Invulnerability of power grids based on maximum flow theory^{*}

Fan Wenli, Huang Shaowei, Mei Shengwei[†]

State Key Laboratory of Power System, Department of Electrical Engineering, Tsinghua University, Beijing, 100084, China

Abstract: The invulnerability analysis against cascades is of great significance in evaluating the reliability of power systems. In this paper, we propose a novel cascading failure model based on the maximum flow theory to analyze the invulnerability of power grids. In the model, node initial loads are built on the feasible flows of nodes with a tunable parameter γ used to control the initial node load distribution. The simulation results show that both the invulnerability against cascades and the tolerance parameter threshold α_T are affected by node load distribution greatly. As γ grows, the invulnerability shows the distinct change rules under different attack strategies and different tolerance parameters α respectively. These results are useful in power grid planning and cascading failure prevention.

Keywords: Invulnerability, Cascading failures, Maximum flow theory, Complex networks

1. Introduction

The invulnerability analysis of complex network stemmed from the work of Albert et al. in classic network models [1-2]. Nowadays, as complex network theory develops continuously, invulnerability analysis has penetrated into many fields and aroused broad recognition [3-6]. Cascading failures in power systems occurring frequently in recent years [7-8] have fully revealed the invulnerability problem of power grids against blackouts. Thus, the invulnerability analysis can be treated as an important channel to identify the reliability of the power grid when facing catastrophes.

Currently, there are two groups of commonly used approaches for complex network invulnerability analysis, which are analytic methods and simulation methods respectively. Analytic methods focus on searching the phase-transition point when system collapsing by means of percolation theory through which complex network invulnerability can be studied [9-10]. While in simulation methods, the invulnerability can be investigated directly by simulating cascading failures under different attack strategies [11-19]. Albert et al. made his research achievement based on the latter method. Similar work can be found in Ref.[12] and Ref.[13], which investigate the tolerance to errors and attacks in the European power grid. All those researches concerned static connectivity analysis by removing nodes continuously in light of certain strategy, such as removing the most connected nodes under an increasing level of attacks [1,11]. Nevertheless, these researches have not modeled cascading failures, which brought up the problem that the dynamic load distribution was neglected. Consequently, many scholars employed complex system theory and complex network theory to analyze the invulnerability of power grids. The complex system theory models cascading failure based on DC or AC model [14-15]. The models of this kind considers the

^{*} Project supported by the National Natural Science Foundation of China (Grant Nos. U51321005, 51377091).

[†] Corresponding author. E-mail: meishengwei@mail.tsinghua.edu.cn

operation characteristics of power grids, which neglects the influence from topology structure. While in complex network theory, the dynamic load distribution in cascading failures refers to the process that the loads of failed nodes are distributed over the remaining nodes following a strategy, which may cause the breakdowns of newly overloaded nodes. If the redistribution of node loads happens while the loads of all nodes are within their corresponding capacities, the process of load distribution ends. Based on this idea, many scholars have put forward various cascading failure models with dynamic load distributions to study the power grid invulnerability against cascades ^[16-19]. Ref. [16] proposed a cascade model in the power grid which assumed the power transferred via the path efficiency, and the scale of the cascade is reduced under a new load distribution law and a new node removal rule compared to the topology model in the UK power grid. Ref. [17] improved the traditional topological model and redefined the load using power angle information to analysis the vulnerability of a power grid. And the simulation on the IEEE 118-bus system confirmed it more effective compared to the traditional model. Ref.[18] investigated the Iranian high voltage power transmission grid with the assumption that power was exchanged and transmitted along the shortest path between the sources and sinks. Ref. [19] studied the trade-off between robustness and network construction costs in terms of a high-robustness and low-cost cascading failure model established upon node importance in the IEEE_300 bus system. Those cascading failure models related work have established the basis for invulnerability study.

As all known, generation nodes transmit electric power to distribution substation nodes through power grids. Obviously, taking electrical characteristics into consideration, such as power transmission, can provide more overall and accurate results for invulnerability analysis. Therefore, we introduce the maximum flow theory to the power grid so as to calculate the feasible flows in transmission lines and nodes respectively with the consideration of the power transmission limit of transmission lines, the maximum supply of generator nodes and the maximum demand of load nodes. Further, we propose a novel cascading failure model in which the initial node load is a nonlinear function of the feasible flow of node with a tunable load distribution parameter γ used to investigate the invulnerability of power grids.

The paper is organized as follows. In Section 2, we show the topology modeling process based on complex network theory. Then we propose a cascading failure model based on the maximum flow theory in Section 3. In Section 4, we investigate the power grid invulnerability against cascades caused by node breakdowns with different tolerance parameters α and γ . Finally, a summary and some conclusions are provided in Section 5.

2. Modeling power grids

A power grid can be regarded as an interconnected production and consumption network with three function parts corresponding to generation, transmission, and distribution respectively, which are interconnected by transmission lines ^[18]. As one of the typical complex networks, all the buses could be abstracted to nodes consisting of the source nodes (or the generator nodes), the sink nodes (or the load nodes) and the intermediate transmission nodes, and the counterparts of transmission lines or transformer branches are edges. To prepare for the later calculation of the maximum flow in the power grid, here we consider the maximum power supply and

demand for each source and sink, and the power transmission limit or the maximum power for transmission lines when modeling power grids. Now taking IEEE_9 bus system for instance, we show the topology modeling process of the complex power system ^[21-22] in Fig.1. In the meantime, we mark the properties of nodes and edges in the topology architecture.

Fig.1 Topology modeling process of IEEE_9 bus system

In Fig.1, $V = \{v_1, v_2, \dots, v_9\}$ represents the node sets. The red circle and green circle represent the source node and sink node respectively, and the white circle stands for the intermediate transmission node. The corresponding relationship is $(B_1 \rightarrow v_1, B_2 \rightarrow v_2, B_3 \rightarrow v_3, B_4 \rightarrow v_4, B_5 \rightarrow v_5, B_6 \rightarrow v_6, B_7 \rightarrow v_7, B_8 \rightarrow v_8, B_9 \rightarrow v_9)$. The number on the node corresponds to the maximum power supply or demand depending on the color of the node. Similarly, the number on the edge represents the maximum power of transmission lines.

3. Cascading failure model

3.1. Maximum flow in power grid

In 1955, Harris first put forward the maximum flow problem when studying the maximum traffic in the railway. Subsequently, Ford, et al. established the maximum flow theory aiming at solving this problem in 1956^[23], which is an optimization problem about network flows based on graph theory. At present, the maximum flow theory has been widely applied to communication networks, transport networks, power systems and other fields. Actually, the reason for introducing the maximum flow theory to power grids to analyze the cascades is that the constraints of the maximum flow and the power flow calculations are similar. In power grids, the power will be transmitted along all possible paths between sources and sinks under operation constraints, such as generator output constraints, constraints of transmission line capacities and so on. Meanwhile, the power grid is always in a critical or sub-critical state under the dual role of the evolution of power grid itself and the load demands. Coincidentally, the maximum flow theory focuses on the maximum flow between sources and sinks when flows are within the corresponding capacities of transmission lines, which is similar to the power flow calculation of power grids. Besides, the power grid is in the critical state when the network flow achieves its maximum value. In this situation, a minor disturbance is easy to trigger cascading failures, when the actual blackouts often happen. Therefore, we compare network flows to power flows of power grids, based on which the propagation mechanism of cascading failures is investigated and the impacts of load distribution of power grids on the invulnerability of power grids are discussed. Thus, the solution to the maximum flow problem of power grids is to find the

maximum power from source v_g to sink v_d according to the power flow restriction of lines and nodes shown as below [24-26].

$$c(L_{ij}) \geq f(L_{ij}) \geq 0 \quad (1)$$

$$\sum_{j=1}^r f(L_{ij}) = \sum_{s=r+1}^m f(L_{si}) \quad (2)$$

$$|v(f)| = \sum_{L_{gi} \in L} f(L_{gi}) = \sum_{L_{kd} \in L} f(L_{kd}) \quad (3)$$

where i, j, s, g, k are the node labels respectively. $c(L_{ij})$ is the maximum power transmission capacity in line L_{ij} . m is the number of adjacent nodes of node v_i and r is the number of the adjacent nodes from which the feasible flows flowing into node v_i . $f(L_{ij})$ stands for a feasible flow on line L_{ij} from node v_i to node v_j , while $f(L_{si})$ is the one from node v_s to node v_i . $v(f)$ represents the network flow, and L is the set of transmission lines.

Eq.(1) - Eq.(3) restrict the feasible flows in nodes and transmission lines respectively, in which no feasible flow loss appears in the power grid. Eq.(1) ensures that the feasible flow on any transmission line is smaller than or equal to the transmission power limit. Inflow and outflow of intermediate transmission nodes v_i are guaranteed to be equal in Eq.(2). Eq.(3) implies the network flow having a value of $v(f)$ that is generated from source v_g and flows to sinks v_d . Then, the maximum flow of the network is the maximal $v(f)$ satisfying the above three constraints. In this case, the feasible flow of line L_{ij} from source v_g to sink v_d is the maximum feasible flow of line L_{ij} denoted by $f_{ij,gd}$. Since the feasible flow of node v_i relates to the flows of all lines connected to it, the maximum feasible flow of node v_i , denoted as F_i , can be expressed as Eq.(4) when considering all node pairs of sources and sinks.

$$F_i = \begin{cases} \sum_{g \in G} \sum_{d \in D} \left(\frac{1}{2} \sum_{j \in \Gamma_i} |f_{ij,gd}| \right) & v_i \notin \{G \text{ or } D\} \\ \sum_{g \in G} \sum_{d \in D} \left(\sum_{j \in \Gamma_i} |f_{ij,gd}| \right) & v_i \in \{G \text{ or } D\} \end{cases} \quad (4)$$

where Γ_i is the set of the adjacent nodes of node v_i , and G and D are the sets of sources and sinks respectively.

As the feasible flows of source v_g and sink v_d are limited by the maximum power supply P_{Limit}^g and the maximum demand P_{Limit}^d respectively, the corresponding maximum feasible flow of v_g or v_d will be smaller than or equal to $\min(P_{Limit}^g, P_{Limit}^d)$. Meanwhile, the feasible flow of the intermediate transmission nodes can be updated by the exceeding ratio.

3.2. Modeling cascade

The invulnerability analysis based on modeling cascading failures from the perspective of complex network theory helps reflect the impact of topology on dynamic behaviors of power grids. Given that the cascading failure models of power grids built on complex network theory are mainly capacity/load models, we will analyze the invulnerability of power grids through building a capacity/load model. In this section, we take the maximum feasible flow F_i as the initial load of node v_i , which is shown as bellow, so as to fill the gap of ignoring electrical

properties in previous studies.

$$L_i(0) = F_i^\gamma \quad (5)$$

where γ is a tunable parameter mentioned in Introduction and used to control the distribution of the initial loads.

In practice, the node load will fluctuate at the premise of load demand growth or component failures in power grids. Normally, the nodes with bigger load fluctuations are those adjacent to failed nodes, and they receive loads distributed from those failed nodes following certain load distribution principle. In this paper, we adopt the distribution strategy in which the loads of failed nodes are distributed to their adjacent nodes according to the proportions of their residual capacities. Moreover, in order to avoid the breakdown of adjacent node v_i caused by load redistribution in cascading failures, we add some tolerance capacity $\alpha L_i(0)$ to its initial node load so as to resist load fluctuations and enhance the invulnerability of power grids. In this way, the node v_i has the biggest load-carrying ability named the capacity of node v_i devoted as $C_i = (1 + \alpha)L_i(0)$. Generally, bigger α yields better invulnerability, which implies more construction cost of the power grid. As a result, we have to find a trade-off between the power grid invulnerability and its construction cost. A traditional solution to this problem is to find a tolerance parameter threshold α_T . That is, the power grid invulnerability will be maintained in a specific range when $\alpha > \alpha_T$, which can prevent construction cost increase from increasing α too much without affecting the power grid invulnerability.

The invulnerability of a power grid against cascades means the ability to maintain its topology structure integrity or its continuous power supply capability to users through self-regulation when suffering attacks. In addition, the invulnerability of power grids varies with node attack strategies. Thus we explore the invulnerability from structure and power supply capability or load loss under different attack strategies based on high-load nodes, low-load nodes and all nodes respectively, which correspond to three sets of initially failed nodes and are denoted by S_1 , S_2 and S_3 respectively. We simulate cascading failures with the process that every node in the initially failed node set takes turns triggering the cascading failure to examine the corresponding destruction level in power grid. Here we take the average destruction level to measure the invulnerability under each attack strategy. The structural index and electrical index we use to measure the invulnerability are the average scale of the largest connected subgraph G and the average load loss rate L^{lost} respectively. They are shown as below.

$$\begin{cases} G = \frac{1}{n} \sum_i^n n_i^{\max} / N \\ L^{lost} = \frac{1}{n} \sum_i^n L_i^{lost} / \sum_j^N L_j(0) \end{cases} \quad (6)$$

where n is the scale of the initially failed node set, and N is the power grid scale. $n_i^{\max}$ and L_i^{lost} are the scales of the largest connected subgraph and the load loss rate caused by removing the initially failed node v_i respectively. One thing to note here is that the largest connected subgraph possesses both the power supply and demand, which means the largest connected subgraph includes sinks and sources simultaneously.

3.3. Proceeding of cascade simulation

Influenced by faults in operating equipment, man-made operation mistakes, extreme weather and so on, the number of failed nodes can be more than one at a moment in the power grid. Since these failed nodes have complex correlations in both topology structure and running status, the probability of related and unrelated failures increases apparently in the power grid, generating the so-called failure clustering phenomenon or cascading failures which induce the blackouts^[27-28]. In order to reveal the relationship between cascading failures and invulnerability in the power grid, we build a cascading failure model based on the maximum flow theory and further explore the invulnerability against cascades by using the simulation method. The simulation process of cascading failures is shown in Fig.2.

Fig.2 Process of cascades

Step1. Select an initially failed node set S_i ($t \in (1,2,3)$). In this paper, S_1 and S_2 are composed of the first ten and last ten nodes in descending order of node load amount respectively, while the scale of S_3 is the size of the power grid.

Step2. Select an initial failed node v_i from the set S_i and remove it from the grid.

Step3. Calculate the load $L_j(t)$ for node v_i in the t th step of the cascading failures in the residual grid. If $L_j(t) > C_j$, node v_j is overloaded. Then count and record the number of overloaded nodes, donated by n_0 , and remove them. If $n_0 > 0$, repeat this step, otherwise, go to Step 4.

Step4. Calculate the corresponding scale of the largest connected subgraph $n_i^{\max}$ and the load loss rate L_i^{lost} caused by removing node v_i . If $i < n$, go to Step 2; otherwise, go to Step 5.

Step5. Calculate the invulnerability of the power grid according to Eq. (6), and then the process of cascading failures ends.

4. Invulnerability analysis of power grids

As stated above, the invulnerability of power grids based on cascading failure model simulation varies by attack strategy. For example, the breakdowns of high-load nodes can probably cause worse invulnerability of the power grid, but the cases with low-loaded nodes are exactly the opposite^[15,29]. Thus, we can easily and directly find out the impact of attack strategies on the invulnerability throughout cascading failure simulation. In this

section, we investigate the relationship between the node load distribution and the invulnerability under three attack strategies based on high-load nodes (S_1), low-load nodes (S_2), and all nodes of the grid (S_3) in the 500KV Center China power grid respectively. And the grid includes 90 nodes and 128 transmission lines, and the topology is shown in Fig.3. Notice that the invulnerability here is the average invulnerability under each attack strategy, and is the average value for all invulnerability calculated after simulating cascading failures initiated by each node in the sets of initial failure nodes.

Fig.3 the topology of 500KV Center China power grid

The inequality of node load distribution can be depicted by Gini-coefficient g in economics ^[30-31], which can reflect the overall distribution differences of a certain data set ^[32]. For example, it has been used successfully to reflect the inequality of centrality indices on geographic networks of urban streets to classify cities ^[33]. Note that larger g implies greater differentiation of node load distribution. Since the inequality of node load distribution varies depending on γ , we show the value changes of g with γ in Tab.1.

Tab.1 Node load distribution with γ

γ	0.4	0.6	0.8	1.0	1.2	1.4	1.6	1.8	2.0	2.2	2.4
g	0.27	0.36	0.44	0.52	0.59	0.65	0.71	0.75	0.79	0.82	0.84

From Tab.1, we can see that the node load distribution becomes more uneven with γ , which suggests the increasing appearance probability of high-load nodes and decreasing for low-load nodes. Moreover, high-load nodes will carry more and more loads, while the case is reverse for low-load nodes. In this case, how do α and γ affect the invulnerability under different attack strategies in the power grid? We will find the answers in cascading failure simulations. We first display the relationship between invulnerability and α under different attack strategies of the 500KV Center China power grid in Fig.4-Fig.6.

Fig.4 Impact of high-load node attacks on invulnerability with α Fig.5 Impact of low-load node attacks on invulnerability with α Fig.6 Impact of attacks based on all nodes on invulnerability with α

As known from Fig.4-Fig.6, the invulnerability is enhanced with the growth of α no matter measured by structural index or electrical index. This is easy to understand: when the residual capacity of each node increases with α , the node is able to accommodate more extra nodes from failed nodes, which equals improving the ability against load fluctuations for each node. Furthermore, we can also find that the tolerance parameter thresholds α_T are the same no matter measured by G or L^{lost} under the same γ , which illustrates that the two

measures have the same evaluation effects in invulnerability. However, the change rules of α_T differ under different γ with the same attack strategy as we can see. Besides, we find that the inequality of the load distribution grows constantly with γ from Tab.1. That is to say, the loads of low-load nodes become less, while the ones of high-load nodes keep growing. Consequently, the damaged area under low-load node attacks can be controlled in a smaller scope than that under high-load node attacks which corresponds to worse invulnerability. Thus, we select $G > 0.98$ for low-load node attacks, $G > 0.93$ for high-load node attacks, and $G > 0.96$ for attacks based on all nodes when we search for α_T under different attacks. The relationship between α_T and γ is shown in Fig.7.

Fig.7 Relationship between α_T and γ

Clearly, the thresholds α_T under attacks based on S_1 and S_3 increase with γ , but it decreases under the attacks based on S_2 as seen in Fig.7. The reason for this phenomenon can be explained from the power shift and blackout risk. As the load distribution becomes more and more uneven, the loads of low-load nodes are smaller and smaller, which leads to the case that the large-scale power shifts caused by load distributions after nodes fail become less and less. Since the large-scale power shift is one of the main factors of blackouts, the blackout risk induced by low-load node breakdowns will decrease as γ increases. At this moment, the threshold of the tolerance parameter when the power grid reaches high robustness is gradually decreasing. While the case is just in the opposite direction for high-load nodes. Therefore, the thresholds α_T under attacks based on S_1 and S_3 increase with γ , but it decreases under the attacks based on S_2 . In addition, it is not difficult to see from Fig.7 that the power grid can completely has the same invulnerability under different attack strategies if we select appropriate γ and α when we neglect the differences of invulnerability values. For instance, the attacks based on high-load nodes and low-load nodes lead to the same invulnerability of the power grid when we select the coordinate with $\gamma \approx 1.15$ and $\alpha = 0.5$.

Moreover, the curve trends of invulnerability against cascades vary with γ under different α . We take $\alpha = 0.35$ and $\alpha = 0.5$ for instance to show the effect of load distribution on the invulnerability in Fig.8~Fig.10.

Fig.8 Invulnerability of the power grid with γ under high-load node attacks ((a) $\alpha = 0.35$, (b) $\alpha = 0.5$)

Fig.9 Invulnerability of the power grid with γ under low-load node attacks ((a) $\alpha = 0.35$, (b) $\alpha = 0.5$)

Fig.10 Invulnerability of the power grid with γ under attacks based on all nodes ((a) $\alpha = 0.35$, (b) $\alpha = 0.5$)

When $\alpha = 0.35$, the invulnerability under high-load node attacks decreasing first and then increasing, tends to be stable with γ at the end. On the other hand, the attacks based on both low-load nodes and all nodes of the power grid make the invulnerability increase all the time until the peak as γ grows. While $\alpha = 0.5$, with the growing of γ , the invulnerability corresponding to high-load node attacks is weakened gradually until a stable state is reached, and the change trend of the invulnerability shows the opposite direction under low-load node

attacks. As for the invulnerability resulted from alternate breakdowns of all nodes in the power grid, it is enhanced at first and then weakened until it becomes stable. The phenomenon above demonstrates that the load distribution of nodes greatly affects the invulnerability of the power grid, and the invulnerability shows totally different change rules under different attack strategies. Therefore, the purpose of the invulnerability enhancement of the power grid can be achieved by selecting proper γ under different α .

5. Conclusion

The invulnerability analysis is the premise of reliability determination of the power grid. In this paper, we have built a cascading failure model based on the maximum flow theory, and then the invulnerability of the power grid has been analyzed by means of cascading failure simulation. The simulation results show that the tolerance parameter threshold α_T increases under attacks of high-load nodes or all nodes of the power grid with γ , but decreases under low-load node attacks. In addition, the distribution of node loads will be more uneven and meanwhile, different attack strategies correspond to different invulnerability change rules as the tunable factor of node load distribution grows. The invulnerability under low-load node attacks shows the increasing trend until a stable value. For the invulnerability corresponding to breakdowns of high-load nodes, it is decreased first and then increased with a smaller tolerance parameter, while decreased first until to a stable with a bigger tolerance parameter. As for the invulnerability corresponding to alternate breakdown of every node in the power grid, it is gradually strengthened and tends to achieve stability under a smaller tolerance parameter, while it is increased at first and then decreased until a stable point under a bigger tolerance parameter. These results may be very useful for the power grid planning against cascades in the future.

Reference

- [1] Albert R, Jeong H, Barabasi A L. Error and attack tolerance of complex networks [J]. Nature, 2000, 406(6794): 378-382.
- [2] Broder A, Kumar R, Maghoul F, et al. Graph structure in the Web [J]. Computer Networks, 2000, 33(1): 309-320.
- [3] Jeong H, Mason S, Barabasi A-L, et al. Lethality and centrality in protein networks [J]. Nature, 2001, 411: 41-42.
- [4] Newman M E J, Forrest S, Balthrop J. Email networks and the spread of computer viruses [J]. Physical Review E, 2002, 66(3): 035101/1-4.
- [5] Chen S M, Jiang J H, Pang S P, et al. Modeling and Optimization of Train Scheduling Network Based on Invulnerability Analysis [J]. Applied Mathematics and Information Sciences, 2013, 7(1): 113-119.
- [6] Peng H, Zhao D D, Han J M, et al. Invulnerability of grown Peer-to-Peer networks under progressive targeted attacks [J]. Physica A: Statistical Mechanics and its Applications, 2015, 428: 60-67.
- [7] US-Canada Power System Outage Task Force, Abraham S, Dhaliwal H, et al. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations [R/OL]. US-Canada Power System Outage Task Force, 2004.
- [8] Central Electricity Regulatory Commission. Report on the Grid Disturbances on 30th July and 31st July 2012 [R/OL]. <http://www.cercind.gov.in>, 2012-08-08.
- [9] Cohen R, Erez K, ben-Avraham D, et al. Resilience of the Internet to random breakdowns [J]. Physical Review Letters, 2000, 85(21): 4626-4628.
- [10] Paul G, Sreenivasan S, Stanley H E. Resilience of complex networks to random breakdown [J]. Physical Review E, 2005, 72(5): 056130/1-6.
- [11] Holme P, Kim B J, Yoon C N, et al. Attack vulnerability of complex networks [J]. Physical Review E, 2002, 65(5): 056109/1-15.
- [12] Casals M R, Valverde S, Sole R V. Topological vulnerability of the European power grid under errors and attacks [J].

International Journal of Bifurcation and Chaos, 2007, 17(7): 2465-2475.

- [13] Sole R V, Casals M R, Murtra B C, et al. Robustness of European power grids under intentional attack [J]. Physical Review E, 2008, 77(2): 026102/1-7.
- [14] Qi J J, Mei S W, Liu F. Blackout model considering slow process [J]. Power Systems, IEEE Transactions on, 2013, 28(3): 3274-3282.
- [15] Qi J J, Dobson I, Mei S W. Towards estimating the statistics of simulated cascades of outages with branching processes [J]. Power Systems, IEEE Transactions on, 2013, 28(3): 3410-3419.
- [16] Ren H P, Song J, Yang R, et al. Cascade failure analysis of power grid using new load distribution law and node removal rule [J]. Physica A: Statistical Mechanics and its Applications, 2016, 442: 239-251.
- [17] Dai Y Y, Chen G, Dong Z Y, et al. An improved framework for power grid vulnerability analysis considering critical system features [J]. Physica A: Statistical Mechanics and its Applications, 2014, 395: 405-415.
- [18] Monfared M A S, Jalili M, Alipour Z. Topology and vulnerability of the Iranian power grid [J]. Physica A: Statistical Mechanics and its Applications, 2014, 406: 24-33.
- [19] Fan W L, Liu Z G, Hu P. A high robustness and low cost cascading failure model based on node importance in complex networks [J]. Modern Physics Letters B, 2014, 28(2): 1450011/1-11.
- [20] Mei S W, Zhang X M, Cao M. Power grid complexity [M], 2011, Springer Science & Business Media.
- [21] Rosato V, Bologna S, Tiriticco F. Topological properties of high-voltage electrical transmission networks [J]. Electric Power Systems Research, 2007, 77(2): 99-105.
- [22] Correa G J, Yusta J M. Grid vulnerability analysis based on scale-free graphs versus power flow models [J]. Electric Power Systems Research, 2013, 101: 71-79.
- [23] Ford L R, Fulkerson D R. Maximal flow through a network [J], Canadian Journal of Mathematics, 1956,8: 399-404.
- [24] Dwivedi A, Yu X, Sokolowski P. Analyzing power network vulnerability with maximum flow based centrality approach [J]. // Proceeding IEEE International Conference Industrial Informatics, Osaka, Japan, Jul. 2010: 336-341.
- [25] Ju W Y, Li Y H. Identification of Critical Lines and Nodes in Power Grid Based on Maximum Flow Transmission Contribution Degree [J]. Automation of Electric Power Systems, 2012, 36(9): 6-12.
- [26] Dwivedi A, Yu X H. A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis [J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 81-88.
- [27] Mei S W, Ni Y X, Wang G, et al. A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin [J], IEEE Transactions on Power Systems, 2008, 23(4): 1719-1726.
- [28] Mei S W, He F, Zhang X M, et al. An improved OPA model and blackout risk assessment [J], IEEE Transactions on Power Systems, 2009, 24(2): 814-823.
- [29] Motter A E, Lai Y C. Cascade-based attacks on complex networks[J]. Physical Review E, 2002, 66(6): 065102/1-4.
- [30] Du W B, Zheng H R, Hu M B. Evolutionary prisoner's dilemma game on weighted scale-free networks [J]. Physica A: Statistical Mechanics and its Applications, 2008, 387, (14): 3796-3800.
- [31] Du W B, Cao X B, Hu M B. Asymmetric cost in snowdrift game on scale-free networks [J]. Europhysics Letters, 2009, 87, (6): 60004/1-6.
- [32] Dagum C. The Generation and Distribution of Income, the Lorentz Curve and the Gini Ratio [J]. Economie Appliquée, 1980, 33(2): 327-367.
- [33] Crucitti P, Latora V, Porta S. Centrality in networks of urban streets [J]. Chaos, 2006, 16(1): 015113/1-9.

Actually, the reason why we introduce the maximum flow to analyze the propagation mechanism of cascading failures in power grids is that the maximal flow calculation is similar to the power flow calculation[改为 the maximum flow theory introduced to power grids to analysis cascades is that the constraints is similar when we calculate the maximum flow and power flow and the background is alike when the cascades happen.]