Computers and Electrical Engineering 81 (2020) 106519

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Analysis of electrical network vulnerability using segmented cascading faults graph ☆

Xiaoguang Wei [a], Shibin Gao [a,*], Tao Huang [b]

[a] School of Electrical Engineering, Southwest Jiaotong University, China
[b] Department of Energy, Politecnico di Torino, Italy

ARTICLE INFO

Article history:
Received 28 September 2018
Revised 21 November 2019
Accepted 21 November 2019
Available online 2 December 2019

Keywords:
Vulnerability indices
Transmission network vulnerability
Fault chain
Cascading fault graph

ABSTRACT

To reveal the mechanism of fault propagation and temporal information between electrical network branches intuitively and vividly, we have proposed a fault chain-based cascading fault graph (CFG) that considers the topological, physical, and fault operational features from an overload mechanism perspective. The proposed CFG is used to construct metrics to identify vulnerable branches of an electrical network. Furthermore, because the vulnerable branch rankings change with the changing fault chain length, the ranking results' change rules are investigated. As a result, the branch vulnerabilities' characteristics are found to be different at different stages under sequential attacks. Inspired by the characteristics, the CFGs are divided into three sub-CFGs, based on load shedding threshold, to identify the vulnerable branches at different stages. The proposed method is used to identify the vulnerable branches of the IEEE 39- and 118-bus systems, and its effectiveness is validated by investigating load shedding of the systems under deliberate attacks.

1. Introduction

Transmission network vulnerability (TNV) assessment is important to power system security because it helps identify critical components to safeguard them against accidents or malicious threats [1–3]. Due to the increasing scale of electrical networks, and developing data-processing technology such as cloud computing, complex network theory is one of the main methods used to analyze the power system's cascading blackout mechanism [4,5]. From a complex network theory perspective, by investigating the electrical networks' topological structures, many existing studies have confirmed many electrical networks are small-world graphs [6,7]. The small-world features of the topological structures demonstrate that a branch can easily propagate a fault to other branches, including non-adjacent branches; therefore, small-world features reveal the fault propagation mechanism to some extent. In addition, by removing network branches to investigate the extent of structural damage or function loss of the systems, some authors also discovered that electrical networks have scale-free features [8,9]. The scale-free features demonstrate there are few critical branches in the networks. The systems are vulnerable once the critical branches are attacked deliberately, but the systems are robust under random attacks.

A popular way to identify critical branches is to construct statistical indices based on complex network theory. First, an electrical network can be abstracted as a topological graph. The electrical network's bus nodes can be viewed as

☆ This paper is for CAEE regular issues. Reviews processed and approved for publication by the Editor-in-Chief.

* Corresponding author.
E-mail address: gao_shi_bin@126.com (S. Gao).

https://doi.org/10.1016/j.compeleceng.2019.106519
0045-7906/

Nomenclature

L	set of branches (i.e. branches, transformers) in a transmission network, L=$\{\cdots, L_j, \cdots\}$, dim $\{L\} = N_L$.
B	set of vertexes (i.e. buses) in a transmission network, dim $\{B\} = N_B$.
L^i	set of branches in fault chain i, $L^i = \{\cdots, L^i_j, \cdots\}$, $L^i \subseteq L$, dim $\{L^i\} = n^i$.
$\mathbf{C}^i$	fault chain i, $\mathbf{C}^i = (L^i, n^i, \Lambda^i)$.
α^i_j	loading assessment index of branch j in fault chain i generation process, $L_j \in L$.
f^0_j	power flow of branch j under normal operation, $L_j \in L$.
f^i_{jx}	power flow of branch j during contingency x in fault chain i generation process, $L_j \in L$.
f^M_j	flow limit of branch j, $L_j \in L$.
P^i_{dx}	active power withdraws of load bus during contingency x in fault chain i generation process, $d \in B$.
δ^i_x	load shedding percentage during contingency x in fault chain i generation process.
Λ^i	total load shedding of fault chain i.
Δ	threshold for total load shedding.
T^i	contingency set in fault chain i generation process, $T^i = \{L_j\}$, dim $\{T^i\} = 1 \vee 0$, $L_j \in L$.
V	set of vertices in a graph, dim $\{V\} = N_L$.
E	set of edges in a graph, dim $\{E\} = N_q$.
G	a cascading faults graph, $G = \{V, E\}$.
$F(\bullet)$	mapping function to convert a fault chain $\mathbf{C}^i$ into a graph g^i, i.e., $g^i = F(\mathbf{C}^i)$, $g^i \subseteq G$.
V^i	set of vertexes in g^i, $V^i = \{\cdots, L^i_j, \cdots\}$, dim $\{V^i\} = n^i$, $V^i = L^i$.
E^i	set of edges in g^i, $E^i = \{\cdots, e^i_q, \cdots\}$, e^i_q=$L^i_j L^i_{j+1}$, $q = j$, dim $\{E^i\} = n^i - 1$.
α_q	weight of edge e_q in cascading faults graph G, $e_q \in G$.
l	number of considered branches in graph variation operation.
r^i	relative position of targeted vertex of edge e' in g^i.
β	adjustable parameter, $\beta \geq 0$.
ξ_{vz}	number of the same branches in the zth ranking by employing different G.
ξ	threshold value.
K	number of top critical branches.

topological graph vertices, while the branches can be viewed as the edges. Second, statistical indices, based on the graph, are constructed to assess the TNV. In previous research, pure statistical metrics based on complex network theories, such as average path length [10], betweenness [11], centroid [12], and degree [13] were used to assess the TNV. Some of them have been applied to practical power grids, such as the European power grid [10] and the North American power grid [14]. However, pure statistical metrics neglect physical features and cannot capture some actual information from the power grids [15].

To overcome this problem, extended statistical indices are proposed, which involves integrating electrical quantities with complex network theory [16–20]. Its core idea is that electrical quantities are used to define the weights or direction of the edges (or vertices) of the topological graph. Then, the extended statistical indices, via the weighted (or directed) topological graph, are constructed [17]. For instance, in reference [18], the electrical betweenness is redefined by introducing electrical distance. Because the actual flow path is a critical attribute of power grids, it is employed in hybrid flow betweenness used to identify vulnerable electrical network branches [19]. In reference [20], the maximum flow from the generator nodes was integrated into the load nodes with centrality to evaluate the TNV. Although the extended statistical indices can reveal some of the electrical networks' physical features, they still focus mainly on topological features and do not consider operational characteristics [21,22], especially fault operational characteristics.

For full consideration of the topological, physical, and operational features of the electrical network, we propose a cascading fault graph (CFG) based on fault chain theory. Compared to the topological graph, in our proposed method, the electrical network is mapped to an operational graph by constructing the fault chains. The operational graph can reveal not only the fault propagation mechanism, but also the temporal fault relations among branches. On this basis, the statistical indices based on complex network theory, via the operational graph, are constructed to assess the TNV.

In our previous papers [23–25], we introduced the CFG generation algorithm. We analyzed the CFGs' model properties and constancy of the corresponding properties in detail. The result indicates that CFGs are scale-free graphs. Different CFGs' scale-free characteristics, constructed using fault chains with different length or threshold for load shedding percentage in a given electrical network, are stable. However, when we used the statistical indices (vertex degree, in-degree or out-degree) of the different CFGs to rank critical branches, the critical branch ranks were different. That is, the CFGs ranking results were unstable; this is called metric instability. Compared to our previous paper, the contributions of this paper are as follows:

(1) To reveal the reasons for metric instability, we investigated the change rules of the rankings of branches according to different CFGs. Further, we analyzed the relationships between the metric instability and the relative position of branches in fault chains by introducing an adjustable parameter to improve the fault chains' weights.
(2) Inspired by metric instability reasons, we propose segmented CFGs by dividing a CFG into three sub-CFGs, based on the load shedding threshold, to identify valuable branches of different stages, after which we employed IEEE 39- and 118- bus systems to verify the proposed method's effectiveness.

In addition, for the sake of the paper's integrity, the CFG generation method was introduced succinctly. The remaining part of the paper is organized as follows. Section 2 introduces the CFGs development method. The reasons for metric instability of CFGs are analyzed in section 3. Furthermore, segmented CFGs proposed to evaluate the TNV are discussed in Section 4. Finally, further discussions and conclusions are presented in Section 5.

2. CFGs development method

2.1. Fault chain generation

Generation ideas: In this paper, we construct the fault chain [26] from a sequential attack perspective [27]. To explain our ideas clearly, suppose we take a cup of water, as shown in Fig. 1. The cup represents an electrical network's topological structure. In Fig. 1(a), the water in the cup represents the operational status. The height of the water represents the corresponding optimal operating point. If the cup has a flaw "A," as shown in Fig. 1(b), the cup will turn and the optimal operating point will change. That is, when one branch is attacked from the electrical network, the operational status of the network will change until a new optimal operational point from normal operation to contingency 1 is reached. In contingency 1, suppose there are two potential flaws, "B" and "C". If "C" can cause more damage to the network's operational status than "B," which leads to the lower optimal operational point, then "C" will be selected in contingency 2, shown in Fig. 1(c). In analogy to the electrical network under the sequential attacks, we attempt to remove the targeted branch, which causes maximum damage to the network's operational status in the next contingency. Therefore, a fault chain can be viewed as a set of branches, as shown in Fig. 2, that can cause maximum damage to the operational status of the network in the different contingency.

Generation method: We employed a load shedding technique to the network to measure the degree of damage to the network's operational status. DC OPF is employed to calculate the load shedding percentage (LSP) as an objective function. The LSP is defined as

$$\delta_x^i = 1 - \frac{\sum_{d\in B_z} P_x^i}{\sum_{d\in B_z} P_{(x-1)}^i} \tag{1}$$

$$\Lambda^i = \sum_{x\in \mathbf{C}^i} \delta_x^i \tag{2}$$

This definition which is similar to that in [28,4], is the normalized load shedding, which implies $0 \le \Delta \le 1$. The larger the value of Λ^i, the larger the blackout scale. To mark the end of the fault chain, we define a threshold Δ. When $\Lambda^i \ge \Delta$, we terminate the fault chains generation process.

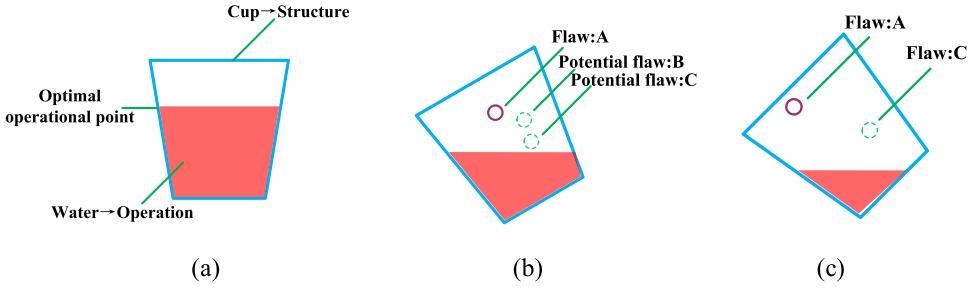


Fig. 1. Explanation of fault chain generation method. (a):Normal operation; (b) Contingency 1; (c) Contingency 2.

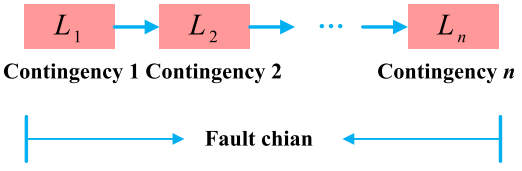


Fig. 2. Logic diagram of a fault chain.

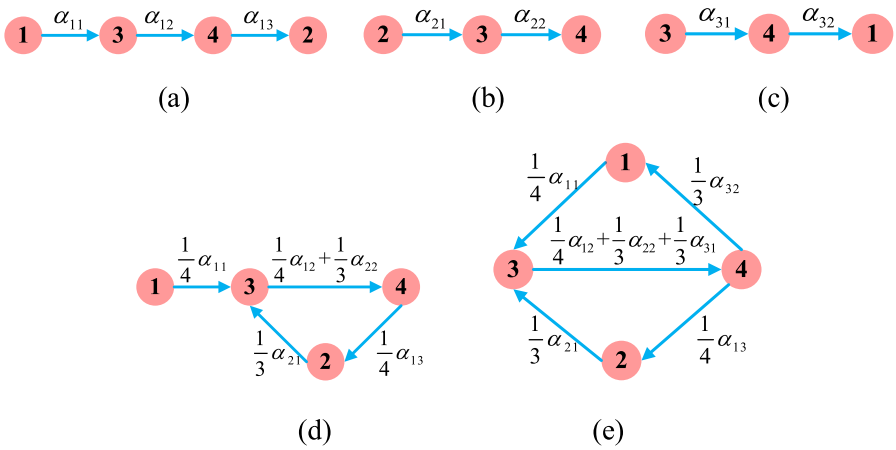


Fig. 3. A demonstration of CFG construction. (a), (b), (d) are the fault chains; (c) was obtained by merging (a) and (b); (e) was obtained by merging (c), and (d).

In an electrical network with N_L branches, when an initially targeted branch is given, we need to remove N_L-1 branches respectively by calculating the DC OPF to research the targeted branches in the next contingency. Therefore, for a fault chain with n^ibranches, we need to calculate the DC OPF for $(NL - n^i + 1)^{n^i}$ times. With the increasing N_L, the calculation time will increase exponentially, thus leading to high time complexity. Therefore, to reduce the complexity, a branch loading assessment index (BLAI) was constructed to search the targeted branches. When a branch fails in an electrical network, the transmitted power will be redistributed over the network, which can cause increased power flow over other branches and could even lead to overload. Therefore, BLAI can be calculated to reflect the load burden of a branch and its possibility to fail under current contingency as follow:

$$\alpha_j^i = \frac{f_{jx}^i - f_j^0}{f_j^M} \exp\left(\frac{f_{jx}^i - f_j^M}{f_j^M}\right) \tag{3}$$

The bigger the value of α_j^i, the higher the vulnerability of branch j. $(f_{jx}^i - f_j^0)/f_j^M$ reflects the power flow deviation in different situations. The exponential term $\exp((f_{jx}^i - f_j^M)/f_j^M)$ describes the possibility of branch j overload.

According to the above definition, a fault chain i can be briefly represented as

$$\mathbf{C}^i = \left(L^i, n^i, \Lambda^i\right) \tag{4}$$

2.2. Cascading fault graphs

To study the CFG topology, a fault chain $\mathbf{C}^i$ into a directed and weighted graph $g^i = \{V^i, E^i\}$, i.e., $g^i = F(\mathbf{C}^i)$, where V^i is the set of vertices (i.e., $V^i = \{L_j^i | j = 1, 2, \ldots, n\}$) and E^i is the set of edges (i.e., $E^i = \{e_j^i | e_j^i = L_j^i L_{j+1}^i, j = 1, 2, \ldots, n-1\}$).

For a CFG formed by m fault chains g^1,g^2,..., g^m, the CFG is then represented as

$$G = \left\{(V, E) | V = V^1 \cup V^2 \cup \cdots \cup V^m, E = E^1 \cup E^2 \cup \cdots \cup E^m\right\} \tag{5}$$

For an edge e_q whose weights are α^i in $g^i (i = 1, 2, \ldots, h, h \le m)$, its weight in the CFG is given as

$$\alpha_q = \sum_{i=1}^{h} \frac{1}{n^i} \alpha^i \tag{6}$$

Based on the CFG generation method, we employed an IEEE 39-bus system as an example to construct the CFG shown in Fig. 4.

For a specific electrical network, construction of CFG includes the following steps.

Step 1: Capture the N_L fault chains based on each branch as a starting point. Suppose a fault chain of the electric network is {1, 3, 4, 2} and 1,3,4,2 are the number of branches. First, add directed edges to the nodes (i.e., branches), that is, $1 \to 3 \to 4 \to 2$. Secondly, assign weight to each edge. For each edge, take the LVAI of its starting node as the weight. Figs. 3(a), (b), and (d) demonstrate examples of fault chains.

Step 2: Merge all fault chains to generate the CFG. Three fault chains are given in Fig. 3(a)–(c) respectively. First, put all nodes in the three fault chains into a new CFG and merge the repeated nodes. Second, put all edges in all fault chains into the new CFG. For the repeated edges, merge them and employ Eq. (6) to calculate the new weight. For

non-repeated edges, you only need to calculate their weights using Equation 6 as their new weights. Figs. 3(c) and (e) show the results of merging fault chains or CFG. Fig. 3(c) was captured by merging Fig. 3(a) and(b). Fig. 3(e) was captured by merging Fig. 3(c) and (d).

In the CFG, we employ the degree, in-degree and out-degree as the vulnerable metrics to identify the vulnerable branches. For example, in Fig. 3(e), the degree, in-degree, and out-degree of node 1 are $\alpha_{32}/3+\alpha_{11}/4$, $\alpha_{32}/3$, and $\alpha_{11}/4$, respectively. In these metrics, a branch with high in-degree can be easily affected by a fault, while a branch with high out-degree can easily spread a fault to other branches. Therefore, it is necessary to distinguish between the two metrics to refine the vulnerability assessment.

3. Analysis of Metric instability of CFGs

In the previous paper, we revealed that CFGs are scale-free graphs and have stable properties when the length of fault chains change. However, the critical branches' ranking results are unstable (i.e., metric instability) under different conditions. In this section, we examine the reasons for metric instability using two test benchmarks: IEEE 39- and 118- bus systems. Brief descriptions of the two test benchmarks are given in Table 1 and Fig. 4.

We consider two conditional variants:

(a) **Threshold for LSP of fault chains:** For IEEE 39-bus system, we change Δ from 20% to 60% with a 5% interval. Similarly, for the IEEE 118-bus system, the threshold Δ was set from 10% to 30% and the 5% interval was changed.
(b) **Length of fault chains:** For each $g^i = F(\mathbf{C}^i)$, we only use the first l branches in $\mathbf{C}^i$ and disregard the rest, i.e., $\mathbf{C}^i = \{L^i_l, l, \Lambda^i_l\}$, $L^i_l = \{L_j | j = 1, 2, \ldots, l\}$. In this way, we can obtain a new CFG. For the IEEE 39-bus system, we chose l from 3 to 9 with an interval of 1. For IEEE 118-bus system, l was chosen from 3 to 30 with an interval of 1.

Both methods mentioned above change the fault chains' lengths, either directly or indirectly. However, the change caused by the latter results in equal length for each fault chain. In the case of the former, the opposite is the case.

3.1. Ranking of critical branches based on CFGs

We employ CFGs to rank the branches' vulnerability according to the vertex degree, in-degree, and out-degree. Using two test benchmarks, we observed that, for different CFGs under different l or Δ, the critical branches' ranking results have some differences, especially in the case of the IEEE 118-bus system. To find out the reason, we analyze the ranking result changes of a single branch with l or Δ increasing. Because of the large number of branches, we can only select some branches randomly to analyze their change characteristics. Fig. 4 shows that the branches' rankings have obvious change regularities for both test benchmarks, especially in the case of IEEE 118-bus system with increasing l. Due to space limitation, the change regularities with increasing Δ are not given. The change regularities have three main types with l or Δ increasing.

(a) The rankings of some branches, such as branch 13 in Fig. 4(a), branch 26 in Fig. 4(b), and branch 90 in Fig. 5(d) showed a gradual upward trend.
(b) Some branch rankings showed a gradual downward trend; examples are branch 41 in Fig. 5(c) and branch 105 in Fig. 5(d, f).
(c) Some branch rankings increased (or decreased) first and then decreased (or increased); examples are branch 18 in Fig. 5(d), branch 67 in Fig. c 5(e), and branch 149 in Fig. 5(f).

The simulation analysis result shows that the CFGs' metric constancy was unstable, i.e., the rankings of vertex degree, in-degree, and out-degree had significant differences when CFGs were generated by fault chains with different l or Δ. The reason is that, as l or Δ increases, the number of attacked branches increases; this causes the values of metrics of later attacked branches to increase.

3.2. Ranking of critical branches based on improved CFGs

In line with the above analysis, the CFGs' metric constancy is unstable. To make the metric stable, for a fault chain $\mathbf{C}^i$, $\mathbf{C}^i = (L^i, n^i, \Lambda^i)$and two branches $L^i_{j1} \in L^i$ and $L^i_{j2} \in L^i$, in sequential attacks, if L^i_{j1} is removed earlier than L^i_{j2} (the

Table 1
Description of test benchmarks N_B, N_W and N_L represent the number of buses, generations, and branches.

Test benchmarks	N_B	N_W	N_L
IEEE 39- bus system	39	10	46
IEEE 118-bus system	118	54	186

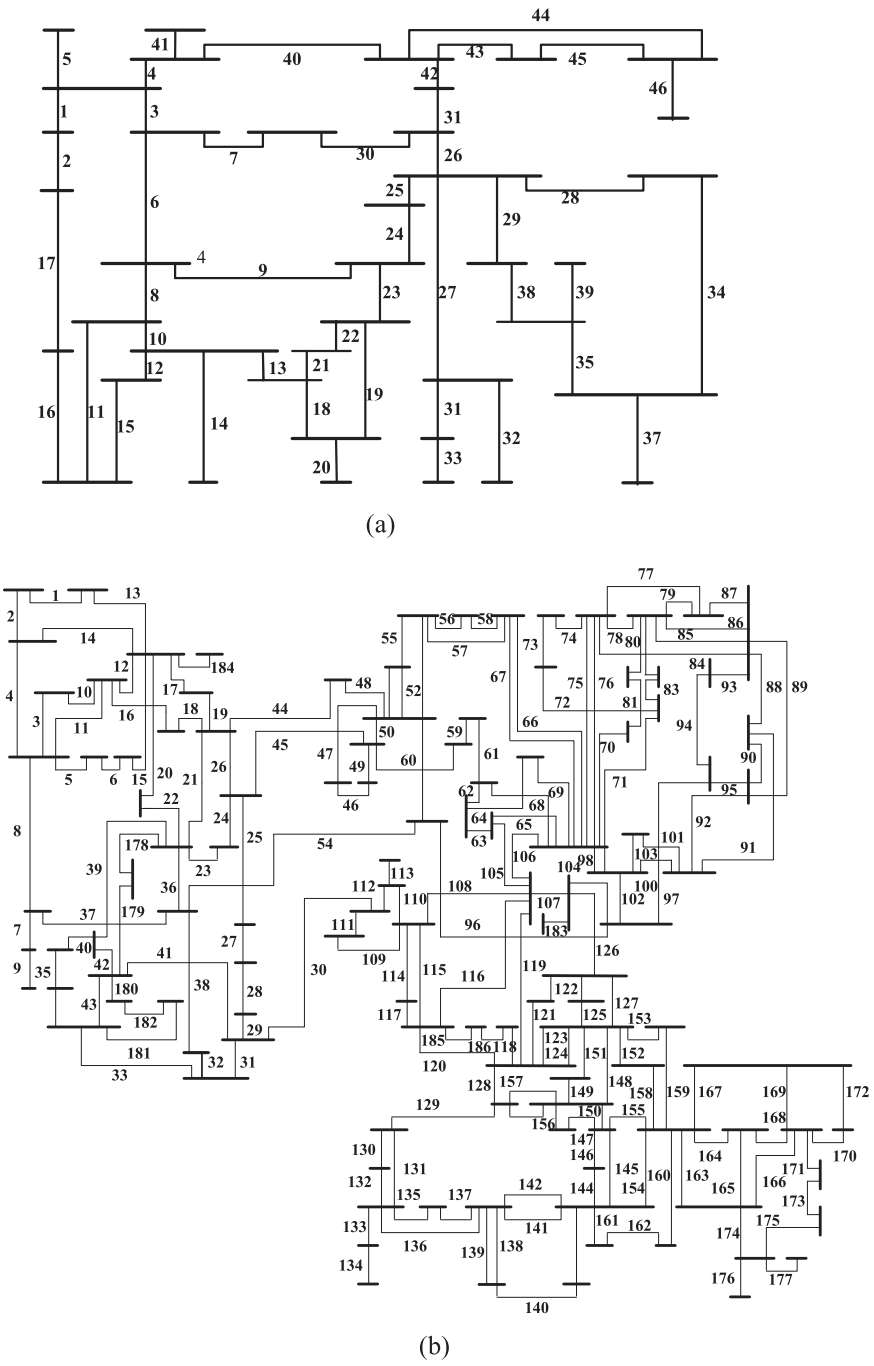


Fig. 4. ID number of branches of two IEEE systems. (a) IEEE 39-bus system; (b) IEEE 118-bus system

position of L_{j1}^{i} in $\mathbf{C}^{i}$ is more forward than L_{j2}^{i}), we give L_{j1}^{i} a larger weight than L_{j2}^{i}. Therefore, Eq. (6) can be improved as follows.

$$f\left(r^{i}\right)=\left(\frac{1}{r^{i}}\right)^{\beta} \tag{7}$$

$$\alpha_{e'}=\sum_{i=1}^{h}\frac{1}{n^{i}}\alpha^{i}f\left(r^{i}\right) \tag{8}$$

where $\beta > 0$ is an adjustable parameter that controls the proportion of the weights in Eq. (8). When β is greater, the branch with a more front position in $\mathbf{C}^{i}$ has greater $\alpha_{e'}$. Due to the positive correlation between $\alpha_{e'}$ and vulnerability, that

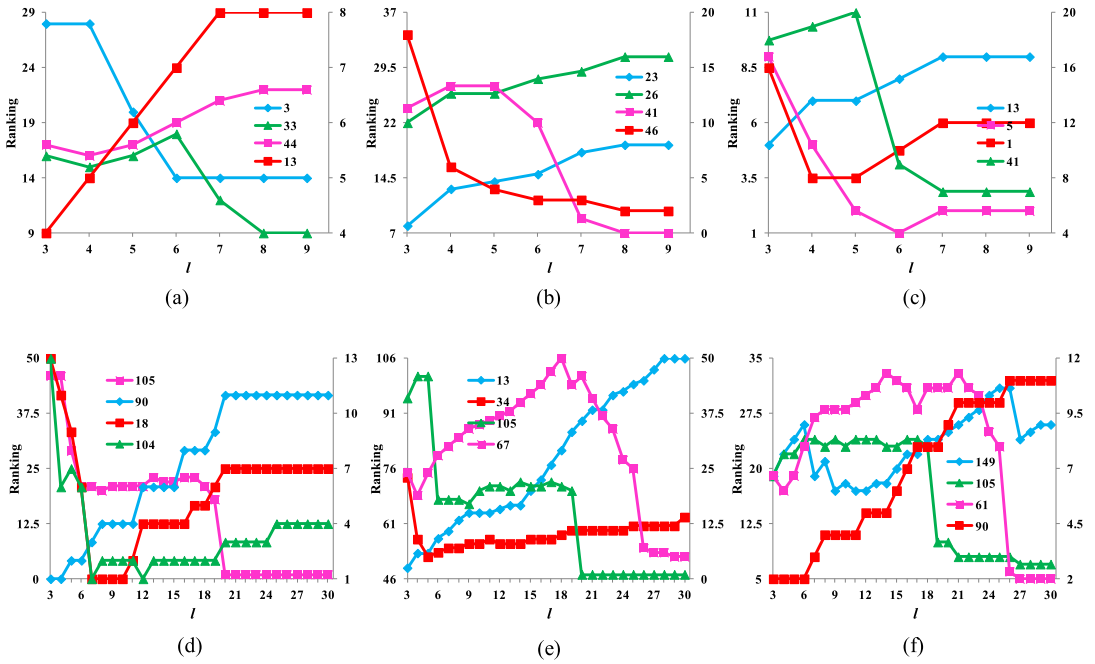


Fig. 5. Change regularities of ranking of branches with l increasing. (a-c): IEEE 39-bus system and (d–f): IEEE 118-bus system. (a, d): Degree, (b, e): In-degree and (c, f): Out-degree.

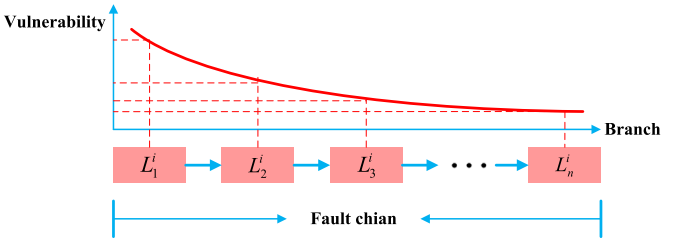


Fig. 6. The relationship between relative position and vulnerability of branches in a fault chain

the branch with a more front position should be more vulnerable than other branches, as shown in Fig. 6. Hence, we can improve the metric constancy of CFGs.

Furthermore, we analyzed the impacts of β on branches' vulnerability using the IEEE 39- and 118- bus systems. We investigated the outage size by sequentially attacking critical branches. For the IEEE 39-bus system, we removed the top 11 critical branches ranked by metrics, as shown in Fig. 7. For the IEEE 118-bus system, we removed the top 10 and 20 critical branches, respectively, as shown in Fig. 8. In these figures, we show the percent of the remaining load as a function of removed critical branches. In two test benchmarks, with β increasing, the percent of remaining load showed an upward trend at first and then became relatively stable. In addition, when $\beta \in [0, 1]$, the remaining load was less; this led to more outage size than $\beta \in [1, 10]$. It shows that, with β increasing, a targeted branch with a more front position, leading to a higher ranking is not necessarily more vulnerable to attacks.

Based on the foregoing, although adding the importance of relative positions of branches to the weight of edges in CFGs can improve their metric constancy, the accuracy of ranking results reduces when investigating the remaining load. With an increase in β, the branches with higher rankings in improved CFGs are less vulnerable than other branches. Therefore, how to choose β is an important issue in making sure the CFG metrics not only have good constancy but also to ensure the accuracy of identification of critical branches.

4. Vulnerability assessment based on segmented CFGs

4.1. Segmented CFGs

We revealed the reason for metric instability in Section 3. Meanwhile, we found that the branch with a more frontal position in fault chains was not necessarily more vulnerable than other branches. It shows that, in sequential attacks, a branch

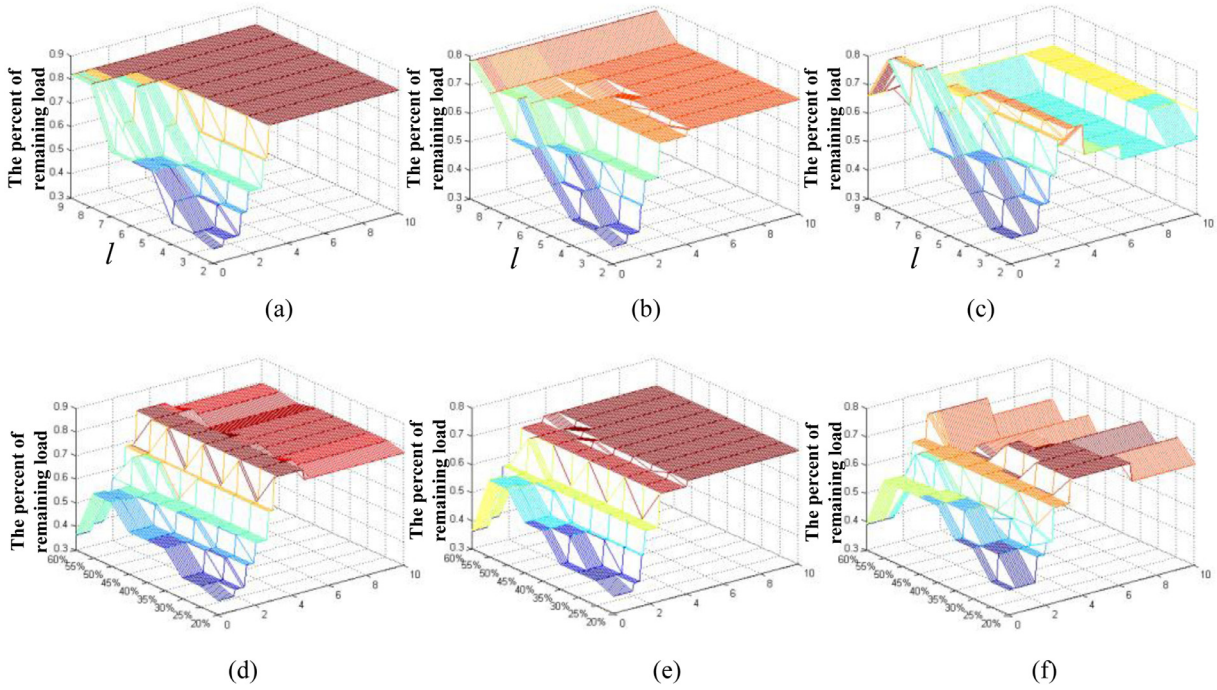


Fig. 7. Percentage of the remaining load in IEEE 39-bus system when removing the top 10 critical branches. (a), (b), and (c) are the removing branches. They are ranked by degree, in-degree, and out-degree under different l, respectively. (d), (e), and (f) are the removing branches. They are ranked by degree, in-degree, and out-degree under different Δ of the fault chains, respectively. Δ

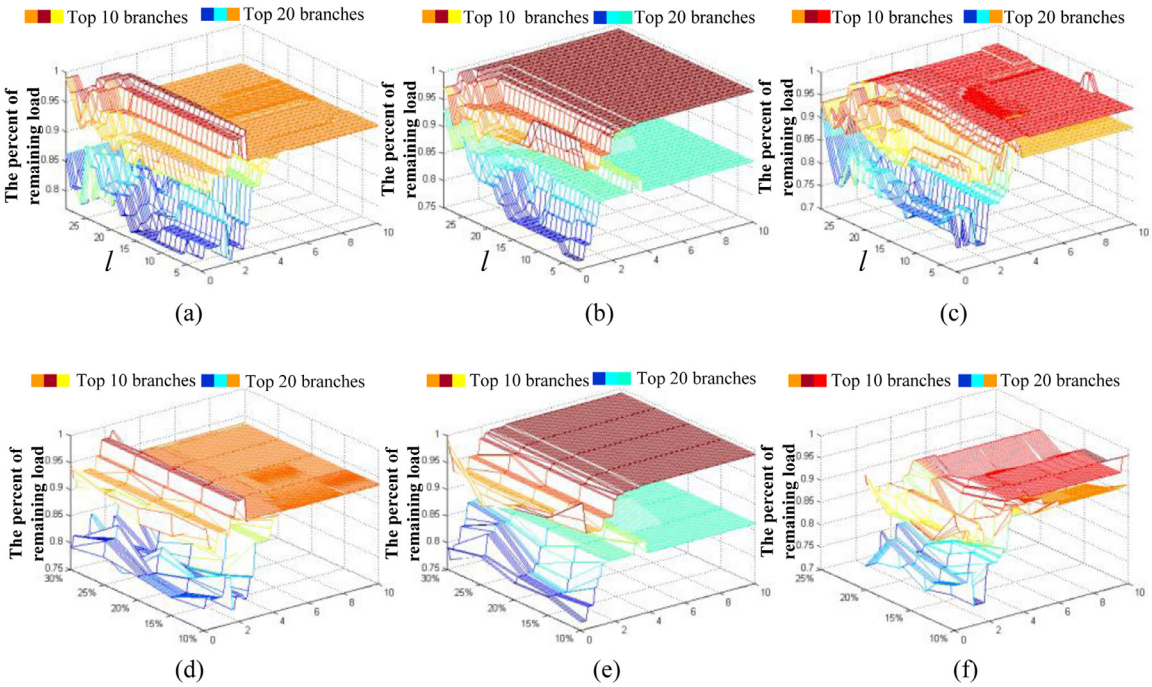


Fig. 8. Percentage of remaining load in IEEE 118-bus system when removing top 10 and 20 critical lines. (a), (b) and (c) are the removing lines ranked by degree, in-degree and out-degree under the different l of fault chains, respectively. (d), (e) and (f) are the removing lines ranked by degree, in-degree, and out-degree under the different Δ of fault chains, respectively.

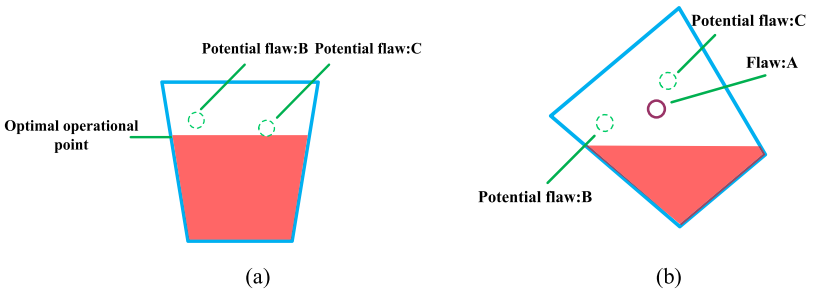
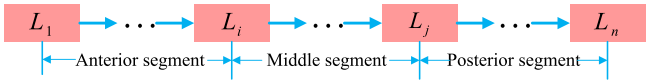


Fig. 9. An example to explain the different vulnerabilities in different time points. (a) Normal operation; (b) Contingency 1.



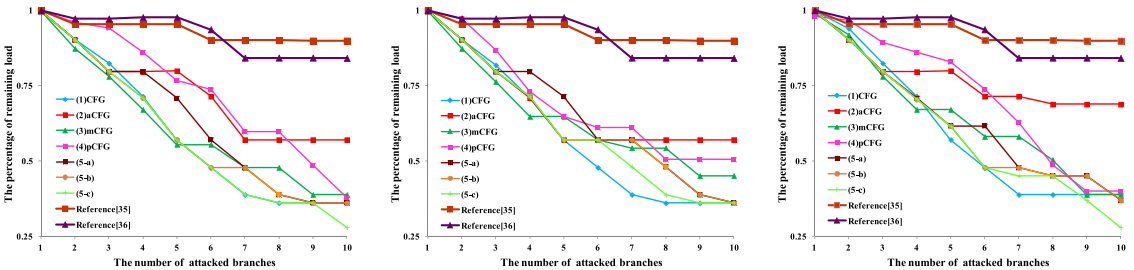


Fig. 10. Segmented fault chains. Percentage of the remaining load on IEEE 39-bus system with the number of critical branches increasing.

Table 2
Top 10 critical branches of IEEE 39-bus system based on different periods of cascading faults.

Rank	aCFG			mCFG			pCFG		
	D	InD	OutD	D	InD	OutD	D	InD	OutD
1	27	27	27	5	39	46	41	33	41
2	20	20	20	46	5	5	33	13	39
3	37	37	37	39	46	37	13	34	33
4	13	5	13	37	37	20	34	41	46
5	9	46	9	20	42	7	39	4	34
6	46	13	46	7	41	27	4	39	4
7	5	9	25	27	7	33	46	37	31
8	4	1	4	42	27	21	31	46	5
9	1	4	6	41	20	39	5	14	16
10	6	6	38	21	21	4	37	15	17

attacked at a different time points has different vulnerabilities. We will still use a cup with water to explain the reason for this, as shown in Fig. 9. Under normal operation, suppose there are two potential flaws: “B” and “C.” In Fig. 9(a), “C” is more vulnerable than “B”. However, when the cup had flaw “A”, its operational status will change to reach a new optimal operational point from normal operation to contingency 1. In contingency 1, “B” is more vulnerable than “C.” Therefore, at different time points, the vulnerability of branches will change.

Inspired by the above analysis, we propose segmented CFGs to improve the accuracy of assessment results. First, based on the change regularities of ranking results in Section 3 (a), a fault chain can be divided three segments: anterior segment, middle segment, and posterior segment as shown in Fig. 10. We employ the threshold for total load shedding Δ as a yardstick to divide the fault chain. In the IEEE 39- and 118- bus systems, the thresholds of the three segments are 20%, 45%, and 60%. Secondly, we construct the three sub-CFGs based on the three segments, i.e., anterior CFG (aCFG), middle CFG (mCFG), and posterior segment (pCFG), respectively.

Furthermore, the aCFG, mCFG, and pCFG are employed to rank the branches according to the vertex degree, in-degree, and out-degree, respectively. The top 10 critical branches on IEEE 39-bus system and the 20 critical branches on the IEEE 118-bus system are summarized in Tables 2 and 3. We can observe that the rankings of critical branches have obvious

Table 3
Top 20 critical branches of IEEE 118-bus system based on different periods of cascading faults

Rank	aCFG			mCFG			pCFG		
	D	InD	OutD	D	InD	OutD	D	InD	OutD
1	127	127	104	105	106	105	38	32	38
2	104	124	125	106	30	108	32	136	149
3	125	107	127	108	105	97	136	134	136
4	107	123	7	30	108	116	149	149	61
5	90	90	90	116	102	96	61	30	67
6	123	104	107	97	116	128	134	61	33
7	7	119	119	96	97	30	67	106	108
8	124	125	176	102	31	66	30	105	105
9	119	7	96	128	67	106	105	29	106
10	176	102	123	31	96	31	106	67	66
11	96	176	102	67	92	102	108	108	22
12	102	96	9	91	61	91	33	38	137
13	9	126	124	66	91	124	29	115	9
14	126	128	126	137	89	137	66	54	134
15	128	9	31	88	128	88	54	37	54
16	31	31	128	92	137	67	22	91	29
17	149	149	97	89	88	89	137	45	23
18	129	129	149	61	66	95	37	88	91
19	97	37	129	124	136	94	115	66	88
20	37	106	8	119	104	92	91	22	37

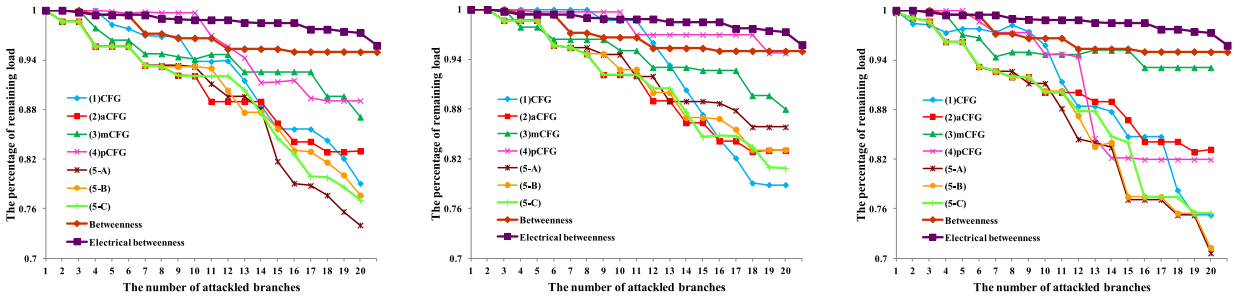


Fig. 11. Percentage of the remaining load on IEEE 118-bus system when removing critical nodes increases.

differences. We take the IEEE 39-bus system to analyze the critical vertices ranked by in-degree as an example. In the anterior period of sequential attacks, branches 27, 20, 37,5, and 46 are ranked as the most vulnerable ones affected by a fault. In the middle period, branches 39, 5, 46, 37, and 42 are ranked as the most vulnerable. Similarly, branches 33, 13, 34, 41, and 4 are ranked as the most vulnerable in the posterior period. The analysis shows that under sequential attacks, we need to focus on protecting different critical branches at different time points.

4.2. Critical branch attack

In this section, we investigate the outage size when critical branches ranked by different ways are attacked. We choose the critical branches ranked by degree, in-degree, or out-degree based on segmented CFGs. For the IEEE 39- and 118-bus systems, we choose top 10 and 20 critical branches, respectively. The procedure for selecting critical branches are as follows:

(I) Top 10 and 20 critical branches are chosen based one (1) CFG, (2) aCFG, (3) mCFG, and (4) pCFG metrics for IEEE 39-bus and 118-bus systems, respectively;
(II) Top K_1, K_2, K_3 critical branches are chosen based on the aCFG, mCFG, and pCFG metrics, respectively and use $K_1 + K_2 + K_3$ critical branches as the critical branches in order.

For IEEE 39-bus system, (5-a) $K_1 = 4$, $K_2 = 3$, $K_3 = 3$; (5-b) $K_1 = 3$, $K_2 = 4$, $K_3 = 3$; (5-c) $K_1 = 3$, $K_2 = 3$, $K_3 = 4$.
For IEEE 118-bus system, (5-A) $K_1 = 7$, $K_2 = 7$, $K_3 = 6$; (5-B) $K_1 = 8$, $K_2 = 6$, $K_3 = 6$; (5-C) $K_1 = 10$, $K_2 = 5$, $K_3 = 5$.

The results under the sequential attacks, based on the five ways, are shown in Figs. 10–11. We show the decrease in the remaining load in the two test benchmarks as a function of the number of removed critical branches.

On the IEEE 39-bus system, when the number of targeted branches chosen using the five ways except (4) is relatively small, the load shedding had a small difference between two ways. However, with the number of attacking branches increas-

Table 4
Percent of remaining load when removing 10 critical branches of IEEE 39-bus system and 20 critical branches of IEEE 118-bus system. The minimum remaining load in different indices.

Ways	IEEE 39-bus system			Ways	IEEE 118-bus system		
	D	InD	OutD		D	InD	OutD
(1)CFG	36.04%	36.04%	38.79%	(1)CFG	79.07%	**78.85%**	75.22%
(2)aCFG	57.08%	57.08%	71.47%	(2)aCFG	82.98%	82.98%	83.17%
(3)mCFG	38.79%	38.79%	45.06%	(3)mCFG	87.09%	87.97%	93.07%
(4)pCFG	37.65%	40.00%	50.49%	(4)pCFG	89.07%	94.72%	81.95%
(5-a)	36.04%	36.94%	**36.04%**	(5-A)	**75.65%**	85.83%	**70.63%**
(5-b)	36.04%	36.94%	**36.04%**	(5-B)	77.63%	83.07%	71.26%
(5-c)	**27.92%**	**27.92%**	**36.04%**	(5-C)	77.06%	80.84%	75.46%

ing, generally, there is more load shedding when removing the critical branches ranked by (1) and (5-a, b, c), compared to those ranked by (2), (3), and (4). When removing 10 critical branches ranked by (5- a, b, c), especially 5-c), the remaining load is significantly less, as shown in Table 4 compared to those ranked by ((2), (3), and (4).

On the IEEE 118-bus system, no matter the number of attacked branches, the result based on (5-a, b, c) is better than the one based on (2), (3) or (4). When 20 critical branches were ranked by (5-a, b, c), the remaining load was significantly less, as shown in Table 4, compared to the remaining loads when the critical branches were ranked by (2), (3), and (4).

In addition, Table 4 demonstrates that, whether 10 critical branches on the IEEE 39-bus system or 20 critical branches on the IEEE 118-bus system are attacked or not, the difference between the results when the critical branches were ranked by (1) and (5-a,b,c) is not obvious. In (1), the top critical branches stem from the results of comprehensive rankings, i.e., these critical branches stem from not only the anterior period but also the middle or posterior period. However, on the IEEE 118-bus system, Fig. 11 shows that (5-a, b, c) is better than (1) when the number of removing branches is relatively small. It is because most of the critical branches do not stem from the anterior period due to comprehensive rankings in (1).

Furthermore, to verify the results' accuracy, we compare the proposed method with the existing methods, including the proposed methods in references [29,30], i.e., betweenness and electrical betweenness. Among them, the methods of references [29,30]; were employed to rank the critical branches of the IEEE 39-bus system; in particular, betweenness and electrical betweenness were employed to rank the critical branches of the IEEE 118-bus system. In addition, as mentioned in the introduction, both betweenness and electrical betweenness are constructed based on the topological graph abstracted from the electrical topological structure. Among them, betweenness is the pure metric while electrical betweenness is the extended metric which considers the reactance of the branches as the weights of edges in the topological graph. The compared results (Figs. 10 and 11) show that the remaining load of the systems is obviously smaller, and the rate of the load descent is obviously faster, after removing suggested branches ranked by our proposed method than other methods; therefore, we can infer that employing segments CFGs as the operational graphs to assess the TNV is both effective and accurate.

To sum up, by analyzing the outage size when critical branches ranked using different ways were attacked at a different period, the different period could correspond to different critical branches. Therefore, for a given electric network, the different critical branches should be reviewed in different time points under sequential attacks.

5. Further discussions and conclusions

This paper attempts to analyze CFGs' metric instability and TNV from the angle of sequential attacks. Through analyzing the results of the simulations conducted, we observed the reason for metric instability. To improve the metric constancy, we introduced the relative position of fault chains with adjustable parameter β into the weight of edges in the CFGs. In this manner, improved the CFGs' metric constancy, the ranking results' accuracy reduced, as shown via an investigation of the percentage of remaining load. Meanwhile, in the above process, we also found that, under sequential attacks at different time points, the branches' vulnerabilities were different. This implies that some branches were more vulnerable in a specific period of sequential attacks than other periods. Thus, we divided the fault chain into three segments, which were employed to construct the aCFG, mCFG, and pCFG. The simulation results show that the segmented CFG is effective, which improves the assessment result's accuracy.

There are several possible directions that our future work could take along this topic. First, how to determine the end sign of fault chain needs closer analysis in terms of experimentation and simulation. Second, how to separate the three segments of fault chains is an important issue because they have effects on the critical branches' rankings according to the different period. Thirdly, we employed only the degree (in-degree or out-degree) of CFGs to rank critical branches. It is also an interesting direction to investigate other metrics, e.g., betweenness and centroid in ranking the branches.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Xiaoguang Wei: Conceptualization, Software, Validation, Methodology, Writing - original draft. **Shibin Gao:** Conceptualization, Methodology, Writing - review & editing, Project administration. **Tao Huang:** Formal analysis, Validation.

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).

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2019.106519.

References

[1] Tas S, Bier VM. Addressing vulnerability to cascading failure against intelligent adversaries in power networks. Energy Syst 2016;7(2):193–213.
[2] Hines P, Cotilla-Sanchez E, Blumsack S. Do topological models provide good information about electricity infrastructure vulnerability? Chaos 2010;20(3):033122.
[3] Bompard E, Napoli R, Xue F. Extended Topological Approach for the Assessment of Structural Vulnerability in Transmission Networks. IET Gen Trans Distrib May 2010;4(6):716–24.
[4] Carreras BA, Newman DE, Dobson I. North American blackout time series statistics and implications for blackout risk. IEEE Trans Power Syst Nov. 2016;31(6):4406–14.
[5] Bompard E, Estebsari A, Huang T, et al. A framework for analyzing cascading failure in large interconnected power systems: a post-contingency evolution simulator. Int J Electr Power Energy Syst Oct. 2016;131:12–31.
[6] Zhang G, Li Z, Zhang B, et al. Cascading failures of power grids caused by line breakdown. Int J Circ Theory Appl 2015;43:1807–14.
[7] Dong X, Nyberg TR, Hämäläinen P, et al. Vulnerability analysis of smart grid based on complex network theory. In: Proc. IEEE international conference on information science & technology, Changsha, China; 2015.
[8] Correa GJ, Yusta JM. Grid vulnerability analysis based on scale-free graphs versus power flow models. Electr Power Syst Res 2013;101(Aug.):71–9.
[9] Yang N, Liu W, Gao W. Study on scale-free characteristic on propagation of cascading failures in power grid. In: Proc. 2011 IEEE Energytech, Clevelan , OH, USA; May 2011.
[10] Rosascasals M, Valverde S, Sole RV. Topological vulnerability of the european power grid under errors and attacks. Int J Bifurc Chaos 2007;vol.17(Jul. (7)):2465–75.
[11] Dwivedi A, Yu X, Sokolowski P. Identifying Vulnerable branches in a power network using complex network theory. In: Proc. IEEE international symposium on industrial electronics, Seoul, Korea; July.18-23, 2009.
[12] Bilis EI, Kroger W, Nan C. Performance of electric power systems under physical malicious attacks. IEEE Syst J Dec. 2013;7(4):854–65.
[13] Ding M, Han P. Small-world topological model based vulnerability assessment algorithm for large-scale power grid. Autom Electr Power Syst Aug. 2006;30(8):7–10.
[14] Albert R, Albert I, Nakarado GL. Structural Vulnerability of the North American Power Grid. Phys Rev E Stat Nonbranchar Soft Matter Phys Feb. 2004;69(2) Pt 2.
[15] Bompard E, Pons E, Wu D. Extended Topological Metrics for the Analysis of Power Grid Vulnerability. IEEE Syst J Sep. 2012;6(3).
[16] Alipour Z, Monfared MAS, Zio E. Comparing topological and reliability-based vulnerability analysis of Iran power transmission network. J Risk Reliab 2014;228(2):139–51.
[17] Abedi A, Gaudard L, Romerio F. Review of major approaches to analyze vulnerability in power system. Reliab Eng Syst Saf 2019;183:153–72.
[18] Bompard E, Wu D, Xue F. Structural vulnerability of power systems: a topological approach. Electr Power Syst Res 2011;81(Mar. (7)):1334–40.
[19] Bai H, Miao S. Hybrid flow betweenness approach for identification of vulnerable branch in power system. IET Gener Transm Distrib 2015;9(Aug. (12)):1324–31.
[20] Dwivedi A, Yu X. A maximum-flow-based complex network approach for power system vulnerability analysis. IEEE Trans Ind Inf 2013;9(1):81–8.
[21] Yan J, Tang Y, He H, et al. Cascading failures analysis with DC power flow model and transient stability analysis. IEEE Trans Power Syst Jan. 2015;30(1):285–97.
[22] Yu X, Singh C. A practical approach for integrated power system vulnerability analysis with protection failures. IEEE Trans Power Syst Nov. 2004;19(4):1811–19.
[23] Wei X, Gao S, Duo Li, et al. Cascading fault graph for the analysis of transmission network vulnerability under different attacks. In: Proceedings of the CSEE, 38; Jan. 2018. p. 465–74.
[24] Wei X, Gao S, Huang T, et al. Complex network based cascading faults graph for the analysis of transmission network vulnerability. IEEE Trans Ind Inf 2019;15(Mar.(3)):1265–76.
[25] Wei X, Zhao J, Huang T, et al. A novel cascading faults graph based transmission network vulnerability assessment method. IEEE Trans Power Syst May 2018;33(3):2995–3000.
[26] Wang A, Luo Y, Tu G, et al. Vulnerability assessment scheme for power system transmission networks based on the fault chain theory. IEEE Trans Power Syst 2011;26(Feb. (1)):442–50.
[27] Zhu Y, Yan J, Tang Y, et al. Resilience analysis of power grids under the sequential attack. IEEE Trans Inf Forens Secur 2014;9(Dec. (12)):2340–54.
[28] Zhu Y, Yan J, Sun Y, et al. Revealing cascading failures vulnerability in power grids using risk-graph. IEEE Trans Parallel Distrib Syst 2014;vol.25(Dec. (12)):3274–84.
[29] Tasdighi M, Kezunovic M. Impact analysis of network topology change on transmission distance relay settings. IEEE Power Energy Soc Gen Meet 2015(July).
[30] Jin B, Xiao X, Chen J, et al. A method of risk assessment considering protection failures and dynamic equilibrium of power grid. Power Syst Protect Control 2016;44(Apr. (8)):1–7.

Xiaoguang Wei received his Ph.D. degree from Southwest Jiaotong University, Chengdu, China. His research interests include power system vulnerability assessment, energy internet, complex network theory.

Shibin Gao received his Ph.D. degrees from Southwest Jiaotong University, Chengdu, China. Since 1998, he has been a Professor at the department of Electrical Engineering in Southwest Jiaotong University. 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 received his Ph.D. degree from Politecnico di Torino, Turin, Italy. He is currently a researcher and professor with the Department of Energy, Politecnico di Torino, Italy and Xi Hua University, China, respectively. His research interests include critical infrastructure protection, vulnerability assessment, electricity markets, smart grids, etc.