ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on - Vulnerability Analysis on Cascading Failure in Power Grid Complex Network

Snehal Sanjay Ughade, B.W. Balkhande

Student, Dept. of Computer Engineering, BVCOE, Mumbai University, Navi Mumbai, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering, BVCOE, Mumbai University, Navi Mumbai, Maharashtra, India

ABSTRACT: We live in an advanced world dependent on large, complex networks. Examples world-wide web (WWW), the Internet, electrical power grids etc., present a surprisingly small average distance between nodes and a highly distributed organization of links per node. Sometimes, however, these links are also overloaded and must redistribute their increased load to their neighbors. This finally leads to a cascade of failures. Therefore, we introduce fundamental security techniques, whose integration is essential for achieving full protection against existing and future sophisticated security attacks. While pure topological analyzes their inability to characterize the physical principles requires a model to approximate failure behavior of a complex network. The proposed model called extended betweenness that combines network structure with electrical characteristics to define the load of power grid components. This brings obvious concerns on the security of such systems.

KEYWORDS: network, cascading failure, extended topological model, pure topological model.

I. INTRODUCTION

Complex networks are an essential part of a modern society. The Modern complex network systems, including communication network, social network and smart grid, have become a key focus of security analysis nowadays. With accelerative interconnection of local networks, increasing communication traffic and user demand, as well as diversifying services and emerging new technologies, the complex systems are becoming sophisticated to operate coordinately [1]. It has been shown that networks, such as the world-wide web (WWW), the Internet, and electrical power grids, present a surprisingly small average distance between nodes and a highly organized distribution of links per node. Generally, the average distance will not be affected by the removal of a random subset of nodes, but it will increase significantly if the removed nodes are among the most connected ones. The existence of a giant connected component in the network, however, does not depend on the presence of highly connected nodes [2].

One of many threats posed to complex network systems due to the large scale inter-connectivity is the cascading failure. Cascading failures are common in most of the complex communication and transportation networks that are the basic components of our lives and industry. Cascading failures take place in electrical power grids. In fact, when for any reason a line goes down, its power is automatically shifted to the neighboring lines, which in most of the cases are able to handle the extra load. Sometimes, however, these lines are also overloaded and must redistribute their increased load to their neighbors. This eventually leads to a cascade of failures: a large number of transmission lines are overloaded and malfunction at the same time. This is exactly what happened on 10 August 1996 when a 1300-mw electrical line in southern Oregon sagged in the summer heat, initiating a chain reaction that cut power to more than 4 million people in 11 Western States. And probably this is also what happened on 14 August 2003 when an initial disturbance in Ohio triggered the largest blackout in the U.S.'s history in which millions of people remained without electricity for as long as 15 h [3].

Take the future intelligent power infrastructure, i.e. the Smart Grid, as an example: studies [4]-[7] have put forward the fact that intelligence will bring new security challenges to the power grid; a gigantic system that already yields inherent structural vulnerability of cascading failures due to its physical nature [8]. For instance, malicious attackers can take advantage of the potential open access from smart meters in the Advanced Metering Infrastructure (AMI) [9] to plan the attack with intelligence collected from their penetration, so that they can maximize the impact of their

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

attacks [10]. Therefore, how to secure a complex network system like power grid against cascading failures has been motivating development of models and methodologies to simulate potential selective attacks that result in cascading failures in a power system with the consideration of specific network physical properties. These studies will contribute to both defensive strategies and decision supports to protect the critical components in the complex systems.

II. LITERATURE REVIEW

A. *Scope:*

Power grid is considered as one of the most significant infrastructure on the earth. Within recent decades, several large-scale power outages around the world seriously affected the livelihood of many people and caused great damage. For example, the well-known Northeast blackout in 2003 affected 55 million people and caused an estimated economic loss between $7 and $10 billion. Large scale power outage is often caused by cascading failure. A cascading failure of one or more components (i.e. substations and transmission lines) triggers the sequential failure of other components. Triggers of the initial failures can be natural damage (e.g., the fall of trees), aging equipment, human errors, software and hardware faults, and so on. Within recent years, power grids are facing new threats, e.g., cyber-physical attacks. Therefore, malicious attacks become new and potential triggers of cascading failure.

B. *Pure Topological Model:*

Many existing works have been proposed to investigate the vulnerability of power grids from the attack perspective. Important challenges, however, still remain. First, developing reasonable models that can mimic cascading failures in reality is still a critical challenge. There are three popular models, pure topological models, pure power flow models and extended model (Hybrid model). Second, finding stronger malicious attack strategies is one of the key ways to investigate cascading failures. Finally, attackers might have different knowledge of power grids, such as topological structures, electric features and real-time information. Pure topological models are rooted in complex network theories, and useful to develop strong attack metrics, e.g., degree and load, percentage of failure (PoF) and risk if failure (RIF) and load distribution vector (LDV). Pure power flow model provides the fundamental insights and understanding of cascading behaviors. Finally, the extended model is a new angle in modeling cascading failures because of the following reasons [10]. The power distribution under the extended model is based on power transfer distribution factors (PTDF). The reasons behind developing extended model instead of using pure topological model are as follows:

- Different models have different advantages and disadvantages. First, although pure topological models are useful to develop malicious attack strategies, the related concepts and metric are far from the physical characteristics of power grids. Thereby, these models are far from reflecting the fundamental behaviors of cascading failure.
- Pure power flow models are more accurate to reveal vulnerability of power grids. And are mainly used assess the security and reliability of power grid networks. However, a detailed analysis of large-scale power grid is usually computationally expensive due to its complexity, nonlinearity, and dynamics.
- Thus, the extended model is more accurate than pure topological models in terms of studying cascading failure. In addition, the calculation of PTDFs is less complex than the detailed analysis of power flows in a power grid. That is, the extended model is less complex than pure power flow model.

C. *Extended Model*

The complex network structure under investigation is power transmission networks, which plays a key role in delivering power from power plants to consumers via substations and transmission lines. From the complex network perspective, it can be regarded as a weighted, directed map with two major types of interconnected components, i.e. nodes and edges, referred to as buses and branches in the power system context, respectively. To an attacker in Smart Grid, buses in power grids are ideal targets since the substations they representing are the hubs of control units to regulate power transmission, and their failures prevent any power transmission along transmission lines connected to them. On the other hand, buses are generally better protected in reality, which cost more to attack than branches; also, overloading that leads to cascading failures also occurs more frequently on branches due to relay protections in a power system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Among the efforts to overcome the drawbacks of pure topological measurements for power grid, a recent study by E. Bompard implements an extended topological power-flow analysis using the Power Transfer Distribution Factor (PTDF) [11].

III. EXTENDED TOPOLOGICAL MODEL WITH PTDF

A. *Network Topology:*

Therefore, attacks on both components are covered in this paper. Finally, because the failure propagation process is closely related to a system's tolerance of fault, this paper also investigates the relationship between the final impact of attacks and the tolerance factor of a system. The goal is to provide an integrative tool with a better balance between accuracy and complexity to analyze power system behavior under potential attacks and identify critical components from this combined perspective. Generally, a power grid composes of substations (e.g., generators, transmission and distribution substations) and transmission lines. We model the power grid network as a directed graph, $G = \{B, L\}$, where B is the set of nodes (i.e. substations) and L is the set of links (i.e. transmission lines). **Power transfer distribution factor** (PTDF) can represent the sensitivity of power flow change in each transmission line for power withdrawal at a pair of nodes. In reality, power is only transmitted from generation nodes to distribution node. Under the extended model, power flow on links is considered to be caused by the node pairs that one node is generator and the other node is transmission node. The link **Extended betweenness** (EB) is the summation of power flows caused by each generation-distribution-node pair. The node extended betweenness is defined as the summation of extended betweenness on links that connect to a node.

Combining the power-flow based PTDF parameter with topological analysis, a new definition of load in the network can be introduced to analyze the structural stability. The redefined load on each bus v, proposed by E. Bompard as the Extended Betweenness [12],[13], involves three major steps: First, the power flow sensitivity of branch l with respective to the pairwise unit power transmission is calculated by:

$$f_g^d(l) = F_{lg} - F_{ld}, g \in G, d \in D, l \in L \quad \text{..... (1)}$$

Where f_g^l and f_d^l are the power flow occurred on branch l when a unit power is injected on a generation bus g or a load bus d and withdrawn from a reference slack bus, respectively. Then, with the definition of power flow sensitivity, we can calculate the capacity of power transmission between a transmission pair g and d. Specifically, because of different sensitivities to power flow injection, a more sensitive branch will reach its given power flow limit faster than less sensitive ones given the same capacity. Therefore, the maximal power that could be transferred between any given transmissions pair is limited by the most sensitive branch in the whole grid. This assumption can be easily extended to a more realistic case where the branch capacities are different. Assume that each transmission line has a designed limit $P_{(max)}(l)$ (MW), a pairwise power transmission capacity between g and d when the first branch in the grid reaches its limitation (denoted as P_g^d) is defined as:

$$P_g^d = \min_{l \in L} \left(\frac{P_{max}(l)}{|f_g^d(l)|} \right), g \in G, d \in D \quad \text{..... (2)}$$

Where it should be noted that P_g^d is defined and calculated in pairs between any generation bus g and load bus d in the system. In other words, P_g^d is a theoretical pairwise power transmission upper-bound between a transmission pair due to the limit of branches. Finally, the new defined load, i.e. the extended betweenness of a bus, is calculated as the overall power transmission capacity of a given bus v

$$T(v) = \frac{1}{2} \sum_{g \in G, d \in D, l \in L} P_g^d f_g^d(l), g \neq D \neq v \neq V \quad \text{..... (3)}$$

Where L^v is the set of branches directly connected to a bus v in the set of all buses . The product P_g^d . $f_g^d(l)$ represents the power flow transmitted via branch l when power between a transmission pair g and d is transferred at its pairwise transmission capacity. The discount factor is applied since the total power carried into a bus should equal the total power flowing out of it. Similarly, the extended betweenness for a branch is defined as

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

the overall power transmitted across branch l in a power grid. Since the PTDF F has either a positive or negative sign according to power flow direction, the extended betweenness for a branch l is determined by the greater of absolute in-flow and out-flow:

$$T(l) = \max_{l_+, l_- \in L}\{\sum_{g\in G, d\in D} P_g^d \cdot f_g^d(l_+) \sum_{g\in G, d\in D} |P_g^d \cdot f_g^d(l_-)|\} \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Where l_+ and l_- corresponds to $f_g^d(l)$ with a positive sign and negative sign, respectively. It is notable that in [14] the extended betweenness is interpreted as a representation of the total power transmitted on a branch l in the grid. However, in the power flow theories, the positive and negative power flow on a branch will cancel each other; in this case, the actual load is measured differently as the sum of both values. As the focus of this paper is to develop a CFS based on extended betweenness for cascading failure analysis, we adopted the definition of $T(l)$ as originally proposed by E. Bompard , while further modifications can be implemented to adapt to the power flow assumptions. In this paper, we adopt extended betweenness as the load on each bus and branch because of its strength to capture both topological and electrical characteristics of power grids. Although the term extended betweenness resembles the concept of betweenness centrality in graphic theory and complex network studies, it should be noted that there is a distinctive difference between them as the extended betweenness is not based on the geodesic shortest paths. Although it borrows the idea of pairwise transmission, the "extended betweenness" is not purely topological as it does not characterize the power flow as a geodesic shortest path. Instead, it is the overall power transmission capacity according to a power system based model; consequently, the measurement is closer to the real power systems. In addition, this model utilizes the sensitivity and flow-limit on each branch to calculate the transmission capacity; thereby it provides a better approximation on power transmission than pure topological approaches as well. In summary, it captures physical characteristics of a real power system that add to its robustness while still retains the strength of security analyses of complex networks.

IV. EXTENDED BETWEENNESS BASED CASCADING FAILURE SIMULATOR

On top of the extended betweenness measurement proposed to assess the structural vulnerability of power grid, we also see the potential of improving this model as a cascading failure simulator (CFS). The motivation for developing this simulator has two folds. On one hand, without a complete knowledge of real-time loading information, the extended betweenness can be used as a more power-related approximation of load than pure topological methods, and the overall loss of extended betweenness can be used to approximate the portion of blackout size related to embedded structural vulnerability in power grids. But on the other hand, the extended betweenness is still merely a static structural measurement that cannot fully consider the effect of consequent failure propagation in a cascading failure. A further development of a CFS will help us simulate the consequence of power grid behaviors, including overloading and failure propagation triggered by the initial attack, so that we can better evaluate and understand the impact of attacks that may cause the collapse of power transmission networks.

A. *The general procedure of EB-CFS:*

Step 1: **Initialization:** Calculate the initial extended betweenness T as a system's initial load with the corresponding capacity, which is a value set by the system tolerance parameter Tol;
Step 2: **Initial Attack:** Initiate an attack and update the network topology;
Step 3: **While** any victim or failed component is identified do

- Re-calculate the PTDF and the extended betweenness to acquire the redistribution of load;
- Determine if any component is overloaded, and if this overloading is severe enough that it exceeds the capacity, which is referred to as a fatally overloaded state;
- Trip the fatally overloaded component from grid and update the network topology

Step 4: **End while**
Step 5: **Attack Impact Measurement:** Evaluate the load loss ΔEB as a measurement of victim's vulnerability after the cascading failure.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

1. **Initialization:** the first step is to setup initial status of all network components and related parameters. The capacity in the context of extended betweenness is usually calculated as a function of the initial load of a given benchmark, which assumes that branches carrying heavier power transmission load will be designed to have greater capacity [14]. Therefore, we assume there is a global overload tolerance in a system, denoted as Tol. Numerically, this can be defined as $\mathrm{Tol} = \mathrm{cap(c)}/\mathrm{T}^0\mathrm{(c)}$, where cap(c) is the capacity and $\mathrm{T}^0\mathrm{(c)}$ is the initial load (extended betweenness) of a component c in the given system. Note that by definition, the Tol should always be larger than one, and it can also be viewed as the system redundancy between the initial load and its maximal capacity. In reality, the loading of a transmission network is dynamic which varies over time, resulting in different remaining tolerance ratio even with a constant capacity. Therefore, to evaluate different possible tolerances in reality, a numerical analysis on the relationship between tolerance and the cascading impact will be evaluated. By varying the value of Tol used in simulation, we can generate different situations of system tolerance to measure the vulnerability of cascading failures for different system states.

2. **Initial Attack:** To initiate an attack, we simply choose a number of victims, either buses or branches, and cut them off from the original grid. Then we start the following iterative process of cascading failures in the EB-CFS.

3. **Update System Parameters in the Post-Attack/Post- Failure Stage:** The structure of a power grid will be changed after a direct victim of the initial attack or a component failed by the cascading effect is cut off. Consequently, the extended betweenness should be recalculated to reflect the latest state. It is notable that in this recalculation, updates should be made through the computations from the PTDF matrix F to the extended betweenness T, as all intermediate parameters depend on the current network topology. To be specific, whenever a new grid topology is set up, we will first recalculate the PTDF depending on whether DC or AC model is chosen. Then, the branch sensitivity $f_g^d(l)$ and the pairwise power transmission capacity $P_g^d(l)$ will be updated to $f_g^d(l)$ and $P_g^d(l)$, respectively. Afterwards, the power flow of branch l generated by a transmission pair g and d will be changed to $P_g^d(l) \cdot f_g^d(l)$. Hence a post-attack extended betweenness T' at any given moment is calculated with Eqn. (3) and (4). Also, in the cases where the initially fully-connected grid is broken down into disconnected islands, we will set up a new topology for each of the sub-area and re-calculate the extended betweenness T' locally within each sub-area. As a special case, if a new sub-grid contains no generation buses or load buses, by definition the extended betweenness of all components in this isolated sub-grid will be set to zero.

4. **Detect Failure Components**: A failure that occurs on either a bus or a branch will affect other components in the grid, but it may or may not result in a fatal overloading depending on the capacity of a system and the real-time loading. Meanwhile, as in any CFS, the post-attack overloading degree (if overloading exists) is a critical index affecting whether an overloading is turning fatal. Hereby we define the overloading ratio of a component c, denoted as $r_{(C)}$ as the post-attack extended betweenness over the initial pre-attack betweenness, i.e. $r_{(c)} = \frac{T'_{(c)}}{T_{(c)}}$. It reflects the impact of the previous failure on each component during the cascading process. Because the components in the system subject to a maximal degree of overloading ratio, they will be shut off and disconnected if the upper-bound is reached so as to protect the remaining facilities. Therefore, we consider a component c is fatally overloaded, or failed, if $r_{(C)} > Tol$; if, however, an overloading occurs but not fatal ($1 < r_{(C)} < Tol$), then c is regarded as deficient but still in operation.

5. **Trip Failed Components:** For any failure occurs in the power grid due to direct attack or the failure caused by post-attack overloading, the network topology needs to be modified accordingly. In this paper, the following policy will be carried to update the grid topology:

    - If a bus fails, no more can be transmitted through this nodal connection in the system, and so any branch connecting to it will also lose the ability to transmit any power. Therefore, for any bus failure, the bus itself with all connected branches are removed from the topology;

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

For a branch failure, because a bus connecting to its end can still be linked to the remaining system by other branches, the EB-CFS only performs a removal of the failed branch from the network.

V. CONCLUSION AND FUTURE WORK

We proposed an extended topological vulnerability assessment approach for cascading failure analysis of complex network system via a case study of power grid. By introducing the electrical property based extended betweenness; we proposed an integrated failure cascading simulator. Vulnerability measurements under selective victim attack strategies and cascading failure simulation for both bus and branch attacks were presented. According to the simulation results, our extended topological approach is able to assess the vulnerability of power grid components in cascading failures with only limited knowledge on dynamic real-time information of a power system. Some simulation results show that the vulnerability of branches measured at a low system tolerance. Although it is reasonable for the power transmission network in practice, the complexity indeed poses challenges to the cascading failure analysis and calls for future work to improve this model with less tolerance dependency. In addition, further development of fast multi-victim selection methods and intelligent attack strategies can also extend the utilization of the EB-CFS approach in more complex attack and defense scenarios.

REFERENCES

1. Yan, Haibo He, Yan (Lindsay) Sun and Ying-Cheng Lai, "Integrated security analysis on cascading failure in complex network", *IEEE Transaction on Information Forensics and Security*, Vol. 9, No. 3, March 2014.
2. A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks", *Phys. Rev. E*, vol. 66, no. 6, pp. 065102-1–065102-4, Dec. 2002.
3. P. Crucitti, V. Latora, and M. Mariori, "Model for cascading failures in complex networks", *Phys. Rev. E*, vol. 69, no. 4, pp. 045104-1–045104-4, Apr. 2004.
4. Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee and A. Perrig, *et al.*, "Cyber-physical security of a smart grid infrastructure", *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
5. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid", *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
6. X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges", *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.
7. P.-Y. Chen, S.-M. Cheng and K.-C. Chen, "Smart attacks in smart grid communication networks", *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.
8. M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, *et al.*, "Risk assessment of cascading outages: Methodologies and challenges", *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, May 2012.
9. O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
10. Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph", *IEEE Trans. Parallel Distrib. Syst.*, to be published, doi: 10.1109/TPDS.2013.
11. S. Jonnavithula and R. Billinton, "Topological analysis in bulk power system reliability evaluation", *IEEE Trans. Power Syst.*, vol. 12, no. 1, pp. 456–463, Feb. 1997.
12. E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability", *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012.
13. E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks", *IET Generat., Transmiss. Distrib.*, vol. 4, no. 6, pp. 716–724, Jun. 2010.
14. E. Bompard, M. Masera, R. Napoli, and F. Xue, "Assessment of structural vulnerability for power grids by network performance based on complex networks", in *Proc. Critical Inf. Infrastruct. Security*, pp. 144–154, 2009.
15. M. Eppstein and P. Hines, "A 'random chemistry' algorithm for identifying collections of multiple contingencies that initiate cascading failure", *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

BIOGRAPHY

Ms. Snehal Sanjay Ughade is a student pursuing Master of Engineering (M.E) degree in the Computer Engineering Department, Bharati Vidyapeeth College of Engineering, Mumbai University. Her research interest is Computer Security (Cyber Attacks).