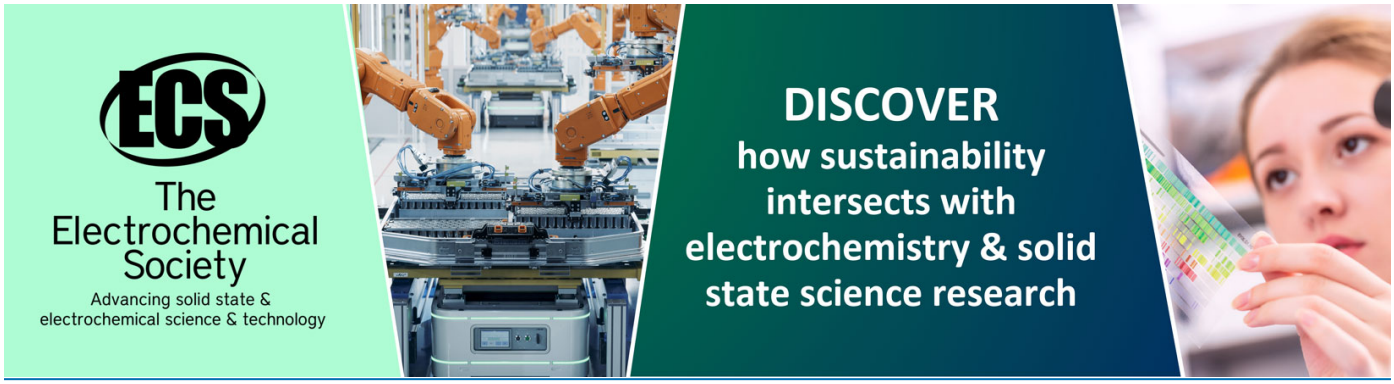
Study on identifying the vulnerability of the data center power network



IOP Conf. Series: Journal of Physics: Conf. Series **1176** (2019) 062054 doi:10.1088/1742-6596/1176/6/062054

Study on identifying the vulnerability of the data center power network

Chunjian Kang[1,*], Xinpei Liu[1], Su Chen[1], Junbiao Xu[1]

[1]National Computer Network Emergency Response Technical Team /Coordination Center of China, Beijing, China

*Corresponding author e-mail: vithon@163.com

Abstract. With the wide application of the internet and rapid development of the information technology, the scale of the internet data center power network is growing larger and larger. Some of the troubles in the internet data center (IDC) power network may cause extensive service out of service or even collapse. However, without considering the characteristics of the IDC power network, the important node identification methods for the IDC power network based on graph mainly focus on the graph structure itself. Since a large number of automatic switching equipment such as ATS, STS and loop switch have been used in IDC, when the electrical fault occurs, the load will be automatically migrated to the adjacent electrical equipment, which may lead to overloading or even tripping. So the failure is extended. So how can we efficiently and effectively capture the fault evolution mechanism of the IDC power network? How do we go about identifying the vulnerable nodes causing the collapse of the IDC power network.

In this article, we propose DCPNFEM, a novel fault evolution model for the IDC power networks, as well as a fitting algorithm, BCBL, which can solve the proposed problems. Our algorithms have the following properties: (a) Intuitively: it detects fault evolution mechanism, such as power load migration, electrical equipment tripping, and so on; (b) Timely: our method is based on the real-time power loads; (c) General: our algorithms are general and practical ,which can be used in various power network topologies, including data center infrastructures from tier1 to tier4.

Extensive experiments on a real IDC power network demonstrate that some particular nodes' failure can lead to the power network crash under DCPNFEM. And BCBL algorithm outperforms better accuracy and speed than many other algorithms.

1. Introduction

With the development of the Internet, cloud computation, artificial intelligence, etc., the scale of the IDC infrastructure increases rapidly. According to statistics, there are more than 3 million data centers in the world, whose power consumption accounts for 1.1%-1.5% of the total global electricity consumption. When Google runs its Oregon data center at full capacity, it can consume almost as much power as all the homes in Newcastle. Unfortunately sometimes, seemingly insignificant accidents may lead to the collapse and paralysis of the entire power distribution network. For example, on July 3, 2009, a fire broke out in a power distribution room in Fisher Square, Seattle, causing the paralysis of Authorize.net, Payment Portal, Microsoft Bing Travel Service, Geocaching.com Service,

Dotster Domain Name Registration Service and dozens of other websites. Therefore, the ultra-large data center has urgent requirements for the security and reliability of the power network.

However, large-scale blackouts and catastrophic accidents may be hidden in the power networks due to the reasons for human factors, computing, communication, protection and control, or internal faults, which are unpredictable and extremely difficult to be detected in advance. But it is predictable to grasp the impact of the power network faults from a macro-global perspective, which can guide the power network planning, help maintenance staff keep a watchful eye on critical nodes which should be involved in targeted maintenance plans and contingency plans. Therefore, it is essential that we analyze the vulnerability of the IDC power network. The studies of vulnerability of the IDC power network are mainly based on operation parameters of electrical equipments and network structure of the IDC power network.

Related works. The researches based on the operating parameters of electrical equipments mainly include analytical method and Monte Carlo method. Article [1, 3] analyzed the vulnerability of power system based on energy function, article [4, 6] analyzed the inherent vulnerability of power system based on the reliability parameters of electrical equipments.

American scholar Dobson, Carreras, Thorp, etc., studied the occurrence mechanism of the power failure accident by the achievement of complex theory. And they put forward OPA model [7], Hidden Failure model [8, 9], Cascade model [10] and HOT model [11], which described the occurrence of blackouts. Article [12, 13] pointed out that nodes with higher betweenness and degree play a diffused role in the transmission of faults as well as make sure the connectivity of the IDC power network, and analyzed the structural vulnerability of the IDC power network from the perspective of network topology.

Characteristics of the IDC power network. However, differ from the traditional power system, the power network in data center applies a lot of automatic switching electrical equipments such as loop switch, ATS, MTS, STS, etc., for redundancy and mutual standby. As a result, the IDC power network presents non-lined fault diffusion characteristics when some faults occur. Moreover, the impact is different when some power loads lose due to the importance of the power loads. So the characteristics of application scenario should be considered when analyzing the vulnerability of the IDC power network.

In this paper we present a fault evolution model and a novel algorithm for identifying vulnerable nodes based on characteristics of the IDC power network topology as well as the requirements of the power load classification.

Outline. Other parts of this article are organized as follows: Next we build a graph model for the IDC power network, followed by the proposed model and the novel algorithm, simulations, discussion and conclusions.

2. Model of the IDC power network

The large-scale IDC power network consists of various electrical devices as well as various power loads. All the electrical devices can be divided into power transformation equipment (transformers, etc.), transmission equipment (such as various distribution cabinets), and power consumption equipment (such as various loads). All kinds of electrical equipments are connected by cables or buses to transmit electricity. The power can only be transmitted from the power sending-end (power grid) to the receiving-end (load).

Therefore, the topology of large-scale IDC power network can be modeled by directed acyclic graph $G=(V,E)$, where V is the vertex set and $E \subseteq V \times V$ is the directed edge set. $e=(x,y)$ in set E is an electrical line connecting two devices x and y, including transmission cables and power buses.

According to the input and output mode of electrical equipments, there are three types of nodes in the IDC power network (Figure 1). The first type of node $\tau_1 \in V$ is single input and single output, such as circuit breaker. The second kind of node $\tau_2 \in V$ has dual power inputs, but the output is single. Normally it works on one road, for example road *A*. Once the power *A* is cut off, it will automatically switch to another road (the power road *B*), so that the loads are transferred from one road to another. Typical equipments are as loop switches, ATSs and so on. The third kind of node $\tau_3 \in V$ has a single

power input, but multiple outputs, that is, many loads get power from this output terminal of the electrical equipment. For example multiple loads are connected to the output terminal of a circuit breaker.

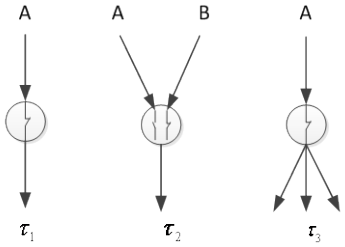


Figure 1. Connection mode of the IDC power network nodes.

Theorem 1. When a power network works normally, it is a spanning tree of the graph G.

Demonstration. Because the function of the power supply system is to transfer electricity from the power grid to the loads. So it is obviously that the graph *G* and its spanning subgraph *T* are connected. Node τ_2 can be thought of as τ_1 when the power network works normally, so there are only two kinds of nodes in the graph, which are τ_1 and τ_3. Obviously, the two kinds of nodes have only one input, so there is only one path e for any two adjacent nodes (Figure 2). Cutting off e will lead to the back nodes be disconnected from the subgraph *T*, so the subgraph *T* is a tree.

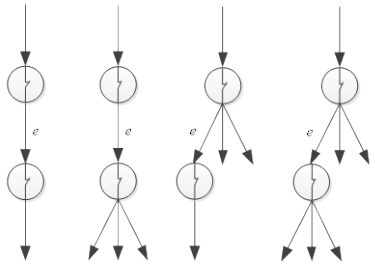


Figure 2. Connection of adjacent nodes in normal power networks.

3. Proposed model

In this part we raise our novel model DCPNFEM (Data Center Power Network Fault Evolution Model).

3.1 Characteristics of the IDC power network

The IDC power network can be thought of as a tree *T* when it works normally. As a node a fails, if the following node b of the fault node is of type τ_1 or τ_3, it will lead to the node b be disconnected from the graph *T*. This will lead the load getting power from a to loss.

If the following node b of the fault node is of type τ_2, then the connecting edge from the father node to node τ_2 is transferred from A to B (Figure1), or from B to A. And the working topology of the IDC power network is transferred from T_1 to T_2.

Sometimes the working road *A* of node τ_2 may loss power, then the working road is switched to road *B* with the father node c automatically for automatic switching equipments. And this will result in the load of node c which is another father node of b be overlapped with the additional loads from road *A*. If the new load of node c exceeds its setting capacity value, the node c trips. So that the node following the node c may be disconnected from the graph T_2, but the node b must be disconnected from the graph T_2. And then the working topology of the power network is transferred from the graph T_2 to T_3.

When a node is disconnected from the graph as the reason of fault or trip, the power supply does not recover automatically even if the node recovers from failure. Therefore, the impact of the initial

failure tends to be expanded. Figure3 shows one of the fault evolution proceedings when the child node b is type of τ_2.

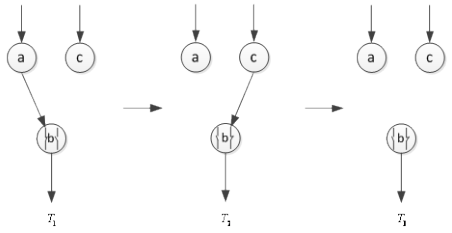


Figure 3. A fault diffusion process.

For convenience, we define the symbols and its definitions in Table 1.

Table 1. Symbols and definitions.

Symbol	Definition	Symbol	Definition
I_α	The setting value of the tripping current of node α	$\dot{I}_u$	The output current's vector value of UPS_u
i_j^a	Phase a's working current of load j	$\dot{L}_i$	The working current's vector value of load i
i_j^b	Phase b's working current of load j	L_i	The effective value of working current of load i
i_j^c	Phase c's working current of load j	η_u	The working efficiency of UPS_u
θ_x	The power-factor angle of load x	$\dot{I}_u^{in}$	The input current's vector value of UPS_u

The IDC power network is linear, so the load current of each linear node satisfies the superposition theorem. The following formulas should be satisfied when the node α works normally:

$$\begin{aligned} I_\alpha &> \sqrt{(\sum_{j=1}^{N_\zeta} i_j^a \cos\theta_a)^2 + (\sum_{j=1}^{N_\zeta} i_j^a \sin\theta_a)^2} \\ I_\alpha &> \sqrt{(\sum_{j=1}^{N_\zeta} i_j^b \cos\theta_b)^2 + (\sum_{j=1}^{N_\zeta} i_j^b \sin\theta_b)^2} \\ I_\alpha &> \sqrt{(\sum_{j=1}^{N_\zeta} i_j^c \cos\theta_c)^2 + (\sum_{j=1}^{N_\zeta} i_j^c \sin\theta_c)^2} \end{aligned} \tag{1}$$

$$\dot{I}_u = \sum_{i=1}^{n} \dot{L}_i \tag{2}$$

There are factor correction circuits and reactive power compensation circuits in uninterruptable power supply (UPS), Therefore, the input current's vector value of an UPS should not be simply and linearly superimposed, it should be calculated as follows:

$$\dot{I}_u^{in} = \frac{\sum_{i=1}^{n} L_i \cos\theta_i}{\eta_u \cos\theta_u} \angle\theta_u \tag{3}$$

3.2 Proposed model

In this paper we proposed a data center power network fault evolution model (DCPNFEM) based on the characteristics of the IDC power network.

1) Input the initial state of the power network T_0 and the initial fault node's set $Tr = \{v_1, v_2, \ldots, v_r\}$, the number of which is r.

2) Calculate the child set S_m of the fault node m by applying depth-first search (DFS) or breadth-first search (BFS) in T_0. And then calculate the father nodes for every node n of S_m in graph *G*, in the meantime, delete the edge from m to n. If there is only one father node of n (that is *m*), put the node n into the fault nodes' set Tr as well as the set of new fault nodes Tr'. If there are two father nodes, enable the edge from normal father node n' to n.

3) If the set of new fault nodes Tr' is not empty, then go back to step 2). Now the fault node m belongs to Tr'. When Tr' is empty, the power network stays in state T_1.

4) Calculate the shortest path for every load $l_i \in L$ from power grid to load l_i in T_1.

5) Use the formula (2) to calculate the output load of an UPS. And then calculate the input current of UPS *u* by applying formula (3).

6) With regard to the load of the middle nodes between source nodes and UPSs in the shortest path of load l_i, it should be superimposed by the input of UPS （i_u^{in}）. And the load of the other middle nodes between UPS and load l_i, it can be superimposed by the load of l_i.

7) Inspect the working load of all the middle nodes in graph T_1, and determine whether it satisfies the formula(1). If one of the middle nodes does not satisfy the formula (1), put it into the fault nodes' set Tr. If all the middle nodes satisfy the formula (1), then the power network works in stable state T_Π.

The pseudo-code of our proposed model is as follows:

Model： **DCPNFEM** (A Data Center Power Network Fault Evolution Model) // Return T_Π

Require: *G*(The graph of the power network), T_0 (The initial state of data center power), $Tr = \{v_1, v_2, ..., v_r\}$（The set of initial fault nodes）, Tr' (The set of new fault nodes)

```
function Get_T1 (Tr)
    for m in Tr do
        Remove m from Tr'
        S_m = succesors of fault node m in T_0
        for n in S_m
            F_n = fathers of node n in G
            if length(F_n)==1
                Add n to Tr and Tr'
                Remove edge from m to n in T_0
            else if all of F_n in Tr or Tr'
                Add n to Tr and Tr'
                Remove edge from F_n to n in T_0
            else:
                Remove edge from m to n in T_0
                Add edge from F_n (without m) to n in T_0
    if length(Tr') == 0
        Return T_0
    else
        Get_T1 (Tr')
function Get_load (T_1)
    for l_i in L
        path_li = the shortest paths of l_i from source to load l_i in T_1
    for ups_u in path_li
        i_u += load(l_i)
    i_u^in = I_u /cos θ_u / η_u
    for node_k in path_li
        if node_k is before ups_u
            i_k += i_u^in
        else
            i_k += load(l_i)
T_1 = Get_T1 (Tr)
Tr' ← ∅
Get_load (T_1)
for n in G
    if I_n < sqrt((i_n cos θ_n)^2 + (i_n sin θ_n)^2)
        Add n to Tr and Tr'
if Tr' ≠ ∅
    DCPNFEM(Tr)
else
    T_Π = T_1
    Return T_Π
```

4. Proposed algorithms for identifying important nodes

Node centrality is an index for assessing the importance of a vertex in a graph. Many centrality indexes are used in the analysis of graphs, such as degree centrality, closeness centrality, betweenness centrality and eigenvector centrality. But the above methods for identifying the importance of nodes in the graph mainly focus on the topological structure of the graph itself, without considering the characteristics of the IDC power network.

In the IDC power network, electrical loads are classified into different levels, for example Load Level I, Load Level II and Load Level III. In this paper we propose a novel betweenness centrality based on load characteristics (BCBL) to identify the important nodes of the IDC power network. The formula is as follows:

$$C_L(i) = \frac{\sum_{s\in S, t'\in T'\subseteq T} \varphi_{st'}(i)\chi(t')}{\sum_{s\in S, t\in T} \varphi_{st}\chi(t)} \tag{4}$$

Where, S is the set of source nodes (power grid and diesel generators), T is the set of destination nodes (electrical loads), $T' \subseteq T$ is the set of destination nodes passing through node *i* in the routes from source to destination, $\varphi_{st'}$ is the capacity of load t'. $\chi(t) \in (0,1)$ is the load level of load *t*, which depends on the nature of the electrical load itself.

From formula (4) we can find that the identification algorithm we proposed not only considers the topological structure of the IDC power network, but also the load capacity and load nature. Our algorithm focuses on the important loads.

5. Experiments and results

The vulnerable nodes of the IDC power network mean that these nodes will cause a large-scale blackout failure after the fault occurs. The impact of outage failures is evaluated by two indicators: loss of load and loss of load in risk. The calculation methods are as follows

$$Loss = (1 - \frac{\sum_{i\in t\subseteq T_{\Pi}} load_i \times \chi_i}{\sum_{j\in t\subseteq G} load_j \times \chi_j}) \times 100\% \tag{5}$$

In formula (5), $Loss$ is the ratio of lost load after some nodes do not work, T_{Π} is the operation topology of the IDC power network after fault stabilization, G is the topological graph of the normal power network, $load_i$ is the capacity of load *i*, χ_i is the load level of load *i*. The calculation method of load lost in this paper reflects not only the amount of lost loads but also the importance of lost loads.

$$Loss\_risk = Loss \times \sum_{i\in tr} -\log_{10}(10^4 \times (1 - re(i))) \tag{6}$$

In formula (6), *Loss_risk* is the product of the value of the load lost and the logarithm failure probability of the broken-down nodes after failure occures, *tr* is the set of initial fault nodes, *re(i)* is the reliability of node *i*, *Loss* means the capacity of lost load. From formula (6), we can find that the vulnerability of failure nodes includes both the loss of load after failure and the possibility of losing these loads.

In this paper, Python 3 and Networkx which is a software for modeling graph theory and complex network are used to model and simulate one IDC power network. The simulated power network consists of 594 nodes, 719 edges and 205 loads. The graph model of the distribution system is shown in Figure 4. Partial simplified topology of the IDC power network is shown in Figure5.

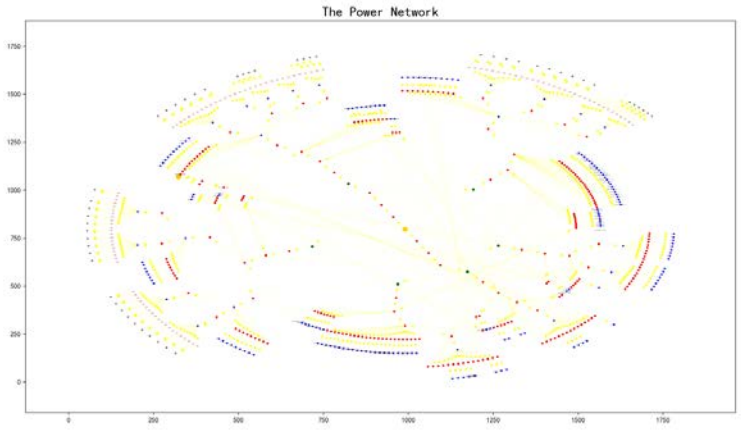


Figure 4. Modeled graph *G* of one IDC power network

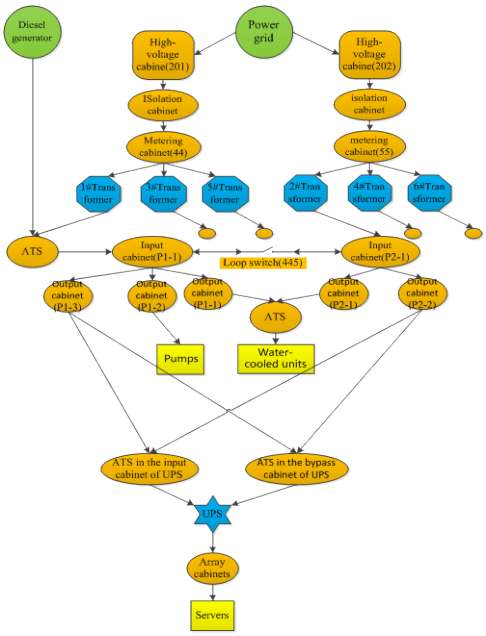


Figure 5. Partial simplified topology of the IDC power network

We removed some of nodes by random attacks and deliberate attacks. The result of random attack is the average value of 10 times' simulation result. The deliberate attack includes node degree centrality attack, node closeness centrality attack, node betweenness centrality attack, node eigenvector centrality attack and BCBL centrality attack. Figure 6 shows the relation curve of loss of loads (Formula 5) with the number of initial fault nodes. Figure 7 shows the variation between the number of initial fault nodes and the system vulnerability index Formula 6). From the results we can find that:

(1) Deliberate attack has a great influence on a power network. Attacking two (0.34%) nodes of this power network deliberately may cause more than 20% power loads loss, which indicates that there are **weak links** in the power network.

(2) Attacking four (0.68%) nodes of the power network with the proposed BCBL algorithm will lead to **crash of all loads**. This is because the BCBL algorithm takes both the topology of the power network and the load's characteristics into account. In addition, from Figure 5 we can find that there are two high-voltage cables in the power network. All load currents need to pass through these two

high-voltage devices. Therefore, the nodes in these two high-voltage road are vulnerable nodes of this power system.

(3) When attacking eight nodes of this power network by betweenness centrality, all the load crash. This shows that our proposed BCBL algorithm is more **effective** for finding the vulnerability of the power network. The efficiency of BCBL is twice of the betweenness centrality.

(4) Our proposed BCBL algorithm is **superior** to other important node analysis algorithms in terms of lost load and risk of load loss when the number of fault nodes is between 4 and 9. Because the possibility of more than 9 nodes failure is very low, so we do not discuss more nodes failure scenario.

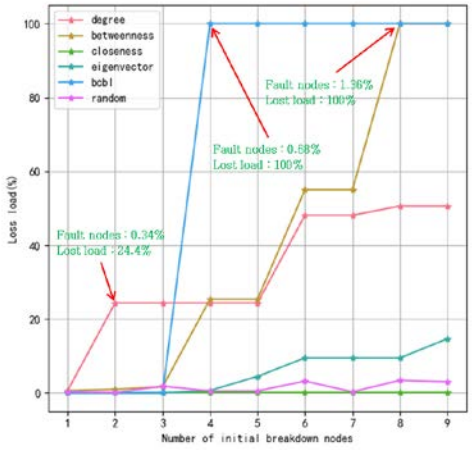


Figure 6. Relationship between the number of initial fault nodes and lost load

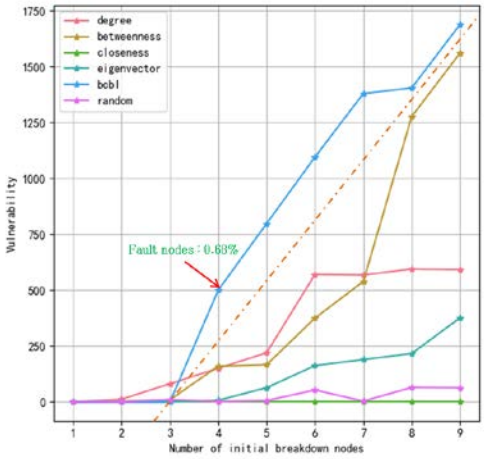


Figure 7. Relationship between the number of initial fault nodes and the power system vulnerability

6. Conclusions

In this article, we focused on the problems of analyzing the failure evolution mechanism and finding vulnerable nodes of the IDC power network. Our proposed model DCPNFEM and algorithm BCBL exhibits all the satisfactory properties:

(1) Intuitively: our modeling framework is based on the characteristics of the IDC power network, our method can simulate the fault evolution process, such as power load migration, electrical equipment tripping, and more.

(2) Timely: our method is based on the real-time power load, the fault evolution process varies as the power load changes. The power loads can be easily get from the power and environment monitoring system which is real-time.

(3) General: our algorithms are general and practical, which can be used in various power network topologies, including data center infrastructure from tier I to tier IV [14].

(4) Effectively: our algorithm is more efficient and effective than other algorithms in identifying the vulnerability of the IDC power network.

Acknowledgements

This work was supported by CNCERT/CC Foundation for Young Scholars.

References

[1] Demarco C L, Qverbye T J, An energy based security measure for assessing vulnerability to voltage collapse, J. IEEE Transactions on Power Systems, 5(2)(1990) 419-427
[2] Liu Qunying, Liu Junyong, Liu Qifang, Reactive power margin estimation by the view of the heuristic energy function, J. Proceedings of the CSEE, 28(4)(2008) 29-36.
[3] Nima Amja, Masoud Esmaili, Improving voltage security assessment and ranking vulnerable buses with consideration of power system limits, J. Electrical Power and Energy Systems, 25(2003) 705-715.
[4] Singh C, Patton A D, Protection system reliability modeling: Unreadiness probability and Mean duration of undetected faults, J. IEEE Transactions on Power Systems, 29(1980) 339-340.
[5] Yu Xingbin, Singh C, A practical approach for integrated power system vulnerability analysis with protection failures, J. IEEE Transmissions on Power Systems, 19(4)(2004) 1818-1820.
[6] Su Sheng, Li K K, Chan W L, et al, Monte Carlo based maintenance resource allocation considering vulnerability, C. Transmission and Distribution Conference & Exhibition: Asia and Pacific, (2005) 1-5.
[7] DOBSON I, CARRERAS B A, LYNCH V E, et al, An initial model for complex dynamics in electric power system blackouts, C. Proceedings of the 34th Hawaii International Conference on System Sciences, (2001) 710 - 718.
[8] BAE K, THORP J S , A stochastic study of hidden failures in power system protection, J . Decision Support Systems, 24(3)(1999) 259 - 268.
[9] CHEN J, THORP J S, Study on cascading dynamics in power transmission systems via a DC hidden failure model, C. Proceedings of the IEE Fifth International Conference on Power System Management and Control, (2002) 384 -389.
[10] DOBSON I, CHEN J, THORP J S, et al, Examining criticality of blackouts in power system models with cascading events, C. Proceedings of the 35th Hawaii International Conference on System Sciences, (2002) 7- 10.
[11] STUBNA M D, FOWLER J, An application of the highly optimized tolerance model to electrical blackouts, J. Int J of Bifurcation and Chaos, 13(1)(2003) 237 - 242.
[12] MENG Zhong-wei, LU Zong-xiang, SONG Jing-yan, Comparison analysis of the small-world topological model of Chinese and American power grids, J . Automation of Electric Power Systems, 28(15)(2004) 21-24.
[13] DING Ming, HAN Ping-ping, Small-world topological model based vulnerability assessment to large-scale power grid, J. Proceedings of the CSEE, 25(2005) 118 – 122
[14] Sonny K. Siu, John Lopopolo, Compatibility, sizing, and design considerations for generators and UPSs in Tiers I, II, III, and IV topologies, J. IEEE Transactions on Industry Applications, 47(2011) 2324-2329