Complex Science Application to the Analysis of Power Systems Vulnerabilities

Ettore Bompard, Di Wu, Enrico Pons

1 Introduction

Power systems are one of critical infrastructures since they are widely distributed and indispensable to modern society. Both accidental failures and intentional attacks can cause disastrously social and economic consequences. For example, in August 1996, a 1300-MW line failure initiates a cascading failure that cut power to an area spanning several Western states and containing more than 4 million people [1]; in August 2003, the historic blackout of United States and Canada in which 61,800 MW of power were disconnected to an area spanning most of the north-eastern states of United States and two provinces of Canada, and more than 50 million people remained without electricity for 15 hours [2]. Therefore, it is necessary for electrical utility operators to understand and analyze power systems in order to maintain a more robust system against natural or malicious threats.

However, frequent blackouts in United States have not decreased from 1984 to 2006, though advanced technologies and huge investments have been exploited in sustaining the reliability and security of power systems [3]. The reason for this is that electrical engineering analysis methods are based on given contingencies, but it is computationally infeasible to check all possible combinations of successive contingencies simulating cascading failures in large-scale power grids. Even though large-scale blackouts can be explained as a main result of a chain of failures after some rare events happen, it is not easy to indentify all possible rare events for a blackout in a large-scale power grid with thousands of components. On the other hand, in terms of various research phenomena which possible threat the security of power systems, electrical engineering analysis methods can be classified different assessment programs such as static security assessment [4-6], transient security assessment [7], voltage stability assessment and small signal stability analysis, and so forth. Nevertheless, these assessment programs are sensitive to operational conditions of power systems. This means these programs could provide different analysis results due to different operational conditions. As a result, it is difficult to prevent the collapse of power systems using these assessment programs because of unexpected or unforeseen operational conditions. Besides, most of these programs just focus on understanding one of various phenomena in power systems rather than overall phenomena, but serious consequence of power systems, like large blackouts, usually happen as a consequence of complicated interactions between system operators and power grids via communication, which is reflected by power systems as a whole and cannot be analytic description. These challenges advance new insights and approaches applied to comprehension of power systems.

Power systems could be considered as a complex system, so power systems can be
analyzed and comprehended in the framework of complex system theory, which is able to help us comprehend power systems from a new angle to improve the operation and reliability of the system. In this survey, we will review complex system researches on power systems. In the following sections, section 2 will give the possible reason why power systems could be considered as a complex system; section 3 will introduce complex network methodology to analyze complex systems from a topological point of view and then will review the applications of the methodology in power grids; In section 4, we will survey the understanding and analysis of blackout dynamics in power systems from complex system standpoint. The conclusion will be presented in section 5.

2 Power systems as a complex system

Complex systems could be described as a system which has the following properties: the system consists of a multitude of simple components; each of components has its own behavior, attitude and goal; complicated interactions among these components result in organization and emergent behaviors of the system which cannot be expressed by a set of equations or functions. Power systems as a whole could be regarded as a complex system due to its complexity not only resulting from power grids themselves but from complicated interactions in power grids as well. Specifically, assume that power grids are composed of 3 layers: physical layer, cyber layer and decision-making layer. In the physical layer, there exist generator stations, transmission networks, distributions networks and final users, and the basic objective of the physical layer is transferring power energy from generation stations to final users. The decision making layer which is composed of transmission system operators and electrical market players sends commands to control power systems to operate securely and economically. The cyber layer is an interface between physical layer and decision-making layer to transfer reliably information between them. In each layer, there are a large number of simple components such as generators and transformers in physical layer, measure equipments in cyber layer, system operators and electrical market players in decision-making layer. These simple components have their own behavior and goal to secure operation of power systems as a whole. Meanwhile, the organization and emergent behaviors of power systems such as blackouts are resulted from complicated interactions among these simple components. Although, in power grids, the action transferring power from generators to final users can be expressed in a set of equations, the complicated behavior of power systems as a whole cannot be simply described by whichever a set of functions or equations. As a result, power systems could be considered as a complex system.

3 Structure and robustness

3.1 Complex networks methodology

To understand the emergent behaviors of a system as a entirety, the structure of interactions among components in a system firstly need to be studied for comprehending the structure of a complex system can better understand its evolution mechanism and dynamical behavior [8]. Complex network methodology is widely accepted and used method to analyze the networked complex systems from topological perspective [9-10]. Complex networks methodology can be conceptualized as the intersection between the
graph theory and statistical mechanics [11]. Specifically, a complex system is firstly abstracted as a network with a set of edges (or lines) connecting a set of vertices (or nodes). Then, structural properties of the abstracted network and its evolution process can be studied by a set of informative indices based only on the geometric features of the system that do not change over time. However, the real networks are inherently difficult to understand due to its structural complexity: the connection can be represented as various ways since vertices and edges have different functions in different complex systems; network is evolving with time when some of old vertices and edges as a part of a network (or network as a whole) are replaced with new ones; the various factors impacting the structural complexity could have interactions which lead to more complicated effect on network structure.

3.2 Structure property analysis

With the aim at explaining and comprehending common principles and properties in real networks, three general network models have been intensely researched: random network [12], small-world network [13] and scale-free network [14], though these models cannot interpret all phenomena observed in real networks. Random network has binomial or Poisson degree distribution [15], so random network is rather robust since it is a homogeneous network where majority of vertices almost have the same number of edges to be connected. However, real networks do not shown random distribution and properties. Small-world is a network between a lattice and random networks. Small-world network has smaller average path length like a random network but larger clustering coefficient like a lattice network. Rather unexpectedly, the degree distribution of small-world network is mathematically explained by binomial distribution that is same as random network. Besides, most of real networks have the degree distribution that is power law [16] rather than Poisson distribution and these networks are called as scale-free network which is sensitive to intentional removal of vertices but robust against randomly removing vertices because the power law distribution shows it is a heterogeneous network where a larger number of vertices have larger edges to be connected and these vertices are called as hubs that play important role in connectivity of networks [17].

When considering power systems as a complex system, power grids are naturally regarded as research objects to study the behavior of power systems as a whole from a topological standpoint. Although lack of actual topological data of power grids limits the investigation of structure of power systems, a few existing researches find that power grids exhibit some properties of non-random network. Specifically, United States western power grid showed small-world properties [13]. North American power grid has exponential degree distributions, though the betweenness [18] [19] displays a power law distribution [20]. Similarly, the power grid of Western United States and Canada also has an exponential degree distribution [21] while Eastern Interconnected and Western System electrical transmission networks are scale-free networks because these transmission networks have a power law degree distribution [22]. Also, the high-voltage transmission networks of Spain, Italy, French show small-world properties and exponential degree distributions [23]. Furthermore, the investigation of UCTE (the Union for the Coordination of Transport of Electricity) power grid shows power grids of UCTE and its members have
exponential degree distribution, but most of them lack typical small-world characteristics [24].

### 3.3 Structural robustness analysis

Topological complex network characterization, such as random, small-world or scale-free networks is only a label for network classification without further structural analysis. Therefore, structural robustness analysis needs to be implemented [25-26]. The structural robustness is the ability of a network to avoid malfunctioning when a fraction of its components is damaged, and it can be classified in two different variants: static robustness and dynamic robustness. At the same time, both variants can be implemented in two main ways: errors (or random failures) and attacks (or selective failures). Errors are the ability of the system to maintain its network properties after the random deletion of a fraction of its vertices or edges whilst attacks are the ability of the system to maintain its properties when a deletion process is targeted to a particular class of vertices like the highly connected ones.

Static robustness is the act of deleting vertices without the consideration of redistributing any quantity that is possibly transported in the network. The analysis of North American power grid shows the power grid is vulnerable to attacks of transmission substations [20]. Power grids of UCTE and its members display patterns of reaction to attacks of vertices similar to those observed in scale-free networks, though the degree distributions of these power grids is exponential [24]. Further analysis shows that power grids of UCTE members could be classified as robust and fragile groups using mean field theory, and there is a positive correlation between the classification of two groups and real reliability measure of UCTE [27]. Besides, critical vertices and edges, whose removal has a serious impact on network structure, can be identified in Italian, Spanish and French power grids using efficiency [28].

Unlike static robustness, dynamic robustness considers the dynamics of flows of the physical quantities of interest over a network when removing vertices. When it comes to modeling the dynamics, the situation is far more complicated since the components of a network may have different dynamical behaviors and flows are often a highly variable quantity, both in space and time. The topological measure has selected the betweenness centrality [18] to be considered as the load of an element in a network. The dynamic robustness of the network is then evaluated in the following way [29-32]: each element is characterized by a finite capacity (defined as the maximum load that the element can handle). Once a deletion of a vertex (or an edge) has taken place, it changes the shortest paths between vertices. Consequently, the redistribution of betweenness possibly creates overloads on some other vertices (or edges). All the overloaded vertices (or edges) are removed simultaneously from the network. This leads to a new redistribution of loads and subsequent overloads may occur again. The new overloaded vertices (or edges) are removed and the redistribution process continues until at a certain time all the value of betweenness of the remaining vertices (or edges) under or equal to their each own capacity. For dynamic robustness, the analysis of North American [20] and Italian power grid [33] shows that they are rather vulnerable after selective failures happen in vertices with high betweenness because these power grids have heterogeneous vertex
betweeness distribution. In North American power grid, when considering selective failures on high load transmission substations, only 2% loss of the transmission substations can lead to almost 60% of its connectivity loss. An overloaded cascade triggered by loss of a single substation can result in up to 25% loss of transmission efficiency [34]. The results of UK power transmission grid shows that the network dynamic robustness could be reduced when transient oscillations or overshooting is considered in the kind of flow dynamics model [35]. In another dynamic robustness analysis of Western United States power grid, the load of a vertex is modeled based on degree measure. The analysis discovers that selective failures in vertices with lowest loads are more harmful for the power grid than the vertices with highest loads [36]. Also, the dynamic robustness is analyzed in the case of considering the interaction between Italian power grid and its internet communication network [37]. Surprisingly, it is found that a broader degree distribution increases the vulnerability of interdependent networks to random failure, which is opposite to the behavior of a single network to dynamic analysis. Therefore, it is necessary to consider interdependent network properties in designing robust networks. Besides, by virtue of a simple cascading failure model, it is quantitatively confirmed that the reliability of the North American electric grid can be estimated by combing the Barabasi–Albert model [22]. The cascading failure of Chinese power grid is investigated by small-world model and results shows that the cascading failure of Chinese power grid is closely correlated to critical vertices and edges which have high degree and short geodesic distance after each step of components out of service [38]. Likewise, it is found that the increase of average path length has a close link to 1996 blackout in United States western power grid [39].

3.4 Extended topological method

Initial application of complex network methodology in power grids overlooked the electrical engineering properties, so analyzing results could be far from the reality in power systems. For example, topological and electrical measures of vulnerability is compared in Eastern US power grid, and the results indicate that there is only mild correlation between tow groups of measures; thus, the vulnerability evaluation in power grids could lead to misleading conclusion using purely topological metrics [40]. Similarly, in the analysis of impact of topology on Italian power grid, it seems that the topology analysis is only able to provide complementary information on analyzing power systems [41].

To attack this problem, electrical engineering characteristics are introduced into complex network methodology, which is type of extended topological method. When power grids are regarded as weighted graph [11], instead of unweighted graph, where weights is line impedance, power grids appears to be scale-free network and so they have a number of highly-connected “hub” buses which possibly have an important impact on reliability and security of power grids [3]. Besides, the transmission capability of power grids has a closed link to their long connection in terms of line admittance, which is independent of power grid scale [42].

With the aim at measuring the importance of buses and lines in power grids and then analyzing the vulnerability of power grids, a set of metrics in complex network
methodology is redefined according to electrical engineering features. *Entropic degree* is proposed to measure importance of bus by considering distribution of line impedance on each line [43]. *Net-ability* [44] is defined instead of *efficiency* [45-47] to measure the transmission performance of power grids using electrical equivalent impedance in terms of line impedance. Also, in *path redundancy* metric [48], power contribution in paths is considered into evaluating the redundancy of available paths after power grids are attacked. Further, based on net-ability and path redundancy, *survivability* is created by combining net-ability and path redundancy together to evaluate the whole performance of power grids (i.e., transmission capability and robustness) [48]. Betweenness is a significant metric to measure the significance of a vertex or edge in a network. At the beginning, it is assumed that information exchanges or transmits in networks along the *shortest path* [49] between any pair of vertices, so *betweenness* is originally defined as the number of shortest paths between vertex pairs that pass through the vertex or line of interest. When line impedance is considered as weight in power grids, shortest path is the path that has minimum sum of weights on each line instead of the minimum number of lines [50]. Further, when power grids are regarded as flow-based network where flow transmits not only along the shortest paths but also along the remaining paths (i.e., non-shortest paths), *current-flow betweenness* [51] is defined as the amount of current flowing through a given bus or line when a unit of current is injected at each pair of generator and load, and then the amount is averaged over all pairs of generator and load. Actually, the current-flow betweenness can be considered as the special example of *random-walk betweenness* [52]. On the basis of current-flow betweenness, another two electrical betweenness is proposed: one considers the power transmission capacity [53]; another takes capacity of generator and peak value of load into account [54]. Clearly, these results shows that electrical betweenness is better than topological one in identification of critical buses and lines in power grids.

Power grids seem to be an optimal candidate for this kind of dynamic robustness analysis because of frequent large-scale blackouts with cascading failures in power grids. Topological model of dynamic robustness analysis is based on topological betweenness centrality modeling the redistribution in networks. It is natural that above-mentioned types of electrical betweenness are introduced into the topological model to create model analyzing dynamical robustness in power grids. For example, weighted electrical betweenness and current-flow betweenness are used to analyze the dynamic robustness in [55] and [56], respectively. However, simple models of the dynamic robustness analysis are motivated by the propagation of failures and congestion in the internet where considers flows of discrete packets injected at and withdrawn from all vertices along shortest path. Even though these models consider electrical engineering features, they are only to some sense quantitatively explanatory theory. Hence, they are not realistic and sufficiently accurate to understand complicated mechanism of blackouts in power grids. Power grids are special networks where the flow is power governed by Kirchhoff's Law and electrical engineering constraints; *hidden failure* [57] [58] could play important role in large-scale blackouts; some control strategies such shed load or shed generator need to be adopted to manage power grids in order to reduce in consequence of blackouts; the increase of load demand resulting in power grid expansion could also drive blackouts.
Some hybrid methods associate dynamic robustness analysis with specificity of blackouts in power systems to more approach to real situation of blackouts in power systems. For instance, in Ref. [59], power flow distribution is computed by DC power flow computation [60] instead of betweenness centrality and hidden failure are combined with the topological dynamical model to evaluate dynamical robustness in power grids. In addition, the concept of entropy [61] quantifying the distribution of flow on each line is also introduced into dynamic model to study the impact of heterogeneity of flow distribution on dynamics robustness of power grids [62]. Nevertheless, the hybrid method still focuses on structural vulnerability of power grids rather than analyzing vulnerability of power systems in light of understanding dynamics of its blackouts. In next section, we will review the research on mechanism and models of blackout dynamics in power systems from complex system angle.

4 Blackout dynamics

Blackouts in power grids were traditionally considered to be a consequence of accidental faults. But, recently, power systems and other critical infrastructures seem to fail more frequently than desired. Besides random failures, the threat of malicious attacks has increased, which transforms infrastructural vulnerability into a hot economical, social and political issue [63]. Analyzing time series of blackout data can understand the origin and distribution of power system blackouts. At the beginning, there are two different models to statistically analyze major blackouts in power systems from a complex system perspective [64]. One is an optimization model based on highly optimized tolerance (HOT) theory [65-66] that presumes that power engineers make conscious and rational choices to focus resources on preventing smaller and more common disturbances on the lines while large blackouts occur because the grid is not forcefully engineered to prevent them. Another model in basis of self-organized criticality (SOC) [67-69] views disturbances as a result of constructive force resulting from attraction to critical point in an unconscious feedback loop that operates over years or decades. Macroscopic behavior of complex systems with the SOC property displays the power law distribution [16] which implies the spatial and/or temporal scale-invariance characteristics of critical point of a phase transition [70] without the need of precisely adjusting parameter values.

The model based on SOC theory, rather than HOT theory, has been much more widely accepted in the power systems community to explain the laws of blackouts in power systems, after power law distributions have seemly been found in time series of blackout size data in North America [71-73], Sweden [74], Norway [56], New Zealand [75-76] and China [77]. This distribution implies that large blackouts are much more likely than expected, and when costs are considered, the risk of large blackouts in the tail of the power law is comparable to or even exceeding the cumulate risk of small blackouts. Moreover, there is dependency in large blackout events of the heavy tail [72]. As small blackouts occur, the power system become more stressful and vulnerable and so larger blackouts are more likely to happen in the brittle power system. Eventually, a small disturbance could trigger a large-scale blackout in the more and more vulnerable power system.

Instead of analyzing the details of particular blackouts, most of research studying
statistics, dynamics and risk of series of blackouts found that the increase of load and economic operation could lead to stressful power systems which are more likely to have a large-scale blackout. As the load increases, average blackout size will increase much more sharply and quickly after the load exceeds a threshold value called as critical load. The critical load defines a reference point for increasing risk of cascading failure in power systems. The critical load emerges in abstracted model of cascading failure [78] and power systems model reflecting the cascading failure mechanism [79-81]. Besides, the probability of cascading failure can be assessed when the load increases in power systems [82].

From the self-organized point of view, there are two opposing forces driving a power system towards critical load. The load growth and economical operation increase the stress of power systems while, in contrast, the stress decreases owing to upgrades and improvement of power systems in engineering response to blackouts. The dynamics of blackouts can be understood as a result of power systems slowly evolving towards criticality under the interaction between the two forces [83-85]. When we understand mitigation of blackout risk from self-organized critical system perspective, the mitigation seems to have an counter-intuitive effects on the system evolution. The explanation for this is that the occurrence of small blackouts is not independent of large blackouts. Suppressing small blackouts could lead the system to be operated closer to the criticality and ultimately increase the risk of large blackouts [83, 86].

5 Conclusions

Power systems are a complex system due to its complexity resulting from non-analytic interaction among its huge number of components in different layers. Understanding and analyzing power systems from complex system standpoint is a promising approach to address technological challenges in power practices to guarantee security and reliability of power systems. The methodology studies the structure and dynamics of power systems as a whole instead of analyzing details. Although the structure of networked complex systems can be effectively studied by complex network method, electrical engineering specificity should be considered in complex network methodology when it is used to analyze real topological features of power systems and to identify critical components in power grids.

On the other hand, dynamical robustness model in complex network method cannot reflect dynamics of cascading failures in power systems. But another complex system theory (i.e., self-organized criticality) could to some degree explain the mechanism of blackouts in power systems. Some blackout models based on the insights of self-organized criticality are proposed to study the impact of interactions among control strategy, overloaded components and network evolution. But the introduction of dynamic stability and interaction of complex systems still remain challenge in existing models. In addition, lack of real blackout data hampers to understand blackouts and then develop and test high-level statistic model to reduce the risk of large-scale blackouts in power systems.
6 Reference


[42] L. Xu and X. Wang, "Topologic analysis on effect of UHV long connections on energy..."


