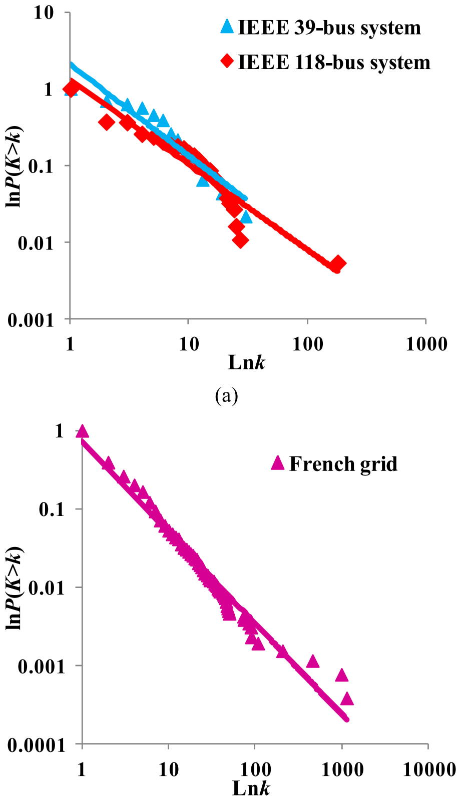
iTSCGs of the IEEE 39-bus system, IEEE 118-bus system and French grid follow the power-law degree distribution (Fig. 7 in log-log scale). The fitting functions can be formulated as Equations (8) - (10) with goodness of fitting $R^2 > 80\%$.

$$\ln P\,(K > k) = -1.1860 \ln k + 0.7131(R^2 = 0.8892) \quad (8)$$

$$\ln P\,(K > k) = -1.1070 \ln k + 0.2621(R^2 = 0.8932) \quad (9)$$

$$\ln P\,(K > k) = -1.1640 \ln k - 0.0367(R^2 = 0.9640) \quad (10)$$

Generally, when $R^2 > 80\%$, we consider that the fitting curve has satisfactory fitting effectiveness, especially, $R^2 > 95\%$ in the iTSCG of the French grid. Equations (8) - (10) and Fig. 7 demonstrate that the iTSCGs are scale-free for the IEEE 39-bus system, IEEE118-bus system and French gird. Therefore, most vertexes in the iTSCGs have small degree; however, there are a few vertexes with high degree. This indicates that the three systems have a few high impactable branches that have significant impacts on the vulnerability of the electrical network. If such branches are attacked, the systems would become highly operational vulnerability and it would be easy to spread faults; however, the systems would be robust against random branch attacks. It demonstrates the load shedding will be increased rapidly with the number of deliberated attacked branches increasing but have no obvious change under random attacks.



(a)

(b)

FIGURE 7. iTSCG of (a) IEEE 39-bus and 118-bus systems and (b) French grid.

TABLE 1. Topological statistical metrics of sTSCGs.

Network	l	c	l_{random}	c_{random}
IEEE 39-bus system	2.2378	0.3079	1.8762	0.1673
IEEE 118-bus system	2.1039	0.3796	1.8436	0.0915
French gird	2.6542	0.2469	2.0802	0.0169

(L_{random} and C_{random} represent the average short path and average clustering coefficient of random graphs with the same number of vertexes and average degree as the sTSCGs.)

To confirm the properties of the sTSCGs, we investigated the average shortest path l and average clustering coefficient c (Tab. 1) [35]. By comparing these two parameters of the sTSCGs to random graphs, we conclude that both sTSCGs are small-world graphs. Therefore, because the small-world network has a relatively small average shortest path but a very large cluster coefficient, the vertexes have closer relationships, i.e., the branches mutually affect each other under different contingencies rather than some having distinctive influence on the others. This indicates that under deliberate attacks, the close relationships among susceptible branches will increase the speed of fault propagation.

In summary, the operative vulnerability of electrical networks has the following characteristics.

The scale-free properties of the iTSCGs demonstrate that electrical networks have a few impactable branches that can

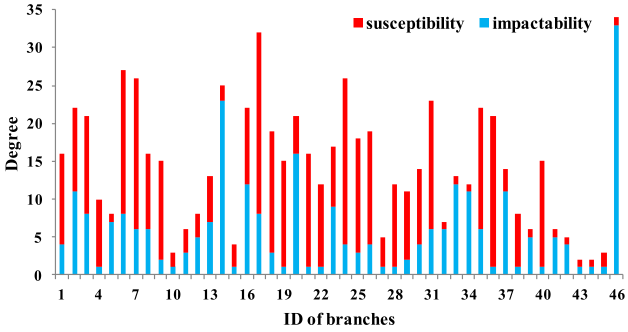


FIGURE 8. Degree of branches in the IEEE 39-bus system.

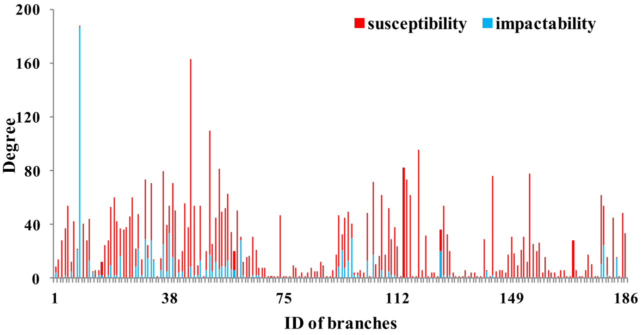


FIGURE 9. Degree of branches in the IEEE 118-bus system.

easily spread faults. The critical impactable branches determine the vulnerability of networks to some extent.

The small-world features of the sTSCGs indicate that most branches have close fault adjacent relationships; therefore, branches have cross susceptibility, which determines the development of fault propagation to some extent.

B. VULNERABILITY ANALYSIS

To demonstrate the effectiveness of the proposed identification approach, numerical tests were conducted on the IEEE 39-bus, IEEE118-bus system and French grid. Here, the proposed method was implemented in MATLAB.

We used the iTSCG and sTSCG to calculate the vertex degree, in-degree, and out-degree as statistical metrics to rank the impactable and susceptible features of branches. Figs. 8 and 9 show the degree of branches with the two features of the two IEEE systems, respectively. Due to space limitations, the other metrics (in-degree and out-degree) of two IEEE systems and the metrics of French grid are not given. The results indicate that some branches have high impactability but low susceptibility, e.g., branches 46 and 34 in the IEEE 39-bus system, and some branches have low impactability but high susceptibility, e.g., branches 24 and 36 in the same system. This confirms that it is necessary to distinguish the two features of branches in vulnerability analysis as this can identify branches with different properties during fault propagation. In addition, as shown in Figs. 8 and 9, we observe that the degree distribution of susceptibility is more uniform than that of impactability due to the small-world features of the iTSCGs.

Furthermore, to verify the real implication of the two features, we sequentially attacked each branch in the identified groups and quantified the severity of the attack via the system's remaining load and network efficiency from the perspective of network function and structure, respectively. The remaining load was calculated by DC OPF, and network efficiency was calculated using Equations (11) and (12). It is noted that the attacked branches are selected according to the rankings of the proposed method.

$$E'_x = \frac{E_x}{E_0} \times 100\% \tag{11}$$

$$E_x = \frac{1}{N_W N_D} \sum_{W_h \in \mathcal{W}} \sum_{D_e (W_h \neq D_e) \in \mathcal{D}} \frac{1}{X_x^{W_h D_e}} \tag{12}$$

Here, $\mathcal{W}$ is the set of nodes with generators, where $\mathcal{W} = \{\cdots, W_h, \cdots\}$ and $\dim\{\mathcal{W}\} = N_W$. $\mathcal{D}$ is the set of nodes with load, where $\mathcal{D} = \{\cdots, D_e, \cdots\}$ and $\dim\{\mathcal{D}\} = N_D$. $X_x^{W_h D_e}$ is the electrical shortest path [20] from generator W_h to load D_e under contingency x. E_0 and E_x represent network efficiency under normal operations and contingency x, respectively.

The simulation results with the IEEE 39-bus system, 118-bus system and French grid are shown in Fig. 10. For the load shedding in Fig. 10(a-c), it is clear that when attacking branches in the impactable branch group, the remaining load reduced quickly. This verifies that branches with high impactability more easily spread faults. In contrast, when we attack branches with high susceptibility sequentially, the load loss was small. Recall that, as susceptible branches have small-world features, they would mutually affect each other during fault propagation and increase its development, albeit with a small load loss.

For the network efficiency in Fig. 10(d-f), highly impactable and susceptible branches have significant impact on the network structure. Therefore, we infer that both types of branches can more easily split the entire network during fault propagation.

The relationships between the two TSCGs and fault propagation under deliberate attacks can be summarized as follows:

- iTSCGs demonstrate highly impactable branches that can easily spread a fault at high probability in an electrical network. The sTSCGs demonstrate that branches can be mutually affected during fault propagation or under deliberate attacks due to the close fault adjacent relationships. Therefore, both the scale-free properties of the iTSCGs and the small-world properties of the sTSCGs reveal the fault propagation mechanism.
- Highly impactable and susceptible branches can have significant impact on the network structure, which can easily lead to a network split.
- For the network function, when branches in an impactable branch group are attacked, the remaining load is reduced quickly, which can easily lead to deterioration of network functionality. However, a susceptible

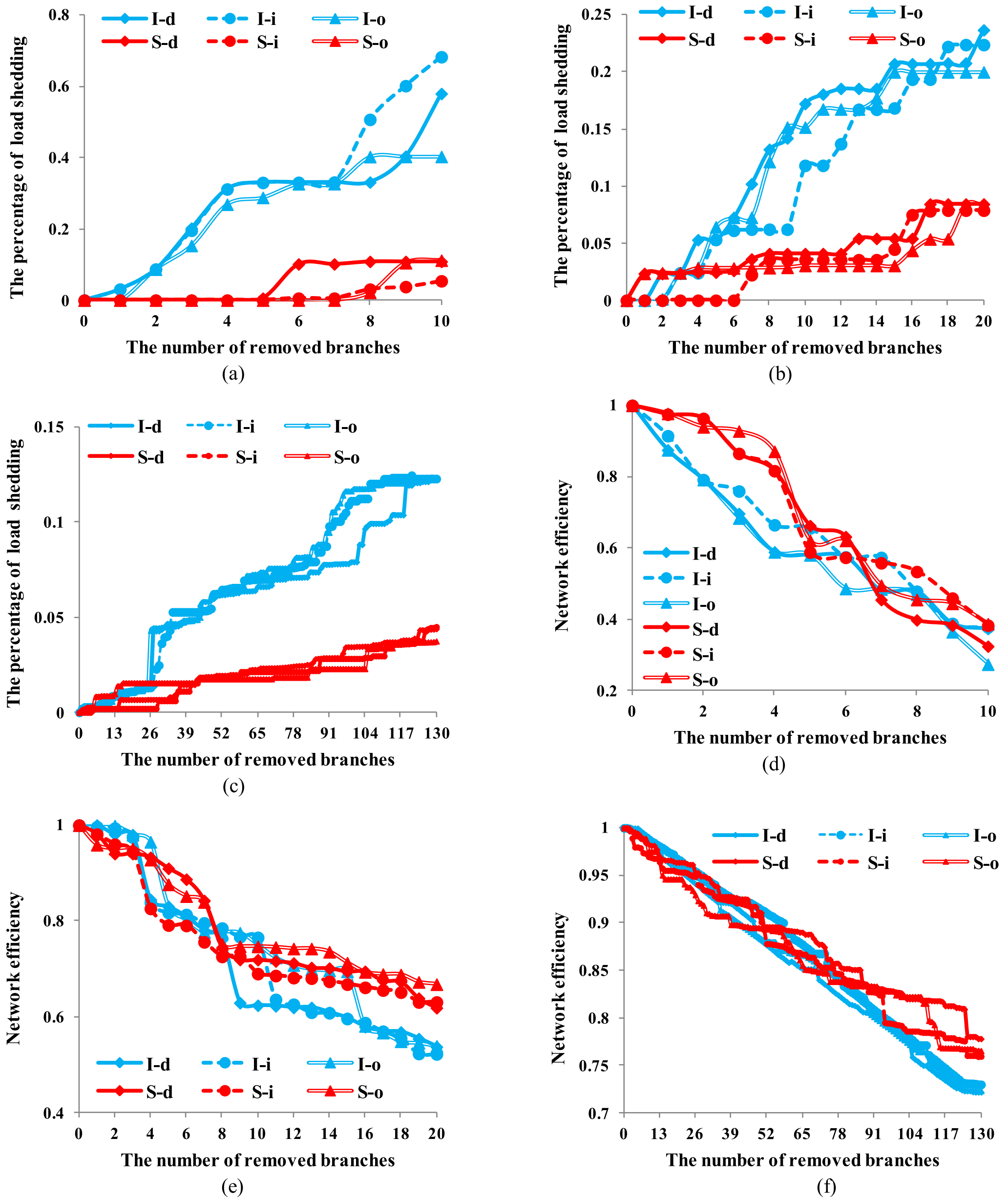


FIGURE 10. Load shedding and network efficiency after attacking branches ranked by indices of the two features for IEEE 39-bus system (a,d), 118-bus system (b,e), and French grid (d,f). I and S represent impactability and susceptibility, respectively, and d, I, and o represent degree, in-degree, and out-degree, respectively.

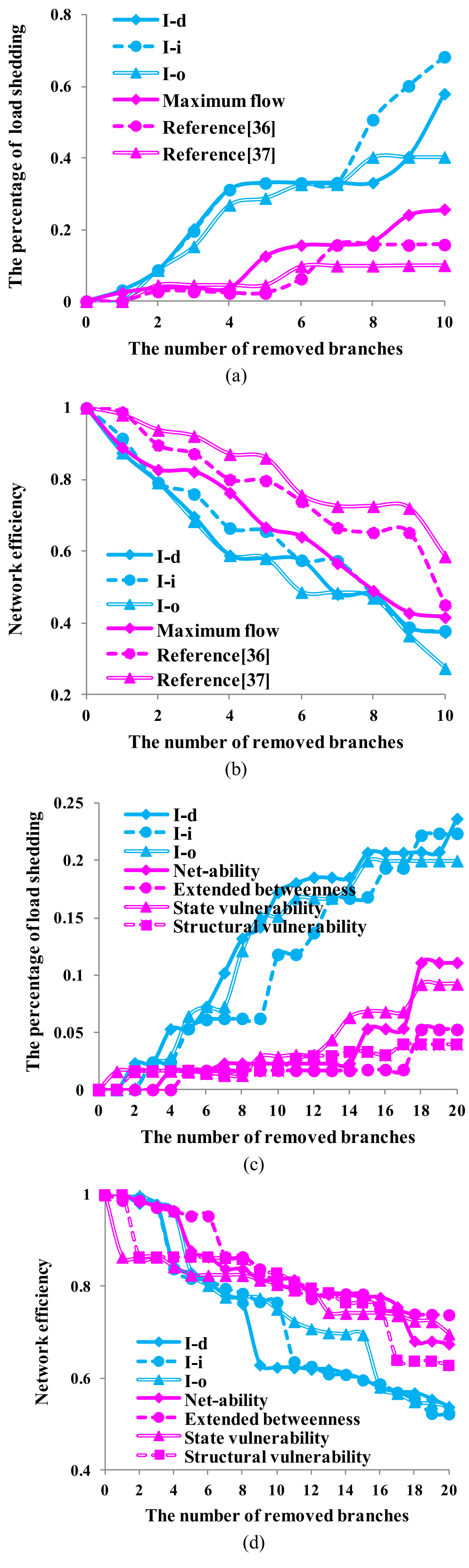
branch group has limited impact on load loss but contributes to faster development of fault propagation.

In addition, traditional complex network methods have studied the scale-free properties of power systems by correlating reduced system demand (or network efficiency) with removed branches. In contrast, this study has introduced the iTSCG to reveal such properties by translating the behaviors of the electrical network by considering its physical and operational rules in a relationship graph.

Furthermore, the small-world properties are conventionally verified only from the perspective of topological structures, which indicates that adjacent or non-adjacent branches can mutually affect each other under different contingencies. However, pure topological analysis cannot reflect the operational features. To overcome this issue, we employed sTSCGs to reveal such properties from a holistic perspective, including the structural, physical, and operational features of the grid.

C. COMPARISON WITH EXISTING METHODS

To verify the effectiveness of the proposed method, we compared the proposed impactability to the maximum flow method [17], [18] and the net-ability, extended betweenness, state vulnerability, and structural vulnerability



(a)

(b)

(c)

(d)

FIGURE 11. Load shedding and network efficiency after attacking branches ranked by the proposed method and reference methods for IEEE 39-bus (a,b) and 118-bus (c,d) systems.

TABLE 2. Performances of different methods.

Network	Methods	Load shedding	Network efficiency
IEEE 39-bus system	I-d	57.98%	37.34%
	I-i	68.30%	37.74%
	I-o	40.29%	27.32%
	Maximum flow	25.59%	41.57%
	Reference [36]	15.82%	45.01%
	Reference [37]	10.02%	58.51%
IEEE 118-bus system	I-d	23.67%	53.74%
	I-i	22.38%	52.24%
	I-o	19.99%	53.91%
	Net-ability	11.10%	67.48%
	Extended betweenness	5.25%	73.84%
	State vulnerability	9.22%	69.65%
	Structural vulnerability	3.94%	62.77%

(10 and 20 top branches are attacked in the 39- and 118-bus systems, respectively)

metrics using the IEEE 39-bus and IEEE 118-bus systems [22], [23], [36], [37]. These methods and metrics were chosen because 1) the rankings of critical branches are given and 2) the methods are proposed from different perspectives relative to vulnerability assessment, i.e., operational vulnerability [36], [37] and CNT-based structural vulnerability [17], [18], [22], [23].

As shown in Fig. 11, the remaining load and network efficiency after removing the branches identified by the proposed method are generally less than that of the compared methods, i.e., the gaps among different curves are already enlarged before reaching the largest number of the removed branches at the X-axe. For example, for the load shedding (Fig. 11(a, c)), after the removal of 3 and 5 branches respectively in the 29- and 118- bus systems, the gaps are already very clearly. Meanwhile, Tab. II shows that the performances of different methods after the removal of 10 and 20 top branches. In the table, our proposed methods are obviously better than compared methods. Therefore, the proposed method's ability to identify vulnerable branches is better than that of the compared methods from both topological and operational respects.

V. CONCLUSIONS

To explore operative vulnerability based on CNT, this paper has proposed two vulnerable features, i.e., the impactability and susceptibility of branches. Based on these features, iTSCGs and mTSCGs that comprehensively consider the topological, physical, and operational features of electrical networks were constructed. Furthermore, to replace the original electrical networks, the TSCGs were employed to indirectly assess electrical network vulnerability based on CNT. By analyzing the graph features, the iTSCGs and mTSCGs were found to represent scale-free and small-world networks, respectively, that reveal the fault propagation mechanism under deliberate attacks. Furthermore, statistical metrics were employed in the TSCGs to rank vulnerable branches, and the accuracy of the ranking results was verified via load shedding and network effectiveness.

APPENDIX

We give the proof of the boundedness:

$$
\begin{aligned}
&S'(\mathbb{X},\mathbb{Y})\\
&=\sum_{i=1}^{N}\left[\sqrt{X_iY_i}\ln\frac{2\sqrt{X_iY_i}}{X_i+Y_i}+\left(1-\sqrt{X_iY_i}\right)\ln\frac{2-2\sqrt{X_iY_i}}{2-(X_i+Y_i)}\right]\\
&=\sum_{p=1}^{N}\left[\sqrt{X_iY_i}\ln 2+\sqrt{X_iY_i}\ln\frac{\sqrt{X_iY_i}}{X_i+Y_i}\right.\\
&\quad\left.+\left(1-\sqrt{X_iY_i}\right)\ln 2+\left(1-\sqrt{X_iY_i}\right)\ln\frac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\right]
\end{aligned}
$$

where

(1) $\sqrt{X_iY_i}\ \ln\dfrac{\sqrt{X_iY_i}}{X_i+Y_i}\le 0$

$\because \dfrac{\sqrt{X_iY_i}}{X_i+Y_i}<1 \quad \therefore \ln\dfrac{\sqrt{X_iY_i}}{X_i+Y_i}<0$

thus $\sqrt{X_iY_i}\ \ln\dfrac{\sqrt{X_iY_i}}{X_i+Y_i}\le 0.$

(2) $\left(1-\sqrt{X_iY_i}\right)\ln\dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\le 0$

$\because X_i\in[0,1]$ and $Y_i\in[0,1]$

$\therefore 0\le 1-\sqrt{X_iY_i}\le 1$ and $0\le 2-(X_i+Y_i)\le 2$

$\therefore \dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\ge 0.$

Suppose $X_i\le Y_i$, we can obtain

$$\frac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\le\frac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}=\frac{1-X_i}{(1-X_i)+(1-Y_i)}\le 1.$$

Similarly, when $X_i>Y_i$, we have $\dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\le 1.$

In summary,

$0\le\dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\le 1$ (iff $X_i=Y_i=1,\ \dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}=0$)

thus $\ln\dfrac{1-\sqrt{X_iY_i}}{2-(X_i+Y_i)}\le 0.$

By (1) and (2), we have

$$
\begin{aligned}
S'(\mathbb{X},\mathbb{Y})&\le\sum_{i=1}^{N}\left[\sqrt{X_iY_i}\ln 2+\left(1-\sqrt{X_iY_i}\right)\ln 2\right]\\
&\le\sum_{i=1}^{N}\left[\sqrt{X_iY_i}+\left(1-\sqrt{X_iY_i}\right)\right]=N\Box
\end{aligned}
$$

REFERENCES

[1] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu , "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 65, no. 3, pp. 346–350, Mar. 2018.

[2] Z. Wang, G. Chen, D. J. Hill, and Z. Y. Dong, "A power flow based model for the analysis of vulnerability in power networks," *Phys. A, Stat. Mech. Appl.*, vol. 460, pp. 105–115, Oct. 2016.

[3] H. Tu, Y. Xia, H. H.-C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 66, no. 1, pp. 126–130, Jan. 2019.

[4] I. Dobson, B. A. Carreras, and V. E. Lynch, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos*, vol. 17, no. 2, Apr. 2007, Art. no. 026103.

[5] R. Rafael, S. Lumbreras, and A. Ramos, "Analysis of transmission-power-grid topology and scalability, the European case study," *Phys. A, Stat. Mech. Appl.*, vol. 509, pp. 383–395, Nov. 2018.

[6] T. Wang *et al.*, "Modeling fault propagation paths in power systems: A new framework based on event SNP systems with neurotransmitter concentration," *IEEE Access*, vol. 7, pp. 12798–12808, 2019.

[7] T. Cai, T. Liang, and A. Rakhlin, "On detection and structural reconstruction of small-world random networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 4, no. 3, pp. 165–176, Jul./Sep. 2007.

[8] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electr. Power Syst. Res.*, vol. 101, pp. 71–79, Aug. 2013.

[9] Y. Nan, L. Wenying, and G. Wei, "Study on scale-free characteristic on propagation of cascading failures in power grid," in *Proc. IEEE EnergyTech*, Clevelan, OH, USA, May 2011, pp. 1–5.

[10] X. Wei, S. Gao, T. Huang, T. Wang, and W. Fan, "Identification of two vulnerability features: A new framework for electrical networks based on the load redistribution mechanism of complex networks," *Complexity*, vol. 2019, Jan. 2019, Art. no. 3531209.

[11] Y. Xie, S. Chang, Z. Zhang, M. Zhang, and L. Yang, "Efficient sampling of complex network with modified random walk strategies," *Phys. A, Stat. Mech. Appl.*, vol. 492, pp. 57–64, Feb. 2018.

[12] J. Wang, C. Ma, C. Li, X. Zhu, and K. Zhao, "Topology modeling and vulnerability analysis of China mine power grid based on complex network theory," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 10, pp. 79–88, Oct. 2016.

[13] Y. Li *et al.*, "Hierarchical decomposition for betweenness centrality measure of complex networks," *Sci. Rep.*, vol. 7, Apr. 2017, Art. no. 46491.

[14] Y. 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, Mar. 2016.

[15] E. I. Bilis, W. Kroger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Syst. J.*, vol. 7, no. 4, pp. 854–865, Dec. 2013.

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

[17] 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.

[18] A. Dwivedi, X. Yu, and P. Sokolowski, "Analyzing power network vulnerability with maximum flow based centrality approach," in *Proc. 8th Int. Conf. Ind. Inform.*, Osaka, Japan, Jul. 2010, pp. 336–341.

[19] 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.

[20] H. Bai and S. Miao, "Hybrid flow betweenness approach for identification of vulnerable line in power system," *IET Generat., Transmiss. Distrib.*, vol. 9, no. 12, pp. 1324–1331, Jan. 2015.

[21] 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, Statist. Mech. Appl.*, vol. 390, nos. 23–24, pp. 4692–4701, Nov. 2011.

[22] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electr. Power Syst. Res.*, vol. 81, no. 7, pp. 1334–1340, Jul. 2011.

[23] V. Rosato, S. Bologna, and F. Tiriticco, "Topological properties of high-voltage electrical transmission networks," *Electr. Power Syst. Res.*, vol. 77, no. 2, pp. 99–105, Feb. 2007.

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

[25] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2995–3000, May 2018.

[26] 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. 2016.

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

[28] C. Ren, Y. Xu, and Y. Zhang, "Post-disturbance transient stability assessment of power systems towards optimal accuracy-speed tradeoff," *Protection Control Power Syst.*, vol. 3, no. 3, p. 19, 2018.

[29] L. Fei and Y. Deng, "A new method to identify influential nodes based on relative entropy," *Chaos, Solitons Fractals*, vol. 104, pp. 257–267, Nov. 2017.

[30] A. Wang, Y. Luo, G. Tu, and P. Liu, "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 442–450, Feb. 2011.

[31] T. Huang, S. L. Voronca, A. A. Purcarea, A. Estebsari, and E. Bompard, "Analysis of chain of events in major historic power outages," *Adv. Elect. Comput. Eng.*, vol. 14, no. 3, pp. 63–70, Aug. 2014.

[32] Q. Sun, L. Shi, Y. Ni, D. Si, and J. Zhu, "An enhanced cascading failure model integrating data mining technique," *Protection Control Mod. Power Syst.*, vol. 2, no. 1, p. 5, 2017.

[33] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids," *Nature Commun.*, vol. 9, p. 1975, May 2018.

[34] M. J. Eppstein and P. D. H. Hines, "A 'Random Chemistry' algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[35] C. Tong, J. W. Niu, G. Z. Qu, X. Long, and X. P. Gao, "Complex networks properties analysis for mobile ad hoc networks," *IET Commun.*, vol. 6, no. 4, pp. 370–380, 2012.

[36] M. Tasdighi and M. Kezunovic, "Impact analysis of network topology change on transmission distance relay settings," *Power Energy Soc. Gen. Meeting*, Jul. 2015, pp. 1–5.

[37] B. Jin, X. Xiao, and J. Chen, "A method of risk assessment considering protection failures and dynamic equilibrium of power grid," *Power Syst. Protection Control*, vol. 44, no. 8, pp. 1–7, Apr. 2016.

XIAOGUANG WEI is currently pursuing the Ph.D. degree in electrical engineering with the Southwest Jiaotong University, Chengdu, China. His research interests include power system vulnerability assessment, the energy Internet, and complex network theory.

SHIBIN GAO received the Ph.D. degree from Southwest Jiaotong University, Chengdu, China, where he has been a Professor with the Department of Electrical Engineering, since 1998. His research interests include power system protection and automation, online monitoring of electrical equipment, rail transit traction power supply system security, and power system vulnerability assessment.

TAO HUANG (M'18) received the Ph.D. degree from the Politecnico di Torino, Turin, Italy. He is currently a Researcher and a Professor with the Department of Energy, Politecnico di Torino, and Xihua University, China, respectively. His research interests include critical infrastructure protection, vulnerability assessment, electricity markets, and smart grids.

TAO WANG received the Ph.D. degree from Southwest Jiaotong University, Chengdu. She is currently with Xihua University, Chengdu. Her research interests include membrane computing, electric power system fault diagnosis, and soft computing.

TIANLEI ZANG received the Ph.D. degree from Southwest Jiaotong University, Chengdu. He held a postdoctoral position with Tsinghua University, Chengdu. His research interests include energy Internet, vulnerability, and resilience assessment.