Static Security Analysis based on Weighted Vulnerability Index

Chengzong Pang, *Student Member, IEEE*, and Mladen Kezunovic, *Fellow, IEEE*

Abstract--**This paper proposes weighted vulnerability index method for power system static security analysis. The power system can be modeled as directed graph network based on the power flow results. Betweenness centrality is calculated to measure the importance of each vertex and edge in the modeled network, which is used to determine the weights for the proposed weighted vulnerability index method. The performance of the proposed method is verified by using the standard IEEE 39-bus New England system. Case studies include the vulnerability analysis for different load conditions and static N-1 contingency. The results indicate that the proposed method is a good way to assess the system security and vulnerability information.**

Index Terms--**Security Analysis, Weighted Vulnerability Index, Betweenness Centrality, Graph Theory, Contingency Analysis**

I. INTRODUCTION

POWER system security analysis is one of the most challenging problems for system operators due to the increasing complexity of power system infrastructure. With the development of competitive electricity markets, customers expect the electric energy with least-cost but high-quality, which requires enhanced security in power system with more sophisticated and reliable operations. North American Electric Reliability Corporation (NERC) defines security as the ability of a power system to withstand sudden disturbances, which is part of the concept encompassed in the definition of reliability [1]. Contingency analysis is widely used to evaluate the system ability to endure unexpected events without violating any operating constraint, such as loss of a transmission line or power generator.

For a large-scale power system, the list of contingencies may be extremely large. It is quite often impractical to examine the all combinatorial cases. Contingency ranking and selecting algorithms are used to reduce the computation burden in contingency analysis. Many methods have been proposed for contingency ranking. Performance Index (PI) is proposed to evaluate the line loading and voltage performance for the automatic contingency selection algorithm [2]. A fast and approximate network solution for contingency screening method is discussed in [3] and [4]. The hybrid method is proposed in [5] and [6] to balance both the speed and accuracy requirements. First-order sensitivity analysis based the traditional power flow is and is a popular choice in contingency analysis [7, 8]. Other approaches include pattern recognition, neural network, genetic algorithm, and etc [9-12]. However, these methods are mostly focused on the line overload and voltage problems, which are not capable of representing the whole system security information.

Vulnerability Index (VI) based security analysis had been proposed in [13, 14], which not only considered overloads and voltage problems like the traditional methods, but also addressed the problems of loadability, distance relay performance, loss of generator and load, line outage, reactive power supply, etc. System operators can assess the power system security and vulnerability information by using these indices. However, the weights in VIs were set as one or chosen by system operators based on their operation experiences. Like any other network, there are some buses and branches in the power system, which are more critical than the others due to their locations, properties, and functions. They have more influences on the system security and hence should have larger weights than the others. It is not an easy task to identify the critical elements in power system only based on the operation experiences.

The centrality indices have been introduced as an essential tool for the analysis of different networks [15, 16]. For example, these centrality indices were designed to rank the actors according to their position in the network and interpreted as the prominence of actors embedded in a social structure [17]. It was an effective way to measure the critical degree of different elements in the network. In this paper, we propose a weighted vulnerability index method for power system static security analysis, which will apply graph-theoretic concept of betweenness centrality to power grid topology. A directed graph is formed with vertices representing busses and the edges representing transmission lines. The weights for each vulnerability index will be calculated based on the values of betweenness centralities for each bus and branch in power system. The weighted vulnerability index method is an effective tool to consider both the inherent electrical properties of power system and the network topological properties.

This paper is organized as follows: Section II introduces the power system graph-based model and betweenness centrality. Section III reviews the concept of vulnerability index method and proposes the improved approach – weighted vulnerability index method. Numerical test results are presented in Section

C. Pang and M. Kezunovic are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA (emails: pangchz@neo.tamu.edu , kezunov@ece.tamu.edu)

IV. Conclusions are given in Section V followed by acknowledgement and a list of references.

II. Betweenness Centrality

Graph theory is a branch of mathematics concerned about how networks can be encoded and how their properties may be measured, which has been used in many areas, such as mathematical research, computer programming, business administration, sociology, communications, etc [18]. Betweenness centrality is one of the most popular individual centrality measures when analyzing graph-based network. In this section, we present a brief introduction of the graph-based model of power grid and the computation of betweenness centrality.

A. Power System as Directed Graph Network

Electric power system is one of the most complex man-made systems. With new advances in complex network theory, the power system can be modeled as a graph network and analyzed to solve practical problems. Watts has proven that the topology of a typical power system network is a small-world network [19]. Hines and Blumsack [20] suggest that the power systems have a scale free structure by accounting for the electrical distances. Leisieutre, et al. [21] refined the topological graph concepts in order to be more consistent with power system generation and load patterns. Motter and Lai [22] tried to formulate the problem of cascading attack and worked on cascading phase transitions by complex networks theory.

Suppose $G = (V, E)$ is a graph network with v nodes (vertices) and e links (edges). V is the set of vertices, and E is the set of connecting edges. The adjacency matrix $A = \{a_{ij}\}$ implies the connectivity of the graph, which is defined by:

$$a_{ij} = \begin{cases} 1 & \text{if there is an edge between } v_i \text{ and } v_j \\ 0 & otherwise \end{cases} \quad (1)$$

When modeling power system, the generators, bus bars and loads can be identified as the graph nodes and the connecting transmission lines can be modeled as the edges. It has been studied that in any steady state, a power system would be a directed graph network [23], because the directions of power flow in the modeled network can be measured in any given steady state. Hence, we will model the power system as the directed graph. The adjacency matrix of the directed graph is asymmetric due to the directions of the power flow on transmission lines. Figure 1 shows a simple example of 4-bus system and its graph. The adjacency matrix of this system is as below:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

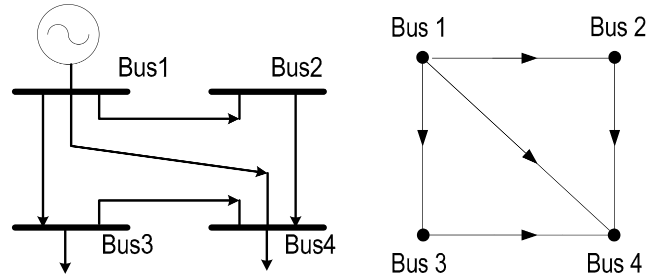


Fig. 1. 4-bus power system and its graph model

B. Vertex and Edge Betweenness Centrality

The concept of betweenness centrality was first defined by Freeman [24], where he defined a number of measures of centrality to find out how influential a person or group is in a social network. Betweenness centrality is one of these measures.

For the given graph $G = (V, E)$, the vertex betweenness centrality $BC(v)$ of a vertex $v \in V$ is the sum over all pairs of vertices $u, w \in V$, of the fraction of shortest paths between u and w that pass through vertex v, which is shown as:

$$BC(v) = \sum_{\substack{u, w \in V \\ u \neq w \neq v}} \frac{\sigma_{uw}(v)}{\sigma_{uw}} \quad (3)$$

where $\sigma_{uw}(v)$ denotes the total number of shortest path between u and w that pass through v, and σ_{uw} denotes the total number of shortest paths between u and w.

Similarly, the edge betweenness centrality $BC(e)$ of a edge $e \in E$ is the sum over all pairs of vertices $u, w \in V$, of the fraction of shortest paths between u and w that pass through edge e, which is shown as:

$$BC(e) = \sum_{\substack{u, w \in V \\ u \neq w}} \frac{\sigma_{uw}(e)}{\sigma_{uw}} \quad (4)$$

where $\sigma_{uw}(e)$ denotes the total number of shortest path between u and w that pass through e, and σ_{uw} denotes the total number of shortest paths between u and w.

The vertex and edge betweenness centrality are the standard measure for the influence of a vertex or an edge over the rest of the system. The vertices and edges with higher betweenness centralities indicate that they have relatively higher importance than the other elements within the graph network. By applying the betweenness centralities of buses and transmission lines to the power system topology, the high-impact buses and lines can be identified, which could be used to calculate the weights for the weighted vulnerability index approach proposed in this paper.

III. Weighted Vulnerability Index Approach

Vulnerability index and margin index are a good way to assess the vulnerability and security margin of the individual element and the whole system [14]. This paper proposes an improved approach, weighted vulnerability index method, by considering the buses and transmission lines with higher importance. The weights for each vulnerability index are based on vertex and edge betweenness centrality.

A. Review of Vulnerability Index

Vulnerability index as well as margin index gives precise vulnerability and margin information for individual system element and the whole system performance [13]. At the generator level, vulnerability indices for real power output, reactive power output and generation loss and margin indices for real and reactive power outputs were considered. At the bus level, vulnerability indices for bus voltage performance, loadability and load loss and margin indices for bus voltage performance and loadability were presented. Islanding and isolated buses due to the line outages were considered in the load loss part. At the transmission line level, vulnerability indices for line real power, reactive power, line charging, line bus voltage angle difference, line distance relay performance, and line-off influence were discussed. Similarly, the margin indices for line flow, line bus voltage angle difference and line distance relay were analyzed. It has been shown that the quantitative information of vulnerability can help system operators to assess the system security level and keep the system operating within normal conditions. The detailed definition about the vulnerability indices can be found in [13] and [14]. Here we list the vulnerability index with weight factor for generators as an example:

$$VI_{Pg,i} = \frac{W_{Pg,i}}{2N}\left(\frac{Pg_i}{Pg_{i,\max}}\right)^{2N} \tag{5}$$

$$VI_{Qg,i} = \frac{W_{Qg,i}}{2N}\left(\frac{Qg_i}{Qg_{i,\max}}\right)^{2N} \tag{6}$$

$$VI_{gen\_loss,i} = W_{gen\_loss,i} k_i \tag{7}$$

where $VI_{Pg,i}$: VI of individual generator real power output;

$VI_{Qg,i}$: VI of individual generator reactive power output;

$VI_{gen\_loss,i}$: VI of individual generator loss;

$W_{Pg,i}$, $W_{Qg,i}$, $W_{gen\_loss,i}$: weights of individual generator real power output, reactive power output, and loss influence, respectively;

Pg_i, Qg_i: individual generator real and reactive power outputs, respectively;

$Pg_{i,\max}, Qg_{i,\max}$: maximum real and reactive power outputs of individual generator, respectively;

k_i: 1 when generator is off, 0 when generator is on;

N: 1 in general.

B. Weight Calculation

In the traditional vulnerability index approach, the weights in VIs are set as one or chosen by system operators based on their operation experience. Since the betweenness centrality has been proved to be a good measure of the importance of a vertex or an edge over the rest of the system, we can calculate the weights based on the quantitative values of betweenness centrality.

When modeling power system into a graph, the generators, buses are identified as nodes and the transmission lines are modeled as the edges. So the weights for VIs of generators and buses will be calculated based on vertex betweenness centrality; the weights for VIs of branches will be calculated based on edge betweenness centrality.

Considering whether the value of betweenness centrality is becoming large with the increasing of bus number in the power system, the normalized vertex and edge betweenness centralities are used when applying them to real world implementation, which are defined as:

$$BC\_Norm(v) = \frac{BC(v)}{(n-1)(n-2)} \tag{8}$$

$$BC\_Norm(e) = \frac{BC(e)}{(n-1)(n-2)} \tag{9}$$

where n is the total number of nodes in the power system.

The detailed procedures of the proposed method to calculate the weights are:

- Run power flow analysis to get the direction of power flow on each transmission line;
- Model the power system as a directed graph according to the graph principles;
- For each pair of vertices (u, w), compute all shortest paths between them;
- For each pair of vertices (u, w), determine the fraction of shortest paths that pass through the vertex in question;
- Sum this fraction over all pairs of vertices (u, w) to get the betweenness centrality for the vertex in question;
- Propagate the calculation to all the vertices and edges to get the betweenness centralities of whole network;
- Normalize the values of betweenness centralities;
- Add the normalized betweenness centrality values to the original weights for each VIs of generators, buses, and branches.

IV. Numerical Test Results

We use the standard IEEE 39-bus New England system to demonstrate the performance of proposed approach. Figure 2 shows the IEEE 39-bus system configuration. The detailed system data can be found in [25].

A. Betweenness Centrality

After running power flow calculation, the basic directed graph-based model of power system is obtained with the directions of power flow on each transmission line. The vertex and edge betweenness centrality is computed according to the adjacency matrix of the power system. The distributions of vertex and edge betweenness centrality with descending sort are shown in Figure 3 and Figure 4, respectively.

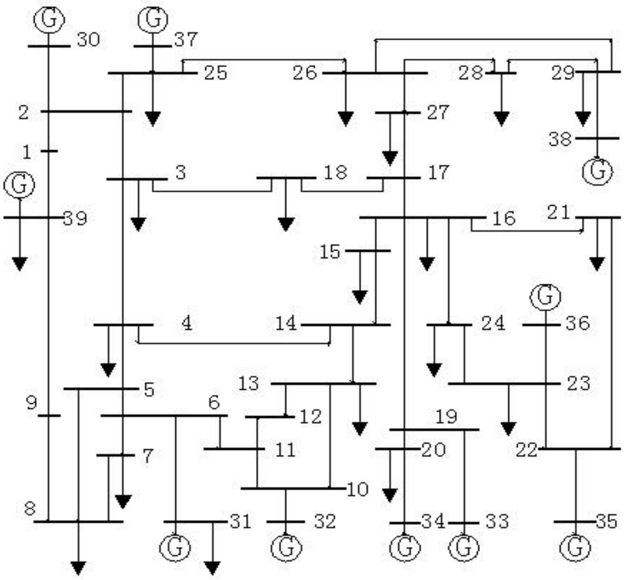


Fig. 2. IEEE 39-bus New England system configuration

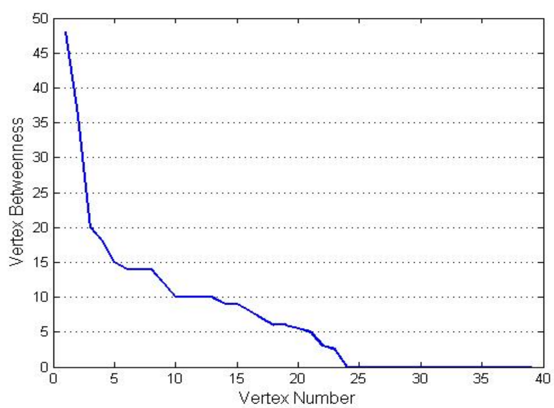


Fig. 3. Vertex betweenness distribution for IEEE 39-bus New England system

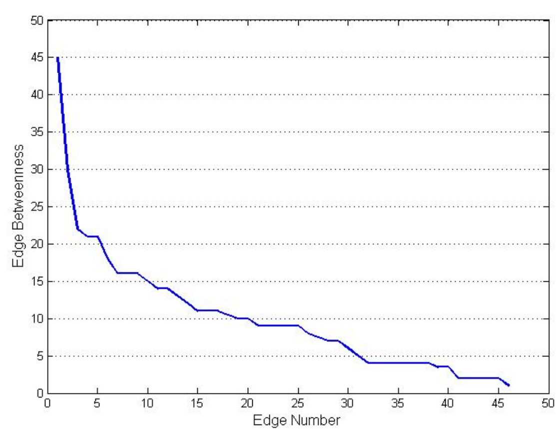


Fig. 4. Edge betweenness distribution for IEEE 39-bus New England system

We can see that there are a small number of vertices and edges that have high betweenness centrality values, which means they have high-impacts to the power system grid. The real world power system holds the same properties found in a small set of buses and transmission lines, which carry significantly higher importance compared with the remaining parts of the system. For example, Bus 16 has the highest value of vertex betweenness centrality. It has a very important topological position in the network.

Regarding topological features, betweenness centralities of buses and transmission lines are good measurements of the influence of selected buses and transmission lines over the rest of the system. Regarding electrical features, the vulnerability indices can provide precise vulnerability measure for individual system element and the whole system performance. Certainly, it is possible that some important nodes or branches may have lower value of betweenness centrality. However, the vulnerability index calculation is capable of detecting all the vulnerable elements. For example, Bus 30 will be very important node if it had a great amount of generation attached to it. The value of its betweenness centrality is not large considering its topological role in this network. However, from Equation (5), large generator means high value of $Pg_{i,\max}$. So any major loss of generation in this node will affect the value of $VI_{Pg,i}$ and $VI_{Qg,i}$ of this generator. This node has low-value betweenness centrality bus still can be picked out as vulnerable element due to its abnormal VI.

B. Weighted vulnerability analysis for different load conditions

For the IEEE 39-bus test system, we compare the weighted vulnerability index values for three difference cases:

- Case A: base load;
- Case B: 1.1 times the base load ;
- Case C: 1.2 times the base load.

The real and reactive power outputs for generators increase with the corresponding same ratio to balance the increasing load. When defining the case study, the following assumptions are taken:

- The branch transfer limits is 3.0 p.u.;
- Voltage variance is 0.075 p.u.;
- Bus voltage angle difference limit for transmission line is set as 40 degrees.

Table I shows the results of weighted vulnerability index values for the three cases under different load conditions. Besides the system total vulnerability index (VI_{total}), Table I also shows the results of some individual vulnerability indices:

- VI_{Loadab} : sum of VI of load bus loadbility;
- VI_{Pg} : sum of VI of generator real power output;
- VI_{Qg} : sum of VI of generator reactive power output;
- VI_{Pf} : sum of VI of branch real power flow;
- $VI_{line\_ang,i}$: sum of VI of bus voltage angle difference.

From the results of Table I, we can see that the whole power system is getting more vulnerable with the load increasing. To balance the load, generators provide more real and reactive power. The power flow and bus voltage angle differences at transmission lines are also increasing. The case studies show that weighted vulnerability index is a good way to assess the system security under different load conditions.

TABLE I
WEIGHTED VULNERABILITY INDEX VALUES AT DIFFERENT LOAD CONDITIONS

	VI_{total}	VI_{Loadab}	VI_{Pg}	VI_{Qg}	VI_{Pf}	VI_{line_ang}
Case A	7.3340	0.9470	2.3496	0.6755	0.0293	0.1837
Case B	7.6871	1.1582	2.8448	1.0104	0.0355	0.2265
Case C	8.5949	1.3949	3.3878	1.4602	0.0423	0.2752

C. Weighted vulnerability analysis for N-1 contingency

For the same IEEE 39-bus system, N-1 static contingency analysis is performed to evaluate our proposed weighted vulnerability analysis approach. For the simple demonstration, we only apply line outages for this case study. From the topological analysis, we can find that there are eleven branches whose tripping will result in islanding, such as the branches L37 – L45 which connect generator G30 – G38, respectively. In our case study, we only rank the non-islanding contingencies. Table II shows the results of the weighted vulnerability index values for top five vulnerable line outages. The results of same individual vulnerability index in Table I are also given in Table II. From the results we can see that the top two vulnerable line outages are the branches connected with bus 16, which holds the most important topological position based on the rank of vertex betweenness centrality.

TABLE II
WEIGHTED VULNERABILITY INDEX VALUES FOR N-1 CONTINGENCY ANALYSIS

Line Outage Number	VI_{total}	VI_{Loadab}	VI_{Pg}	VI_{Qg}	VI_{Pf}	VI_{line_ang}
L20 (B16-15)	9.5948	1.2481	2.3520	0.8483	0.0315	0.1992
L24 (B24-16)	8.9419	1.2800	2.3497	0.7056	0.0296	0.1817
L5 (B4-3)	8.8055	1.0004	2.3498	0.6508	0.0294	0.1860
L31 (B27-26)	8.6649	1.1734	2.3548	0.9809	0.0316	0.1977
L2 (B39-1)	8.6118	0.9773	2.3500	0.6670	0.0303	0.1867

V. CONCLUSION

This paper proposes the weighted vulnerability index method to give a comprehensive representation of power system vulnerability information. The weights for each VIs are determined by the vertex and edge betweenness centrality of power system graph model. Based on the discussions presented in this paper, the following conclusions can be drawn:

- Vertex and edge betweenness centrality is a good measure of the importance of a bus or transmission line in the power system. There is a small portion of buses and lines that have high-impacts to the power system.
- Calculating weights based on normalized betweenness centrality enable weighted vulnerability index method to consider both the topological properties and electrical properties of power system.
- Case studies demonstrate that proposed method can be used in power system static security analysis, which helps system operators to evaluate the system operation condition and most vulnerable elements.

VI. ACKNOWLEDGMENT

The contributions to the earlier developments reported in this paper that came from earlier work of former graduate student Dr. H. Song is gratefully acknowledged.

VII. REFERENCES

[1] North American Electric Reliability Council, “Reliability concepts in bulk power electric system,” 1985.

[2] G. C. Ejebe and B. F. Wollenberg, “Automatic contingency selection”, *IEEE Trans. on Power Apparatus and Systems*, vol. PAS-98, no. 1, pp. 938 – 109, Jan/Feb 1979.

[3] G. C. Ejebe, H. P. Van Meeteren, and B. F. Wollenberg, “Fast contingency screening and evaluation for voltage security analysis”, *IEEE Trans. on Power Systems*, vol. 3, no. 4, pp. 1582-1590, November 1988.

[4] V. Brandwajn and M. G. Lauby, ‘Complete bounding for ac contingency analysis’, *IEEE Trans. on Power Systems*, vol. 4, no. 2, pp. 724-729, May 1990.

[5] A. P. S. Meliopoulos, C. S. Cheng, and F. Xia, “Performance evaluation of static security analysis methods”, *IEEE Trans. on Power Systems*, vol. 3, no. 4, pp. 1441-1449, August 1994.

[6] A. P. S. Meliopoulos and C. Cheng, “A new contingency ranking method,” in *Proceedings of the Southeastcon ’89*, Columbia, SC, pp. 837-842, Apr. 1989.

[7] C. A. Castro and A. Bose, “Correctability of voltage violations in on-line contingency analysis,” *IEEE Trans. on Power Systems*, vol. 9, pp. 1651-1657, Aug. 1994.

[8] Y. Chen and A. Bose, “Security analysis for voltage problems using a reduced model,” *IEEE Trans. on Power System*s, vol. 5, pp. 933-940, Aug. 1990

[9] A. Ozdemir, J. Y. Lim, and C. Singh, “Contingency screening for steady state analysis by using genetic algorithms”, in *2002 proceedings of the IEEE PES Summer Meeting*, pp. 1142 – 1147, July 2002.

[10] N. Balu, etc., “On-line power system security analysis”, in *1992 proceedings of the IEEE*, vol. 80, no. 2, pp. 262 -282, February 1992.

[11] L. Srivastava, S. N. Singh, and J. Sharma, "Knowledge-based neural network for voltage contingency selection and ranking," *Generation, Transmission & Distribution, IEE Proceedings*, vol.146, no.6, pp.649-656, Nov 1999.

[12] S. Weerasooriya, M. A. El-Sharkawi, M. Damborg, and R. J. Marks, "Towards static-security assessment of a large-scale power system using neural networks," *Generation, Transmission and Distribution, IEE Proceedings C* , vol.139, no.1, pp.64-70, Jan 1992.

[13] H. Song and M. Kezunovic, “Static security analysis based on vulnerability index (vi) and network contribution factor (ncf) method,” in *Proc. IEEE PES Transmission & Distribution Asia Pacific*, Dalian, China, Aug. 2005.

[14] H. Song and M. Kezunovic, “Static analysis of vulnerability and security margin of the power system,” in *Proc. IEEE PES Transmission & Distribution Conference & Exposition*, Dallas, Texas, May. 2006.

[15] A. Bavelas, “A mathematical model for group structure,” *Human Organizations*, vol. 7, pp.16-30, 1948.

[16] G. Sabidussi, “The centrality index of a graph,” *Psychometrika*, vol. 31, no. 4, pp. 581-603, 1966.

[17] L. C. Freeman, “Centrality in social networks: Conceptual clarification,” *Social Networks*, vol. 1, pp. 215-239, 1979.

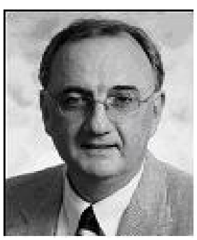
[18] J. Zhu, *Power system applications of graph theory*, New York: Nova Science Publishers, Inc., 2009.

[19] D. J. Watts, *Small worlds, The dynamics of networks between order and randomness*, Princeton: Princeton University Press, 2003

[20] P. Hines and S. Blumsack, "A centrality measure for electrical networks," 41st Hawaii International Conference on System Sciences, Hawaii, Jan. 2008.
[21] B. C. Lesieutre, S. Roy, V. Donde, and A. Pinar, "Power system extreme event screening using graph partitioning," 38th North American Power Symposium, Southern Illinois University Carbondale IL USA, Sept. 2006.
[22] A.E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no.6, 2002
[23] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabasi-Albert network model," *Physica A: Statistical Mechanics and its Applications*, vol. 355, no. 2-4, pp. 667-677, September 2005.
[24] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, pp. 35-41, 1977.
[25] M. A. Pai, *Energy Function Analysis for Power System Stability*, Norwell: Kluwer Academic Publishers, 1989, pp.222-227

VIII. Biographies

Chengzong Pang (S'07) received his B.S and M.S. degrees in electrical engineering from North China Electric Power University, China in 2000 and 2003, respectively. Since Aug. 2006, he has been with Texas A&M University pursuing his Ph. D. degree. His research interests are power system protection, power system analysis and control,



Mladen Kezunovic (S'77-M'80–SM'85–F'99) received the Dipl. Ing., M.S. and Ph.D. degrees in electrical engineering in 1974, 1977 and 1980, respectively. Currently, he is the Eugene E. Webb Professor and Site Director of Power Engineering Research Center (PSerc), an NSF I/UCRC.at Texas A&M University He worked for Westinghouse Electric Corp., Pittsburgh, PA, 1979-1980 and the Energoinvest Company, in Europe 1980-1986, and spent a sabbatical at EdF in Clamart 1999-2000. He was also a Visiting Professor at Washington State University, Pullman, 1986-1987 and The University of Hong Kong, fall of 2007. His main research interests are digital simulators and simulation methods for relay testing as well as application of intelligent methods to power system monitoring, control, and protection. Dr. Kezunovic is a Fellow of the IEEE, member of CIGRE and Registered Professional Engineer in Texas.