Attack Structural Vulnerability of Complex Power Networks

Guo Chen, Student Member, IEEE, Zhao Yang Dong, Senior Member, IEEE
David J. Hill, Fellow, IEEE, Guo Hua Zhang

Abstract— Electric power networks have been studied as a typical example of real-world complex networks. Different from previous approaches, in this brief, a hybrid algorithm for structural vulnerability analysis of power networks is proposed. In the algorithm a DC power flow model with hidden failures is embedded into the error and attack tolerance methodology. The scheme embodies some important characteristics of power networks, which had been ignored in previous approaches. Furthermore, the simulation test on the standard IEEE 118 bus system demonstrates different phenomena from previous results which said that power grids are robust to random failure but vulnerable to intentional attacks. We find that there exists a critical region and when the power grid operates in the critical region, it is vulnerable to both random and intentional attacks. Finally, an analytical method is presented to support the new result.

Index terms- Complex networks, Power networks, Vulnerability, DC flow model

I. Introduction

Since its naissance, power networks have received much attention and electricity is recognized as a key to societal progress throughout the world. However, the frequency of large blackouts has not decreased in spite of technological progress and huge investments in system reliability and security. For instance, in July and August 1996, two blackout events took place successively in the power grid of west American, which led to more than 4 million people in 11 states out of power service [1]. In August 2003, a historic blackout is triggered in the power grid of the United States and Canada, which disconnected 61,800 MW of power to an area spanning most of the north-eastern states and two provinces of Canada, totally, containing 50 million people [2]. This event astonished the whole world and even reminded many people of 9.11. Although American government has ruled out terrorism as a possible cause for the blackout, it does not mean that power systems could not became the next targets to terrorists with a broad range of terrible motives [3].

Because the loss of large blackouts is usually huge, identifying the vulnerability of power grids and defending terrorist attacks become an urgent and important work for government and researchers. The frequent occurrence of blackouts exposes potential problems of current mathematical models and analysis methodology in power systems, which simulates researchers to seek solutions from alternative means.

Recently, complex networks theory and its error and attack tolerance methodology have drawn the link between the topological structure and the vulnerability of networks. Initially, the methodology was proposed by physicists and they mainly focused on complex abstract networks, such as ER random networks, BA scale-free networks etc. [4-8]. Then some physicists tried to employ the methodology into analyzing structural vulnerability of power networks because mathematically, power networks can be described as a complex network with nodes connected by edges [9]. Motter et al. [1] discussed cascade-based attacks on real complex networks and pointed out that the Internet and power grids were vulnerable to important node attacks but evolved to be quite resistant to random failure of nodes. Casals et al. analyzed topological vulnerability of European power grid [10] and found that power grids display patterns of reaction to node loss similar to those observed in scale-free networks, namely robust-yet fragile property. Similar results could be found in Crucitti et al.' and Kinney et al.' work, in which they made structural vulnerability analysis for Italian electric power grid [11] and North American power grid [12] respectively.

Above work is a good start to analyze vulnerability of power networks and complex network theory inaugurates a new direction for power systems research. However, electrical power networks are quite different from those abstract networks. They are governed by Kirchoff's Voltage and Current Laws, not simply by topological structure, which might result in a unique pattern of interaction between different nodes. Consequently, whether these results [9-12] will remain valid when dealing with power systems given the characteristics of the system and power flow constraints is still unknown.

In this brief paper, a hybrid algorithm will be proposed, which includes a DC power flow model with hidden failures. The error and attack tolerance methodology is still adopted in the algorithm by which we will further investigate the structural vulnerability of power networks.

II. Error and Attack Tolerance Methodology

The aim of the methodology is to investigate structural vulnerability by removing a single or a group of nodes randomly (error) or intentionally (attack) and then evaluate how much the performance of the network is affected. In

G. Chen is with the School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, Australia (e-mail: guochen@itee.uq.edu.au) He is currently conducting research at the Department of Information Engineering, Research School of Information Sciences and engineering, the Australian National university, Australia.
Z.Y. Dong is with the School of Electrical Engineering and Computer Science, the University of Newcastle, Australia (e-mail: zydong@ieee.org)
D. J. Hill and G.H. Zhang are with the Department of Information Engineering, Research School of Information Sciences and Engineering, the Australian National University, Canberra, ACT 0200, Australia (e-mail: David.Hill@anu.edu.au, guohua.zhang@rsise.anu.edu.au).

fact, in most real complex networks the breakdown of a single node can be sufficient to cause the entire systems to collapse due to the dynamics of redistribution of flows on the networks. Therefore, a dynamical model is adopted widely [5-6 11-12].

The model iteratively applies a rule for mimicking the cascading failure by removing a node in each iteration. In order to evaluate how well a system works before and after the breakdown, the average efficiency or average efficiency loss of networks [5-6, 11-12] is introduced. To characterize the load distribution in the network, the concept of betweenness is used [5-6 11-12]. The betweenness at a node *i* is defined as the total number of shortest paths passing through this node. The capacity of a node is the maximum betweenness that the node can handle. For a real world network, the capacity is severely limited by cost. Thus it is natural to assume that the capacity C_i of a node *i* is proportional to its initial load carried by *i*

$$C_i = \alpha L_i(0) \qquad i = 1,2,\cdots,N, \tag{1}$$

where α>=1 is a tolerance parameter of the network and $L_i(0)$ is the initial betweenness handled by node *i* at iteration step *t*=0, viz. before the removal [5-6, 11-12]. With such a definition of capacity, the network is in a stationary state in which it operates with an initial average efficiency. The removal of a node triggers the dynamics of redistribution of flows on the network. In fact the removal of a node changes shortest paths between nodes and consequently the distribution of loads, which would create overloads on some nodes. At each iteration step *t*, the following iterative rule is adopted [5-6, 11-12]

$$w_{ij}(t+1) = \begin{cases} w_{ij}(0)\dfrac{L_i(t)}{C_i} & if\ L_i(t) > C_i \\ w_{ij}(0) & if\ L_i(t) \le C_i \end{cases} \tag{2}$$

where *w* is the adjacency matrix of the network and *j* extends to all the first neighbors of *i*. In this way if at each iterative step, a node *i* is overloaded, the length of all the edges passing through it is increased, which can change the shortest paths between nodes, leading to a new redistribution of the loads and then some nodes may be overloaded. The process will continue and produce a dynamic evolution of networks namely a cascading failure, which can cause the average efficiency degradation.

The methodology has been employed in abstract networks and real world networks. However, it ignores some important characters of power systems when it was applied in this field directly. Firstly, the dynamical evolution of real power networks is based on power flow distribution not betweenness distribution. Secondly in power networks, cascading failures largely come from overloaded lines viz. transmission lines, and nodes (usually substation) are not easy to fail because of special protection. Thirdly, hidden failures are quite common in blackouts of power networks. Finally, electrical engineers usually use the amount of load shedding, namely loss of supply to customer, as a measure for damage of power networks, not average efficiency loss. Therefore, in order to better study the vulnerability of power networks, considering power systems characters and power flow equations are needed.

III. The Hybrid Algorithm

A. Hidden failures in protection systems

Recent NERC [15] (North American Electric Reliability Council) studies of major blackouts have shown that more than 70% of those blackouts involved hidden failures, which are incorrect relay operations, namely removing a circuit element(s) as a direct consequence of another switching event [16-17]. When a transmission line trips, there is a small but significant probability that lines sharing a bus (those lines are called as expose to hidden failures) with the tripped line may incorrectly trip due to relay misoperation.

The probability of such occurrence is small but not negligible. In this paper, we model hidden failures in the following way [16]. Each exposed line has a different load dependent probability of incorrect failure that is modeled as an increasing function of the power flow on the line. The probability is low below the line security limit and increases linearly to 1 when the line flow is 1.4 times of the safe limit.

B. The DC Power equations model

Usually the *DC* power flow equations [16, 18-19] can be defined as

$$F = AP \tag{3}$$

where $F = (F_1(t), F_2(t),..., F_{nline}(t))^T$ is the vector of real power flows on the transmission lines. *A* is a constant matrix and $P = (p_1, p_2, p_3,..., p_{nbus-1})^T$ is a vector whose *nbus*-1 components are real power injections at all buses except slack bus to avoid singularity of *A*. *nline* is the number of transmission lines and *nbus* is the number of buses in the system.

When a line trips, it is necessary to redispatch the injected power to satisfy the system constraints. The redispatch is formulated as a linear programming problem [16, 18-19] there the cost function is minimized as,

$$\cos t = \min \sum_{j \in load} c_j \tag{4}$$

subject to the DC load flow (3) and overall power balance.

$$\sum_{i \in generators} p_i + \sum_{j \in loads} c_j - \sum_{j \in loads} d_j = 0 \tag{5}$$

where p_i is generated power for generator *i*, c_j is load shedding for load *j* and d_j is initial load. Furthermore, this minimization is done with the following constraints:

(a) Generation capacity limits for generator *i*

$$p_i^{\min} \le p_i \le p_i^{\max} \tag{6}$$

(b) The constraints of load shedding limits for load *j*

$$0 \le c_j \le d_j \tag{7}$$

(c) The line flow limits

$$|F_k| \le 1.4 * F_k^s \tag{8}$$

where F_k^s is the secure line flow limit of line *k*. If $|F_k| > F_k^s$, the line *k* is considered as overload, and 1.4

times of F_k^s is the maximum flow that line k can bear. When a line is overloaded and if it is not exposed to hidden failures, it is still possible to fail. Thus, we set a probability p_0 to consider this failure.

Similar with (1) F_k^s can be defined as

$$F_k^s = \alpha L_k \tag{9}$$

where the constant $\alpha \geq 1$ is a tolerance parameter and L_k is the initial power flow on line k when power grids are operated normally before disturbance.

This linear programming (*LP*) problem can be numerically solved by using the simplex method as implemented in [20].

C. *Algorithm procedure*

The algorithm starts at a feasible solution of the system as in (3). The initial disturbance is triggered by different attacks on nodes or edges and then hidden failures are tested for possible lines tripping. Then the power flow equations and *LP* programming are recalculated. When a solution is found, the overloaded lines of the solution are tested for possible outages. The process will continue until a solution is found with no more line overloaded. The flowchart of the procedure is shown in Figure 1.

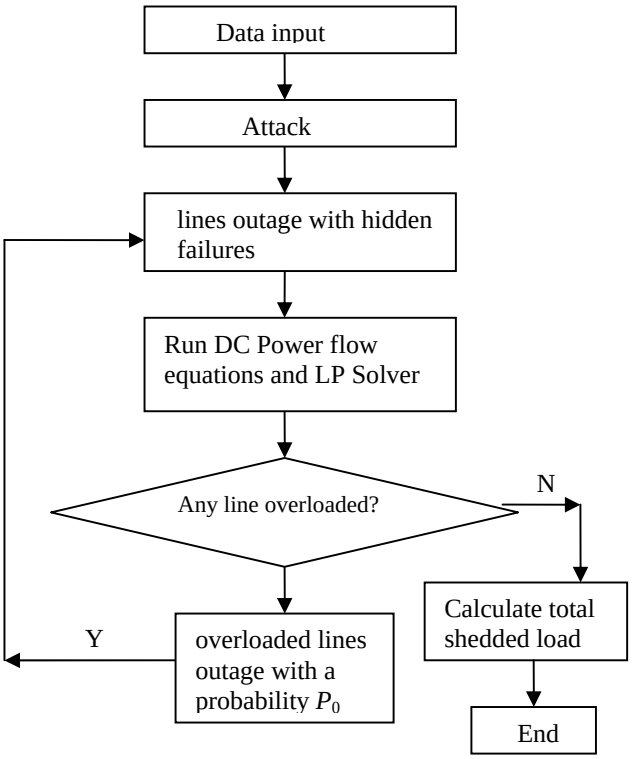

Fig. 1: Flowchart of the proposed algorithm

IV. Simulations Results and Theory Analysis

A. *Numerical analysis*

In this paper, IEEE 118 bus test system is selected to test the proposed method. It has 54 generator buses, 64 load buses and 186 transmission lines. In the simulation, we choose nodes either randomly (random failure, the curve is an average over 50 different random choices) or selectively by highest degree (degree-based attack) or highest betweenness (betweenness-based attack).

For comparison purpose, firstly, we repeat the simulation of previous model described in section 2. Figure 2 displays the result of average efficiency loss under the three attacks and it clearly shows that power grids are robust to random failure but vulnerable to intentional attacks (degree and betweenness) in this scenario.

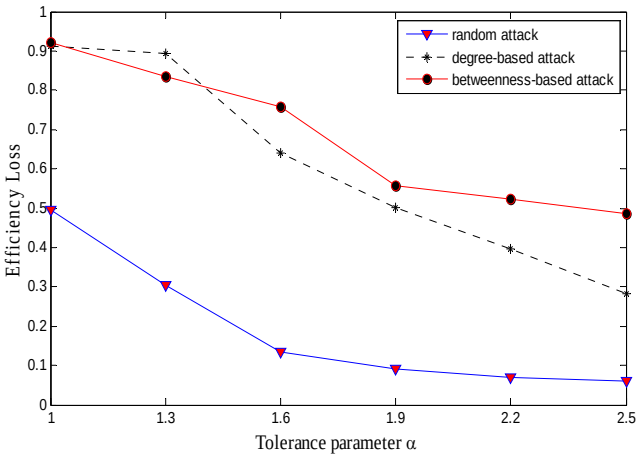

Fig. 2 Efficiency loss

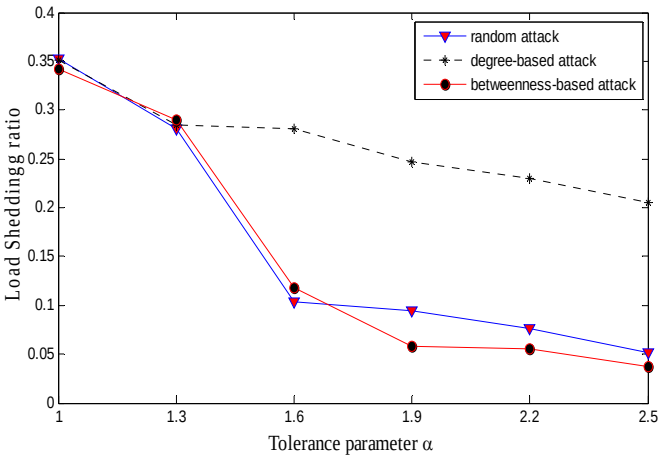

Fig. 3 Load shedding ratio under node attacks

However, if we consider the proposed algorithm, the situation is different. Figure 3 displays the load shedding ratio after removing a node by the three attacks. It can be observed from the figure that when the tolerance parameter α is above 1.6, the power network is quite robust to random attack and betweenness-based attack but vulnerable to degree-based attack, which might implicate that the measure "degree" is more important than the "betwenness" in power networks. Furthermore, there exists a critical point α_0 for the tolerance parameter at which the power loss will increase greatly. When tolerance parameter a is less than the α_0, meaning that a enters into a region $1 < a < a_0$,in which the power network is fragile to all the three attacks. Similar

results can be seen from Figure 4 which displays the numbers of broken lines in this scenario.

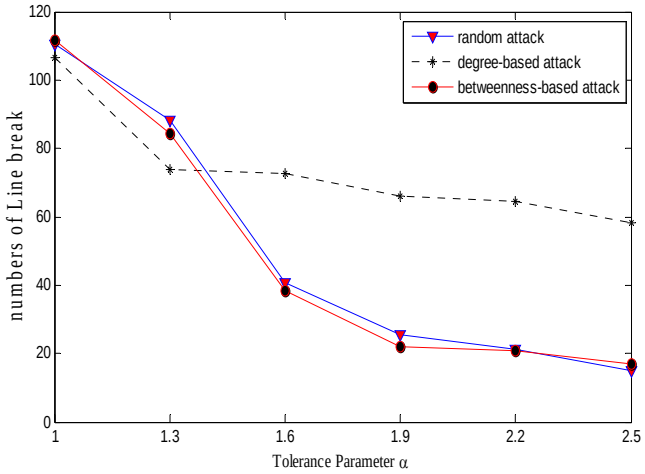

Fig. 4 number of broken lines under node attacks

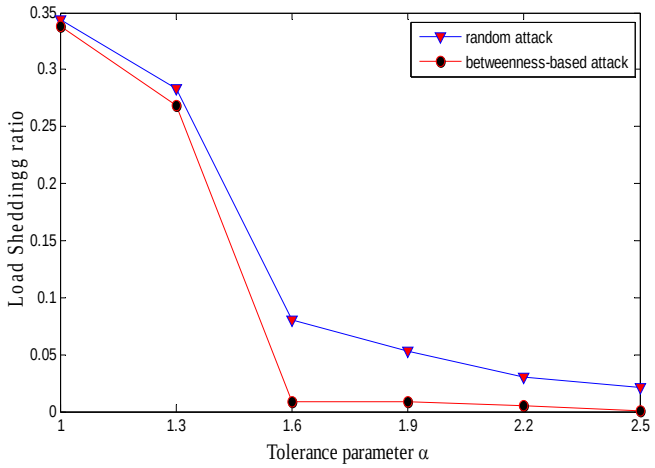

Fig. 5 Load shedding ratio under line attacks

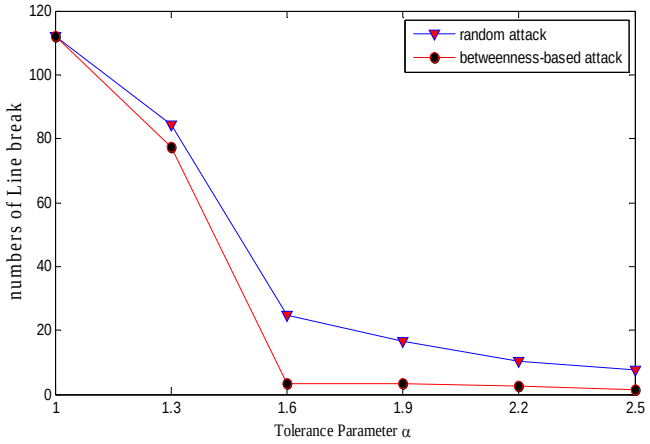

Fig. 6 number of broken lines under line attacks

To study the problem further, we employ single line removal strategy, namely choosing lines either randomly or selectively by highest betweenness (note: there is no degree conception for lines.) Figure 5 and Figure 6 illustrate the load shedding ratio and number of broken lines respectively, after occurrence of a breakdown of a line. It can be observed that a similar region of the tolerance parameter still exists, in which the power network is vulnerable to both the two attacks. Furthermore, betweeness still does not demonstrate its importance in this scenario. Therefore, it might be concluded that using betweenness distribution instead of real power flow distribution might be not practical in power networks.

B. *An analytical analysis*

Tolerance parameter α characterizes the capacity of nodes or lines in a network and the fall of α will cause the network or system more stressful. The simulation demonstrates that there exists a region in the tolerance parameter $1 \le \alpha \le a_0$, in which power systems are fragile to both random and intentional attacks. In this section, a brief theory analysis is presented to support the simulated results.

The analytical approach to study errors and attacks tolerance has been traditionally based on percolation theory, by which Newman et al. [21] and Callaway et al. [22] have respectively investigated some abstract complex networks and found that a critical point widely exists: the nodes (site percolation) or edges (bond percolation) are removed with a probability 1-p, or are considered "keeping" with a probability p. Below a critical probability p_c, the system will become disconnected into some smaller and disintegrated clusters. For a power network, if such p_c exists, it will inevitably cause the lost of load increasing sharply, meaning that power systems will experience large blackouts. Here, we employ the theory to study power networks and try to quantify the critical point p_c.

In this brief, for a power network, only edge outages are considered (exclude the initial attacked node). Therefore, it is a bond percolation problem: what a percentage (1- p_c) of edges break, the system will be split into some smaller clusters. Here, we consider it in an inverse way, namely keeping edges above a percentage (p_c), there exists a large connected cluster that spans the entire system.

Suppose that we have a power network described by an undirected graph with N vertices and M edges. $G_0(x)$ is defined as the generating function for the degree distribution of vertex degree k.

$$G_0(x) = \sum_{k=m}^{M} p(k)x^k \qquad (10)$$

where $p(k)$ $(m \le k \le M)$ is the degree distribution that a randomly chosen vertex on the graph has degree k. The distribution $p(k)$ is assumed correctly normalized, so that

$$G_0(1) = 1 \qquad (11)$$

The average of the degree distribution is given by

$$z =< k >= \sum_k kp(k) = G'_0(1) \qquad (12)$$

Moreover, the generating formula $H_1(x)$ is used to determine the probability that an edge chosen at random leads to a percolation cluster. For bond percolation with uniform occupation probability of edges, $H_1(x)$ is denoted as [22]

$$H_1(x) = 1 - q + qx\,(G_1(H_1(x)) \quad (13)$$

where $G_1(x) = G'_0(x)/z$ [21] and q is the overall fraction of keeping lines.

Moreover, the generation function for a vertex that exists in a percolation cluster can be given by [22]

$$H_0(x) = xG_0(H_1(x)) \quad (14)$$

Although it is not usually possible to find a closed-form expression for the complete distribution of component size in a network, we can derive a closed-form expression for the average component size <s> from eq. (14) as follows

$$< s >= H'_0(1) = 1 + G'_0(1)H'_1(1) \quad (15)$$

From Eq.(13) we have

$$H'_1(1) = q + qG'_1(1)H'_1(1) \quad (16)$$

And hence

$$< s >= 1 + \frac{qG'_0(1)}{1 - qG'_1(1)} \quad (17)$$

We can see that this expression diverges when $1 - qG_1'(1) = 0$. Thus the critical point is

$$q_c = 1/G_1'(1) \quad (18)$$

This point marks the percolation threshold of the system. $G_1'(1)$ is subject to initial degree distribution and q_C is the critical fraction of keeping lines that can form a large connected cluster spanning the entire network. On the other hand, q_C is also the critical point that the network can be spit. For a fixed power network, initial degree distribution is a constant. Therefore, q_C is also a constant, meaning that breaking more than (1- q_c)*M edges, the power network will be split. Under the three attacks, the fractions of malfunction lines denoted as R_1, R_2, R_3 are different in a fixed α. With the α decreases, R_1,R_2 and R_3 rise respectively. Without of generalization, there exists α_0 and a set $\{R_{10},R_{20},R_{30}\}$, which satisfy that the minimum element in the set is larger than (1- q_c). Thus, when tolerance parameter a is less than α_0, namely $1 \le \alpha \le a_0$, power networks will be spitted into smaller and disconnected parts under the three attacks, which will result in large scale blackouts. Therefore, in this region, power networks are fragile to both random and intentional attacks.

V. Conclusions and Future Work

Complex networks theory and its error and attack methodology were initially proposed by some physicists and then have been employed in different fields. They are general methods, which usually ignore some concrete characteristics of power systems. To better explain complex blackouts, power network features and power flow constraints are needed. In this brief, a hybrid algorithm is proposed to further investigate the vulnerability of power networks. This algorithm employs DC power flow equations, hidden failures and error and attack tolerance methodology together to form a comprehensive approach for power network vulnerability assessment and modeling. The numerical simulation reveals some new useful results which are also verified by an analytical method.

Since power system cascading failure is diverse and complicated, it is impossible to consider all factors of cascading failure led blackouts in this brief. Instead, we demonstrate that complex networks theory provides a new direction for complex power networks research. However, at present this work is still in its early age and physicists' work neglected some concrete engineering features. Therefore, there are good prospects for researchers to further investigate the complex problems by considering power system characteristics and complex network theory together, which are our further work.

References

[1] A.E. Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. Physical Review E 66. 065102(R) (2002)

[2] Making the Nation Safer. The Role of Science and Technology in Countering Terrorism," National Research Council, National Academy Press, Washington, D.C., 2002.

[3] A.J. Holmgren, E. Jenelius and J.Westin. Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks. IEEE Trans. Power Systems, Vol 22, No.1 Feb. 2007

[4] R. Albert, H.Jeong and A.L. Barabasi. Error and attack tolerance of complex networks. Nature, 2000, 406: 378～382

[5] P. Crucitti,V. Latorab, M. Marchioric. Error and attack tolerance of complex networks. Physica A, 340(2004)388-394

[6] P.Crucitti, V.Latora, M. Marchiori. Efficiency of scale-free networks: error and attack tolerance. Physica A 320(2003) 622-642.

[7] V.Latora,M.Marchiori. Efficient Behavior of Small-World Networks. Phys.Rev.Lett.2001, 87:198-701.

[8] A.E.Motter,T. Nishikawa, Y.C. Lai. Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon? Phys. Rev. E 66, 065103 (2002)

[9] David J. Hill, Guan Rong Chen. Power Systems as Dynamic Networks. 2006 IEEE International Symposium on Circuits and Systems.

[10] M.R.casals, S.Valverde, R.Sole. Topological vulnerability of the European power grid under errors and attacks. Int. J. Bifurcation Chaos. 2007; 17(7). 2465-75

[11] P. Crucitti, V. Latora. A Topological Analysis of the Italian Electric Power Grid. Physica A,338(2004) 92-97

[12] R.Kinney, P. Crucitti, R. Albert. Modeling cascading failures in the North American power grid. Eur. Phys.J. B 46 2005

[13] R. Albert, A. Barabási. Statistical mechanics of complex networks. Reviews of Modern Physics, 2002, 74: 47-97

[14] IEEE PES Computer and analytical methods subcommittee. Vulnerability assessment for cascading failure in electrical power systems. IEEE Power and Energy Society Power Systems Conference and Exposition 2009, Seattle, WA.

[15] North American Electric Reliability Council Disturbances Analysis Working Group Database [Online]. Available: http://www.nerc.com/~dawg/database.html

[16] Jie Chen James S. Thorp and Ian Dobson. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. Electrical Power & Energy Systems. 27(2005) 318-326

[17] Yi Jun, Zhou Xiaoxin. Xiao Yunan. Model of Cascading Failure in Power Systems. 2006 International Conference on Power System Technology.

[18] I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization, Chaos, vol. 17, no. 2, 026103, June 2007.

[19] Hui Ren, Ian Dobson,B.A.Carreras. Long-term effect of n-1 Criterion on Cascading line outages in an evolving power transmission grid. IEEE Trans. Power Syst., accepted in April 2008

[20] W. H. Press, B. P. Flammery, S. A. Teukolsky et al. Numerical Recipes in C (Cambridge University Press, Cambridge, 1988)

[21] M.E.Newman,S.H.Strogatz, D.J.Watts. Random graphs with arbitrary degree distributions and their applications. Physics Review E 64, 026118

[22] D.S.Callaway, M.E.Newman, S.H.Strogatz et al. Network robustness and fragility: percolation on random graphs. Phys Rev Lett, 2000, 85:5468-5471.