Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability

How to cite: X. Wei, S. Gao, T. Huang, E. Bompard, R. Pi and T. Wang, "Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1265-1276, March 2019. doi: 10.1109/TII.2018.2840429

Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability

Xiaoguang Wei, Shibin Gao, Tao Huang, *Member*, *IEEE*, Ettore Bompard, Renjian Pi, and Tao Wang

***Abstract*—Transmission network vulnerability (TNV) assessment is a key issue in power systems to identify the vulnerable components against accidents or malicious threats. Recently, constructing the topological vulnerability indices, particularly extended topological indices, is a popular method to evaluate the network vulnerability. However, the topological vulnerability indices cannot reveal the mechanism of fault propagation. To overcome the shortcomings, this paper proposes a new method to assess the TNV through the cascading faults graph (CFG) based on fault chains, which is a statistical graph that comprehensively considers the physical, operational and structural features of electrical networks. Based on the complex network theory (CNT), the scale-free properties of the CFG are revealed through simulations on various transmission networks by corresponding the degree distribution of the CFG; then, the model constancy of the CFG is analyzed. Resorting**

X. Wei and S. Gao are with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China (e-mail: wei_xiaoguang@126.com and gao_shi_bin@126.com).

T. Huang, E. Bompard and R. Pi are with the Department of Energy, Politecnico di Torino, Torino 10129, Italy (tao.huang@polito.it;ettore.bompard@polito.it;renjian.pi@polito.it).

T. Wang is with the School of Electrical Engineering and Electronic Information, Xihua University, Chengdu 610039, China (e-mail: wangtao2005@163.com).

This work was supported by the Key Projects of National Natural Science Foundation of China (No. U1734202), National Key Research and Development Plan of China(No. 2017YFB1200802-12), National Natural Science Foundation of China(No. 61703345)

to the CFG, a set of indices from the CNT is used to identify the vulnerable branches of transmission networks. Illustrative applications are applied to the IEEE 39-bus and 118-bus test systems to demonstrate the effectiveness of the proposed method.

***Index Terms*—Network vulnerability, topological vulnerability indices, fault propagation, cascading faults graph, scale-free.**

SYMBOLS

$\mathcal{L}$ Set of branches (i.e., lines, transformers) in a transmission network, $\mathcal{L}=\{\ldots,L_j,\ldots\}$, $\dim\{\mathcal{L}\}=N_L$.

$\mathcal{B}$ Set of nodes (i.e., buses) in a transmission network, $\dim\{\mathcal{B}\}=N_B$.

$\mathcal{W}$ Set of nodes connected with generators, $\mathcal{W}=\{\ldots,W_h,\ldots\}$, $\mathcal{W} \subseteq \mathcal{B}$, $\dim\{\mathcal{W}\}=N_W$.

$\mathcal{D}$ Set of nodes connected with the load, $\mathcal{D}=\{\ldots,D_e,\ldots\}$, $\mathcal{D} \subseteq \mathcal{B}$, $\dim\{\mathcal{D}\}=N_D$.

Δ Threshold for the total load shedding.

Λ^i Total load shedding of fault chain i.

$\mathcal{L}^i$ Set of branches in fault chain i, $\mathcal{L}^i=\{\ldots, L_j^i,\ldots\}$, $\mathcal{L}^i \subseteq \mathcal{L}$, $\dim\{\mathcal{L}^i\}=n^i$.

$\boldsymbol{C}^i$ Fault chain i, $\boldsymbol{C}^i=(\mathcal{L}^i, n^i, \Lambda^i)$.

α_j^i Loading assessment index of branch j in the generation process of fault chain i, $L_j \in \mathcal{L}$.

f_j^0 Power flow of branch j under normal operation, $L_j \in \mathcal{L}$.

f_{jx}^i Power flow of branch j during contingency x in the generation process of fault chain i, $L_j \in \mathcal{L}$.

f_j^M Flow limit of branch j, $L_j \in \mathcal{L}$.

P_{dx}^{i} Active power withdrawal of the load bus during contingency *x* in the generation process of fault chain *i*, $d \in \mathcal{B}$.

δ_{zx}^{i} Load shedding percentage in the *z*th island during contingency *x* in the generation process of fault chain *i*.

Z_{x}^{i} Number of islands during contingency *x* in the generation process of fault chain *i*.

$\boldsymbol{P}_{x}^{i}$ Net active power injection.

$\boldsymbol{B}_{x}^{i}$ Susceptance matrix.

$\boldsymbol{\theta}_{x}^{i}$ Phase angle of bus voltages.

$P_{h}^{\min}$ Lower bound of the generated power of generator *h*, $w_h \in \mathcal{W}$.

$P_{h}^{\max}$ Upper bound of the generated power of generator *h*, $w_h \in \mathcal{W}$.

P_{hx}^{i} Generated power of generator *j* during contingency *x* in fault chain *i* generation process, $w_h \in \mathcal{W}$.

S_{x}^{i} Minimal load curtailment during contingency *x* in the generation process of fault chain *i*.

$\mathcal{T}^{i}$ Contingency set in the generation process of fault chain *i*, $\mathcal{T}^{i}=\{L_j\}$, $\dim\{\mathcal{T}^{i}\}=1 \cup 0$, $L_j \in \mathcal{L}$.

$\mathcal{V}$ Set of vertices in a graph, $\dim\{\mathcal{V}\}=N_L$.

$\mathcal{E}$ Set of edges in a graph, $\dim\{\mathcal{E}\}=N_q$.

$\mathcal{G}$ A cascading faults graph, $\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$.

$F(\bullet)$ Mapping function to convert a fault chain $\boldsymbol{C}^i$ into a graph $\mathcal{g}^i$, i.e. $\mathcal{g}^i = F(\boldsymbol{C}^i)$, $\mathcal{g}^i$ Í $\mathcal{G}$.

$\mathcal{V}^i$ Set of vertices in $\mathcal{g}^i$, $\mathcal{V}^i$ ={…, L^i_j,…}, dim{$\mathcal{V}^i$}=n^i, $\mathcal{V}^i = \mathcal{L}$.

$\mathcal{E}^i$ Set of edges in $\mathcal{g}^i$, $\mathcal{E}^i$ ={…, e^i_q,…}, $e^i_q = L^i_j L^i_{j+1}$, $q = j$, dim{$\mathcal{E}^i$}=n^i-1.

α_q Weight of edge e_q in cascading faults graph $\mathcal{G}$, e_q Î $\mathcal{G}$.

r Power exponent of cumulative distributions.

R^2 Fitting effect of the power law.

l Number of considered branches in the graph variation operation.

$X_x^{W_h D_e}$ Electrical distance between a pair of generator W_h and load D_e under contingency *x*.

E_0Network efficiency under normal operation.

E_xNetwork efficiency under contingency *x*.

$E_x^{¢}$ Percentage of network efficiency under contingency *x*, w.r.t. normal operation.

I. INTRODUCTION

TRANSMISSION network vulnerability (TNV) assessment is necessary for transmission system operators to identify the vulnerable components against accidents or malicious threats. The TNV is commonly evaluated using two methods: 1) time domain simulation [1] and 2) vulnerability indices (VI) [2]. Currently, in constructing the VIs, two aspects are relevant: 1) structural indices based on the topology of transmission networks and complex network theory [3], and 2) operative indices based on the steady or transient operation of power systems [4][5].

Many studies in structural indices based on the complex network theory can be classified into two categories: pure topological methods [6]-[10] and extended topological methods [3][12]-[14]. The first category employs pure topological metrics to analysis the TNV, such as average path length [6], betweenness [7], centroid [8] and degree [9]. Some metrics have been applied to actual power grids, for instance the European power grid [6] and the North American power grid [10]. However, these methods only depend on pure topological metrics and neglect the physical characteristics of the power grids. Hence the assessment results fail in apprehending real responses of power grids and are inaccurate [11]. To overcome these problems, many scholars proposed the extended topological methods by capturing and integrating specific physical behaviors of power grids into the complex network method. For instance, in [12], the hybrid flow betweenness is defined by considering the actual path of power flow and the transmission capacity of lines. The centrality in [13] is redefined by the maximum flow from the generator nodes to the load nodes. Reference [3] introduces flow paths, line flow limits and gen/load bus distribution into the complex network method.

In addition to the structural indices, there are vulnerability indices derived from the steady-state or transient simulation of power grids. In [4], the static performance index (via optimal power flow) and dynamic performance index (via transient stability) are proposed to rank critical nodes. References [15][16] considers the protection system failure to assess the power system vulnerability.

However, these VI-constructing methods still have problems. First， the VIs only give the ranks of branches and cannot identify the fault propagation mechanism. Secondly, the VIs cannot distinguish the roles of transmission branches under cascading failure [17][18]. For example, some transmission branches can easily spread their fault to other transmission branches and cause a

blackout with high probability. In contrast, others are more easily affected by a propagated fault.

Therefore, in this paper, we solve the aforementioned limitations by employing directed graphs based on the following considerations. First, the direction of an edge in a directed graph can reflect the route of information, such as the flow of currents in a water net and fault propagation path in transmission networks. Secondly, the nature of the criticalities of vertices can be easily identified. For instance, high out-degree vertexes are critical for spreading information whereas high in-degree vertices are critical for receiving information.

To use the directed graphs to evaluate the TNV, we construct a statistical graph, called the cascading faults graph (CFG), which comprehensively considers the physical, operational and structural features of electrical networks. The CFG can reveal the scale-free properties of the nature of fault propagations of the transmission network by translating the electrical physical network into the relationships of branches in cascading failures; whereas the traditional complex network methods study the scale-free properties by correlating the drop of system demand (or network efficiency) and the removed branches.

In this work, we first generate fault chains to reflect cascading paths. Next, we map the fault chains into a CFG. Then, based on the complex network theory, we study the CFG in terms of its characteristics and relevant indices are performed. Finally, the indices are used to identify the TNV in the IEEE 39-bus and 118-bus systems as application examples.

II. CASCADING FAULTS GRAPHS: MODEL AND METHOD

CFGs are direct-weighted graphs derived from fault chains. They are created, based on complex network theory, from the perspective of the load redistribution for networks in the fault propagation process. The direction of the CFG identifies the paths of the fault cascades, whereas its weight reflects the probability of propagation of a fault. Therefore, the cascading failure of a

given network can be graphically and intuitively represented.

A. Cascading failures

The occurrence and propagation of cascading failures depend on several factors, which include internal factors such as the types and locations of fault components, settings of automations (e.g. protections and controls), dynamic and transient features of equipment, pre-fault system operation conditions and external factors [19], such as load variances, emergency management plans and skills of system operators.

At present, there are two catalogues of methodologies to study cascading failures: static methods and dynamic methods. For the static methods, power-flow-based models have been a main method to study the cascading failures because of its efficiency, simplicity and scalability. For instance, OPA models study cascading failures by using the optimal power flow to analyze the load changes of the entire network [20][21]. The CASCADE model [22] and Manchester model [23] are proposed based on AC power flows. However, the DC power flow is the most widely used method to analyze cascading failures because of its exceptional convergence and stability, and computational simplicity [17][24]. The main features of these models focus on topological structures [25] and system overload from the perspective of the complex network theory [26][27]. In addition, stochastic models such as Markov chain [28] and Monte Carlo [29] are also developed to simulate cascading failures, which regard the fault features of components and protections as distribution functions.

By contrast, the dynamic methods focus on the dynamics of cascading failures such as oscillations and transients, angular stability, and frequency stability. Reference [30] analyzes the interrelationship of different mechanisms through a dynamic simulation by considering protection systems. Reference [1] employs PSAT (power system analysis toolbox) to simulate the transient

behaviors of cascading failures. In [31], the voltage and current stresses of individual elements are exploited to determine the sequence of failures. In general, the study of the dynamics of cascading failures depends on time-domain simulation tools [32] incorporated into static models, for example, optimal power flow [33]. Thus the dynamic methods are more comprehensive, but they require much longer simulation time and immense computational burden. Therefore, the dynamic methods are not suitable for the analysis of system vulnerability, particularly from the statistic viewpoint, which involves many times of simulations.

B. Fault chain generation method

As a media connecting equipment in the power system, the transmission network has notably fast dynamics/transients, compared to rotating devices. In other words, the transmission network *per se* can usually be considered static components in cascading failure studies. In addition, this paper focuses on understanding the nature of the transmission network in the cascading failure through the load redistribution mechanism; thus, the static model is used and the following simplifications are made: 1) the dynamic/transient stability features of generators or load are not considered; 2) only static behaviors of the network are considered; 3) the protections and controllers of electronic devices or generators are ignored; and 4) only protections related to the transmission branch are modeled.

Based on the above simplifications, the studies of cascading failures can be investigated by static models through the fault chains. A fault chain [34][35] is a set of multiple branches that are cut off one after another in a certain order, which eventually causes an outage. When a branch fails, it is likely to cause overload in other branches, which trips one or more new branches and results in cascading failures. Hence, a fault chain can record a chain reaction process of a fault propagation path in a transmission network.

To create a fault chain, the generation method must address two key issues:

(a) How to define a set of branches caused by tripping current selected branches.

(b) How to determine the end of a fault chain.

Branch loading assessment index: to solve the issue (a), we propose a branch loading assessment index (BLAI) to identify possible fault branches to form a fault chain from the perspective of load transfers. To construct the BLAI, three main factors are considered. First, when a branch fails in an electric network, the transmitted power over it will be redistributed in the network and may increase the flow in other branches and even cause an overload. Therefore the BLAI is constructed to reflect the loading burden of a branch and its possibility to fail under current contingency. Secondly, the construction of the formulation should be simple. Thirdly, the formulation should be sufficiently distinctive to identify different cases. Thus the BLAI index is proposed as

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

Obviously, a bigger value of α_j^i indicates a more vulnerable branch *j*. $\left(f_{jx}^i - f_j^0\right) / f_j^M$ reflects the deviation of power flow for different situations. The exponential term $\exp\left((f_{jx}^i - f_j^M) / f_j^M\right)$ describes the possibility of branch *j* overload. The right-hand-side measurements of equation (1) can be easily obtained or calculated, which results in simplicity in practical application.

Load shedding percentage: to address issue (b), we adopt the load shedding percentage to measure the scale of power outage and mark the end of a fault chain. The load shedding percentage is defined as

$$\delta_{zx}^{i} = 1 - \frac{\sum_{d \in \mathcal{B}_z} P_{dx}^{i}}{\sum_{d \in \mathcal{B}_z} P_{d(x-1)}^{i}} \tag{2}$$

$$\Lambda^{i} = \sum_{x \in \mathbf{C}^{i}} \sum_{z=1}^{Z_x^i} \delta_{zx}^{i} \tag{3}$$

Λ^{i} ($0 \# \Lambda^{i} \quad 1$) is the normalized total load shedding percentage [36]. A larger Λ^{i} indicates a larger outage scale. To determine the end of the cascading failure, we define a threshold Δ. When Λ^{i} 3 Δ, we terminate the fault chain generation process.

The load shedding percentage under each contingency is calculated using a DC optimal power flow (DC OPF) [4]. The DC OPF can be formulated as

$$S_x^i = \min \delta_x^i \tag{4}$$

$$s.t. \quad \boldsymbol{P}_x^i = \boldsymbol{B}_x^i \boldsymbol{\theta}_x^i \tag{5}$$

$$\left| f_{jx}^{i} \right| £ f_j^M \quad , j=1,2,\ldots,N_L \tag{6}$$

$$P_h^{\min} \# P_{hx}^{i} \quad P_h^{\max} , h=1,2,\ldots,N_W \tag{7}$$

Objective (4) considers the minimal load curtailment. Equality constraints (5) are the linearized power flow equations. Inequality constraints (6) are the operational requirements. The Constraints (7) are the generation technical limits.

Fault chain generation algorithm: The algorithm to capture a fault chain is as follows:

Fault chain $\boldsymbol{C}^i$ generation algorithm (assuming a given triggering event)
Step 1: Read transmission network information.
Step 2: Initialize $\mathcal{F}^i = \{L_j\}$, $\boldsymbol{C}^i = (\phi, 0, 0)$ and Δ.

Step 3: **WHILE**($\Delta \pounds \Lambda^i$)

Step 4: Cut off the branch in $\mathcal{T}^i$ from system, delete it from $\mathcal{T}^i$ (i.e., $\mathcal{T}^i = \phi$) and $\mathcal{L}$ and add it to $\mathcal{L}^i$.

Step 5: Island detection and partition. Suppose there are Z_x^i islands.

Step 6: **FOR** $z = 1 : Z_x^i$

Step 7: Calculate the DC power flow of the zth island.

Step 8: Employ **Equation 1** to calculate α_j^i of branch *j* of the zth island in $\mathcal{L}$.

Step 9: Calculate the minimum δ_{zx}^i in the zth island under contingency *x* using the DC OPF algorithm.

Step 10: **END FOR**

Step 11: Calculate $\delta_x^i = \sum_{z=1}^{Z_x^i} \delta_{zx}^i$.

Step 12: Calculate $\Lambda^i = \Lambda^i + \delta_x^i$.

Step 13: $\mathcal{T}_{x+1}^i = \{L_j \mid L_j ? \mathcal{L}, j : \arg \max_{j \in \{1,2,\ldots,N_L\}} (\alpha_j^i)\}$, $\boldsymbol{C}^i = (\bigcup_0^x \mathcal{T}_{x+1}^i, n^i ++, \Lambda^i)$. Record the $\max(\alpha_j^i)$.

Step 14: **END WHILE**

Step 15: Output the $\boldsymbol{C}^i$, α_j^i of the branches in $\boldsymbol{C}^i$.

Because the method is proposed from the perspective of the load redistribution of the entire network, for a given combination of network topology, operation condition, initial condition and position of the fault, the generated fault chain is unique.

Fault chain feature: For two fault chains $\boldsymbol{C}^{i¢}$ and $\boldsymbol{C}^i$ **,** if $\Lambda^{i¢} \geq \Lambda^i$ and $n^{i¢} < n^i$, the fault propagation of $\boldsymbol{C}^{i¢}$ is faster than that of $\boldsymbol{C}^i$ and the gravity of $\boldsymbol{C}^{i¢}$ is higher than $\boldsymbol{C}^i$.

C. CFG generation method

To study the topology of a CFG, we employ $F(\bullet)$ to convert a fault chain $\boldsymbol{C}^i$ into a directed and weighted graph $\mathcal{G}^i = \{\mathcal{V}^i, \mathcal{E}^i\}$, i.e. $\mathcal{G}^i = F(\boldsymbol{C}^i)$, where $\mathcal{V}^i$ is the set of vertices (i.e., $\mathcal{V}^i = \{L_j^i \mid j = 1, 2, \ldots, n\}$) and $\mathcal{E}^i$ is the set of edges (i.e., $\mathcal{E}^i = \{e_j^i \mid e_j^i = L_j^i L_{j+1}^i, j = 1, 2, \ldots, n-1\}$). The mapping operator $F(\bullet)$ is shown in Figure 1.

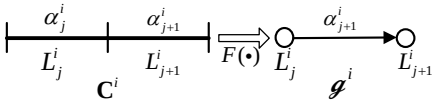


Fig. 1. Scheme of the mapping operator $F(\cdot)$

For a CFG formed by m fault chains $\mathcal{g}^1, \mathcal{g}^2, \ldots, \mathcal{g}^m$, the CFG is represented as $\mathcal{G} = \{(\mathcal{V}, \mathcal{E}) \mid \mathcal{V} = \mathcal{V}^1 \cup \mathcal{V}^2 \cup \ldots \cup \mathcal{V}^m, \mathcal{E} = \mathcal{E}^1 \cup \mathcal{E}^2 \cup \ldots \cup \mathcal{E}^m\}$. For an edge e_q whose weights are α^i in $\mathcal{g}^i$ (i=1,2,…,h, $h \leq m$), its weight in the CFG is defined as:

$$\alpha_q = \sum_{i=1}^{h} \frac{1}{n^i} \alpha^i. \tag{8}$$

According to the fault chain feature, the inclusion of length n^i to α_q can reflect the gravity of e_q in each $\mathcal{g}^i$.

III. Characteristic Analysis of CFGs of Electric Networks

We investigate the CFG characteristics of electric networks on two different test benchmarks, the IEEE 39-bus and 118-bus systems. The brief description of the two test benchmarks is provided in Table I. The IEEE 39-bus system represents a small-scaled electric network and the IEEE 118-bus system represents a relatively large-scaled electric network. In this section, we mainly study two features of the CFGs of electric networks.

TABLE I
DESCRIPTION OF THE TEST BENCHMARKS.

Test benchmarks	N_B	N_W	N_L	Network model
IEEE 39- bus system	39	10	46	Small-world [37]
IEEE 118-bus system	118	54	186	Small-world [37]
IEEE 300-bus system	300	69	411	Small-world [37]

Feature 1 Whether the CFGs of electric networks belong to one or more specific graph models, such as the small-world graph, regular graph or scale-free graph, etc.

Feature 2 Whether the graph model of the CFGs changes when the number of considered branches (e.g. l) or threshold for load shedding percentage (e.g. Δ) of fault chains change because the CFG of an electric network is composed of many fault chains, which are affected by their length and threshold for load shedding percentage.

A. Graph model of CFGs

To study **Feature 1**, we construct the CFGs of the IEEE 39-, 118- and 300-bus systems by setting Δ=20% (20% power loss is a sufficiently large event for a power grid [38]). Their CFGs are shown in Figure 2.

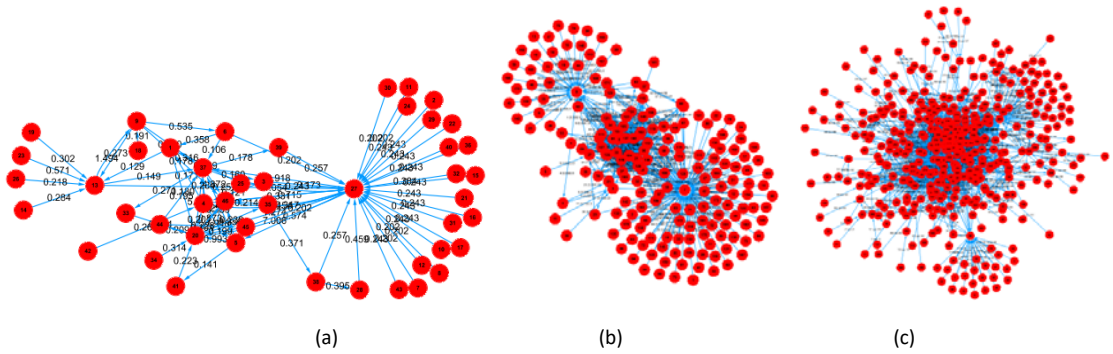


Fig. 2. CFGs of the branches. (a) IEEE 39-bus system. (b) IEEE 118-bus system. (c) IEEE 300-bus system.

Figure 2 shows that compared with the electric networks which are spatial networks (i.e., branches' geographic positions), the CFGs are time correlated graphs which can intuitively and simply reflect the fault spreading mechanism among branches. The edges of the CFGs can reveal the temporal relationships among the branches in a fault propagation.

We analyze the cumulative distribution of the vertex degree of CFGs $P(K>k)=\sum_{K>k}P(k)$, which is expressed with the log-log scale (Figure 2).

$$\ln P\left(K > k\right) = -1.0327 \ln k + 0.0097 \left(R^2 = 0.9888\right) \quad (8)$$

$$\ln P\left(K > k\right) = -1.1124 \ln k + 0.1313 \left(R^2 = 0.9261\right) \quad (9)$$

$$\ln P\left(K > k\right) = -1.3495 \ln k + 0.5675 \left(R^2 = 0.9166\right) \quad (10)$$

Equations (8)-(10) and Figure 3 are for the IEEE 39- , 118- and 300-bus systems, which show that the CFGs are scale-free graphs. Therefore, most of the vertices in the CFGs have small degrees, but few vertices have high degrees. Thus, the systems are robust under random vertex attacks, but they are highly vulnerable if the critical vertices are attacked [39].

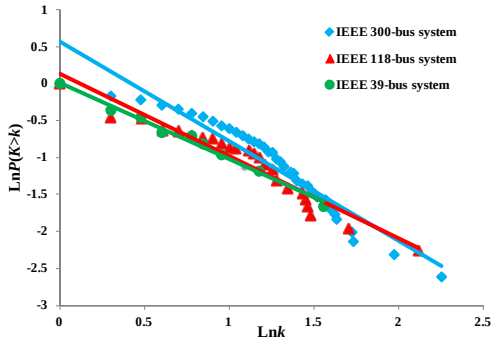


Fig. 3. Cumulative distributions of vertex degree in CFGs

Many electric networks have been proven to be small-world networks, including the two selected benchmark systems [37][40]-[42]. For a small-world network, if a node (or branch) fails in the network, it can cause the failures of adjacent and even non-adjacent nodes (or branches), which causes cascading failures. However, small-world networks fail in reflecting the extent of the node (or branch) vulnerability. In contrast, the proposed CFGs can reveal the vertex vulnerability. Hence, the branches easily interact with one another from the spatial relationship when an electric network fails (small-world characteristics), whereas the extent of vertexes

vulnerability and fault propagation mechanism can be captured through the corresponding scale-free CFGs from their temporal relationship.

B. Graph model constancy of CFGs

In the previous section, we conclude that CFGs are scale-free graphs. However, as described in **Feature 2**, we must further analyze the constancy of the graph features of CFGs, i.e., whether CFGs remain scale-free graphs under different conditions. Here we mainly focus on the following two conditional variants:

(a) length of fault chains: to investigate whether the length of fault chains can change **Feature 1** of a CFG, for each $\mathscr{G}^i = F\left(\boldsymbol{C}^i\right)$, we only use the first *l* branches in $\boldsymbol{C}^i$ and disregard the remainder, i.e., $\boldsymbol{C}^i = \{\mathscr{L}_l^i, l, \Lambda_l^i\}$, $\mathscr{L}_l^i = \{L_j \mid j = 1, 2, \ldots, l\}$. Thus, we can obtain a new CFG and analyze its graph features.

(b) threshold for load shedding percentage of fault chains.

In essence, both the two variants (a) and (b) can directly or indirectly change the length of fault chains. However, the former is an equal length change for each fault chain, whereas the latter is the opposite.

We employ the IEEE 39- and 118- bus systems to analyze the graph model constancy of CFGs. For the IEEE 39-bus system, we vary *l* and Δ from 2 to 9 with an interval of *l* and from 20% to 60% with an interval of 5% respectively to investigate the cumulative distribution of the vertex degree, in-degree and out-degree. Similarly, for the IEEE 118-bus system, we vary *l* and Δ change from 2 to 30 with an interval of 1 and from 10% to 30% with an interval of 5% respectively. Figures 4(a)-

(c) and 6(a)-(c) show the cumulative distributions of the vertex degree under different *l* of the two test systems; while Figures 5(a)-(c) and 7(a)-(c) show the cumulative distributions under different Δ. Subfigures (d) and (e) of Figures 4-7 illustrate the power exponent *r* of the cumulative distributions and the corresponding fitting effect of the power law, respectively.

As shown in (a), (b) and (c) of Figures 4-7, all CFGs of the two test benchmarks remain as power law distribution in the log-log scale. Thus, the graph models of CFGs are unchanged and scale-free graphs. We can observe the fitting effects R^2 from (e) of Figures 4-7. In addition to R^2<0.8 of the vertex degree and in-degree when *l*=2~4 in the IEEE 118-bus system (Figure 6), R^2 of the remainder is greater than 0.8, even most R^2>0.9. The fitting results are notably good and CFGs are undoubtedly scale-free graphs. Thus, we can conclude that CFGs are scale-free graphs and their graph models are not affected by *l* or Δ.

Furthermore, we analyze the power exponent *r* of cumulative distributions by (d) of Figures 4-7. The power exponent *r* of cumulative distributions of the vertex degree and in-degree is 1~1.2, whereas that of the vertex out-degree is approximately 1.3~2 for the two test benchmarks. The greater *r* can result in a faster drop of the power law curve, which indicates that fewer vertices have high degrees (in-degrees or out-degrees), which results in a more uniform degree distribution of the graph. Therefore, we can easily know that in the test cases, there are fewer vertices of the high out-degree than those of high degree and in-degree. In addition, when the *l* or Δ increases the power exponent *r* of cumulative distributions of the vertex in-degree trends to roughly ascend, which indicates that the number of vertexes of high in-degree shows a decreased trend. The vertex out-degree has the opposite trend, whereas the vertex degree has a smooth trend.

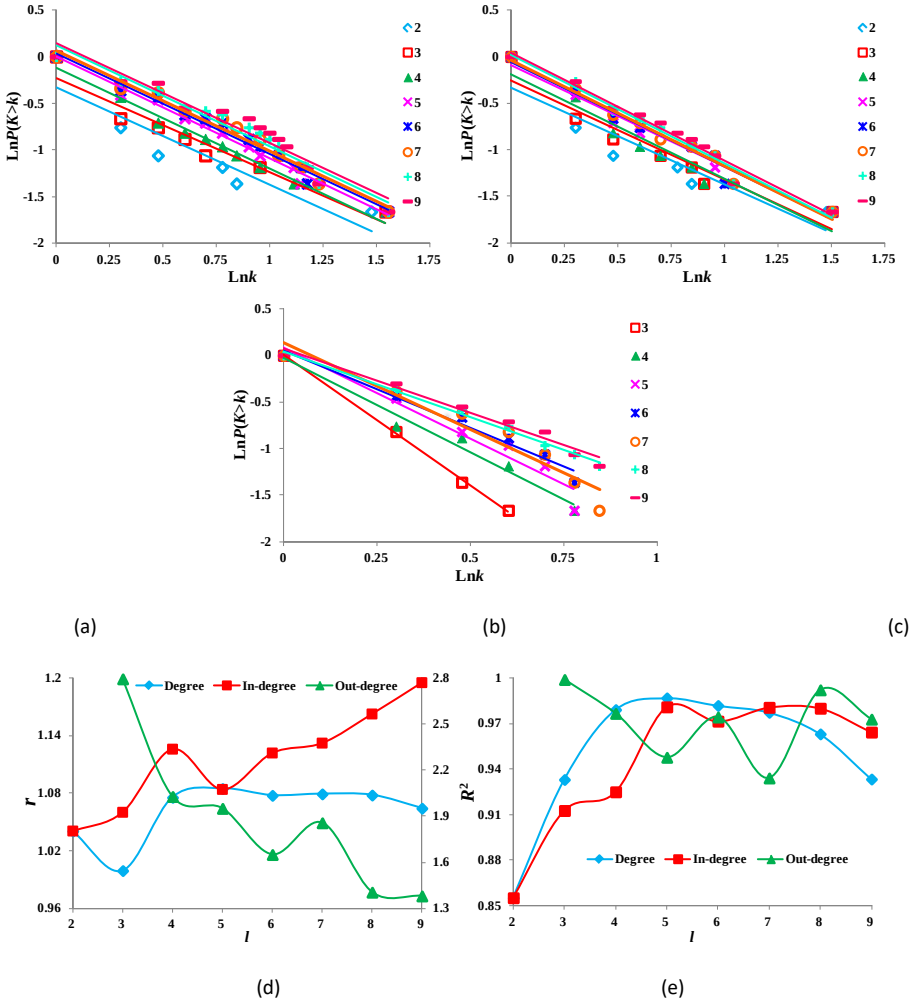


Fig. 4. The graph characteristics of CFGs under the different *l* in the IEEE 39-bus system. Cumulative distributions of vertex (a) degree, (b) in-degree and (c) out-degree. (d) the power exponent r of cumulative distributions, where degree and in-degree are measured by the left ordinate scale and out-degree is measured by the right ordinate scale. (e) the fitting effect R^2 of power law. Generally, $R^2 \geq 80\%$ has a satisfactory fitting effect.

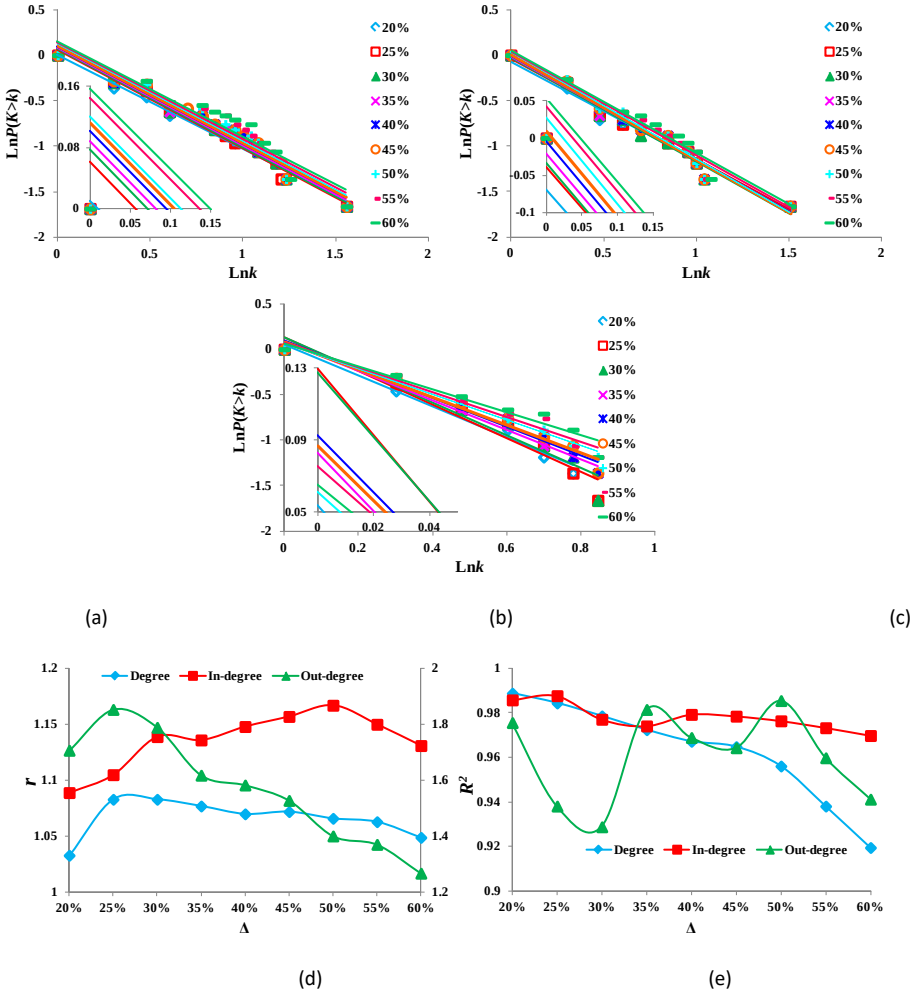


Fig. 5. The graph characteristics of CFGs under the different Δ in the IEEE 39-bus system[1].

[1] The meanings of (a)~(e) in Fig.5-7 are the same as in Fig.4.

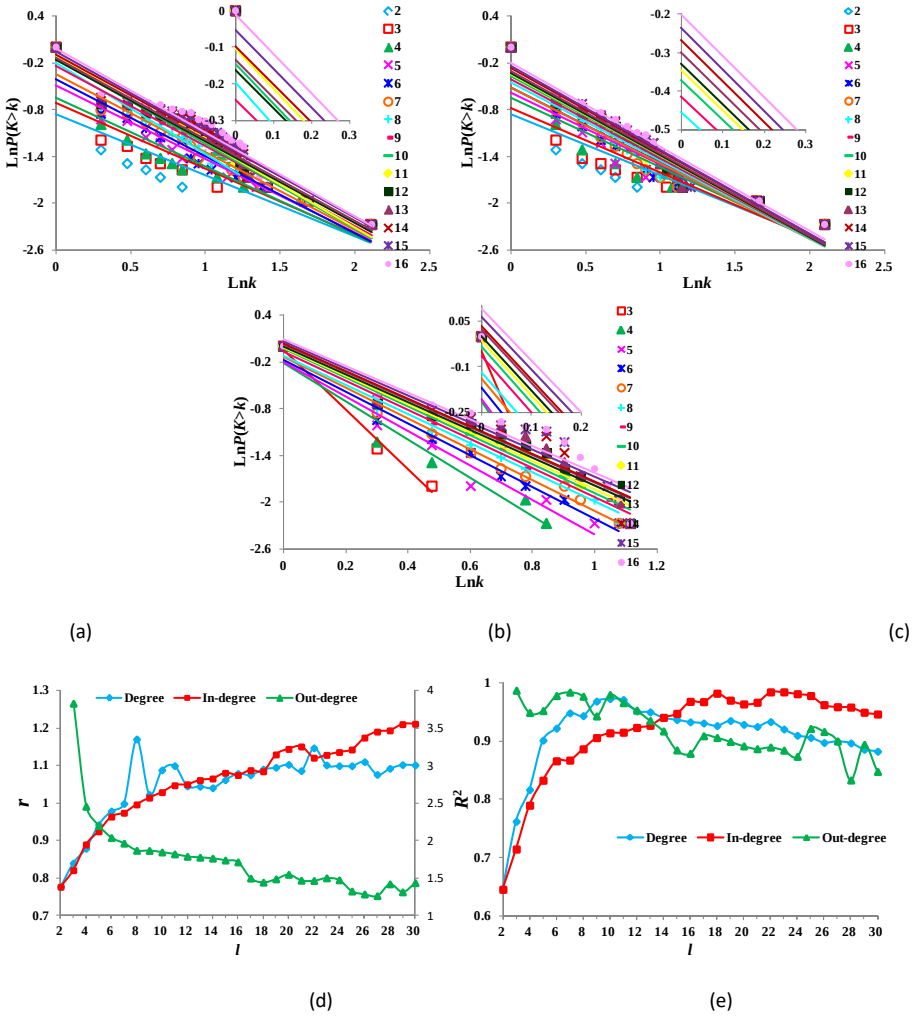


Fig. 6. The graph characteristics of CFGs under the different *l* of fault chains in the IEEE 118-bus system.

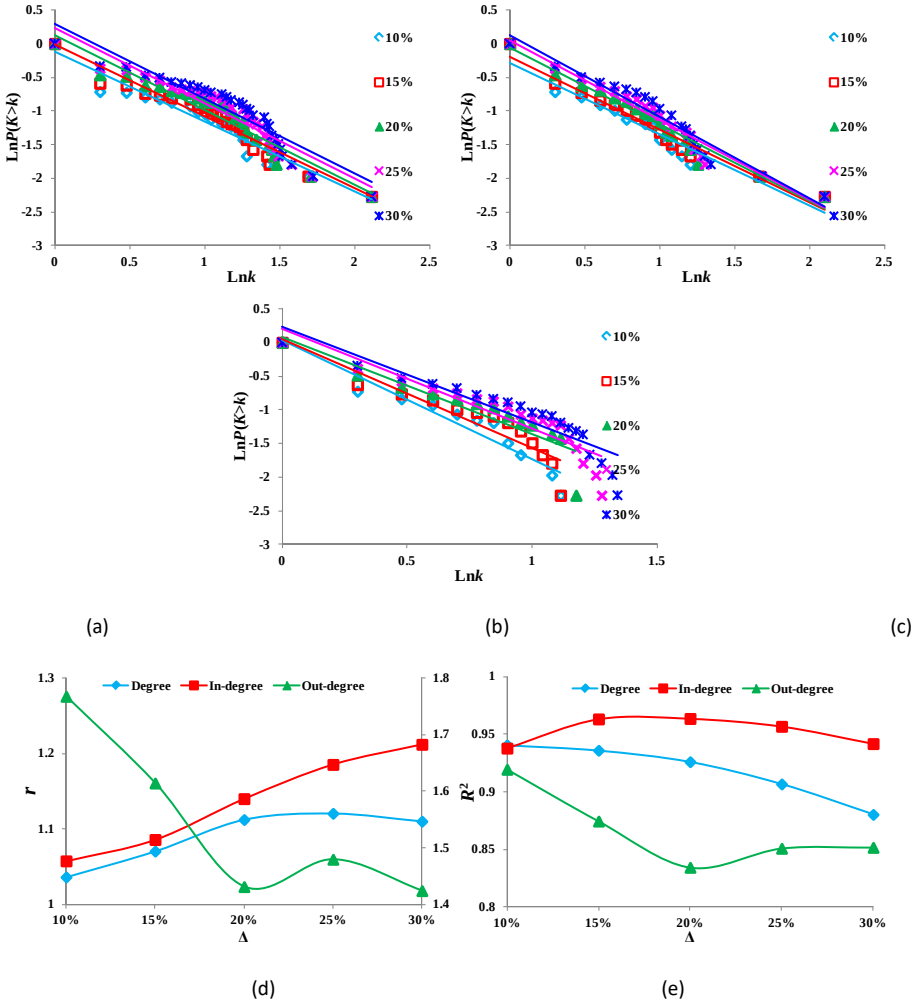


Fig. 7. The graph characteristics of CFGs under the different Δ in the IEEE 118-bus system.

In summary, CFGs are scale-free graphs and their graphic model is constant. Thus, the system has a high robustness under random branch attacks, but highly vulnerable under critical branch attacks.

Traditional complex network methods study the scale-free properties of the transmission network by correlating the drop of system demand (or network efficiency) and the removed branches. In contrast, this paper introduces the CFGs to reveal such properties by translating the electrical physical network into the relationships of branches in cascading faults.

IV. TNV Assessment Based on CFGs

As demonstrated in Section II, CFGs intuitively and simply reflect the characteristics of fault propagation among branches. Thus they have the advantages that most traditional VIs do not have. Because of the scale-free characteristics of CFGs, there are a few critical vertices with high degree (in-degree or out-degree) which are highly vulnerable. In this section, we illustrate how to use CFGs to capture the critical branches of electric networks by applying the proposed method to the IEEE 39- and 118-bus systems.

A. Rankings of critical branches

We rank the branches' criticality according to the vertex degree, in-degree and out-degree of CFGs. For the sake of space, only the top 10 critical branches are summarized in Tables II-III for the IEEE 39-bus system. Table II shows that for different CFGs formed by different *l* have different rankings of critical branches are varied. Particularly, when *l*=2~5, the rankings of critical branches have a relatively obvious change. However, when *l*=6~9 of fault chains increases, the rankings of critical branches basically remain stable. In Table III, the results can be divided into four groups: (1) Δ=20%~30%, (2) Δ=35%~40%, (3) Δ=45%~50%, and (4) Δ=55%~60%. In each group, the results of the rankings are roughly identical. Among different groups, the results of the rankings have some differences. In addition, when Δ increases, the results of rankings tend to be stable. But since the 39-bus system is a small-scaled electric network, when *l* or Δ increases, the rankings of critical branches do not have drastic changes compared to the 118-bus system whose ranking results are not shown in this paper for the sake of space.

TABLE II
TOP 10 CRITICAL BRANCHES OF THE IEEE 39-BUS SYSTEM UNDER *l*=2~9

Rank	2			3			4			5			6			7			8			9		
	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O
1	27	27	27	27	27	27	27	27	27	27	27	27	27	27	5	27	27	27	27	27	27	27	27	27
2	20	13	20	20	20	20	20	20	20	20	20	5	37	37	27	20	37	5	20	46	5	20	46	5
3	13	20	9	37	13	37	37	37	37	37	37	37	20	46	20	37	46	20	37	37	20	37	37	20
4	9	9	13	13	9	9	46	13	46	46	46	20	46	20	37	46	20	37	46	20	37	46	20	37
5	37	38	37	9	37	13	13	9	5	5	13	46	5	5	46	5	5	46	5	5	46	5	5	46
6	4	23	4	46	4	46	9	46	9	13	5	9	39	13	39	39	39	39	39	39	39	39	39	39
7	38	28	28	4	38	4	5	4	13	9	9	13	13	9	9	41	13	41	41	41	41	41	41	41
8	28	4	38	5	23	6	1	25	1	1	4	1	9	39	13	13	9	9	13	13	33	13	13	33
9	45	45	5	6	5	5	4	6	4	4	25	39	1	4	41	9	41	13	33	9	13	33	9	13
10	23	19	45	38	28	28	6	5	6	39	1	4	41	25	1	4	4	4	9	4	9	9	4	9

(Notes: D, I, O represent the degree, in-degree, out-degree)

TABLE III

TOP 10 CRITICAL BRANCHES OF THE IEEE 39-BUS SYSTEM UNDER Δ=20%~60%

Rank	20%			25%			30%			35%			40%			45%			50%			55%			60%			45%		
	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O	D	I	O
1	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	46	27	27	27	27
2	20	20	20	20	20	20	46	46	20	20	46	20	20	46	20	20	46	20	20	46	20	20	46	20	20	27	20	20	46	20
3	37	37	37	37	37	37	20	20	5	37	20	5	37	20	5	37	20	5	46	20	5	46	20	5	46	20	5	37	20	5
4	46	46	46	46	46	5	37	37	37	46	37	37	46	37	37	46	37	37	37	37	37	37	37	37	37	37	37	46	37	37
5	5	5	5	5	5	46	5	5	46	5	5	46	5	5	46	5	5	46	5	5	46	5	5	46	5	5	46	5	5	46
6	13	13	13	13	13	13	13	13	39	39	13	39	39	13	39	39	39	39	39	39	39	39	39	39	39	39	39	39	39	39
7	9	9	9	9	9	9	9	9	13	13	9	13	13	9	13	41	13	41	41	13	41	41	41	41	41	41	41	41	13	41
8	4	4	4	4	4	4	4	4	9	9	4	9	9	4	9	13	9	13	13	9	13	33	13	33	33	13	33	13	9	13
9	1	25	1	1	25	1	25	25	4	4	25	4	4	39	41	9	4	9	9	4	9	13	9	13	13	9	13	9	4	9
10	6	1	6	6	1	6	1	1	1	1	1	1	41	25	4	4	25	4	4	41	4	9	4	9	9	4	9	4	25	4

In addition, in the same CFG, the rankings results according to the vertex degree, in-degree and out-degree have some differences. The top branches ranked by the in-degree are more easily affected when other branches fail. The failures that occur to the top branches ranked by the out-degree can more easily spread and cause a blackout with high probability. For the top branches ranked by the degree, those branches can be somewhere in between.

B. Attacking critical branches

In this subsection, we investigate the blackout size by randomly and deliberately attacking branches. For random attacks, some branches are randomly selected and successively removed from the IEEE 39- or 118 bus systems in each simulation. For deliberate attacks, critical branches, which are ranked by the vertex degree, in-degree or out-degree based on different CFGs with various l or Δ are removed in the order of rank for targeted attacked. Here, we apply the synchronous attack, i.e. all removals simultaneously occur. The remaining load does not necessarily decrease when we increase the number of attacked branches. In addition, 10 and 20 branches are removed in the IEEE 39- and 118-bus systems, respectively. The results are displayed in Figures 8-9.In these figures, the remaining load in the two test benchmarks is shown as a function of the number of removed branches ranked by the degree, in-degree and out-degree for different l or Δ. As shown in these figures, regardless of l or Δ is, the two test benchmarks are sensitive to intentional attacks but relatively robust to random attacks because the remaining load more quickly decreases when the branches are removed according to the suggested rankings.

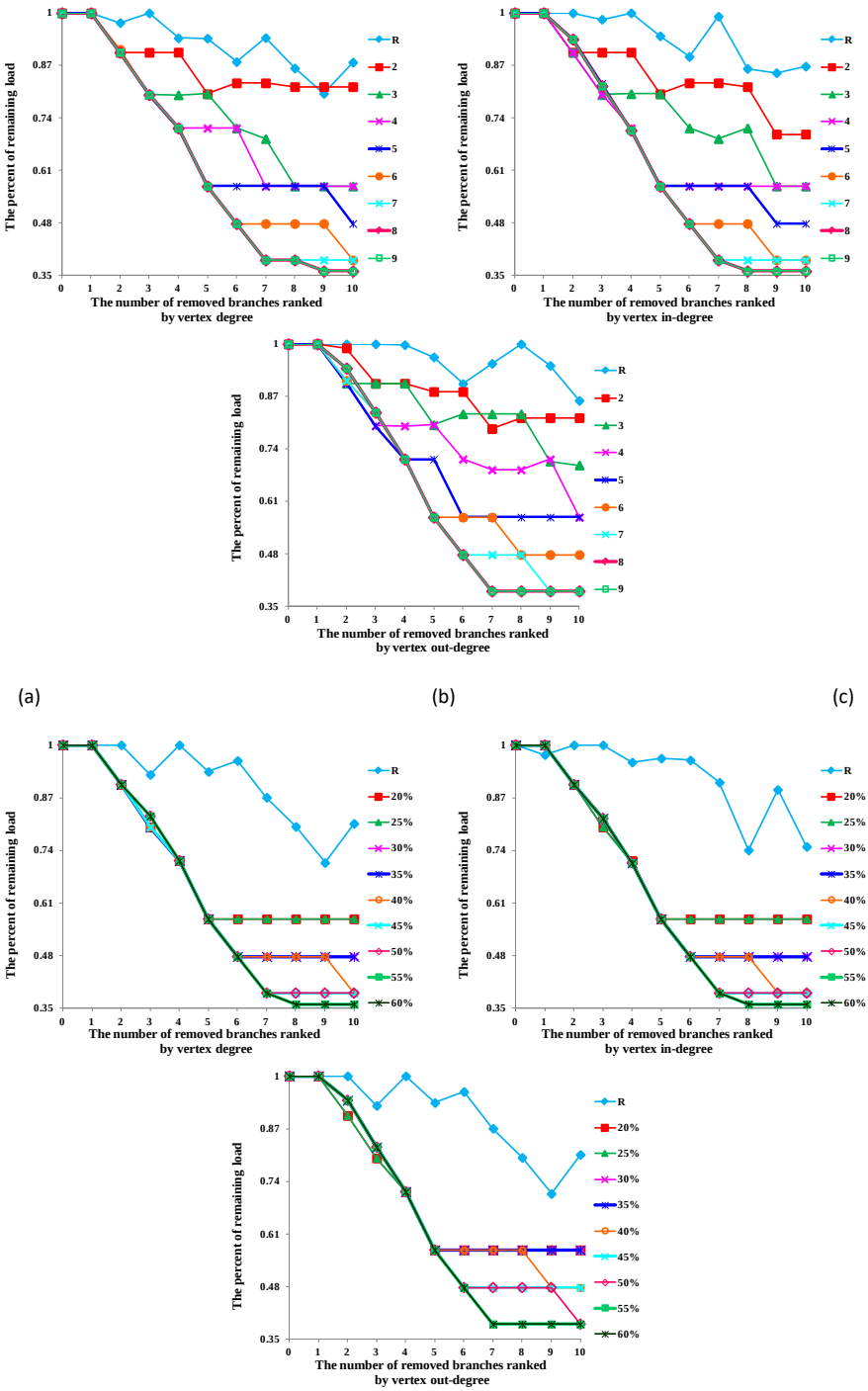
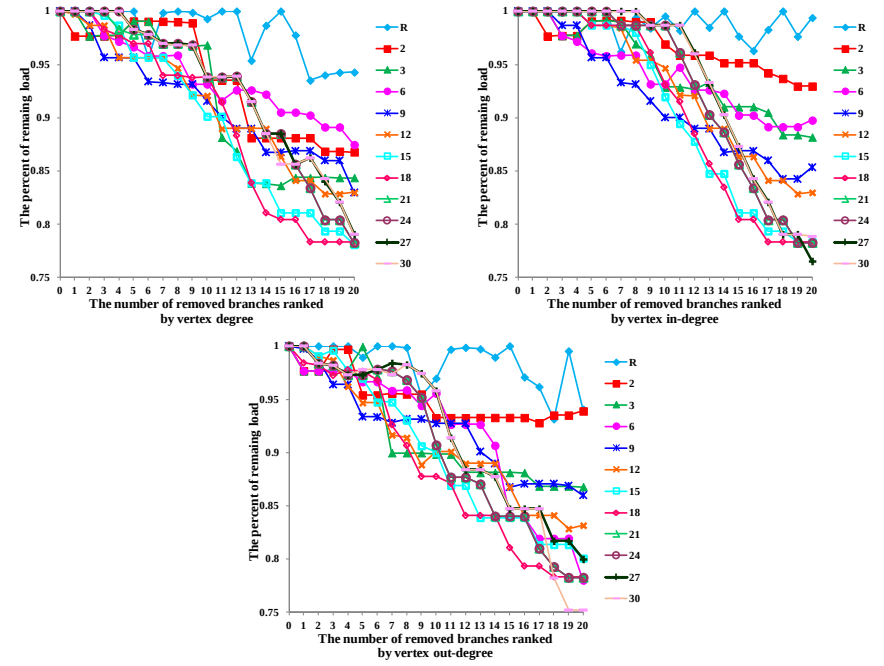
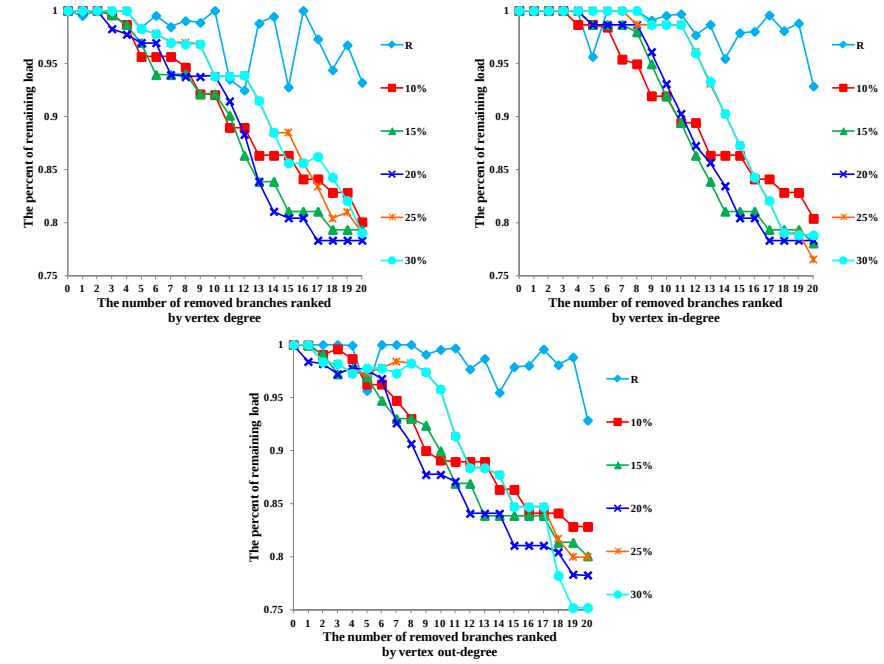


Fig. 8 Remaining load in the IEEE 39-bus system when removed critical branches increase. (a), (b) and (c) represent the different *l*. (d), (e) and (f) represent the different Δ.



(a) (b) (c)



(d) (e) (f)

Fig. 9. Remaining load in the IEEE 118-bus system when removed critical branches increase. (a), (b) and (c) represent the different *l*. (d), (e) and (f) represent the different Δ.

In the IEEE 39-bus system, it is obvious that when the number of attacked branches is relatively small, l and Δ hardly affect the remaining load. The reasons are 1) the 39-bus system is a small-scaled electric network and its robustness is comparatively weak, so it is prominent easily to result in system vulnerability when failures or disturbances occur, and 2) the top four branches in the system barely change when l or Δ increases. In addition, the electric network is more vulnerable when the number of attacked branches that are ranked by the vertex degree, in-degree or out-degree increases with increasing l or Δ when the remaining load more rapidly decreases. In the 118-bus system, it can be observed that when the number of attacked branches is relatively small, a smaller the l or Δ corresponds to a more vulnerable electric network.

In addition, by comparing the three methods of attacked branches ranked by the vertex degree, in-degree or out-degree in the 39-bus system, the electric network is more vulnerable when the attacked branches are ranked by in-degree rather than the other two methods. Thus, we must pay more attention to the protection of the branches affected by failures. However, it can be observed that we need pay more attention to the protection of the branches with easily spreading failures in the 118-bus system.

C. Comparison with existing methods

In this subsection, we compare the proposed method with references [4], [14], [16] and [41] to verify the effectiveness. Two main factors are considered when we select these references: 1) these references provide the suggested rankings of branches in the IEEE 118- and/or 39-bus systems, and 2) reference [14] and a method in [41] belong to the structural metrics, whereas references [4], [16] and another method in [41] belong to the operational metrics.

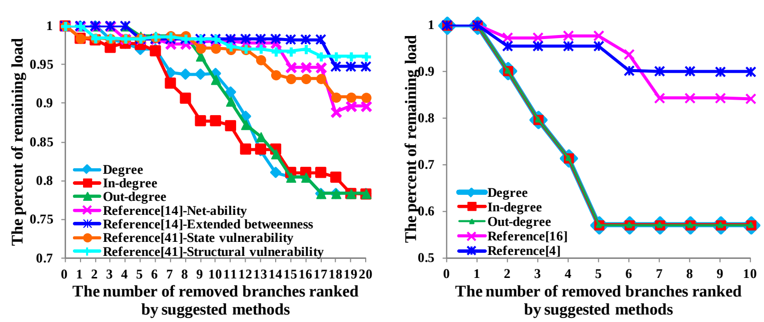
We take the blackout size and network efficiency [12] as measures of the operative and structural vulnerability, respectively. The percentage of network efficiency E'_x during contingency x is defined as

$$E'_x = \frac{E_x}{E_0} \times 100\% \qquad (9)$$

$$E_x = \frac{1}{N_W N_D} \sum_{W_h \in \mathcal{W},\, D_e \in \mathcal{D}\, (W_h \neq D_e)} \frac{1}{X_x^{W_h D_e}} \qquad (10)$$

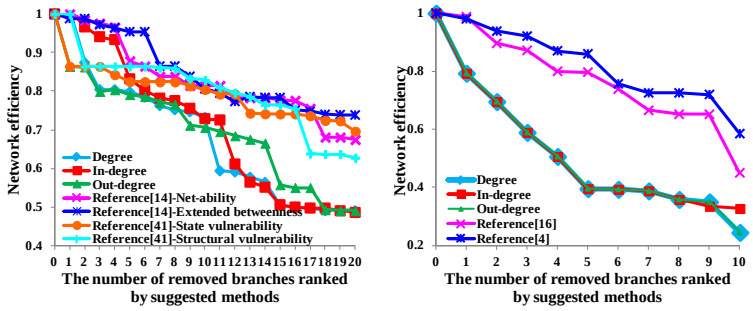
We calculate the remaining load and network efficiency by attacking the branches ranked by the comparative methods and ours. In our method, we set Δ=20% to construct the CFGs.

To compare with the structural metrics, we remove branches from the IEEE 118-bus systems according to the rankings identified by the 1) net-ability and extended betweenness in reference [14]; 2) structural vulnerability method in reference [41]; and 3) our method. Figures 10(a) and 11(b) show that the remaining load and network efficiency after the removal of the branches identified by our method are generally smaller than that of references [14] and [41]. Therefore, the ability of identifying critical branches of our method is better than references [14] and [41].



(a) (b)

Fig. 10. Comparison of the percent of remaining load between the proposed method and other methods. (a) IEEE 118-bus system; (b) IEEE 39-bus system.



(a) (b)

Fig. 11. Comparison of network efficiency between the proposed method and other methods. (a) IEEE 118-bus system; (b) IEEE 39-bus system.

We compare our method with the operational metrics in references [4], [16] and [41] through the IEEE 39 and 118-bus system. Figures 10 and 11 show that the remaining load and network efficiency after the removal of the branches identified by our model are smaller, which indicates a similar conclusion to the previous comparisons.

To summarize, our proposed method can better identify vulnerable branches in the transmission networks both from both topological and operational respects. In addition, in practical applications, we can select the total load shedding percentage Δ=20% to construct the CFGs.

V. Conclusions

In this paper, we propose CFGs to evaluate the transmission network vulnerability. First, the CFG generation method is introduced in detail. Then we employ two test benchmarks to analyze the characteristics of CFGs and the constancy of their graph model. Finally, we use CFGs to rank the critical branches according to the vertex degree, in-degree and out-degree. To validate the proposed method, we compare the blackout size by attacking the critical branches with random

selected branches. According to the simulation and analysis, the advantages and disadvantages of the CFGs are summarized as follows.

Advantages of CFGs: 1) CFGs are temporal graphs, which intuitively and simply reveal the propagation process of branch faults. 2) CFGs are scale-free graphs and their graph model constancy is stable. Thus, the system has a high robustness under random branch attacks, but there is a high vulnerability under critical branch attacks. 3) CFGs are the directed graphs. The direction of the CFG is the sequential relationships among branches, which are cut off because of the contingency selection criterion designed in the paper, i.e., the direction always points to the next contingency branch caused by the current fault branch. Therefore using CFGs can recognize the branches that can be easily affected when the system fails (by calculating the vertex in-degree) and easily spread failures (by calculating the out-degree). 4) CFGs are not only simple and intuitive and easy to understand.

Disadvantages of CFGs: 1) When a power system is notably large, constructing the corresponding CFG can have a large time complexity. 2) Becasue the different CFGs are formed by fault chains with various lengths or thresholds for the load shedding percentage, the rankings of critical branches have differences. Hence, some metrics of the CFG are not stable, although the graph model of the CFG is certain. The reason will be analyzed in a future paper. Thus in practical application we must be cautious in selecting an appropriate CFG to optimally evaluate branch vulnerability for a system needs to be cautious.

Our work provides a new method to assess transmission network vulnerability. In the future, we plan to overcome the disadvantages of CFGs and employ CFGs to assess the bus node vulnerability of actual electric networks.

REFERENCES

[1] J. Yan, Y. Tang and H. He, et al, "Cascading Failures Analysis with DC Power Flow Model and Transient Stability Analysis," IEEE Trans. Power Syst., vol. 30, no. 1, pp. 285-297, Jan. 2015.

[2] E. Cotilla-Sanchez, P.D.H. Hines, C. Barrows, et al, "Comparing the Topological and Electrical Structure of the North American Electric Power Infrastructure," IEEE Syst. J., vol. 6, no. 4, pp. 616-626, Dec. 2012.

[3] E. Bompard, R. Napoli and F. Xue, "Extended Topological Approach for the Assessment of Structural Vulnerability in Transmission Networks," IET Gener. Transm. Distrib., vol. 4, no. 6, pp. 716-724, May 2010.

[4] M. Tasdighi, M. Kezunovic, "Impact Analysis of Network Topology Change on Transmission Distance Relay Settings," Power & Energy Society General Meeting, 2015 IEEE, July. 1-5, 2015.

[5] A. M. Leite da Silva, J. L. Jardim, and L. R. de Lima, et al, "A Method for Ranking Critical Nodes in Power Networks Including Load Uncertainties," IEEE Trans. Power Syst., vol. 31, no. 2, pp. 1341-1349, Mar. 2016.

[6] M. Rosascasals, S. Valverde, and R. V. Sole, "Topological Vulnerability of the European Power Grid Under Errors and Attacks," International Journal of Bifurcation & Chaos, vol.17, no. 7, pp. 2465-2475, Jul. 2007.

[7] A. Dwivedi, X. Yu, and P. Sokolowski, "Identifying Vulnerable Lines in a Power Network Using Complex Network Theory," in Proc. IEEE International Symposium on Industrial Electronics, Seoul, Korea, July.18-23, 2009.

[8] E.I. Bilis, W. Kroger, C. Nan, "Performance of Electric Power Systems Under Physical Malicious Attacks," IEEE Syst. J., vol. 7, no. 4, pp. 854-865, Dec. 2013.

[9] M. Ding, P. Han, "Small-world Topological Model Based Vulnerability Assessment Algorithm for Large-scale Power Grid," Automation of Electric Power systems, vol. 30, no. 8, pp.7-10, Aug. 2006.

[10] R. Albert, I. Albert, G.L. Nakarado, "Structural Vulnerability of the North American Power Grid," Physical Review E Statistical Nonlinear & Soft Matter Physics, vol. 69, no. 2 Pt 2, Feb. 2004.

[11] E. Bompard, E. Pons and D. Wu, "Extended Topological Metrics for the Analysis of Power Grid Vulnerability," IEEE Syst. J., vol. 6, no. 3, Sep. 2012.

[12] H. Bai, S. Miao. "Hybrid flow betweenness approach for identification of vulnerable line in power system," IET Gener. Transm. Distrib., vol. 9, no. 12, pp. 1324-1331, Aug. 2015.

[13] 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.

[14] E. Bompard, D. Wu, and F. Xue, "Structural Vulnerability of Power Systems: a Topological Approach," Electric Power Systems Research, vol. 81, no. 7, pp. 1334-1340, Jul. 2011.

[15] X. Yu and C. Singh, "A Practical Approach for Integrated Power System Vulnerability Analysis with Protection Failures," IEEE Trans. Power Syst., vol. 19, no. 4, pp. 1811-1819, Nov. 2004.

[16] B. Jin, X. Xiao, and J. Chen, et al, "A Method of Risk Assessment Considering Protection Failures and Dynamic Equilibrium of Power Grid," Power System Protection and Control, vol. 44, no. 8, pp.1-7, Apr. 2016.

[17] Y. Zhu, J. Yan and Y. Sun, et al, "Revealing Cascading failures Vulnerability in Power Grids Using Risk-Graph," IEEE Trans. Parallel Distrib. Syst., vol. 25, no.12, pp. 3274-3284, Dec. 2014.

[18] Y. Cai, Y.J. Cao and Y. Li, et al, "Cascading Failure Analysis Considering Interaction between Power Grids and Dispatching Data Networks," IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 1-9, Oct. 2015.

[19] S. L. Voronca, M. M. Voronca, and T. Huang, et al, "Applying the Analytic Hierarchy process to Rank natural Threats to Power System Security," U. P. B. Sci. Bull, Series C, vol. 77, no. 3, 2017.

[20] S. Mei, F. He, and X. Zhang, et al, "An Improved OPA Model and Blackout Risk Assessment," IEEE Trans. Power Syst., vol. 24, no. 2, pp. 814-823, May 2004.

[21] X. Liu, Z. Li. "Revealing the impact of multiple solutions in DCOPF on the risk assessment of line cascading failure in OPA model," IEEE Transactions on Power Syst., vol. 31, no. 5, pp. 4159-4160, Sep. 2016.

[22] I. Dobson, B. Carreras, and D. Newman, "A Probabilistic Loading- Dependent model of cascading failure and possible implications for blackouts, " in Proc. 36th Annu. Hawaii Int. Conf. System Sciences, 2003, vol. 19, no. 1, pp. 15-32.

[23] D. Kirschen, D. Jayaweera, and D. Nedic, et al, "A Probabilistic Indicator of System Stress," IEEE Trans. Power Syst., vol. 19, no. 3, pp. 1650-1657, Aug. 2004.

[24] Y. Zhu, J. Yan, and Y. Tang, et al, "Resilience Analysis of Power Grids Under the Sequential Attack," IEEE Trans. Info. Forensics Security, vol. 9, no. 12, pp. 2340-2354, Dec. 2014.

[25] P. Dey, R. Mehra, and F. Kazi, et al. "Impact of Topology on the Propagation of Cascading Failure in Power Grid," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1970-1978, July, 2016.

[26] W. Fan, Z. Liu, and P. Hu, et al, "Cascading failure model in power grids using the complex network theory," IET Generation, Transmission & Distribution, vol. 10, no. 15, pp. 3940-3949, 2016.

[27] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," IEEE Trans. Info. Forensics Security, vol. 9, no. 3, pp. 451-463, Mar. 2014.

[28] M. Rahnamay-Naeini, Z. Wang, and N. Ghani, et al, "Stochastic Analysis of Cascading-Failure Dynamics in Power Grids" IEEE Trans. Power Syst., vol. 29, no. 4, pp. 1767-1779, July, 2014.

[29] P. Rezaei, P. D. H. Hines, and M. J. Eppstein, "Estimating Cascading Failure Risk with Random Chemistry," IEEE Trans. Power Syst., vol. 30, no. 5, pp. 2726-2735, Oct., 2014.

[30] J. Song, E. Cotilla-Sanchez, and G. Ghanavati, et al, "Dynamic Modeling of Cascading Failure in Power Systems," IEEE Trans. Power Syst., vol. 31, no. 6, pp. 4887-4900, Nov. 2016.
[31] X. Zhang, C. Zhan, and C. K. Tse, "Modeling the Dynamics of Cascading failures in Power systems," IEEE J. Em. Sel. Top. C., vol. 7, no. 2, pp. 192-204, Mar. 2017.
[32] J. Bialek, E. Ciapessoni, and D. Cirio, et al, "Benchmarking and Validation of Cascading Failure Analysis Tolls," IEEE Trans. Power Syst., vol. 31, no. 3, pp. 2085-2095, May, 2016.
[33] R. Zarate-Minano, T. Van Cutsem, and F. Milano, et al, "Securing Transient Stability Using Time-Domain Simulations within an Optimal Power Flow," IEEE Trans. Power Syst., vol. 25, no. 1, pp. 243-253, Feb., 2010.
[34] A. Wang, Y. Luo, and G. Tu, et al, "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.
[35] T. Huang, S.L. Voronca, and A.A. Purcarea, et al, "Analysis of Chain of Events in Major Historic Power Outages," Advances in Electrical and Computer Engineering, vol. 14, no. 3, pp. 63-70, Aug. 2014.
[36] P. Hines, E Cotilla-Sanchez, and S. Blumsack, "Do Topological Models Provide Good Information about Electricity Infrastructure Vulnerability? " Chaos, vol. 20, no. 3, pp. 033122, 2010.
[37] Y. Cao, J. Guo, and S. Mei, et al. System Complexity Theory of Security Assessment for Large Power grids. Beijing, China: Tsinghua University Press, 2004.
[38] M. J. Eppstein, P. D. H. Hines, "A 'Random Chenmistry' Algorithm for Identifying Collections of Multiple Contingencies That Initiate Cascading failures," IEEE Trans. Power Syst., vol. 27, no. 3, pp. 1698-1705, Aug. 2012.
[39] X. Wang, Z. Chen, and P. Liu, et al, "Edge Balance Ratio: Power Law From Vertices to Edges in Directed Complex Network," IEEE Journal of Selected Topics in Signal Processing, vol. 7, No. 2, Apr. 2013.
[40] E. Cotilla-Sanchez, P.D.H Hines, and C. Barrows, et al, "Comparing the Topological and Electrical Structure the North American Electric Power Infrastructure," IEEE Syst. J., vol. 6, no. 4, Dec. 2012.
[41] V. Rosato, S. Bologna, and F. Tiriticco, "Topological Properties of High-voltage Electrical Transmission Networks," Electric Power Systems Research, vol. 77, no.2, Feb. 2007.
[42] L. Fu, W. Huang, and S. Xiao, "Vulnerability Assessment for Power Grid Based on Small-world Topological Model," In Proc. APPEEC, Chengdu, China, Apr.28-31, 2010.
[43] H. Qi, L. Shi, and Y. Ni, et al "Study on Power System Vulnerability Assessment Based on Cascading Failure Model" PES General Meeting | Conference & Exposition, 2004 IEEE, July.1-7, 2014.

Xiaoguang Wei is currently pursuing his Ph.D. degree in electrical engineering at the 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 (M'18) 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.

Ettore Bompard received his Ph.D. degree from Politecnico di Torino, Turin, Italy. He is currently a professor at the department of Energy, Politecnico di Torino. His research interests include critical infrastructure protection, electricity markets, smart grids, etc.

Renjian Pi is currently pursuing his Ph.D. degree in electrical engineering at Politecnico di Torino, Turin, Italy. His research interests include power system vulnerability assessment and critical infrastructure protection.

Tao Wang received her 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.