A robustness metric for cascading failures by targeted attacks in power networks

Yakup Koç[1] Martijn Warnier[1] Robert E. Kooij[2,3] Frances M.T. Brazier[1]
[1]Systems Engineering Section
Faculty of Technology, Policy and Management
Delft University of Technology
[2]Network Architecture en Services Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
[3]TNO (Netherlands Organisation for Applied Scientific Research) Information and Communication Technology
{Y.Koc,M.E.Warnier,R.E.Kooij,F.M.Brazier}@tudelft.nl

***Abstract*—Cascading failures are the main reason blackouts occur in power networks. The economic cost of such failures is in the order of tens of billion dollars annually. In a power network, the cascading failure phenomenon is related to both topological properties (number and types of buses, density of transmission lines and interconnection of components) and flow dynamics (load distribution and loading level). Existing studies most often focus on network topology, and not on flow dynamics. This paper proposes a new metric to assess power network robustness with respect to cascading failures, in particular for cascading effects due to line overloads and caused by targeted attacks. The metric takes both the effect of topological features and the effect of flow dynamics on network robustness into account, using an entropy-based approach. Experimental verification shows that the proposed robustness metric quantifies a power grid robustness with respect to cascading failures.**

I. Introduction

The power grid is one of the most important critical infrastructures in today's society. Due to careful control and management, it has been operating for decades most often with great reliability. Careful control and management of the power grid greatly limits the risk of failures. Massive blackouts in the power grid, however, still occur. Blackout analysis of 15 years of data by the North American Electrical Reliability Council (NERC) shows that blackouts happen on average once every 13 days [1] causing economic costs in the order of tens of billion dollars per year. For example, in 2003, the North-eastern and Mid-western United States and, South-eastern Canada suffered a catastrophic blackout leaving 50 million people without power for up to several days [2]. A more recent example is the large blackout in Brazil in 2009 that left 40% of the country without power [3].

In a power grid, power flows from generation to distribution stations through the transmission lines. Failure of any single line, by random breakdown or attack, changes the balance of power flow and leads to global redistribution of flows over the grid. Global redistribution of flows, in turn, may lead to overloaded transmission lines. Circuit breakers trip these overloaded lines when these lines reach their maximum flow limits (due to thermal, stability or voltage drop constraints) and new overload failures follow. This cascading process may stop after a few steps but it can also propagate and leave a considerable part of a network without power.

The electric power grid has grown into one of the most complex technological networks. The highly interconnected structure of power grid enables it to deliver power over huge distances. Yet, it also propagates local failures into the global network causing cascading failures. To counter this effect, the problem of cascading failures has to be analysed from the point of view of the system level and from the perspective of global network [4], [5]. A global analysis of a large-scale power grid is a challenge for traditional approaches relying purely on power flow based analysis (e.g. *N-x* contingency analysis) due to the complexity and extremely large amount of computational time. On the other hand, recent advances in the field of complex networks theory [6], [7] have shown the promising potential of the complex networks approach to model and analyse power networks at the system level.

This paper proposes a metric that quantifies robustness of a power transmission grid with respect to cascading failures by targeted attacks. A power grid is considered to be a complex network, and the electric power the physical quantity flowing through it. Steady-state operation and cascades due to the overloads are considered. A power grid is characterized by its topology and physical properties. Its topology describes the interconnection between its individual components, namely, transmission lines and generation, transmission and load buses. The power flow in a network is controlled by its physical properties: impedances, voltage levels at each individual power station, voltage phase differences between power stations and loads at terminal stations. This paper models a power grid as a directed graph [8], in which nodes represent buses while lines correspond to transmission lines. The flow values in the lines are computed by using direct current (DC) load flow analysis [9], [10].

II. Cascading Failures in Power Grids

Power grid robustness, including cascading failures phenomena, is an active field of research. Most contributions from the literature are based on modelling and analysing cascading failure mechanisms in power networks using complex network approaches. In a vast majority of these papers, authors consider the power grid as a complex network in which electricity is exchanged between nodes through the shortest or most efficient path. Cascading failure mechanism is simulated in the resulting models of power grids [11], [12], [13]. In these approaches, the load of a particular component is modelled by betweenness centrality [14]. The capacities of individual transmission lines are assumed to be proportional to their initial loads with a modelling parameter, namely, network tolerance parameter α (See Eq. (3) in Section III for details). In [11] and [13] the damage of cascading failures is quantified in terms of the relative size of the giant component [14] while in [12] it is measured in terms of the decrease in network efficiency [15]. In contrast to these more theoretical studies, Kinney et al. [16] have deployed the model proposed in [12] to simulate cascading failures in the North American power grid. They assess network robustness with respect to cascading failures for different tolerance parameter values in targeted- and random failure scenarios. In addition to these cascading failure modelling studies, other power grid vulnerability studies address the problem of locating the most important components in the network so that these components can be backed up in emergency cases to avoid overloading of these components [17], [18], [19].

Although there is substantial literature on recovery strategies in the case of cascading failures and understanding/analysing cascading failures in power networks, hardly any attention has been paid to quantifying network robustness with respect to cascading failures. To the best of our knowledge, Youssef et al. [20] is the only study that proposes a metric to measure network robustness with respect to cascading failures. Their robustness metric depends on the probability of link survivals as well as the depth of the cascading failure.

As pinpointed by several authors [11], [12], [13] heterogeneous load distribution in the network is one of the main driving forces behind cascading failures due to line overloads. This paper proposes a robustness metric that incorporates heterogeneity of load distribution and loading level of the network using an entropy-based approach.

III. Robustness Metric

The proposed robustness metric relies on two main concepts: nodal robustness and electrical node significance . This section elaborates on these new concepts and explains the computational algorithm with which to calculate the robustness metric value.

A. Nodal robustness

The robustness metric this paper introduces is an aggregate of local robustness values that indicate *nodal robustness*. Nodal robustness quantifies the ability of a node to resist cascades of link overload failures. Quantifying nodal robustness requires both flow dynamics and network topology to be taken into account. Three factors are of importance: (i) the homogeneity of load distribution on out-going links; (ii) the loading level of the out-going links; and (iii) the out-degree of the node.

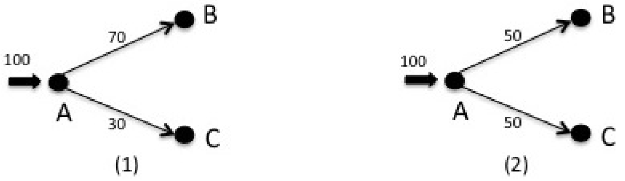

Fig. 1. Different load distribution homogeneities, same node out-degree

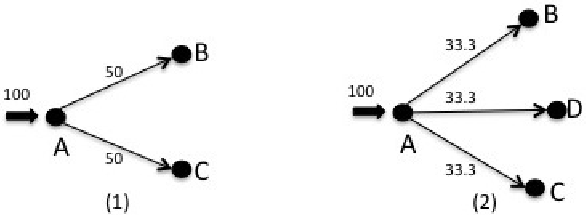

Fig. 2. Same load distribution homogeneities, different node out-degree

In Figure 1, the effect of load distribution homogeneity on cascades of link overload failures is considered in a very simple case to provide a basic intuition about cascading failure robustness. Assuming a network tolerance parameter α of 2 (i.e. a loading level of 50%), for a load distribution of 70 and 30 (i.e. capacity of lines A-B and A-C are 70 × α = 140 and 30 × α = 60, respectively), a failure in line A-B results in a load increase of line A-C to 100 that exceeds the maximum capacity of the line A-C (i.e. 60), causing an overload failure in line A-C. However, if the load is distributed perfectly homogeneously over lines (i.e. 50 and 50: capacity values for both links are 100), then, there will be no link overload failure (the capacity of 100 is not exceeded) when one of links fails. Consequently, a more homogeneous load distribution across lines increases robustness with respect to cascades of link overload failures while a relatively heterogeneous load distribution increases the chance of link overload failure spread. Note that for an increased loading level of 60%, link overload failure occurs in both of the cases in Figure 1, whereas for a loading level of 30%, in neither of the cases failure spreads. This shows that there is an inverse relationship between nodal robustness and loading level of the network. Finally, the effect of node out-degree on the nodal robustness is illustrated in Figure 2. In both of the cases, flow is perfectly distributed over available paths. However, again for the loading level of 50%, Case 2 is more tolerant to link overload failure spread than Case 1. This reflects the effect of out-degree on nodal robustness: the larger out-degree a node possess the higher nodal robustness it has.

Quantifying nodal robustness entails incorporating the three factors illustrated in Figure 1 and Figure 2. To capture the first and the last behaviours a well-known concept from information theory is used: entropy. Furthermore, the network tolerance parameter (i.e. α), proposed in [11], is used to incorporate the loading level of the network. Deployment of entropy for the nodal robustness computation makes it possible to capture important cascading failure dynamics. Entropy of a flow distribution of a node increases as flows over lines are distributed more homogeneously and the node out-degree increases.

The entropy of a given distribution is computed by Equation (1), in which p_i stands for values in the distribution under consideration, while L refers to the number of the sample values in the distribution.

$$H = \sum_{i=1}^{L} p_i \log p_i \tag{1}$$

Tailoring Equation (1) to the nodal robustness concept, L refers to the out-degree of the corresponding node, whereas p_i corresponds to normalized flow values on the out-going links, which is given as:

$$p_i = \frac{f_i}{\sum_{j=1}^{L} f_j} \tag{2}$$

In Equation (2) f_i refers to the flow value in line i. When applying Equation (1) to the cases in Figure 1, the entropy values are 0.2653 and 0.3010, respectively. Assuming the same network loading level for each case, these values imply that the second case is more robust than the first case with respect to cascades of overload failures coinciding with the aforementioned observations. When computing entropy values for cases in Figure 2, 0.3010 and 0.4772 are obtained for Case 1 and Case 2 respectively. Note that in case of a higher out-degree and a more homogeneous load distribution, the resulting entropy value becomes larger. This illustrates how the entropy concept captures topology-and load distribution homogeneity effects on cascading failure robustness.

The effect of loading level of the network on robustness is incorporated using the network tolerance parameter α, that relates initial load to the capacity of a line as:

$$C_i = \alpha_i L_i \tag{3}$$

The capacity of a line is defined as the maximum load that can be carried by the line while the loading level (LL_i) of an arbitrary line is the ratio between the load and the capacity of the corresponding line. Hence, there is an inverse relationship between the loading level and the tolerance parameter of a line:

$$\alpha_i = \frac{1}{LL_i} \tag{4}$$

Combining Equations (1), (2) and (4), nodal robustness of a node i (i.e. $R_{n,i}$), that takes both the flow dynamics and topology effects on network robustness into account, is then defined as:

$$R_{n,i} = -\sum_{i=1}^{L} \alpha_i p_i \log p_i \tag{5}$$

In Equation (5), the minus sign (-) is used to compensate the negative nodal robustness value that occurs due to the logarithm of normalized flow values (i.e. p_i).

B. Electrical node significance

Due to the scale-free nature of power grids, some of the buses act as hubs i.e. deal with a relatively larger amount of power, while other nodes distribute a relatively small amount of power. When a failure occurs at a link that originates from one of the hub buses, a significant amount of power is exposed to the remainder of the network. Redistributing this excess power over adjacent components eventually causes further link overload failures, which potentially results in a large-scale power outage. Nevertheless, if a failure occurs at a link that is connected to a less important node, its power is immediately re-routed to adjacent components and the disturbance can, usually, be suspended. This shows that nodes have different impacts on the context of cascading failure robustness and this impact depends on the amount of power, distributed by the corresponding node. In this paper, impact of a particular node is reflected by electrical node significance δ. Electrical node significance of an arbitrary node i is computed as:

$$\delta_i = \frac{P_i}{\sum_{j=1}^{N} P_j} \tag{6}$$

where P_i stands for total power distributed by node i while N refers to number of nodes in the network.

C. Network Robustness Metric

After computing nodal robustness and electrical node significance values, two different values are obtained for each node in the network. The product of these two values indicates the individual contribution of each node to the network robustness. The network robustness metric calculation is finalized by summing up these individual contributions of each node in the network. The resulting metric R_{CF}, shown in Equation (7), quantifies network robustness with respect to cascading failures in power networks.

$$R_{CF} = \sum_{i=1}^{N} R_{n,i}\delta_i \tag{7}$$

The normalized nature of electrical node significance assures that the robustness of power networks with different size can be compared.

IV. Experimental Set-up

This section explains the experimental set-up used for robustness metric verification analysis.

A. Power grid networks: IEEE 14 bus test system and synthetic networks

The data required for the robustness metric verification analysis includes the admittance matrix of the network, the number of buses, their types and finally their generation capacity and load values. The IEEE test systems [21] include all of these data. In this paper the IEEE 14 bus test system (see Figure 3) is used as a reference, additional synthetically generated networks based on this system are also used. The (generated) synthetic networks have exactly the same properties as the IEEE 14 network (e.g. topology, number of buses and links, type of buses and their demand/generation capacity values) except for the admittance matrix. The synthetic networks are derived from the IEEE 14 bus network by randomly shuffling transmission lines in the network. For example, a link l_{ij} (with an admittance value y_{ij}) connecting nodes i and j is exchanged with another link l_{mn} (with an admittance value y_{mn}) connecting nodes m and n so that nodes i and j are connected by l_{mn} and nodes m and n by l_{ij}. This exchange of links results in a different admittance matrix for the generated network. Consequently, the distribution of power flow in the network is influenced causing the synthetic grid to have a different load distribution (i.e. a different level of load distribution heterogeneity). This in turn causes different R_{CF} values and different cascading failure survivability performances for each generated grid.

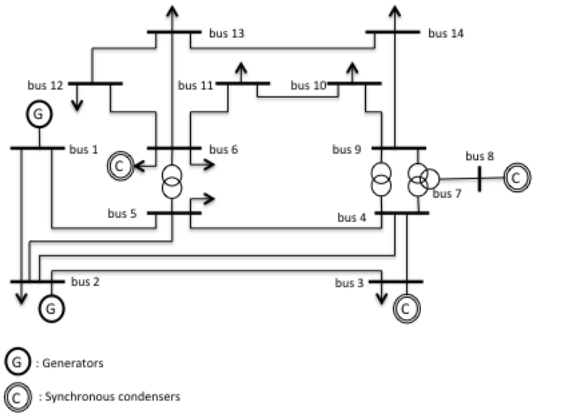

Fig. 3. IEEE 14 busses test system

B. Attack scenario

An effective attack will always target the most critical components in a network. This paper assess the criticality of a node in the context of cascading failures based on its electrical node significance value. The node with the highest electrical node significance is determined to be the most critical node in the network. The largest cascading failures in a power network, most likely, occur if this node is attacked. For the purpose of verification, this paper assumes that an intelligent attacker will target *the most important outgoing link (i.e. most heavily loaded outgoing link) from the most critical node in the network*. Removal of this link will result in a cascading failure for the power network, that relates directly to the robustness of the power network with respect to targeted attacks.

C. Cascading failure simulation and assumptions

This paper models a power grid as a complex network in which generation, transmission and load buses are modelled as nodes while transmission lines are represented by edges. In a power grid model, flow values through the network can be estimated by AC or DC load flow equations. AC power flow equations are non-linear equations modelling the flows of both active and reactive powers, while DC load flow equations are a simplification and linearisation of AC power flow equations considering only flow of active power [9], [10]. Throughout this paper, DC load flow analysis is performed for the given test systems with the MATPOWER power network simulation package [22], resulting in a flow matrix for each network. A flow matrix is basically a connection matrix in which the element f_{ij} corresponds to the power flow between node i and node j. The robustness metric for each network setting is computed by applying the theoretical approach (given in Section III) on its flow matrix.

For the purpose of simulation, each network has to be initialized in a similar manner for the results of the attack scenario to be compared : (i) the node from which the line-to-be-attacked origins, has the same electrical node significance in each setting; and (ii) the line-to-be-attacked has the same relative amount of power flow (compared to its adjacent lines) in each setting. This approach ensures a fair initialization for each network and that the same relative amount of excess power is redistributed in each network.

To simulate a cascading failure, the line-to-be-attacked is removed from the topology. Once a line is pruned, its flow is distributed over its neighbours. This simulation assumes that the excess power is distributed over all adjacent lines based on their initial load [23]. Distribution of the excess power may cause overloading of other neighbours resulting in tripping of these lines by circuit breakers. This paper considers line failures due to cascading effects and not on node failure. The power carried by the newly failed lines is redistributed as well. This procedure continues until no more lines are overloaded and stability is attained. For sake of simplicity, this paper assumes a deterministic model for line tripping mechanism. A circuit breaker for a line l trips at the moment the load of the line l exceeds its maximum capacity. Furthermore, no mitigation strategies are deployed to alleviate cascade process.

The survivability of a network against cascading failures is quantified empirically by the metrics Link Survivability (LS) and Capacity Survivability (CS). LS is defined as the fraction of lines that are still in operation after a cascading failure, whereas CS is formulated as the fraction of the capacity of these operational lines. A line is considered to be operational if it is not tripped by the protection mechanism and if it is not disconnected from generators so that it still delivers power after the cascading failure. LS and CS are given in Equation (8) and Equation (9). L and C stand for the total number of links and the sum of the capacity of these links in the original network while $L^{'}$ and $C^{'}$ are the new values after the cascading failure.

$$LS = \frac{L^{'}}{L} \tag{8}$$

$$CS = \frac{\sum_{i=1}^{L^{'}} C_i}{\sum_{j=1}^{L} C_j} \tag{9}$$

Both LS and CS are simulation-based metrics quantifying power network robustness empirically. They are computed offline and require substantial computational power and time for large networks, unlike R_{CF}. Both LS and CS are used to verify R_{CF} in Section V.

Prior to starting the cascading failure simulation, the most important node is determined based on the electrical node significance values. The node that has the highest electrical node significance value in the IEEE 14 bus test system is determined: node 1 (see Figure 3). After that, the flow distribution at node 1 is modified in such a way that 55% of the flow goes through line 1-2 while the rest is sent through line 1-5. This is done to provide a fair initialization (as explained in Section IV-C). Note that 55% is just a matter of choice, it is important this value is the same for each generated network.

V. Experimental Verification

Verifying the robustness metric (R_{CF}) entails (1) generating synthetic sample networks from the given reference network, (2) computing robustness metric values for sample networks (i.e. obtaining theoretical results: R_{CF} values), (3) simulating a cascading failure in each network and quantifying the network robustness against cascading failure empirically (i.e. obtaining experimental results: LS and CS values), (4) calculating the correlation between robustness metric R_{CF} values (i.e. theoretical results) and simulation-based LS and CS values (i.e. experimental results), (5) assessing whether the robustness metric quantifies the network robustness with respect to attack-based cascading failures.

The synthetic sample networks are generated from IEEE 14 test network following the method explained in Section IV-A. The robustness metric values (i.e. R_{CF}) are computed applying the theoretical approach explained in Section III on these networks. A cascading failure is simulated in each topology as described above in Section IV. Line 1-2 (see Figure 3) is attacked and the network cascading failure robustness is quantified empirically by LS and CS. This analysis is performed for a set of 100 different sample networks. R_{CF}, LS and CS values for the first five sample networks are shown in Table I. It suggests that computed robustness metric (R_{CF}) and empirically-obtained cascading failure quantifiers (LS and CS) values are in line (e.g. R_{CF} indicates Synthetic network 1 is more robust than Synthetic network 2, and this is also shown to be correct by the means of simulation-based metrics LS and CS), with an exception (network 5). Additionally, the correlation between R_{CF} and LS-CS values for the whole set (i.e. 100 networks) is determined. Table II shows the result. The correlation level of around 75% between the theoretical approach and simulation results indicates that the R_{CF} quantifies the cascading failure robustness of a given network to a reasonable extent.

TABLE I
Robustness metric (R_{CF}) and cascading failure survivability metrics (LS and CS) for first 5 synthetic networks

	R_{CF}	LS(%)	CS(%)
Synthetic network 1	0.7143	0.5263	0.6771
Synthetic network 2	0.6096	0.3158	0.6182
Synthetic network 3	0.7065	0.4737	0.6482
Synthetic network 4	0.7587	0.5789	0.7469
Synthetic network 5	0.7483	0.6316	0.7435

TABLE II
Correlation levels between robustness metric (R_{CF}) and cascading failure survivability metrics (LS and CS) for 100 different network settings

Set size	R_{CF}-LS cor(%)	R_{CF}-CS cor(%)
100	76	75

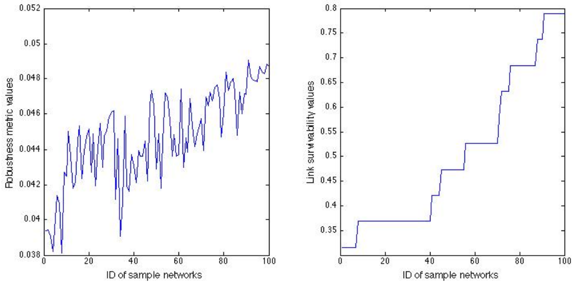

Fig. 4. Robustness metric (R_{CF}) and Link Survivability (LS) values for 100 synthetic networks

To assess the effect of the number of different network configurations (which was 100 in Table II) on the correlation value, the analysis above is repeated for 3 different sets of random networks. These sets consist of 1000, 5000 and 10.000 network configurations that are synthetically generated with the reference to the IEEE 14 bus test system (see Section IV-A). Resulting correlation levels are almost the same for all different test sets (ranging from 74-76%).

There are two main reasons for a relatively low correlation level (i.e. around 75%) between theoretical and experimental results. As mentioned before, it is very important to provide a fair initialization for each network setting. One of the conditions for fair initialization is that the node-to-be-attacked has the same electrical node significance in each sample network. Although these node significance values are very close to each other in our experiments, they are not exactly equal meaning that some of networks are exposed to a higher amount of power to redistribute than others. This biased condition results in a decreased correlation level between R_{CF} and LS- values.

Another factor that influences the correlation level can be better understood when considering the R_{CF} and LS values plotted in Figure 4. Notice that LS has a discrete underlying distribution meaning that it can adopt only certain values (i.e. $1/L$, $2/L$, .., 1) while R_{CF} can have any value between $R_{CF,min}$ and $R_{CF,max}$. This suggests that the effect of even a very small change in input parameters (e.g. a small change in loading level) can be observed in the aggregate R_{CF} value while this is not the case for LS. Consequently, a group of R_{CF} values is assigned to the same LS value. This results in a decreased correlation level between the robustness metric and the network cascading failure survivability quantifiers. However, if both R_{CF} and LS are approximated by a 4th order polynomial the correlation increases to over 90%.

VI. Discussion and Conclusion

This paper proposes a robustness metric (R_{CF}) to assess the robustness of a given power network with respect to cascading failures. The proposed robustness metric accounts for effects of topological properties as well as flow dynamics on network robustness. The key factors to model for covering these effects are (i) homogeneity of load distribution; (ii) loading level of the network; and (iii) out-degree of each particular node. These factors are incorporated in the robustness metric definition by using entropy and network tolerance parameter concepts. When simulating cascading failures in networks, the node-to-be-attacked is selected based on electrical node significance values. Experimental verification shows that the proposed metric anticipates the cascading failure robustness of a given power network.

Assessing the cascading failure robustness in power networks relies mainly on two aspects: the structure of the network and the operative state. The former aspect defines the interconnection of the components together with their specific attributes (e.g. electrical characteristics), while the latter aspect relates to the loading level and load distribution heterogeneity in the network. The structure of the network is static while the operative state in the network is continuously changing. This dynamic character of operative state makes cascading failure robustness of power networks also dynamic. This means that a power grid G with a certain operative state can be assessed as very robust at time t, while a new operative state (e.g. a new loading profile) at time $t + k$ can make the same grid critically vulnerable.

Although the significance of operative state on the cascading failures occurrence is emphasized by numerous researchers [11], [12], [13], the existing studies most often attempt to assess the cascading failure robustness by focusing only on the structural aspect, and not on operative state of the grid. Differently than existing studies, the proposed robustness metric R_{CF} takes both relevant aspects into account: the topological effects and the operative states in determining network robustness. Additionally, calculating the robustness metric R_{CF} does not require significant computational power and time and it can be done in a distributed manner.

Future work will focus on increasing power network robustness by adapting power flow dynamically in a distributed and self-organized manner. Within the context of SmartGrids, dynamically optimizing power flow in the grid based on the proposed robustness metric R_{CF} has the potential to ensure a higher level of cascading failure robustness in the network.

Acknowledgements

This work is funded by the NWO project *RobuSmart: Increasing the Robustness of Smart Grids through distributed energy generation: a complex network approach*, grant number 647.000.001. The authors also thank Evangelos Pournaras for fruitful discussions, and Prof. Ray Zimmerman for assistance related to MATPOWER.

References

[1] J. Chen, J. S. Thorp, and M. Parashar, "Analysis of electric power system disturbance data." in *HICSS*, 2001.

[2] "U.S.- Canada Power System Outage Task Force, Final Report on the August 14th Blackout in the United States and Canada: Causes and Recommendations," April 2004.

[3] J. Conti, "The day the samba stopped," *Engineering Technology*, vol. 5, no. 4, pp. 46 –47, March 2010.

[4] S. Y. Auyang, *Foundations of complex-system theories: In economics, evolutionary biology, and statistical physics*. Cambridge, UK: Cambridge University Press, 1998.

[5] K. Sun and Z.-X. Han, "Analysis and comparison on several kinds of models of cascading failure in power system," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 2005.

[6] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998.

[7] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[8] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabási Albert network model," *Physica A*, vol. 355, pp. 667–677, 2005.

[9] J. J. Grainger, J. Stevenson, and D. William, *Power System Analysis*. McGraw-Hill, 1994.

[10] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling, "Usefulness of dc power flow for active power flow analysis with flow controlling devices," in *The 8th IEEE International Conference on AC and DC Power Transmission*, march 2006.

[11] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys Rev E*, Dec. 2002.

[12] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, p. 045104, 2004.

[13] Y.-C. Lai, A. Motter, and T. Nishikawa, "Attacks and cascades in complex networks," 2004, pp. 299–310.

[14] P. Van Mieghem, *Performance analysis of communications networks and systems*. Cambridge University Press, 2006.

[15] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Letters*, vol. 87, no. 19, p. 198701, 2001.

[16] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *The European Physical Journal B*, vol. 46, 2005.

[17] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1-2, pp. 5–12, May 2009.

[18] A. Dwivedi, X. Yu, and P. Sokolowski, "Identifying vulnerable lines in a power network using complex network theory," in *IEEE International Symposium on industrial Electronics*, july 2009, pp. 18 –23.

[19] P. Hines and S. Blumsack, "A centrality measure for electrical networks," in *Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences*. IEEE Computer Society, 2008.

[20] M. Youssef, C. Scoglio, and S. Pahwa, "Robustness measure for power grids with respect to cascading failures," in *Proceedings of the Cnet 2011*. ITCP, 2011, pp. 45–49.

[21] [Online]. Available: http://www.ee.washington.edu/research/pstca/

[22] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12 –19, feb. 2011.

[23] J. W. Wang and L. L. Rong, "Cascade-based attack vulnerability on the us power grid," *Safety Science*, vol. 47, pp. 1332–1336, 2009.