ANALYSIS OF CASCADING FAILURE IN POWER SYSTEMS FROM A COMPLEX NETWORK PERSPECTIVE

XI ZHANG

Ph.D

The Hong Kong Polytechnic University

2017

The Hong Kong Polytechnic University

Department of Electronic and Information Engineering

Analysis of Cascading Failure in Power Systems from a Complex Network Perspective

Xi ZHANG

A thesis submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

July 2017

Certificate of Originality

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgment has been made in the text.

_____(Signed)

Xi Zhang (Name of student)

Abstract

In this thesis, a complex network perspective is taken to study the robustness of power systems against cascading failure. By abstracting generators, loads, and substations as nodes, and transmission lines as edges, a power system can be described by a network representation, through which the topological characteristics can be examined. The robustness of a power system is interpreted as its ability to resist cascading failure. In order to investigate the relationship between the network topology and the robustness performance, the key factor is to model the cascading failure processes appropriately. This thesis aims to study the cascading failure mechanism in power systems and to identify ways to enhance their robustness from a complex network perspective.

First, we propose a circuit-based power flow model for the simulation of cascading failures and the robustness assessment of power systems. Based on Kirchhoff's laws and the properties of network elements, and combined with a complex network structure, this model is able to assess the severity of a blackout. The blackout size is measured by the percentage of unserved nodes (PUN) caused by a failed component. For each component chosen as an initially failed component, a value of PUN can be found. Based on the PUN of each node, the percentage of non-critical links (PNL) is used to measure a power system's robustness quantitatively. Simulation results on several real and synthesized networks show that connection having a short average shortest path length can jeopardize a power system's robustness.

Then, we model the dynamic propagation processes of cascading failures in power systems beginning from a dysfunctioned component and developing eventually to a

large-scale blackout. Observing that in several historical power blackout events, the failure propagation profiles share a common pattern characterized by a relatively slow initial phase followed by a sharp escalation of failure events, we further develop a method for finding the time instants of failure events to complete the cascading failure modeling. The proposed circuit-based power flow model is adopted to derive the overloading conditions, which determine the failure rates of the elements. A stochastic method is then used to generate the uncertain failure time instants. The use of stochastic method addresses the uncertainties in individual components' physical failure mechanisms. Simulation results for the UIUC 150 Bus system show that the dynamic cascading failure profiles generated by this model contain the typical features displayed in historical blackout data.

Finally, we present a study of cascading failure in power systems that are coupled with cyber networks. In reality, the power network is linked to the cyber network for control purposes, and the cyber network is powered by the power network. The failure in one network can propagate to the other, and vice versa. Thus, we consider the failure cascade in a coupled system (smart grid) comprising a power grid and a cyber network caused by the attack of a cyber malware. The effects of power overloading, contagion, and interdependence between a power grid and a cyber network are taken into consideration in the model. Different coupling patterns and different cyber network structures are compared to study their effects on the robustness of the coupled system. Simulation results show that cyber coupling can intensify both the extent and rapidity of power blackouts, and that the cyber network structure and the coupling patterns affect the propagation of cascading failures in cyber-coupled power networks.

Publications

Journal papers

- **X. Zhang**, D. Liu, C. Zhan, and C. K. Tse, "Effects of cyber coupling on cascading failures in power systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 2, pp. 228–238, Jun. 2017.

- **X. Zhang**, C. Zhan, and C. K. Tse, "Modeling the dynamics of cascading failures in power systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 2, pp. 192–204, Jun. 2017.

- Z. Chen, J. Wu, Y. Xia, and **X. Zhang**, "Robustness of interdependent power grids and communication networks: A complex network perspective," *IEEE Transactions on Circuits and Systems II: Express Briefs*, to appear.

- **X. Zhang** and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 456–464, Sept. 2015.

Conference papers

- D. Liu, **X. Zhang** and C. K. Tse, "A stochastic model for cascading failures in smart grid under cyber attack," in *Proc. International Future Energy Electronics Conference*, Kaohsiung, Taiwan, 2017.

- D. Liu, **X. Zhang**, C. Zhan and C. K. Tse, "Modeling of cascading failures in cyber-coupled power systems," in *Proc. IEEE International Symposium on Circuits and Systems*, Baltimore, USA, 2017.

- **X. Zhang**, C. Zhan and C. K. Tse, "Modeling cascading failure propagation in power systems," in *Proc. IEEE International Symposium on Circuits and Systems*, Baltimore, USA, 2017.

- **X. Zhang** and C. K. Tse, "An effective generator-allocating method to enhance the robustness of power grid," in *Proc. IEEE International Symposium on Circuits and Systems*, Montreal, Canada, 2016, pp. 674–677.

- **X. Zhang** and C. K. Tse, "Assessment of robustness of power systems from the perspective of complex networks," in *Proc. IEEE International Symposium on Circuits and Systems*, Lisbon, Portugal, 2015, pp. 2684–2687.

Acknowledgments

I would like to express my eternal gratefulness to my supervisor Prof. Michael Tse for his continuous support, patient guidance and valuable advice. Prof. Michael Tse is very active and open-minded, and always encourages me to think deeply and freely during the course of this project. His enthusiasm in research and insights into the area of network science have inspired me a lot. Without his help, I could not have accomplished this Ph.D. study.

I would also like to thank Dr. Choujun Zhan and Dr. Jiajing Wu for many inspiring discussions on the topic of complex network applications. The numerous discussions with them have benefited me immensely. At the same time, I am grateful to the students and staff in our Nonlinear Circuits and Systems Group. Their company makes the 4-year study more enjoyable, and I will remember the pleasant experiences shared with them forever.

I acknowledge the Research Committee of the Hong Kong Polytechnic University for the financial sponsorship during the entire period of the project.

Finally, I would like to thank my parents. Their love, care, and support make me stronger.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

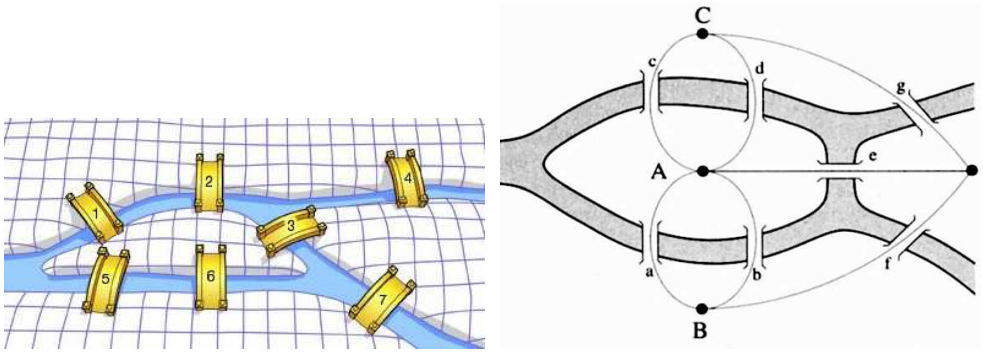
1.1 Background

A complex system consisting of a large number of interacting elements can be represented and analyzed with a "graph" (network), whose entities are a set of "nodes" and "edges". In the graph representation, the elements are abstracted as nodes and the interactions among the elements are abstracted as edges. Analyzed from a network perspective, it is found that many real-world systems share some unified structural characteristics.

The use of graph representation to solve real-world problems dates back to the 18th Century. Königsberg was a town of former Prussia, whose land was divided into four isolated parts by a river named Pregel. Seven bridges were constructed over the river to connect the four lands, as shown in Fig. 1.1 (a). There was a debate among the citizens of Königsberg: "if someone could walk through all the seven bridges and then return to the starting point without going over any bridge for more than once". This debate had lasted for a long time, until mathematician Euler gave an answer to it in 1736. By abstracting each part of land as a node and each bridge as an edge, Euler converted the routing problem to a network description, as shown in Fig. 1.1 (b), and pointed out that to realize the task in the debate, each node in the graph must have an even number

of edges connected to it.

Euler started the era of using graphs to analyze real-world systems, and since then, graph theory continued to develop with a series of new findings and achievements, and became an important discipline.



(a) (b)

Figure 1.1: The Königsberg seven-bridge problem. (a) Geographical representation of the seven bridges and the isolated lands. (b) Corresponding network representation. Picture (a) is obtained from https://www.britannica.com/topic/Konigsberg-bridge-problem. Picture (b) is obtained from https://physics.weber.edu/carroll/honors/konigsberg.htm.

In the late 1950s, two Hungarian mathematicians, Paul Erdös and Alfréd Rényi introduced an algorithm for generating random networks, which is regarded as a notable milestone in the history of graph theory history. An Erdös and Rényi (ER) random network is constructed by adding a specific number of links to a set of nodes randomly. A Poisson node degree distribution is observed in ER random networks. For the following more than forty years, ER random networks were the dominant networks on which the majority of network dynamical studies were performed.

Although the ER random network is a popular model of connectivity, many later empirical studies showed that most of the real-world networks are not completely random. In 1969, Stanley Milgram conducted an experiment to test the average intermediate friends that connect two randomly selected persons in the United States, i.e., the average shortest path length of the American social network. In this experiment, Milgram randomly chose two persons from a town named Sharon and the city Boston

as two targets. Further, he selected two groups of volunteers in Kansas and Nebraska as start points. Milgram asked each volunteer to compose a letter to the two targeted people and then send the letter to a friend. If the receiver was not either one of the two targets, he would be asked to forward the letter to another friend of his. This forwarding process continued until the letter reached one of the two destinations. Milgram reported the results in ref. [1] that although many folders were lost, for the successfully delivered letters, the average path length was only 5.2 hops. Such a phenomenon where the average distance between two randomly selected people in the American social network was so short was interpreted as "small-world" phenomenon.

With the emergence of computers, the World Wide Web (WWW) has become an important information space, in which the documents are identified with URLs and interconnected by hypertext links. By considering the URLs as nodes and the hyperlinks as edges, the network can characterize the information connection relationship on the WWW. In 1999, Réka Albert *et al.* [2] reported that the distribution of the number of incoming hyperlinks and the distribution of the number of outgoing hyperlinks of the URLs both follow a power law. The power-law distribution of the WWW network connectivity was also validated by Huberman and Adamic [3]. As the power-law distribution property is independent of the network size [4], the network with power-law node degree distribution is also termed as a scale-free network.

Empirical observations, which are noted first by people, usually lead to impactful theoretical models for reproducing the features observed and explaining the formation mechanism of real systems. The small-world network model and the scale-free network work model are two most popular examples. In 1998, Watts and Strogatz introduced a model that can display small-world characteristic [5]. In Watts and Strogatz's work, they rewired the links in a regular ring network with probability p, and found that the average shortest path length of the rewired network decreases drastically even when p is very small. The resulting network having relatively short average path length is now recognized as a small-world network.

Although the small-world phenomenon is observed in this model, the power-law distribution cannot be reproduced. Albert and Barabási introduced a growth network model in 1999 [6], with new nodes being added in a preferential attachment manner. Through mathematical derivation as well as computer simulation, they showed that scaling emerges in their growing network whose node degree distribution follows a power law.

The small-world and the scale-free network models invoked intense research in the field of network science in the past two decades. New structural parameters that can characterize the network features have been proposed [7]. Various dynamical processes have also been simulated and investigated in some synthesized networks [8, 9]. It should also be noted that real-world systems are characterized by their own operating properties and physical laws in addition to the basic structural properties. To maximize the benefits of this new promising discipline, the next step is to apply the complex network methodologies to real-world problems appropriately, with the due consideration of the physical properties of the practical systems under study.

Many practical systems have been viewed and analyzed from a network science perspective, such as the protein-protein network [10], the world stock market network [11], the music network [12], and so on. Specifically, the power system is one of today's most important man-made infrastructures, whose safety and robustness are of great significance to almost all human activities. A power system delivers electricity from the generating units to the consumers through a network of substations and transmission lines. By representing the generators, consumers, transformers and distribution stations as nodes and the transmission lines as edges, the power grid is amenable to complex network analysis. Empirical studies on the topology of power systems [13–19] are still in the initial stage, and detailed modeling considering the electrical properties are necessary in order to find the intrinsic relationship between the functionality and the structure.

1.2 Motivation

It is widely known that the structure of a network influences its functional performances. For example, the study in ref. [20] showed that the scale-free network is more vulnerable to intentional attack while more resilient to random attack, compared with a random network. In this thesis, cascading failure in a power system and the robustness against repeated component failures are the key concerns related to functional performance. The objective is to apply complex network theory to the analysis of power systems, establishing a clear link between the specific aspects of operational performance of the power grid and the network structure. As the power system is a huge complex system, the relationship between the functionality and the structure is not as simple as that between the "debate" and the "solution" in the Königsberg problem. To achieve the objective, appropriate modeling is a crucial step. The choice of modeling approach and the level of complexity to be incorporated in the model should be carefully considered. Oversimplified models may fail to describe the essential properties while overly complicated models would incur high analytical and computational costs. Based on this cognition, three models with the following practical emphases are proposed.

First, considering the objective electrical features of a power system, power flow information is incorporated in the cascading failure simulation model. In this model, the element failure is due to power flow overloading, and the power flow is governed by Kirchhoff's laws and the electrical properties of the network elements. This part of the model is based on deterministic processes.

Second, considering the complexities and uncertainties, apart from power overloading, the failure of a component may also have multiple complex causes, including production quality, temperature, and other environmental factors, which are not always precisely deterministic. A model that combines power flow analysis and a stochastic method to determine the time to the next failure is proposed to produce the time profiles

of cascading failure propagation.

Third, the smart grid that takes advantage of information technologies is an interdependent system, where the physical power network depends on a cyber network for control while the cyber network is powered by the power network. Witnessing the blackout in the Ukrainian power grid in 2015 that was caused by a cyber malware attack [21], a model that can simulate the cascading failures in the interdependent networks is proposed to study the effects of cyber coupling.

Several metrics for indicating the robustness of a power system based on the simulated cascading failure results with the above models are used to investigate the influences of network structure on its robustness.

1.3 Thesis Organization

This thesis is organized as follows.

Chapter 2 provides a literature review. Key results from complex network research, the new requirements and challenges for power grids, and some recent works of applying complex network theories to power systems are reviewed.

Chapter 3 discusses the robustness assessment of power systems from a network perspective. Based on Kirchhoff's laws and the properties of network elements, and combined with a complex network structure, a deterministic model is introduced to analyze the severity of a blackout, measured by the percentage of unserved nodes (PUN) caused by a failed component. To quantitatively measure a power system's robustness, the percentage of non-critical links (PNL) is used. Different network structures that influence a power grid's robustness are discussed.

Chapter 4 studies the dynamic processes of cascading failures. We propose a model that gives a complete dynamic profile of the cascading failure propagation beginning from a dysfunctioned component and developing eventually to a large-scale blackout. In the model, we use the circuit-based power flow model introduced in Chapter 3 to

derive the overloading conditions, and combine it with a stochastic model to describe the uncertain failure time instants. The simulation results based on the model are compared with the recorded data of historical blackouts.

Chapter 5 presents a preliminary study of the cascading failures in power systems considering the cyber-coupling effects. In this chapter, a coupled system (smart grid) comprising a power grid and a cyber network is considered. In the model, we take into consideration the effects of power overloading, contagion, and interdependence between a power grid and a cyber network on failure propagation in the coupled system to investigate the cascading failures caused by the attack of cyber malwares. Different coupling patterns and different cyber network structures are compared to study their effects on the robustness of a smart grid.

The thesis concludes in Chapter 6, where major findings of the project are summarized and some thoughts on the future works are presented.

Chapter 2

Literature Review

In this chapter, some fundamental concepts of complex network theory and their applications to power systems are reviewed. A set of basic measures of network topology, three classical network models, empirical studies of power networks, and several power system models are discussed.

2.1 Measures of Network Topology

As artificial or natural networks are usually of large scale and with high complexity, their characteristics need to be abstracted and quantified by computable measures. In this section, several important measures that are most widely used in the field of complex networks are reviewed, such as node degree, degree distribution, average path length, and so on.

2.1.1 Node Degree

The *degree* of a node is a simple and basic measure for indicating the structural importance of the node in a network. In an undirected network, the degree k_i of node i is defined as the total number of edges connecting to the node. In a directed network where an edge can have two directions, the *out-degree* of a node is the number

of its outward-directed edges, and the *in-degree* is defined as the number of its inward-directed edges.

Usually, in a real-world complex network that contains a large number of nodes, the degrees of different nodes vary over a wide range. In terms of the network topology, the nodes with higher degrees usually have stronger impacts on the whole system and are called the *hubs* of the network. Albert *et al.* [20] demonstrated that removing the high-degree nodes destructs the network connectivity much more severely than removing the same fraction of low-degree nodes from the network.

To show the overall properties of a network, several metrics have been proposed by processing the degrees of all the nodes with statistical methods, such as the average node degree, the node degree distribution and the node assortativity coefficient.

Average Node Degree

The *average node degree* $\langle k \rangle$ of a network is the average value of the degrees of all the nodes of the network. Thus, $\langle k \rangle$ can be written as

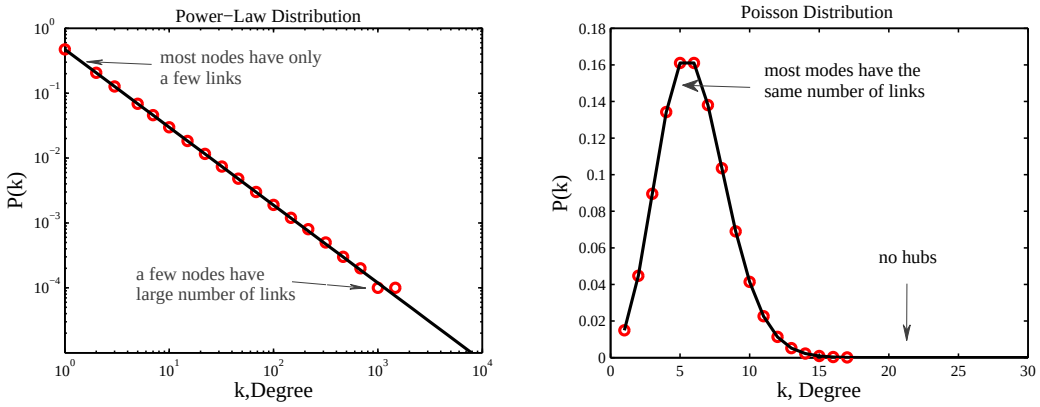
$$\langle k \rangle = \frac{1}{N} \sum_{i=1}^{N} k_i, \tag{2.1}$$

where N is the total number of nodes in the network. The value of $\langle k \rangle$ characterizes the network's connection density, and a higher $\langle k \rangle$ means that the nodes are more densely connected with each other.

Node Degree Distribution

The average node degree captures a specific topological property of a network, and different networks with the same average node degree can have quite different topologies. The *node degree distribution* is used to capture another aspect of information of the network topology. A network's node degree distribution, denoted by $P(k)$, is defined as the probability that a randomly picked node has degree k. And $P(k)$ can be represented as follows:

$$P(k) = N(k)/N \tag{2.2}$$



(a) (b)

Figure 2.1: Node degree distributions: (a) Power-law distribution; (b) Poisson distribution.

where $N(k)$ is the number of nodes having degree k.

The Poisson distribution and the power-law distribution are two most frequently observed node degree distribution forms in real-world networks as well as in mathematical network models. For a power-law distribution, the probability $P(k)$ varies as a negative power of k, i.e., $P(k) \sim k^{-\gamma}$, where γ is the power-law exponent. As shown in Fig. 2.1(a), a network with a power-law degree distribution is heterogeneous, where most nodes have a few edges while only a small portion of nodes occupy a large number of connections. For the Poisson distribution, the relation between $P(k)$ and k can be represented as $P(k) \sim e^{-\lambda}\lambda^{-k}/k!$, where λ is the average node degree of the network. Figure 2.1(b) plots a Poisson distribution, where the peak of the curve appears when k is around the average node degree. From Fig. 2.1(b), in a network with a Poisson distribution, most of the nodes have the same degree, and there exists no network hub. Such a network is homogeneous. In addition to the above two distributions, the exponential distribution in the form of $P(k) \sim e^{-\lambda k}$ has also been observed in some real networks, for example, the power grid in North America [13].

Degree Assortativity Coefficient

In order to characterize the correlations between nodes with similar degree in the

network, the *assortativity coefficient* r has been proposed [22]. The definition of r is

$$r = \frac{m^{-1}\sum_{(i,j)\in M} k_i k_j - [m^{-1}\sum_{(i,j)\in M}\frac{1}{2}[k_i + k_j]]^2}{m^{-1}\sum_{(i,j)\in M}\frac{1}{2}[k_i^2 + k_j^2] - [m^{-1}\sum_{(i,j)\in M}\frac{1}{2}[k_i + k_j]]^2}, \tag{2.3}$$

where k_i and k_j are the degrees of the two nodes of edge (i, j), M is the set of edges in the network, and m is the number of edges in M. Here, r characterizes the likely extent to which the nodes with similar degree are connected by a link.

Also, $r > 0$ indicates that the network is assortative where high-degree nodes are more likely to connect to high-degree nodes. On the other hand, $r < 0$ indicates that the network is disassortative where low-degree nodes tend to connect to high-degree nodes.

2.1.2 Shortest Path Length

The *distance* d_{ij} between node i and node j in an undirected and unweighted network is defined as the number of edges along the shortest path connecting the two nodes. In a network, there usually exist many paths that connect two nodes, among which the shortest one is usually considered as the most dominant connection. For example, the shortest path is often chosen for data transmission between two data centers in a communication network, which is also identified as the min-delay path problem [23]. The shortest path concept can also be applied in transportation, robotics, and VLSI design [24]. Several algorithms have been proposed to efficiently find the shortest path between node pairs in a network, such as the Floyd-Warshall algorithm, the Johnson's algorithm, and so on [25].

In a network with N nodes, there exist $2N(N-1)$ pairs of nodes in total, with each node pair having a corresponding distance. The longest distance in the network is termed the *diameter*. The *average path length* (or average shortest path length) of

a network denoted by L is the average value of all the node pairs' distances in the network, i.e.,

$$L = \frac{1}{2N(N-1)} \sum_{i \neq j} d_{ij}. \tag{2.4}$$

Here, L measures how close the nodes are interconnected with each other in a network. For example, in a social network of relatively large scale, the value of L is very small. The experiment conducted by Milgram in 1969 showed that the average distance of two randomly chosen persons in the American social network was less than 6. Later studies showed a 4 degree separation in 2012 [26] and a 3.5 degree separation in 2016 [27] based on the online social network Facebook.

2.1.3 Betweenness Centrality

As the shortest path is often chosen as the preferred transportation route in delivery networks, the nodes and edges that lie on the shortest path are more critical. Based on the concept of shortest path, the *node betweenness centrality* (*edge betweenness centrality*) has been proposed to characterize the centrality of a node (edge) in a network [28]. Node i's betweenness centrality is defined as the number of shortest paths that pass through it, i.e.,

$$B_i = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}}, \tag{2.5}$$

where σ_{st} is the total number of shortest paths between nodes s and t, and $\sigma_{st}(i)$ is the number of those paths that pass through node i.

Similarly, the betweenness of edge (i, j) is defined as

$$B_{ij} = \sum_{(s,t) \neq (i,j)} \frac{\sigma_{st}(ij)}{\sigma_{st}}, \tag{2.6}$$

where $\sigma_{st}(v)$ is the number of shortest paths traversing edge (i, j).

The betweenness of a node (edge) measures how frequently a node (edge) stands on the connection between other elements and can be applied to many practical prob-

lems. For example, Newman and Girvan [29] made use of edge betweenness to detect the underlying communities in a network. The nodes within the same community are more closely interconnected compared with the nodes in different communities, and the edges that connect different communities are usually with high values of betweenness centrality. Based on this cognition, Newman and Girvan proposed a method to remove a set of edges iteratively to split the network into different communities. For each step, the edge to be removed is with the highest value of edge betweenness. The authors then demonstrated the efficacy of this method in a variety of real networks with known community structure.

2.1.4 Clustering Coefficient

The *clustering coefficient* of a node measures the connectivity among its neighbors. For node i with degree k_i, there exist at most $k_i(k_i - 2)/2$ possible connections among its k_i neighbors. Among these $k_i(k_i - 2)/2$ possible connections, E_i is the number of links that actually exist. The clustering coefficient C_i of node i is defined as the ratio between E_i and $k_i(k_i - 2)/2$, i.e.,

$$C_i = \frac{2E_i}{k_i(k_i - 1)}. \tag{2.7}$$

To characterize the overall clustering level of a network, the *average clustering coefficient* C of a network is used. Here, C is defined as the average value of the clustering coefficient of all nodes, which can be written as

$$C = \frac{1}{N}\sum_{i=1}^{N} C_i. \tag{2.8}$$

A network's clustering coefficient ranges from 0 to 1. Clustering coefficients can vary distinctly for different networks. A star network has a zero clustering coefficient, and a fully connected network has a unity clustering coefficient. The clustering co-

efficient of real-world social networks is relatively high. Thus, for a social network, it is common that two friends of an individual are more likely to know each other as well, and this feature is used for recommending new friends in online social platforms. Moreover, the clustering coefficient of hierarchical networks can be quite low, such as the power grid and the Internet [30].

2.2 Theoretical Topology Models

From some previous empirical studies, certain distinct features of real-world networks were identified, for example, the small-world property of social networks and the power-law degree distribution of the World Wide Web (WWW) network. These observations motivated the development of mathematical network models that can reproduce the observed statistical features. The models offer plausible explanations for the formation mechanisms of real networks and provide a platform for studying the dynamic processes [31]. In this section, we review three most widely known network models: the Erdös-Rényi (ER) random network, the Watts-Strogatz (WS) small-world network, and the Barabási-Albert (BA) scale-free network.

2.2.1 ER Random Network

The ER random network, proposed by Erdös and Rényi in 1959 [32], is the first model for generating an autonomously formed network. An ER random network can be generated as follows:

(1) First, take N isolated nodes.

(2) Then, for each pair of nodes, add an edge with probability p.

For an ER random network, when N is large enough, there are about $pN(N-1)/2$ edges in total, and the average node degree is $\langle k \rangle = (N-1)p \approx Np$. The node degree

distribution of the ER random network can be expressed as follows:

$$P(k) = (\langle k \rangle)^k \frac{e^{-\langle k \rangle}}{k!}. \tag{2.9}$$

From equation (2.9), we can see that the node degrees of the generated ER random network follow a Poisson distribution, indicating that the ER random network is a homogeneous network.

Assuming that $N \gg \langle k \rangle \gg \ln(N) \gg 1$, the ER random network's average path length L_{random} and clustering coefficient C_{random} can be written as $L_{\text{random}} \sim \ln(N)/\ln(\langle k \rangle)$ and $C_{\text{random}} \sim \langle k \rangle / N$, respectively [33]. We can see that L_{random} and C_{random} are both very small and that increasing p lowers L_{random} and C_{random} at different rates.

2.2.2 WS Small-world Network

Empirical studies showed that many large-scale real networks have short average path length and maintain relatively large clustering coefficient. In 1998, Watts and Strogatz [5] introduced a rewiring model to mimic the two features observed in many real networks. Noticing that the ER random network exhibits a short average path length and a low value of clustering coefficient and that the regular network has a high clustering coefficient and a long average path length, they built interim networks between the two kinds of networks.

In this model, the construction process begins with a regular ring network that has N nodes, each node's degree being a constant number k. Then, for each link in the network, with probability p, one of its terminal nodes is reconnected to another randomly selected node in the ring. The average path length $L(p)$ and the clustering coefficient $C(p)$ are used to indicate the topological characteristics of the resulting networks under different rewiring probabilities. When $p = 0$, the resulting network is the regular ring network, and $C(0) \approx 3/4$, $L(0) \approx N/2\langle k \rangle$. When $p = 1$, the resulting network is the ER random network, and $C(0) \approx \langle k \rangle / N$, $L(0) \approx \ln(N)/\ln(\langle k \rangle)$. Figure

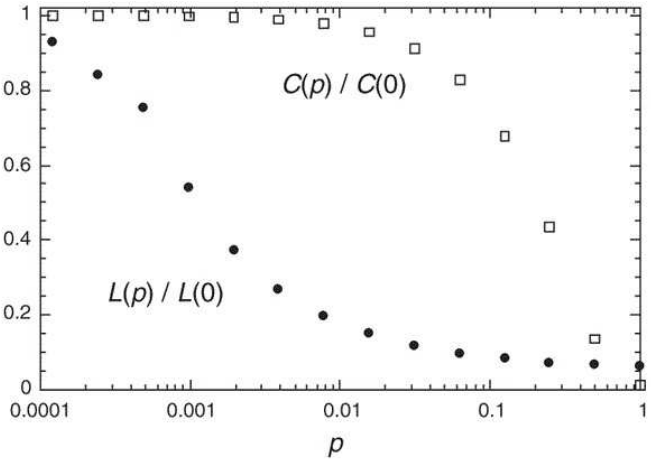


Figure 2.2: $C(p)/C(0)$ and $L(p)/L(0)$ decrease at different rates as p increases. Small-world properties are shown in the interim networks. This figure is extracted from *Nature* [5].

2.2 shows the values of $C(p)/C(0)$ and $L(p)/L(0)$ as p increases from 0 to 1. We can see that when p is small, an interim network appears with the characteristics that the clustering coefficient is almost as high as regular networks and that the average path length decreases to a very low value. Such interim networks are called SW small-world networks. Table 2.1 summarizes the average path length and clustering coefficient of different network models when $N \gg \langle k \rangle \gg \ln(N) \gg 1$.

Table 2.1: Average path length and clustering coefficient of different network models

	Average Path Length	Clustering Coefficient
Regular ring network	$N/2\langle k \rangle$	3/4
WS small-world network	close to $\ln(N)/\ln(\langle k \rangle)$	close to 3/4
ER random network	$\ln(N)/\ln(\langle k \rangle)$	$\langle k \rangle / N$

2.2.3 BA Scale-free Network

As mentioned in Section 2.1.1, the degree distribution gives important clues about the structure of a network. Both the ER random and WS small-world networks do not display a power-law degree distribution which is widely observed in many real-

world networks. To mimic the power-law degree distribution, Barabási and Albert [6] proposed another network model, in which growth and preferential attachment are two important rules in the formation of the network. The procedures for generating the network are as follows:

(1) Start with m_0 nodes, and at each step, a new node is added and connected to $m \leqslant m_0$ existing nodes.

(2) The probability Π_i that the newly added node is connected to node i is proportional to the degree of node i, denoted as k_i, i.e., $\Pi_i = k_i / \sum_j k_j$.

After t time steps, the above algorithm generates a network with $m_0 + t$ nodes and mt edges. When t is large enough, the network's node degree distribution follows a power law with exponent -3. When t continues to increase, this degree distribution remains unchanged, and the scale-free property emerges. Thus, this network model is called the BA scale-free network. The scale-free network is highly heterogeneous, where a small fraction of nodes have a large number of connections while the majority of nodes have only a few edges. The BA scale-free network model is a remarkable milestone in the history of graph theory which aroused the interest of many researchers in the field of applied mathematics and physics.

2.3 Empirical Study of Power Networks

The power grid is one of the most critical man-made infrastructures, whose operational performances influence almost all human activities today. In a power grid, the generators, loads, and substations are interconnected by transmission lines, aiming at transmitting electricity safely and efficiently among. Evolving with the development of human society, the topology of power grids has become quite large and complex. The topological characteristics of this huge and complex system have drawn much attention. By abstracting the generators, transformers, and substations as nodes and the transmission lines as edges, much research has been devoted to the study of the

topologies of different regions' power grids from a complex network perspective with the aforementioned measures and models [15, 34]. This section reviews the results of some empirical studies on the topological features of real power grids.

To measure how densely the substations are interconnected by the transmission lines in a real power grid, the average node degree was used in much of the previous study. Table 2.2 summarizes the results obtained from refs. [13,16,35–37]. From Table 2.2, we can see that all the average node degrees of networks fall in the range [2, 3], indicating that the stations in real grids are not very densely connected. One possible reason for the sparse connection is that the power grid is designed economically to lower the cost of transmission lines. Another reason is related to the spatial constraint, and the transmission lines could not be established arbitrarily to connect the elements in the grid.

Table 2.2: Average node degree of different real power grids

Region	Number of Nodes	$\langle k \rangle$	Region	Number of Nodes	$\langle k \rangle$
North America	19.600	2.08	Belgium	53	2.18
West America	4941	2.67	Holland	36	2.11
North China	8092	2.23	Germany	445	2.51
Central China	2379	2.32	Italy	272	2.70
Spain	474	2.82	Romania	166	2.49
France	667	2.69	Greece	27	2.44

As the small-world property is one prominent feature observed in many kinds of real networks, several studies have attempted to investigate whether the power grids fall into the small-world network category. The average path length and the clustering coefficient are two important parameters used to examine the small-world property of a power grid. Compared with a random network of the same scale, the small-world network has a similar average path length but a much larger clustering coefficient. Let C_{random} and L_{random} be the clustering coefficient and the average path length of an ER

random network having the same number of nodes with the power grid. If a power network satisfies $C/C_{\text{random}} \gg 1$ and $L/L_{\text{random}} \approx 1$, we can say that the grid exhibits the small-world property. Table 2.3 lists the values of L and C for different real grids, and the corresponding values for the random network. From Table 2.3, we can see that the Western American and French power grids exhibit the small-world property, with $C \gg C_{\text{random}}$ and $L \approx L_{\text{random}}$. However, the other power networks in Table 2.3 cannot be classified as small-world networks as they have a relatively low clustering coefficient.

Table 2.3: Clustering coefficient (C) and average shortest path length (L) of different power networks

Region	C	C/C_{random}	L	L/L_{random}
West America [37]	0.0800	148.045	18.7	2.159
North China [36]	0.0017	6.169	32	2.852
Center China [36]	0.0044	4.512	21.08	2.282
Italy [16]	0.1560	7.365	8.47	1.730
France [16]	0.2790	13.355	6.61	1.479
Spain [16]	0.3160	8.675	4.92	1.366

In terms of the node degree distribution, Albert *et al.* [13] reported that the Northern American power grid follows an exponential distribution. The exponential node degree distribution was also reported to be observed in the power networks in Italy [18], Europe [14, 35, 38] and Southern California [43]. However, not all power grids show the exponential distribution. Pagani and Aiello [40] showed that the medium- and low-voltage power network in Northern Netherlands follows a power-law distribution. And even there exist disagreements for the same regions' networks. For the Northern American network, Chassin and Posse [39] claimed that the topology could be scale-free. Contributing to this controversy, Cotilla-Sanchez *et al.* [42] fitted the data from the Northern American grid and the IEEE 300 Bus system and concluded that the

Table 2.4: Fitted node degree distributions of different real power networks

Power grid region	Cumulative degree distribution	Fitted representation
North America [13]	exponential	$P(k) = e^{-0.5k}$
Italy [18]	exponential	$P(k) = 2.5e^{-0.55k}$
Europe [35]	exponential	$P(k) = 2.5e^{-0.81k}$
Europe [14]	exponential	$P_1(k) = e^{-0.56k}$ $P_2(k) = e^{-0.54k}$
Europe [38]	exponential	$P_1(k) = e^{-0.60k}$
North America [39]	power-law	$P_1(k) = 0.84k^{-3.04}$ $P_2(k) = 0.85k^{-3.09}$
Northern Netherlands [40]	power-law	$P(k) = k^{-1.49}$
Italy, France and Spain [16]	other form	–
New York [41]	other form	–
North America [42]	other form	–

two cases are neither scale-free nor small-world. Table 2.4 summarizes the best fitted representations of the node degree distributions of different real power grids.

Up to now, no consensus has been reached on whether the real power grids share uniform topological characteristics in terms of small-world and scale-free properties [44]. We can thus conclude that there exist distinct differences between different real power networks.

It has been demonstrated that there exists a strong correlation between the structure and the function of a network [45–48]. For example, in a social network, the small-world connection enhances the contagion spreading process among people compared with the regular connection. Such structure-function correlation can also exist in power systems. In this thesis, the functional performance under study is related to the robustness of the system, as the safe operation of a power system is of great importance today. Power blackouts indeed happened, each causing enormous economical

loss as well as undue inconvenience. The 2003 blackout in North America and Canada left about 50 million people in the dark and caused a loss of estimated 10 billion dollars. The 2015 blackout in the Ukrainian power grid affected 80,000 customers for six hours. One can see a summary of historical power blackouts in ref. [49]. Thus, preventing disturbances in power systems has always been a prime goal of electrical engineers and power companies.

It should be noted that the power grid is not constrained to adopt any typical network topology. In other words, a power grid can be designed to optimize performance by choosing appropriate structure. It is therefore very meaningful to explore the relationship between the functional performance of a power grid and its structure, thus providing useful hints to improve the functional performance via optimizing the structure [50, 51]. Having studied the empirical properties of the power grids' topologies, the next step is to carefully model the dynamics of power systems.

2.4 Models for Power System Analysis

An appropriate model is the key tool for exploring the relationship between the function and structure of a power network. This thesis focuses on the robustness property and modeling of cascading failures in power systems. In this section, we review the important models used in the field of complex networks and electrical engineering.

2.4.1 Static Model

One area of research falls in the category of static analysis of the structural vulnerability of power networks to attacks. In this kind of study, attacks refer to jointly removing a fraction of elements (nodes or edges) from a power network, which can destruct the connection of the network. Then, a comparison will be made between the remaining network and the original network to indicate the severity of the damages

caused by the attacks. Several metrics have been proposed as the measures of the damages, for example, the global network connection efficiency [52] and the relative size of the largest cluster of the network [13, 38]. In ref. [52], the global efficiency $E(G)$ was used to indicate the connection efficiency of network G. And $E(G)$ is defined as $E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}$, where d_{ij} is the shortest path length between nodes i and j. If $E(G)$ becomes much lower after the attacks, the network is very vulnerable to these attacks. The simulation results reported in ref. [52] showed that the power grid is very vulnerable to intentional attacks and that the removal of only three targeted edges can decrease $E(G)$ dramatically. In ref. [38], the relative size of the largest connected component S_{inf} was used as a metric, based on which the authors drew the conclusion that the Italian power grid is more robust than the French power grid under both intentional attacks and random attacks.

In practical cases, a severe power blackout is usually the result of a series of failures successively taking place in the power network following the initial one or a few failures [53–56]. The above structural vulnerability assessment models are limited to static analysis, and are unable to capture the properties of the dynamic failure propagation process in a power system. Witnessing this drawback, several dynamic models were proposed for the cascading failure analysis of power networks. In the following sections, we will review the dynamic models used for investigating the network vulnerability and the failure cascade mechanisms.

2.4.2 Motter-Lai Model

Motter and Lai [57] proposed a model that simulates the cascading failure process in power networks in a step-by-step process, where the dynamics of flows are taken into consideration. By assuming that the energy is transmitted along the shortest paths in power networks, load L_i of node i is represented by the total number of shortest paths that pass through it, i.e., the node's betweenness. Each node has a maximum load limit

called capacity. If the load of node i exceeds its capacity, it will fail instantly and be removed from the network. Node i's capacity C_i is set as follows:

$$C_i = (1 + \alpha)L_i(0), \ \ j = 1, 2, ...N, \tag{2.10}$$

where $\alpha > 0$ is a tolerance parameter, and $L_i(0)$ is the load of node i when the power network is in the normal state.

In this model, before the initial failure, the capacities of the nodes are set based on equation (2.10). Then, a single node is removed from the network as the initial failure. The removal changes the network topology and the distributions of shortest paths, which may cause other nodes to be overloaded and failed. Such removal-redistribution process continues until no overloaded nodes exist in the remaining network. The damage caused by the failure cascade is quantified by the relative size of the largest connected component, i.e., $S_{inf} = N'/N$, where N and N' are the numbers of nodes in the largest component before and after the cascade, respectively. Based on this model, the simulation results in the Western American power grid showed that attacking the node with the largest load can damage the grid more severely compared with attacking the node with the maximum degree or the node randomly chosen. However, the basic assumption of power being transmitted along shortest paths is not fully consistent with the physics of electric networks where topologies and impedances dictate the manner in which power flows in the network.

2.4.3 Effective Efficiency Model

By assigning an effective efficiency to each edge in the power network, Crucitti *et al.* [18] used a weighted network to analyze the power grid. The effective efficiency e_{ij} of edge (i, j) in the range $[0, 1]$ characterizes how effectively its terminal nodes i and j exchange electricity. The efficiency of a path is the sum of the effective efficiencies of all the edges along the path. The path that has the highest efficiency between a pair of

nodes in the network is chosen as the best path of the two nodes. The authors assumed that the electricity transmitted between a source node and a targeted node flows along the best path. Further, $L_i(t)$ is defined as the number of best paths passing through node i at time t.

Instead of removing the overloaded elements as in the Motter-Lai model, Crucitti *et al.* [18] used degraded effective efficiencies to characterize the effects of power overloading. Initially, the efficiencies of edges are set to be 1. If node i works within its capacity C_i, its efficiency remains to be the same. If node i's load $L_i(t)$ exceeds C_i, the effective efficiencies of the edges that connect to node i will be degraded as follows:

$$e_{ij}(t) = \begin{cases} e_{ij}(0)\dfrac{C_i}{L_i(t)}, & \text{if } L_i(t) > C_i, \\ e_{ij}(0), & \text{if } L_i(t) < C_i, \end{cases} \tag{2.11}$$

where $e_{ij}(0)$ is the initial efficiency of edge (i, j) and C_i is set based on equation (2.10).

In the effective efficiency model, the initially failed node is removed from the network, which triggers the following iterative steps: (1) the distribution of the best paths changes in the network, thus causing the load changes of other nodes; (2) new overloaded nodes may emerge, and instead of being removed, they degrade the efficiencies of affected edges. These two steps iterate until the network enters a steady state. The average efficiency of all the best paths in the network is used as an indicator to measure the effects of the cascading failures. With this model, the authors concluded that the failure of the most heavily loaded node can cause a catastrophic power outage to the Italian power grid.

Though the Motter-Lai model and the effective efficiency model investigate the cascading failures from a dynamic viewpoint, they fall short of only using topological parameters to represent power flow in a power grid. Besides, the power flow redistribution algorithm used cannot capture the electrical properties of the power systems under study. Similar improper algorithms were also used in ref. [58], where after a node fails,

the load it carries will be dispatched to its neighbors and in ref. [59] where power flow will be equally redistributed among the remaining lines after a line is removed.

2.4.4 AC/DC Model

To study the power flow distribution in power systems, the following two factors should be considered. First, the amount of power that flows in a power network should be determined by the actual variations of voltages and currents in the constituent elements as well as the way they are connected. Second, the power flow distribution in the power network must obey the relevant physical laws like Kirchhoff's laws and Ohm's law. Based on these recognitions, in this section, we introduce the AC and DC power flow models used in electrical engineering to compute the distribution of power flow in a power network. We use the terms "node" and "bus" interchangeably in the following.

AC Power Flow Model

The power flow study is to obtain the voltage at each bus point and the current through each transmission line in a power grid. In real power systems, an AC power flow model is used to derive the alternative voltage and current information by solving a set of nonlinear equations [60]. It is only applicable when the power system is in the steady state with no transient changes in power consumption, power generation, and frequency.

The voltage at bus i is denoted by $V_i = |V_i| \angle\theta_i$, where $|V_i|$ is the voltage amplitude and $\angle\theta_i$ is the phase angle. Similarly, $V_k = |V_k| \angle\theta_k$ is the voltage at bus k. Further, $\theta_{ik} = \theta_i - \theta_k$ denotes the phase difference between nodes i and k. For a transmission line (i, k) that connects nodes i and k, the current flowing though it can be calculated as $I_{ik} = (V_i - V_k)(G_{ik} + jB_{ik})$, where B_{ik} and G_{ik} are the susceptance and conductance of line (i, k), respectively.

Thus, the power S_{ik} injected to node i through transmission line (i, k) is

$$S_{ik} = V_k I_{ik} = P_{ik} + jQ_{ik}, \tag{2.12}$$

where P_{ik} is the active power, and Q_{ik} is the reactive power. Here, P_{ik} and Q_{ik} can be further written as follows:

$$P_{ik} = |V_i|^2 G_{ik} - |V_i||V_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}), \tag{2.13}$$

$$Q_{ik} = |V_i|^2 B_{ik} + |V_i||V_k|(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}). \tag{2.14}$$

For bus i, the externally injected power is denoted by $S_i = P_i - jQ_i$, where P_i and Q_i are the real and reactive power. As the sum of the externally injected power and the power injected to node i through the transmission lines is 0, for each node i in the network, we have the following two equations:

$$P_i = -\sum_{k=1}^{N} P_{ik} = \sum_{i=1}^{N} |V_i||V_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}), \tag{2.15}$$

$$Q_i = \sum_{k=1}^{N} Q_{ik} = \sum_{k=1}^{N} |V_i||V_k|(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}), \tag{2.16}$$

where $G_{ii} = -\sum_{k\neq i} G_{ik}$ and $B_{ii} = -\sum_{k\neq i} B_{ik}$. If there is no transmission line between nodes i and k, G_{ik} and B_{ik} are both 0.

For a power system with N nodes, there are $2N$ such nonlinear equations, solving which the voltage information (the magnitude and phase angle) at each bus can be derived. In the AC power flow problem, three kinds of buses are considered: load buses, generator buses, and slack buses. It is assumed that for each load bus, the real power and reactive power are given. For each generator bus, the voltage magnitude and real power generated are given. Also, the voltage magnitude and voltage phase

are given for the slack buses. With these known variables, several methods have been proposed to solve the nonlinear equations, such as the Newton-Raphson method, the Gauss-Seidel method, the Fast-decoupled-load-flow method, and so on [61].

DC Power Flow Model

Due to nonlinearity, the AC power flow model takes quite a long time to compute a solution. Though accurate, the high computational cost of the AC power flow model makes it infeasible to analyze large networks. By linearizing the equations in the AC power flow model, a DC power flow model is often used instead. In the DC power flow model, the following assumptions [62, 63] are made:

(1) The voltage magnitude at each bus is constant being 1 p.u.

(2) The resistance is much smaller compared with the reactance for each transmission line, so that it can be ignored.

(3) The phase difference θ_{ik} between the two terminal nodes of a transmission line (i, k) is very small so that $\sin\theta_{ik} \approx \theta_{ik}$ and $\cos\theta_{ik} \approx 0$.

Equation (2.13) can be written as

$$P_{ik} \approx -B_{ik}\sin(\theta_i - \theta_k) \approx -B_{ik}(\theta_i - \theta_k). \tag{2.17}$$

Thus, for each bus, there is one linear equation

$$P_i = -\sum P_{ik} = \sum_{k=1}^{N} B_{ik}(\theta_i - \theta_k). \tag{2.18}$$

Equation (2.18) is also called the nodal equation of node i. By writing all the nodal equations in a matrix form, we have

$$P = B\theta, \tag{2.19}$$

where $P = \begin{bmatrix} P_1 & P_2 \cdots & P_N \end{bmatrix}^T$, $\theta = \begin{bmatrix} \theta_1 & \theta_2 \cdots & \theta_N \end{bmatrix}^T$ and B is a $N \times N$ matrix containing the admittance of each transmission line of the power network.

In order to have a solution, the real power consumed at each load node and the real power generated by each generator node in the power grid should be given. As it is assumed that there is no power loss in the DC power flow model, the sum of the power consumed should be equal to the sum of the power generated. Thus, the externally injected power of $N-1$ nodes in the network and the voltage phase of one node as the reference phase should be known.

It is worth mentioning that MATPOWER is a powerful Matlab toolbox designed by Zimmerman *et al.* [64] to compute power flow using the AC and DC power flow models.

The AC and DC power flow models are feasible for the long-term planning of power systems as they are suitable for analyzing power systems in the steady state. Besides, Dobson *et al.* [65] adopted the DC power flow model in the cascading failure simulation in power systems, known as the ORNL-Pserc-Alaska (OPA) model. In the OPA model, when a failure occurs in the power grid and before the next failure, the externally injected powers of all the nodes in the grid will be reassigned to new values to balance the power in the network. The power reassignment plan is given by minimizing $\sum_{i\in G}|\Delta P_i|$, where ΔP_i is the difference between the reassigned externally injected power and the former externally injected power of node i. After the power reassignment, the DC power flow model is used to derive power flows of all the remaining elements. Then, based on the newly updated power flow information, new failures are determined. The OPA model is more practical for power system analysis, but it still has some limitations. First, the optimal power dispatch method is usually for long-term operation planning of power systems. In the OPA model, it requires the power system to frequently change its power dispatch schedule. But during a fast cascading failure process, the power system does not have the capability to achieve such a delicate power balance plan so quickly in the network before the next failure. In practice, the transient power rebalance after a failure should rely more on the automatic control of power generation, as indicated in refs. [66, 67]. Second, even if the

power system has the frequent and fast power redispatch ability in a cascading failure process, it is more reasonable to adopt the plan for prohibiting failure cascade rather than the method for minimizing $\sum_{i\in G} |\Delta P_i|$ [68].

2.4.5 Synchronization Model

The DC and AC power flow models are suitable for analyzing the power systems that operate in the steady state, where there are no transient load or frequency changes. For practical operation of power networks, circuit variables associated with the nodes are not constant values. When the power system is in the steady state, we assume that the voltage phases of all the nodes are synchronized. When there is an abrupt change in the power network, for example, in the event of failure of one element, the network can experience non-synchronous oscillations before it enters the next steady state or it can even become unstable. Instead of using constant values to describe the nodal variables, Dörfler and Bullo [69] used a first order formula to describe the active power drawn by a load node and a second order formula to describe the active power generated by a generator node.

In the synchronization model, it is assumed that the power network is lossless. Thus, based on equation (2.17) the power injected to node i through line (i, k) is $P_{ik} = -a_{ik} \sin(\theta_i - \theta_k)$, where $a_{ik} = |V_i||V_k| B_{ik}$.

For load node i, the active power P_i it draws consists of a constant term $P_{l,i}$ and a frequency-dependent term $D_i\dot{\theta}$. Thus, $P_i = -(D_i\dot{\theta}_i + P_{l,i})$, where θ_i is the phase angle, $\dot{\theta}_i$ is the frequency, and $D_i > 0$ is the damping coefficient. Thus, the dynamics of node i can be described by the following ordinary differential equation:

$$D_i\dot{\theta}_i + P_{l,i} = -\sum_{k=1}^{N} a_{ik} \sin(\theta_i - \theta_k). \tag{2.20}$$

Based on the swing equation, $-M_i\ddot{\theta}_i - D_i\dot{\theta}_i + P_{m,i}$ is used to represent the active power injected to the network by generator i, where $P_{m,i} > 0$ and $M_i > 0$ are the

mechanical power input and inertia coefficient of generator i, respectively. Thus, the power balance equation at node i can be written as a second order differential equation:

$$M_i\ddot{\theta}_i + D_i\dot{\theta}_i = P_{m,i} - \sum_{j=1}^{N} a_{ik} \sin(\theta_i - \theta_k). \tag{2.21}$$

Using the above set of differential equations, the synchronization problem in power grids has been widely studied [69–75].

2.5 Summary

In this chapter, we provide a literature review on some basic concepts of complex networks and power systems. In most previously reported work on applying complex network theory to power system analysis, network parameters are directly used to study power networks with either oversimplified or inconsistent assumptions of the physical properties of electrical networks. In order to take advantage of the theoretical achievements of this emerging discipline of complex networks, it is critical to employ models that can describe the behavior of power systems realistically and accurately. Thus, in the following three chapters, we propose power network models considering electrical variables and physical laws, in addition to the network topology. With these models, we further explore the relationship between the topological characteristics and functional performances of a power system.

Chapter 3

Assessing the Robustness of Power Systems

In the previous chapter, we reviewed some basic concepts of complex networks and their current applications to power systems. In this chapter, we study the robustness assessment of power systems from a network perspective. Based on Kirchhoff's laws and the properties of network elements, and combining with a complex network structure, we propose a model that generates power flow information given the electricity consumption and generation information. It has been widely known that large scale blackouts are the result of a series of cascading failures triggered by the malfunctioning of specific critical components. Power systems could be more robust if there were fewer such critical components or the network configuration was suitably designed. The percentage of unserved nodes (PUN) caused by a failed component and the percentage of non-critical links (PNL) that will not cause severe damage are used to provide quantitative indication of a power system's robustness. We also propose a new metric based on node-generator distance (DG) for measuring the accessibility of generators in a power network which is shown to affect robustness significantly. The influence of network structure and location of generators are explored through simulations with the model.

3.1 Introduction

Many researchers have tried to apply complex network theory to power systems, aiming at gaining new insights into the power grid operation that would help enhance the functionality of power systems.

In early studies [13, 15, 16, 34, 36, 39], real data from power grid in different regions were analyzed, with the objective of extracting structural characteristics of this man-made infrastructure. Cotilla-Sanchez *et al.* [42] compared the structural and electrical properties using the concept of "resistance distance" which is an important parameter for measuring accessibility of nodes.

In addition, the functional properties of power grids, e.g., robustness, synchronization and efficiency [74], were explored in the later study, among which robustness has always drawn much attention. Static models were first used to study the grid's resilience to the failure of some specific nodes or lines [16, 38, 52].

Since many severe blackouts were caused by a series of complex dynamic processes which were in turn triggered by some specific component's failure, many researchers began to use dynamic models to study cascading failures. In previous studies [58, 76, 77], each component in the system carries its load as well as its rated capacity. When some of the components break down, the power flow will redistribute in the power system, and the components whose loads exceed their capacities will fail in succession. Such cascading failure continues until all the remaining components can work properly.

In dynamic models, deriving the load distribution in the network is the key issue. Topological parameters were used to represent the loads of the elements in power systems in the previous work [13, 18, 57].

Power flow distribution in a power system is governed by electrical laws and components' properties. Analysis is either inadequate or inaccurate if it is based only on network topology. In order to exploit complex network methods for producing practi-

cally relevant results, better methods are needed [19]. The DC power model [60] has been used to calculate the power flow in a power grid [19,77]. However, the DC power flow model falls short of providing critical information about voltage values [78], let alone giving a complete solution for voltages and currents in the network upon re-balancing of power generated and consumed after a fault (component's failure) occurs.

In this chapter, we first introduce a model that uses the concepts of complex networks and electrical laws to obtain the power flow information in the system in Section 3.2. Then, the cascading failure process is described in Section 3.3. In order to quantitatively describe a system's robustness, two robustness parameters are proposed in Section 3.4, i.e., the percentage of unserved nodes (PUN) caused by a component's failure and the percentage of non-critical links (PNL) that will not cause severe damage. Section 3.5 shows robustness assessment results of some real power systems with the method proposed. Many factors can influence a power system's robustness, and Section 3.6 specifically explores the influence of network structure, the locations of generators. Simulation results show that, for a given set of numbers of generators, consumers, and transmission lines, connections having short average shortest path length can significantly reduce a power system's robustness. To explore the effects of generators' distribution in the grid, we propose, in Section 3.6, a new metric based on node-generator resistance distance [79] (DG) for measuring the degree of accessibility to generators of all consumers in a power network which is shown to affect robustness significantly.

3.2 Basic Model

Our model for the power system is based on the admittance model proposed by Grainger and Stevenson [60]. For a power system with n buses, the admittance model is written as

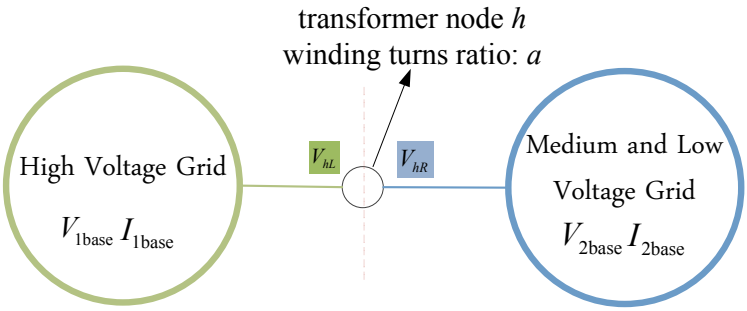


Figure 3.1: Transformer h connecting grids of varying voltages.

$$\begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n} \\ Y_{21} & Y_{22} & \cdots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \cdots & Y_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix}, \tag{3.1}$$

which is composed of Kirchhoff's law equations for all nodes. Here, V_n and I_n are the voltage and externally injected current at node n, respectively, Y_{ij} is the admittance of the transmission line connecting nodes i and j, and $Y_{ii} = -\sum_{j \neq i} Y_{ij}$. If there is no transmission line between nodes i and j, $Y_{ij} = 0$. The values of V_n and I_n are in time domain and can change with time, satisfying the constraints described by Equation 3.1 at any point of time. A time series of values of V_n and I_n describe dynamic behaviors of a power system. Equation 3.1 can be used to analyze the operations of a power system both in AC and DC. If the power system operates in AC and contains nonlinear components, harmonics will be included in Equation 3.1.

Compared to models based on topological loads, where the loads carried by the components in the grid are represented with topological parameters, and one most used parameter is the betweenness of the nodes and edges [18, 58], the above Grainger and Stevenson model provides real power information of the grid. However, since this model cannot perform load balance analysis and includes only a limited choice of types of nodes, it cannot provide a realistic analysis of the grid. For example, the presence of transformers cannot be adequately accounted for. In this chapter we introduce a more

comprehensive model. Four kinds of nodes are considered in our model, namely, the generation node, the consumer node, the distribution node and the transformer node.

(i) Consumer Nodes (Loads)

A consumer node i dissipates power, and at the circuit level, it sinks current I_i. The nodal equation of node i can be written as

$$\begin{bmatrix} Y_{i1} & \cdots & Y_{ii} & \cdots & Y_{in} \end{bmatrix} * \mathbf{V} = I_i, \tag{3.2}$$

where $\mathbf{V} = \begin{bmatrix} V_1 & V_2 & \cdots & V_n \end{bmatrix}^T$.

(ii) Distribution Nodes

A distribution node j is a connecting node that neither produces nor consumes power. Thus, we set $I_j = 0$, i.e.,

$$\begin{bmatrix} Y_{i1} & \cdots & Y_{ii} & \cdots & Y_{in} \end{bmatrix} * \mathbf{V} = 0. \tag{3.3}$$

(iii) Generation Nodes

A generation node k is a fixed voltage source. The current emerging from this node depends on its own voltage, the power consumption of other nodes and the network topology. The nodal equation is

$$\begin{bmatrix} 0 & \cdots & y_k & \cdots & 0 \end{bmatrix} * \mathbf{V} = V_k, \tag{3.4}$$

where $y_k = 1$, and V_k is the voltage of node k.

(iv) Transformer Nodes

Transformer nodes connect the high-voltage grids with mid-voltage or low-voltage grids, as shown in Fig. 3.1. Here, a is the winding turns ratio; V_{hL} and V_{hR} are the voltages at node h's input side and output side. In this study, we perform our analysis in per unit (p.u.), and the base values at the two sides of h are set according to $V_{2\text{base}} = V_{\text{base}}/a$ and $I_{2\text{base}} = aI_{\text{base}}$. Thus, the p.u. voltage values of node h can be represented as $V_{hL} = V_{hR} = V_h$.

The nodal equation of node h is

$$\begin{bmatrix} Y_{h1} & \cdots & Y_{hh} & \cdots & Y_{hn} \end{bmatrix} * \mathbf{V} = 0. \tag{3.5}$$

Combining equations (3.2)–(3.5), we get the following power system equation:

$$\mathbf{A} * \mathbf{V} = \mathbf{B}, \tag{3.6}$$

where

$$\mathbf{A} = \begin{bmatrix} \ddots & & & & & & \cdots & \\ Y_{i1} & \cdots & Y_{ii} & Y_{ij} & Y_{ik} & Y_{ih} & \cdots & Y_{in} \\ Y_{j1} & \cdots & Y_{ji} & Y_{jj} & Y_{jk} & Y_{jh} & \cdots & Y_{jn} \\ 0 & \cdots & 0 & 0 & y_k & 0 & \cdots & 0 \\ Y_{h1} & \cdots & Y_{hi} & Y_{hj} & Y_{hk} & Y_{hh} & \cdots & Y_{hn} \\ & & & & & & \cdots & \ddots \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} \cdots & I_i & 0 & V_k & 0 & \cdots \end{bmatrix}^T,$$

and subscript i denotes a consumer node (load); j denotes a distribution node; k denotes a generation node; h denotes a transformer node. Given the power consumption, the generation information and the topology, the voltage of each node can be found using

(3.6). Then, the currents flowing in the transmission lines can be calculated as

$$I_{ij} = (V_i - V_j) * Y_{ij}. \tag{3.7}$$

Remarks: Equation (3.6) is our basic model, which is derived from consideration of circuit laws and hence realistically describes the behavior of the power network. Furthermore, with the help of computation softwares, this model offers a convenient means for studying the power grid from a complex network perspective, producing results that are not obtainable from conventional circuit analysis. It should be noted that, in a connected system, the power provided by the generators should always be equal to the power consumed. When some changes occurs in a power system, the loads should be balanced manually or automatically. The DC model [80, 81] compute the power flow information when the externally injected power of each node is given. Once some nodes fail and disconnect with the network in a cascading failure, their externally injected power becomes 0, which causes the loads of the remaining system unbalanced. Thus, before using DC model to derive the updated power flow information, loads of the remaining nodes should be balanced. The DC model can not balance the loads automatically, and an algorithm or control method for balancing loads should be added if DC model is used for analyzing cascading failure process. The loads balancing algorithm can have influence on cascading failure process. In our model, the generators are modelled as voltage sources. The power emerging from this kind of nodes depends on their own voltages, the power consumption of other nodes and the network topology. The loads keep balanced automatically with Equation (3.6).

3.3 Cascading Failure Mechanism

When a link or node in the network breaks down, the structure of the power system will change, causing power flow to redistribute in the system according to (3.6). The

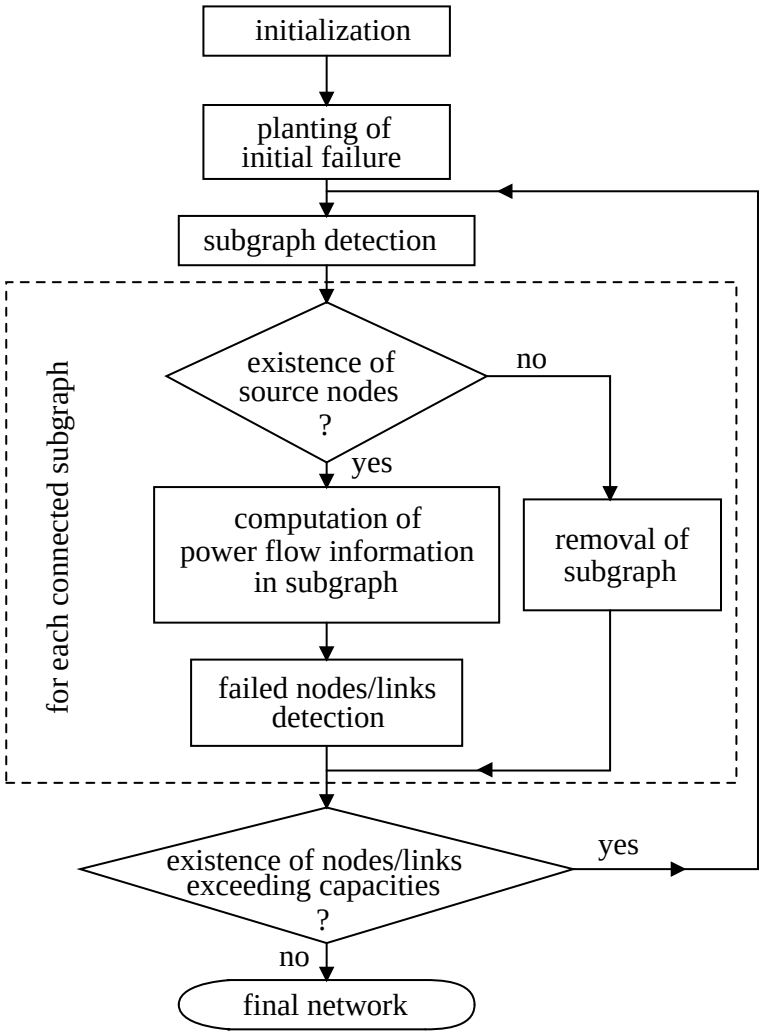


Figure 3.2: Flow chart of cascading failure.

nodes or links whose current loads exceed their capacities will fail successively. Thus, cascading failure continues until all the remaining components of the network can sustain their normal operation. Referring to Fig. 3.2, the cascading failure process can be described as follows.

1. *Initialization Settings:* At the start of the simulation, the voltages at the generation stations, the currents sunk at the consumer nodes, the winding turns ratios of the transformers and the admittances of the transmission lines need to be set. In order to reduce the effects of other factors on robustness and for simplicity, we set the voltages of generators at 1 p.u., nodes except generators each sinking

1 p.u. of current, and the admittance of each transmission line at 11 p.u. Then, with these initial values, we use (3.6) to obtain the initial power flow information in the system, i.e., the voltage at each nodes, the currents flowing through each link, and the load of each component. The node or link whose load exceeds its capacity will be removed. A transmission line's *current loading* is defined as the current through it, and its *capacity* is $1 + \alpha$ times of its initial value $I_{ij}(0)$. A node's *power loading* is defined as $V_i(0) * I_{oi}(0)$, where $I_{oi}(0)$ is the sum of currents flowing out of node i, and its *capacity* is $1 + \beta$ times of its initial value $V_i(0) * I_{0i}(0)$. Here, α and β denote the safety margins of the lines and nodes in the power grid, respectively. In reality, due to economic considerations, the safety margins limited and will not be very high. In this simulation the safety margins are set as $\alpha = 0.2$ and $\beta = 0.5$.

2. *Planting of Initial Failure:* With a set of initial settings, one component is randomly chosen as the first failed component, and it will be removed from the network.

3. *Cascading Iteration:* The removal of a component changes the structure and the operation of the power system. When an initial failure is planted, a series of cascading iterations begins. First, connected subgraphs will be identified. For a subgraph containing no generators, all the nodes in it are *unserved nodes*. For a subgraph containing at least one generator, (3.6) is used to compute the actual power flow distribution. The node or link that exceeds its capacity will be removed. This procedure repeats until all existing nodes and links can sustain their respective loadings. Then, we get the final balanced condition of the system.

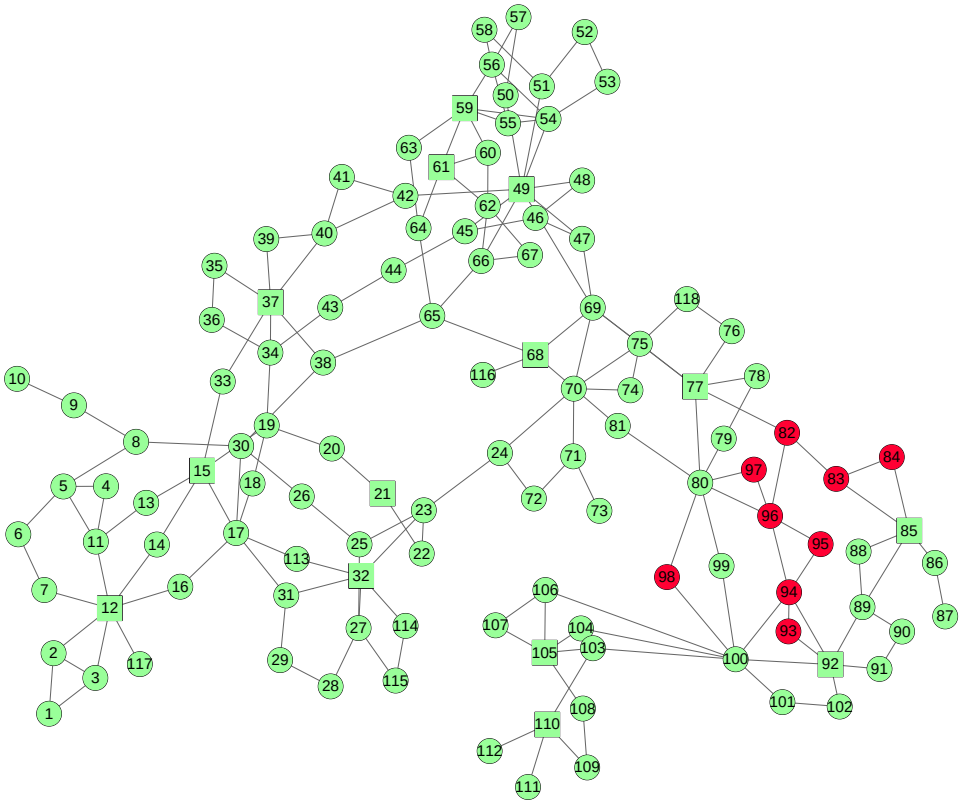


Figure 3.3: Simulation of cascading failure triggered by breakdown of transmission line (77, 82) of IEEE 118 Bus. Squares are generators. Red nodes are unserved nodes.

3.4 Robustness Parameters

Robustness refers to the ability of a system to tolerate faults. For a power system, robustness can be defined in terms of a measure that describes the ability of the system in providing normal service to a critical percentage of clients under the condition that some components of the system fail. It is important to define appropriate metrics that can quantitatively indicate a power system's robustness. In our study, a power system is represented as an undirected graph W with n nodes and m links. Formally, a graph W is $\{N, M\}$, where N is the set of all nodes and M is the set of all links. Also, G represents the set of generators in W, and $G \subseteq N$.

In the field of power system analysis, the extent of unserved area is usually used to measure the size of a blackout [82]. Here, we propose to use the *fraction of unserved*

area caused by failure of a component to indicate the importance of that component. Specifically we define PUN(i) as the *percentage of unserved nodes* caused by failure of component i, i.e.,

$$\text{PUN}(i) = \frac{n_{\text{unserved}}(i)}{n}, \tag{3.8}$$

where $n_{\text{unserved}}(i)$ is the number of unserved nodes due to component i's malfunctioning. Unserved nodes are the nodes that are deprived of power in a blackout. As mentioned previously in Section 3.3, unserved nodes are either nodes whose power loadings exceed their capacities or nodes that exist in a subgraph containing no generators. A component that has a large PUN, upon failure, can seriously damage the network. Conversely, a component with a small PUN will not have a significant influence when it fails. Thus, a power system is more resilient to faults that occur in components having small values of PUN, and we call this kind of components *non-critical components*. If a power system is resilient to faults that occur in most of the components, i.e., most of the components are non-critical, then we can say that the system is robust.

To measure the robustness of the whole system, we propose to use the *percentage of non-critical links* (PNL) whose PUNs are smaller than a *threshold* to indicate the ability of a network in tolerating faults. The PUN threshold is a specific percentage of nodes in the power grid. We define PNL(threshold) as the *percentage of non-critical links* for a given threshold, i.e.,

$$\text{PNL(threshold)} = \frac{1}{m}\sum_{i \in M} \delta(i), \tag{3.9}$$

where

$$\delta(i) = \begin{cases} 1, & \text{PUN}(i) < \text{threshold}, \\ 0, & \text{otherwise}. \end{cases}$$

A large PNL means that the power system has a large portion of links whose failures will not lead to serious damages (i.e., the percentage of unserved nodes remains larger than the threshold) to the grid, in other words the system can tolerate faults oc-

Table 3.1: Average shortest path length (L), and percentage of generators (PG) of networks

	L	PG
IEEE 118 Bus	6.33	8%
Northern European Grid	8.99	50%

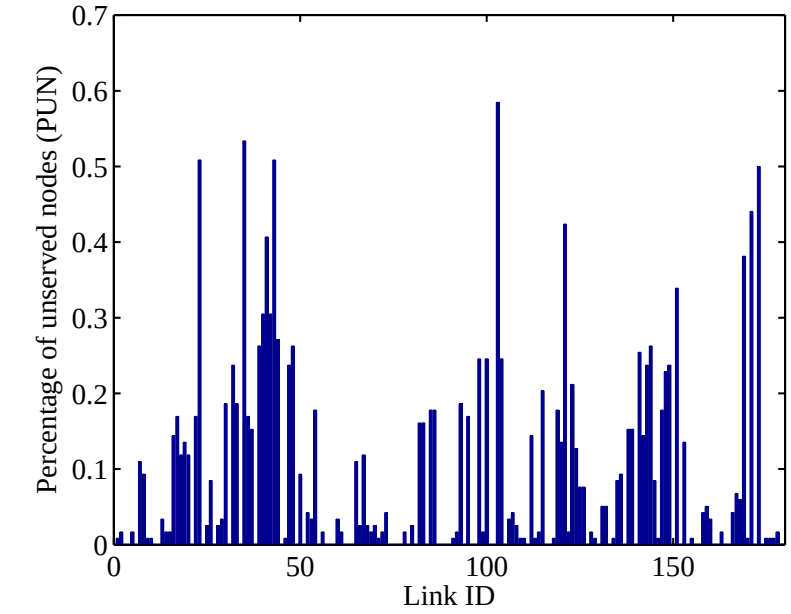
curred a large percentage of components of the system. The power system with a large PNL is robust.

3.5 Preliminary Study of Practical Systems

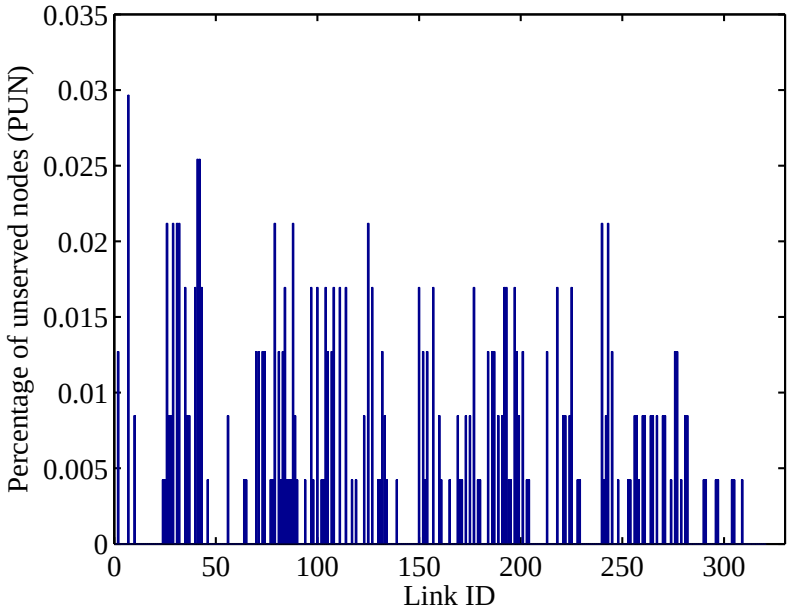
In this section, we present simulation results of robustness assessment of some real power systems. The IEEE 118 Bus is a power flow test case offered in ref. [83] and the Northern European Grid (NEG) data is obtained from ref. [70]. It should be noted that, in our study, we set the voltages of generators at 1 p.u., nodes except generators each sinking 1 p.u. of current; and the admittance of each transmission line to be 11 p.u. Also, the safety margins of nodes and links are set as $\alpha = 0.2$ and $\beta = 0.5$. The simulation software used here is Matlab, with the toolbox library [84] developed by Lev Muchnik which provides the basic functions for the computation of complex network parameters.

Figure 3.3 shows a cascading failure result triggered by malfunctioning of line (77, 82). The rectangular nodes are generators, and the circle nodes are current sinks. The unserved nodes caused by the malfunctioning of this line are colored red. From Fig. 3.3, the PUN of this link is 7.6%, indicating that for the IEEE 118 Bus, the failure of line (77, 82) can deprive 7.6% of the network from power.

Figure 3.4 shows the PUNs of all links in the IEEE 118 Bus and the Northern European Grid. It can be observed that the roles of different links in the same power system are prominently different, as they have different PUNs. From Fig. 3.4, the



(a)



(b)

Figure 3.4: Simulation results of cascading failure and robustness assessment. (a) PUN of each link in IEEE 118 Bus; (b) PUN of each link in Northern European Grid.

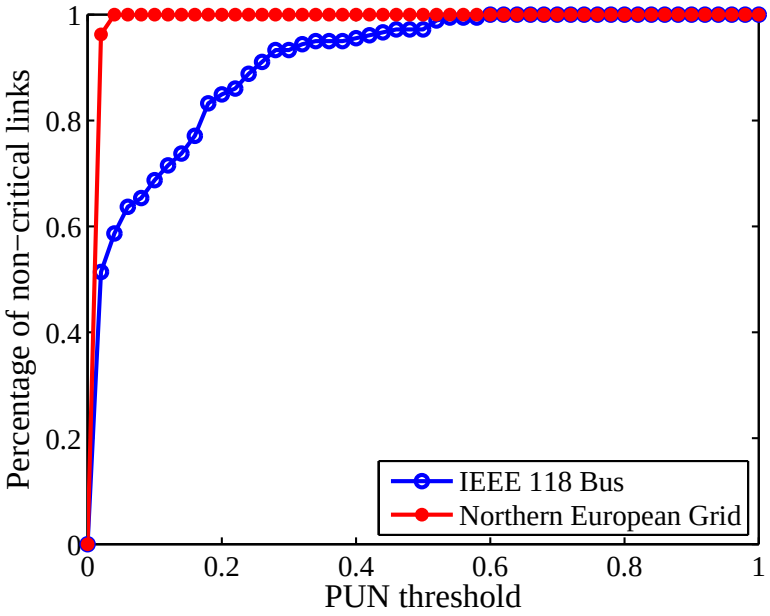


Figure 3.5: Robustness assessment of IEEE 118 Bus and Northern European Grid.

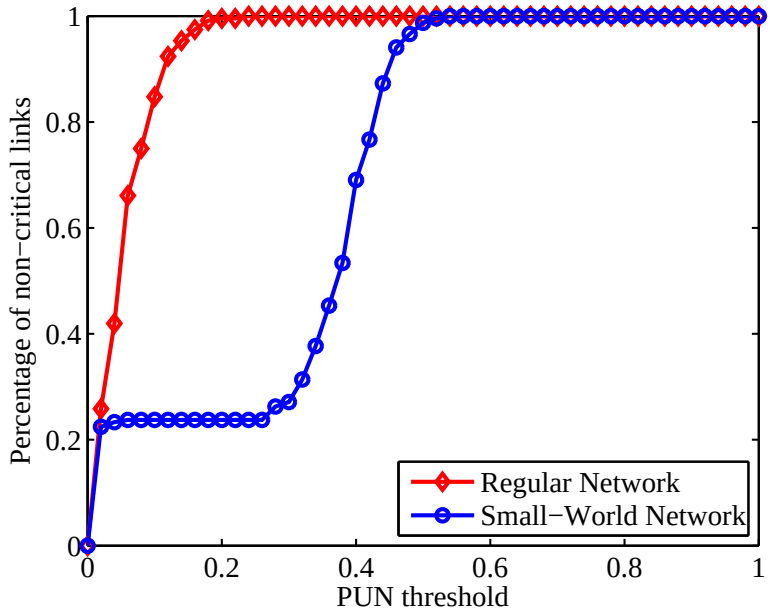
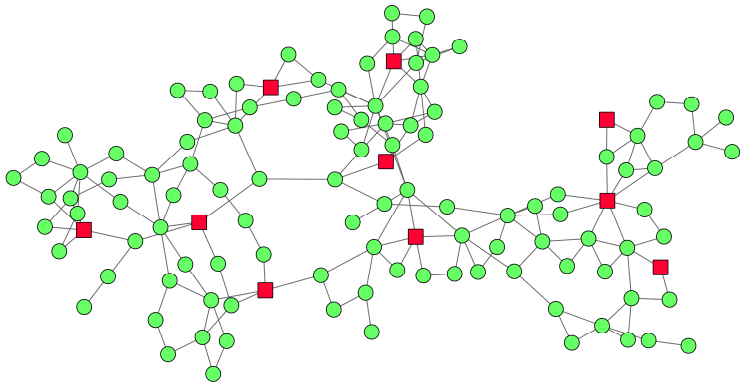


Figure 3.6: Robustness assessment of small-world and regular networks.

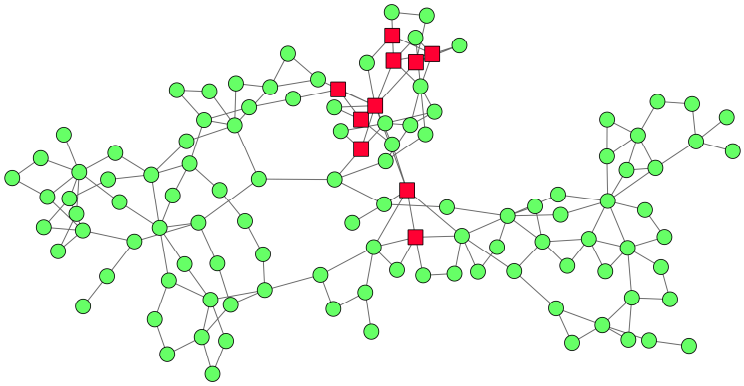
percentage of non-critical links of the Northern European Grid is larger than that of the IEEE 118 Bus. In order to distinguish the robustness of the two systems, we plot the PNLs of these two networks for different PUN thresholds. As shown in Fig. 3.5, the PNLs of the Northern European Grid are always larger than those of the IEEE 118 Bus, for the *threshold* ranging from 0 to 0.33. This means that the Northern European Grid is more robust than the IEEE 118 Bus.

The above result transpires a series of important questions. Why does the Northern European Grid have better robustness than the IEEE 118 Bus? What are the factors that affect a power system's robustness and in what way do these factors influence a power system's robustness? Is there a consolidated metric that can conveniently measure the robustness of a system? The answers to these questions will offer useful clues and design guidelines for power engineers to construct more reliable power transmission systems.

Table 3.1 lists the average shortest path length (L), and the percentage of generators (PG) of the two networks. The metric L describes the structural characteristics of a network, whereas PG gives information about power availability. The Northern European Grid's L is larger than the IEEE 118 Bus', indicating that the nodes of the IEEE 118 Bus are more closely connected. The network structure can play an important role in affecting the robustness of a power system. At the same time, the Northern European Grid has a larger percentage of generators than the IEEE 118 Bus. The percentage of generators is also an important factor. Many other factors can influence the robustness of a power system as well, e.g., the locations of generators, the safety margins, and so on. It should be noted that the robustness of the two systems as inferred from Fig. 3.5 is the result of combined influence of these factors. In the next section, we will compare the effects of various parameters systematically, aiming to develop an effective metric that can be used to assess robustness.



(a)



(b)

Figure 3.7: Topologies of power networks. (a) IEEE 118 Bus A; and (b) IEEE 118 Bus B. Squares represent generators.

3.6 Network Properties and Robustness Assessment

In this chapter, we focus on network properties that determine the robustness of a network. Specifically, we consider the network structure and the availability of generators in a network. Our purpose is to derive effective guidelines that can be used by electrical engineers to determine the network structure and generator distribution in order to optimize robustness. Note that we do not consider component parameters, e.g., ratings and safety margins, which can be considered as post-design parameters and be dealt with separately after the desired network is constructed.

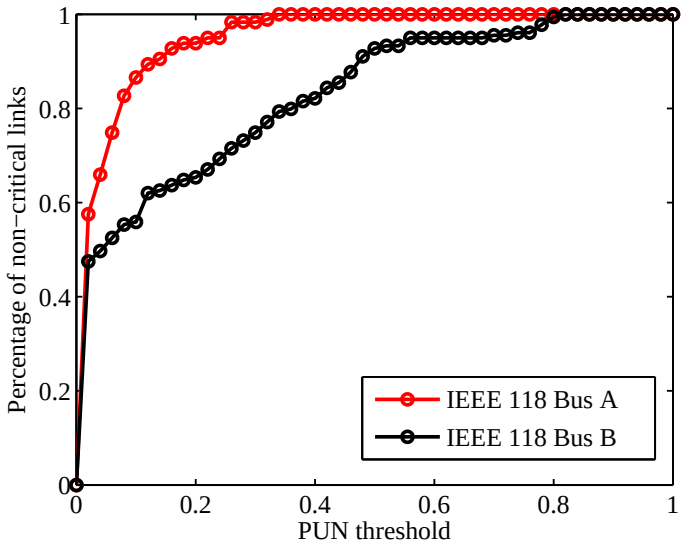


Figure 3.8: Robustness assessment of IEEE 118 Bus. Buses A and B only differ in the locations of generators, with Bus A having more decentralized distribution of generators.

3.6.1 Effect of Network Structure

Phadke *et al.* [85] pointed out that the graph of a power system is relevant to its efficiency and robustness. Here, we investigate the influence of a grid's topology on its robustness. To study the effect of network structure, we generate networks of specific structures for in-depth study. Small-world networks are one typical kind of networks whose L is very small. Watts and Strogatz [5] showed that small-world connectivity could have significant effects on the dynamics of networked systems. To verify the effect of the connection with short L, we first study the robustness of small-world networks. For instance, we construct regular and small-world networks of similar scale and identical percentage of generator nodes. Specifically, we generate a regular network of 118 nodes with an average degree of 4. The small-world network is generated by rewiring the links of the regular network with a probability $q = 0.3$. The percentage of generators is 8%. In order to scale the effects of other factors such as locations of the generators, we construct 100 realizations of the small-world network to get the average results. Figure 3.6 shows that the PNLs of the regular network are much higher than

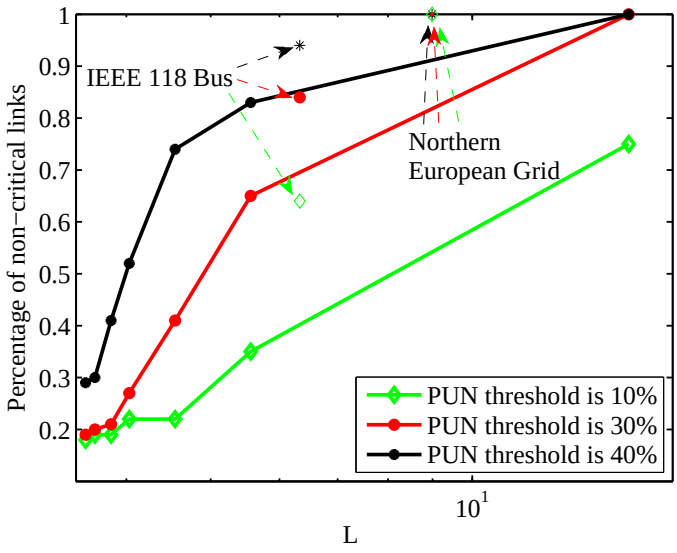


Figure 3.9: Effects of small-world connectivity on robustness of power systems.

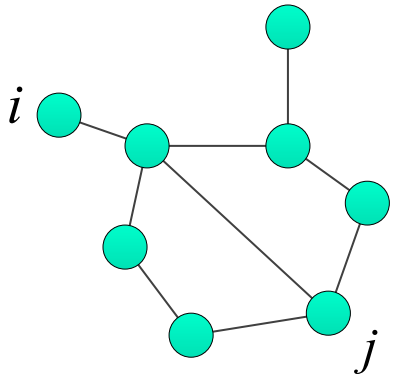


Figure 3.10: An example of electrical network.

those of the small-world network for PUN threshold ranging from 0.02 to 0.60.

In order to further explore the effect of the connection with short L, we generate 7 groups of networks with the link-rewiring probability q ranging from 0 to 0.6. Each group contains 100 realizations, similar to the group with $q = 0.3$ mentioned above. The group with $q = 0$ is essentially the regular network group. Table 3.2 lists the averaged PNLs with three thresholds, along with L and PG of each group. We see that as q increases, L decreases. In Fig. 3.9, we plot the relationship between PNL and L. The lines are results derived from the 7 groups of synthesized networks listed

Table 3.2: Average shortest path length (L), percentage of generators (PG) of networks with different levels of small-world connectivity characterized by the link-rewiring probability q. Their corresponding PNLs for threshold of PUN set at 10%, 30% and 40% are shown.

q	L	PG	PNL(10%)	PNL(30%)	PNL(40%)
0.0	15.13	8%	0.75	1.00	1.00
0.1	5.56	8%	0.35	0.65	0.83
0.2	4.55	8%	0.22	0.41	0.74
0.3	4.03	8%	0.22	0.27	0.52
0.4	3.84	8%	0.19	0.21	0.41
0.5	3.68	8%	0.19	0.20	0.30
0.6	3.59	8%	0.18	0.19	0.29

in Table 3.2, and the dots are robustness assessment results of IEEE 118 Bus and Northern European Grid. It is obvious that the value of PNL will be lower if the system has a smaller value of L. In other words, short L connectivity deteriorates the robustness of a power system. Hence, we can conclude that with equal percentage of generator nodes, transmission lines, and same power consumption, the connection with short L degrades a power system's robustness significantly when the safety margins are limited. This is consistent with the robustness assessment results for the IEEE 118 Bus and the Northern European Grid, i.e., the one with shorter average shortest path length is less robust.

Remarks: Several prior studies have focused on the influence of small-world connectivity on the robustness of a power system. Mei *et al.* [63] drew a similar conclusion that small-world networks are prone to cascading failure, while Quattrociocchi *et al.* [86] reported that small-world networks were more readily recovered from failures, indicating that small-world networks are more robust. The main reason for the discrepancies in these studies is that their assumptions are different. In ref. [86], no constraints are imposed on the amount of flow that can be transported by any link, i.e., the capacities of the components are infinite and the cascading processes are not con-

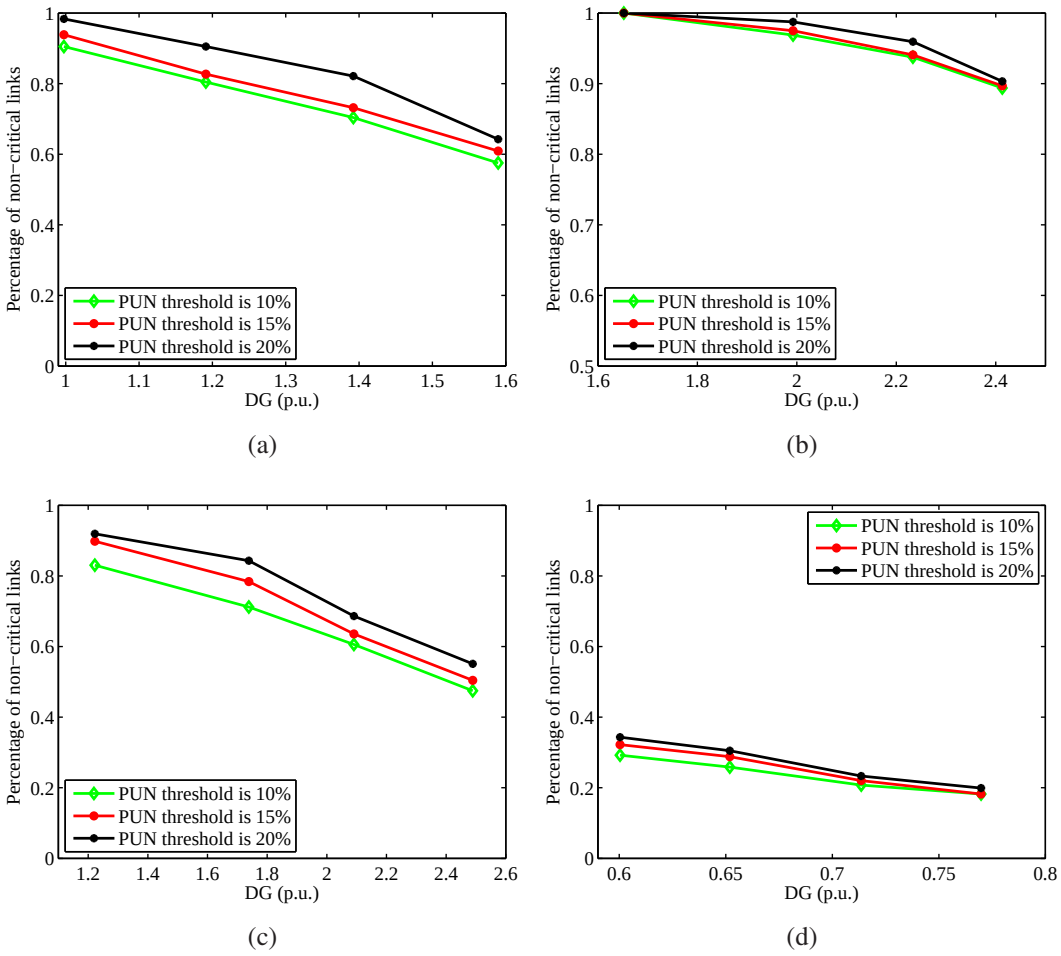


Figure 3.11: Effect of locations of generators. (a) IEEE 118 Bus; (b) Northern European Grid; (c) regular network; (d) small-world network. DG measures nodes' distance to generators. Higher DG means less decentralised distribution of generators.

sidered. From a topological viewpoint, small-world networks have better connectivity than regular networks. Thus, a small-world network is more readily repaired by adding new links when the network decomposes. In reality, due to economic considerations, the safety margins cannot be infinite. It should be noted that the conclusion derived in our model is based on the condition that the capacities of the components of the power system are limited.

3.6.2 Effect of Accessibility to Generators

Power grids of the same structure can also display distinct robustness performances. We generate two power systems based on the IEEE 118 Bus, namely, IEEE 118 Bus A and IEEE 118 Bus B. Figure 3.7 shows the graph layouts of these two systems, where the red rectangle nodes are generators and the green circle nodes are consumers. IEEE 118 Buses A and B share the same characteristics including network structure, percentage of generators, and safety margins, but the generators in the two networks are located differently. From Fig. 3.8, we see that the IEEE 118 Bus A is more robust than the IEEE 118 Bus B. Thus, the locations of the generators affect the robustness of the system.

In terms of generator distribution, the IEEE 118 Bus A is more decentralized than the IEEE 118 Bus B. Theoretically, for a given number (percentage) of available generators, a decentralized distribution of generators permits most of the consumers in the network to reach a power source within shorter distances. To transmit the same amount of power from generators to consumers, highly decentralized locations of generators can reduce the total "traffic" volume in the transmission lines as well as the distribution nodes.

It is desirable to find a variable that quantitatively describes the location information of the generators in a network. Here, we review the concept of *resistance distance* of a power system proposed by Klein and Randić [79]. Essentially, the *resistance*

distance between two nodes refers to the effective resistance between them.

Referring to Fig. 3.10, when calculating the effective resistance between nodes i and j, we set node i as a voltage source with V_i, node j as a current sink with of I_j and all other nodes as distribution nodes with sink currents of 0. Using (3.6), V_j can be readily derived. The *effective resistance* between nodes i and j is defined by

$$R_{ij} = \frac{V_i - V_j}{I_j}. \tag{3.10}$$

The minimum effective resistance of consumer node i to any nearest generator represents its shortest distance to a power source. This is a measure of the distance over which power is transmitted between the pair of nodes. Thus, the minimum effective resistance of consumer i represents the *accessibility* to power sources of this node. Specifically, we define the resistance distance of node i to its nearest generator, $d(i)$, as

$$d(i) = \min\{R_{is}, s \in G\}. \tag{3.11}$$

For a given network structure, if the generators are evenly distributed and the percentage of generator nodes is adequately high, all consumers can reach a power source within a short resistance distance, i.e., all nodes have ready access to a power source. This will reduce the total power load imposed on the transmission lines, making the system more robust. Here, we define *average effective resistance (distance) to a nearest generator of all consumer nodes* (DG) as a measure of the accessibility to generators of all consumers, i.e.,

$$\mathrm{DG} = \frac{1}{(n-g)} \sum_{i \in N \setminus G} d(i), \tag{3.12}$$

where $N \setminus G$ is the set of nodes excluding the generator nodes, n is the total number of nodes, and g is the number of generators in the network. Small DG indicates better accessibility to power sources to generators. A network has a smaller DG if its generators are more decentralized or has a sufficiently large number (percentage) of

Table 3.3: DG and PG of IEEE 118 Bus A and B. Percentage of generators is fixed at 8% for comparison.

	IEEE 118 Bus A	IEEE 118 Bus B
DG (p.u.)	0.9977	1.5334

generators. Thus, in terms of basic network design, DG offers an effective measure of accessibility to power, which is the combined effect of the distribution of generators and the percentage of generators in a network. A large percentage of generator nodes with decentralized locations will make DG small. It is obvious that a power system could be very robust if there exist a large percentage of generator nodes. We therefore focus on the influence of the locations of generators on a system's robustness. Table 3.3 gives the DG values of IEEE 118 Buses A and B, with the percentage of generators fixed at 8%. We see that the DG of IEEE 118 Bus A is smaller than that of Bus B, which indicates that the generators in IEEE 118 Bus A are more decentralized than in IEEE 118 Bus B.

We now study the effect of varying DG in the IEEE 118 Bus, Northern European Grid, regular and small-world networks. For the IEEE 118 Bus system, a series of tests are performed, with generators' locations randomly chosen while keeping the same structure and fixing the percentage of generators at 8%. Then, we sort the results into five groups according to the values of DG. Ten test results are chosen in each group, and we average their PNLs and DGs. Figure 3.11 (a) shows the PNLs with different PUN thresholds for the IEEE 118 Bus. It is obvious that the value of PNL drops significantly as DG increases. We then apply the same test procedure to assess the Northern European Grid, regular network and small-world network. The regular network is the same network generated in Section 3.6.1, and the small-world network is generated by rewiring the links of the regular network with a probability of 0.3. Figures 3.11(b), (c) and (d) show consistent results. Thus, the metric DG proposed here is an effective design parameter for guiding the power engineers to choose appropriate

locations for generators in a given network structure to achieve a more robust power system.

It should be emphasized that our conclusion here has been drawn on the condition that the network structure is fixed. If the network structure is varied, small-world connectivity may also make DG very small. In that case, a small DG does not necessarily describe a decentralized distribution of the generators. In Section 3.6.1 we has observed that small-world connectivity can degrade a power system's robustness even though the DG value is small. The reason for this is that small resistance distances among nodes make the overall sensitivity of all components to a failure relatively high.

3.7 Summary

We assess the robustness of power systems using a model that is derived from consideration of electrical laws and network connectivity. Taking into consideration the properties of the components and their mutual effects, this model offers realistic assessment of the power grid compared to other previously proposed complex-network based models. We define effective robustness metrics to quantitatively describe a system's robustness. Our key conclusion is that the robustness of a power system can be significantly affected by (i) the average shortest path length; and (ii) the consumers' accessibility to generators.

Chapter 4

Modeling the Dynamic Propagation of Cascading Failure

In the previous chapter, we used a deterministic model to quantify the robustness of power systems in respect of cascading failures. In this chapter, we use a model to study the dynamic failure propagation process, consisting of a sequence of failure events occurring at specific time points. In this model, a circuit-based power flow model is used to study the cascading failure propagation process, and a stochastic model is combined to describe the uncertain failure time instants. The sequence of failures is determined by voltage and current stresses of individual elements which are governed by deterministic circuit equations, while the time durations between failures are described by stochastic processes. Simulation results show that our model generates dynamic profiles of cascading failures that contain all salient features displayed in historical blackout data. We further plot cumulative distribution of the blackout size to assess the overall system's robustness. We show that heavier loads increase the likelihood of large blackouts and that small-world network structure would make cascading failure propagate more widely and rapidly compared with a regular network structure.

4.1 Introduction

The power distribution network is a complex and highly interconnected network, consisting of power apparatus, protection equipment and control systems [87]. Protection equipment is responsible for maintaining reliability through applying switching actions of relays and circuit breakers. Relays are essential auxiliary components in transmission lines, generators, transformers, and other kinds of power apparatus. When a relay detects an abnormal operating condition such as over-current and voltage dip, it will switch off the affected component to remove the fault from the network, thereby preventing further damages and hence ensuring the normal operation of the rest of the system. The on/off states of relays determine the structure of the power network, thus influencing the overall operational state of a power system. Normally the power grid is designed to maintain its power distribution function even when a few elements are removed [88]. However, when the power grid is under stressed conditions, for instance, due to heavy loads and outages of equipment, the removal of some elements may lead to huge disturbances and subsequent tripping of other elements, causing a possible severe blackout [87].

The dynamic cascading failure process in a power grid can be viewed as a sequence of tripping events, leading eventually to power outage affecting a very large area. It has been observed that the 1996 Western North America blackouts [89], the 2003 Northeastern America and Canadian blackouts [90] and other historical blackout data all display a typical profile characterized by a relatively slow initial phase followed by a sharp escalation of cascading failures. Such a universal form of dynamic profiles strongly suggests that a common model can be used to describe the dynamic cascading failure process.

The study of the dynamic propagation of cascading failures provides useful hints for system vulnerability detection, robustness assessment and network control. Recently, Chen *et al.* [91] used a generalized Poisson model, negative binomial model

and exponentially accelerated model to generate the probabilities of the propagation of transmission outages which fit the observed historical data. Dobson *et al.* [92, 93] used branching processes to analyze the propagation of cascading failures in power grids. Much of the previous work primarily applied data fitting methods to investigate the statistical characteristics of power systems' blackouts, but fell short of considering the essential electrical circuit operations or the impact of the network structure. Moreover, cascading failures in power grids have also been studied in terms of the sequential trippings of electrical elements in real networks. Among the many switching mechanisms of relays, overloading is the most prominent one and has been widely studied [59, 65, 68, 77, 94, 95]. In a cascading failure process, the failure of one element leads to power flow redistribution in the grid, which can cause some other elements to be overloaded. These overloaded electrical elements can then be tripped by their relays, causing another round of failures until the remaining elements are all within their respective operating limits.

Various of tripping sequence settings of the overloaded elements have been explored [18, 77, 94]. Typically, in each round of the cascading simulations, the power flow distribution in the network is computed, and overloaded electrical elements are removed at the same time. The actual time delays and dynamical profiles of the process are not considered in this kind of models, making them unable to simulate the dynamic propagation of a cascading failure. In order to show the dynamic profile, some previous studies made the simple deterministic assumption that the duration for an overloaded element to be tripped is equal to Δt which is given by $\int_t^{t+\Delta t}(f_j(\tau) - \bar{f}_j)d\tau = \Delta o_j$, where f_j is the power flow of overloaded element j, $\bar{f}_j$ is the flow limit and Δo_j is a specific threshold of that element [66, 96].

Considering the complexities and uncertainties in real power grids [97], a few researchers turned to use probabilistic models to characterize the tripping events of the elements in power grids [68, 95, 98]. For instance, Wang *et al.* [68] used a Markov model to study cascading failures, where the trippings of the elements are regarded

as *state transitions,* which are memoryless and probabilistic. In Wang *et al.*'s work, the overloaded elements share one same tripping rate, which is much larger than the natural failure rate of the electrical equipment. Alternatively, an overall state transition probability can be determined by considering the maximum capacity of the failed elements and a random tripping process [95]. It is also shown [99] that a component will experience more failures under heavy load conditions. The varying tripping rates for elements under different extents of overloading stress have not been thoroughly considered in the aforementioned stochastic models. Study of essential collective behavior of a power network must be pursued according to the governing physical laws which in the case of power systems should involve circuit-based power flow equations [94] (see Section 3.2). By suitably combining the power flow study with probabilistic methods for describing inevitable uncertainties, the dynamic profile of cascading failure processes can be realistically revealed, hence offering important predictive information about the occurrence of large-scale blackouts.

In this chapter, we study the dynamics of cascading failure propagations in power systems. First, we apply circuit-based power flow equations to determine the sequence of failures in accordance to the extent of overloadings of individual components. In order to describe the complete dynamic profile, we need to determine the time durations between failures in the propagation sequence. Due to the complexities and uncertainties of the involving physical failure mechanisms of the components (e.g., manufacturing quality, environmental factors, etc.), stochastic processes are used to model the dynamic changes. Then, to study the collective behavior of the entire system in terms of failure propagation in the whole network, an extended chemical master equation (CME) model is used [100, 101]. Based on the CME model, we show that the failure propagation rate of the network is dependent on the sum of individual extents of overloading of all elements in the network.

Simulation results show that the cumulative number of failed elements triggered by some initial failures shows a universal growing pattern which is consistent with histor-

ical blackout data. Thus, our model can offer insights into the mechanism of cascading propagation in a power system as well as provide predictive information for the failure spreading in the network. Our study also includes the effects of loading conditions and network structure on the extent and rapidity of blackouts in power systems. The UIUC 150 bus system with different consumer load distributions and several types of network structure are studied for comparison purposes. It is shown that heavy load conditions increase the risk of large blackouts in the same power system, and that small-world network structure is more prone to rapid propagation of cascading failures than the regular structure.

4.2 Failure Mechanisms of Components

A power system is composed by various electrical stations connected by transmission lines, and each station or transmission line is protected by protective equipment. In this chapter, we model electrical stations as nodes and transmission lines as links, with nodes being connected by links forming a power network [94]. Deterministic power flow equations are used to generate the sequence of failures and their locations. A node or link is a *basic element* of a power network. We refer to an element's tripping event as an *element state transition* (EST). The cascading failure propagation in a power network can be viewed as a sequence of ESTs in the network. In this section, we investigate the state transition behavior of a basic element, and in the next section, we apply probabilistic theory to study the collective transition behavior of the network.

4.2.1 Time to Failure of a Basic Element

Let $s_i(t)$ be the state of element i of a given network, and $s_i(t) \in [0, 1]$, with $s_i(t) = 0$ corresponding to a connected element i at time t, and $s_i(t) = 1$ corresponding to a removed (tripped or open-circuited) element i at time t, as shown in Fig. 4.1. Here,

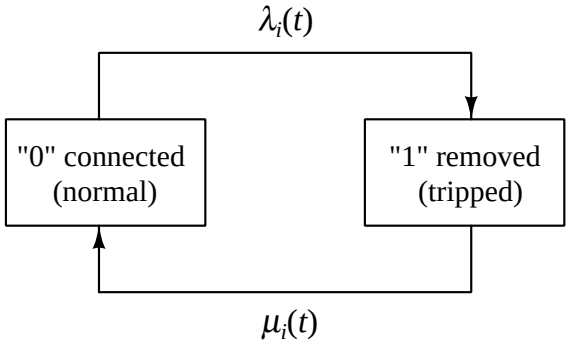


Figure 4.1: Dynamic description of failure in terms of state transitions. State "0" is the normal connected state; state "1" is the removed or tripped state. Arrows represent transitions between different states while self-loop arrows are not displayed in the figure.

$\lambda_i(t)$ is the rate of transition of node i going from state "0" to "1", and $\mu_i(t)$ is the transition rate from "1" to "0". Then, the future state of an element is solely determined by its present state and the transition rule. Suppose the present time is t, and dt is an infinitesimal time interval. As $s_i(t) \in \{0, 1\}$, $P\{s_i(t + dt) = 1\}$ and $P\{s_i(t + dt) = 0\}$ can be written separately as

$$\begin{aligned} P[s_i(t+dt)=1] &= P[s_i(t+dt)=1\,|s_i(t)=0]P[s_i(t)=0] \\ &\quad + P[s_i(t+dt)=1\,|s_i(t)=1]P[s_i(t)=1] \\ P[s_i(t+dt)=0] &= P[s_i(t+dt)=0\,|s_i(t_1)=0]P[s_i(t)=0] \\ &\quad + P[s_i(t+dt)=0\,|s_i(t)=1]P[s_i(t)=1] \end{aligned} \tag{4.1}$$

where $P[s_i(t) = 1]$ and $P[s_i(t) = 0]$ denote the probability that node i is in state "1" and "0" at time t, respectively; $P[s_i(t+dt) = 1\,|s_i(t) = 0)]$ is the conditional probability that given $s_i(t) = 0$ element i transits to state "1" in the time interval $(t, t + dt)$; and $P[s_i(t + dt) = 0\,|s_i(t) = 1)]$ is defined in a likewise manner. Using the state transition rates shown in Fig. 4.1, $P[s_i(t + dt) = 1\,|s_i(t) = 0)]$ can be written as

$$P[s_i(t+dt)=1\,|s_i(t)=0] = \lambda_i(t)dt. \tag{4.2}$$

Also, $P[s_i(t+dt) = 0\,|s_i(t) = 0)]$ is the probability that given $s_i(t) = 0$, element i remains in state "0" in time interval $(t, t+dt)$ (i.e., no state transition occurs). Thus, we have

$$P[s_i(t+dt) = 0\,|s_i(t) = 0\,] = 1 - \lambda_i(t)dt. \tag{4.3}$$

Likewise, we have

$$P[s_i(t+dt) = 0\,|s_i(t) = 1\,] = \mu_i(t)dt, \tag{4.4}$$

$$P[s_i(t+dt) = 1\,|s_i(t) = 1\,] = 1 - \mu_i(t)dt. \tag{4.5}$$

4.2.2 State Transition Rates of Basic Elements

In this section, we discuss the physical meanings of element state transition rates $\lambda_i(t)$ and $\mu_i(t)$ in a fast cascading failure process. In statistical terms, an event rate refers to the number of events per unit time. Specifically, $\lambda_i(t)$ is the rate of element i becoming disconnected in the network which is caused by either a natural equipment malfunction or tripping by its protective equipment, i.e.,

$$\lambda_i(t) = \lambda_i^0(t) + \lambda_i^1(i) \tag{4.6}$$

where $\lambda_i^0(t)$ is the equipment malfunctioning rate in the absence of loading stress and its value is constant and derivable from past statistics [96]; and $\lambda_i^1(t)$ is the removal or tripping rate by protective relays and is determined by the (over)-loading condition and the capacity of element i.

Among the many tripping mechanisms of relays [102, 103], power overloading is a dominant one. In this study, we focus on switching actions caused by overloading. When the load of element i is within its capacity, it is assumed to work in the normal condition and will not be removed or tripped by the protective relay, namely $\lambda_i^1(t) = 0$. However, when the element exceeds its capacity, there will be a short delay before

it is finally removed. The tripping rate is relevant to the extent of overloading. In other words, if there is a large overloading of element i, it will be tripped more rapidly compared to the case of a light overloading [99]. Based on this assumption, we can write $\lambda_i^1(t)$ as

$$\lambda_i^1(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \leq C_i \end{cases} \tag{4.7}$$

where $L_i(t)$ is the power loading of element i that can be found from the power flow calculation, C_i is the capacity of that element, and a_i is the basic unit rate (trippings per second). For normal operating condition, $\lambda_i^1 = 0$. In a cascading failure process, $\lambda_i^1 \gg \lambda_i^0$ [104]. Without loss of generality, we assume that $\lambda_i(t) \approx \lambda_i^1(t)$ in our analysis of cascading failures in power systems.

For the sake of completeness, we also allow a tripped or removed element to be repaired, and hence be restored to its normal connected state. Thus, we define $\mu_i(t)$ as the transition rate of element i going from state "1" to "0" as a result of repair actions or self-healing ability of the power system. In practice, an element's state cannot be switched arbitrarily. Also, the time delay for recovering a tripped element should be considered and can be included in the actual representation of $\mu(t)$. This recovery process can be used to study the power restoration process after the power blackout. In this chapter, we focus on analyzing the cascading failure process. Thus, considering that not all elements could be repaired in a short time and an element cannot keep changing its status frequently, we take $\mu_i(t)$ as 0 for a fast cascading process.

4.2.3 Power Flow Calculation

In addition to equation (4.7), power flow calculation is still needed for the analysis of cascading failures. Several algorithms and tools are available for computing power flows [64, 105]. The actual power system is a high-order complex nonlinear network, and any abrupt change of network structure can change the power flow distribution,

and at the same time cause large transients, oscillations, and bifurcations [106]. Using our definition of state transition of elements, the tripping probability of each element is an integration of the tripping rate (extent of overloading) with time. In this study, we assume that the system can always reach a steady state when tripping occurs and that the transient before the system reaches the next steady state is sufficiently short, making accumulative effects negligible. As far as the propagation of cascading failures is concerned, it suffices to consider blackouts caused by overloading, ignoring the nonlinear characteristics of the circuit elements and possible oscillatory behavior. In Chapter 3, a circuit-based power flow model that can accurately track the load change in a power network during a cascading failure has been developed . We adopt this model in the study here.

4.3 Failure Propagation in the Network

A power network is represented as an undirected graph G consisting of m elements. The state of G is defined as $S = \{s_1, s_2, ..., s_m\}$, which is a vector containing the states of all m elements. Network G can have 2^m possible network states, and any state transition of an element will lead to a network state transition of G.

The dynamic propagation of cascading failures in G is equivalent to the dynamic evolution of $S(t)$. Given the current state of the network, the network state transition can be described by (i) the time of the next state transition; and (ii) identification of the next element that will transit (be tripped).

4.3.1 Basics

First, we consider the network state transitions in an infinitesimal time interval dt. Suppose $S(t) = N_S$, which is a specific network state among the 2^m possible states. Thus, $S(t + dt)$ is the network state after a duration of dt. Only those elements in state "0"

may transit, leading to a network state transition. Let Ω_0 be the set of elements in state "0", and Ω_1 be the set of removed (tripped) elements. From elementary probability theory, we have the following basic results:

1) $o(dt)$ is the sum of the second and higher order terms of dt. Omitting $o(dt)$, the probability that no element undergoes a state transition after dt can be written as

$$\begin{aligned} P[S(t+dt) = N_S \,|S(t) = N_S\,] &= \prod_{i\in\Omega_0}[1-\lambda_i(t)dt)] \\ &= 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt + \sum_{x_1,x_2\in\Omega_0}\lambda_{x_1}(t)\lambda_{x_2}(t)(dt)^2 \\ &\quad - \sum_{x_1,x_2,x_3\in\Omega_0}\lambda_{x_1}(t)\lambda_{x_2}(t)\lambda_{x_3}(t)(dt)^3 + \cdots \\ &= 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt + o(dt) \approx 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt \end{aligned} \tag{4.8}$$

where $x_1, x_2, \cdots$ are the elements in Ω_0.

2) The probability that only one element state transition (say element k) occurs after dt, i.e., only element k transits, can be written as

$$\begin{aligned} P[S(t+dt) = M_S \,|S(t) = N_S\,] &= \lambda_k(t)dt \prod_{i\in\Omega_0\setminus\{k\}}[1-\lambda_i(t)dt] \\ &= \lambda_k(t)dt - \sum_{x_1\in\Omega_0\setminus\{k\}}\lambda_k(t)\lambda_{x_1}(t)(dt)^2 \\ &\quad + \sum_{x_1,x_2\in\Omega_0\setminus\{k\}}\lambda_k(t)\lambda_{x_1}(t)\lambda_{x_2}(t)(dt)^3 + \cdots \\ &= \lambda_k(t)dt + o(dt) \approx \lambda_k(t)dt \end{aligned} \tag{4.9}$$

where $x_1, x_2, \cdots$ are the elements in $\Omega_0 \setminus \{k\}$ and M_S denotes the network state that only one of the "0"-state elements in N_S becomes "1".

3) The probability that two or more element state transitions occur after dt is given by

$$P[S(t+dt) = R_S \,|S(t) = N_S\,] = 0 \tag{4.10}$$

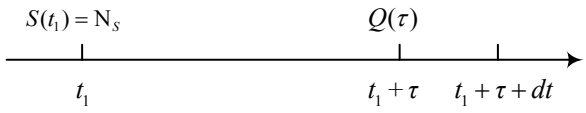


Figure 4.2: Time line of network state transitions.

where R_S denotes the network state that two or more of the "0"-state elements in N_S become "1". From equation (4.10), there is at most one element state transition at a time.

4.3.2 Extended Gillespie Method

In this section, we derive $S(t)$ using an extended Gillespie method [107], which was used for analyzing coupled chemical reactions [100, 101].

As shown in Fig. 4.2, the state of the power system at t_1 is N_S, i.e., $S(t_1) = N_S$. Let $Q(\tau)$ denote the probability that given $S(t_1) = N_S$, no transition occurs in $(t_1, t_1 + \tau)$, i.e.,

$$Q(\tau) = P[S(t_1 + \tau) = N_S \,|S(t_1) = N_S\,]. \tag{4.11}$$

Similarly, $Q(\tau + dt)$ can be written as

$$\begin{aligned} Q(\tau + dt) &= P[S(t_1 + \tau + dt) = N_S \,|S(t_1) = N_S\,] \\ &= P[S(t_1 + \tau + dt) = N_S \,|S(t_1 + \tau) = N_S\,]Q(\tau). \end{aligned} \tag{4.12}$$

Given $S(t_1) = N_S$, power flow calculation can be performed, as described in Section 4.2.3, and $\lambda_i(t_1)$ can be derived based on the settings in Section 4.2.2. If no state transition occurs during time interval $(t_1, t_1 + \tau)$, we have $S(t) = S(t_1)$ and $\lambda_i(t) = \lambda_i(t_1)$ for $t \in (t_1, t_1 + \tau)$. From (4.8), we get

$$P[S(t_1 + \tau + dt) = N_S \,|S(t_1 + \tau) = N_S\,] = 1 - \sum_{i \in \Omega_0} \lambda_i(t_1)dt. \tag{4.13}$$

Thus, by putting (4.13) in (4.12), we get

$$Q(\tau + dt) = Q(\tau)(1 - \lambda^*(t_1)dt), \tag{4.14}$$

where $\lambda^*(t_1) = \sum_{i\in\Omega_0} \lambda_i(t_1)$. Furthermore, re-arranging (4.14) and taking the limit $dt \rightarrow 0$, we get

$$\begin{aligned} &\frac{dQ(\tau)}{d\tau} = \lim_{dt\to 0} \frac{Q(\tau + dt) - Q(\tau)}{dt} = -\lambda^*(t_1)Q(\tau), \\ &\Rightarrow Q'(\tau) = -\lambda^*(t_1)Q(\tau). \end{aligned} \tag{4.15}$$

The probability that nothing happens in zero time is one, i.e., $Q(0) = P\{S(t_1) = N_S \,|S(t_1) = N_S\} = 1$. Then, the analytical solution of (4.15) is

$$Q(\tau) = e^{-\lambda^*(t_1)\tau}. \tag{4.16}$$

Let $h_i(\tau, dt)$ denote the probability of the event that given $S(t_1) = N_S$, the next transition occurs in the interval $(t_1 + \tau, t_1 + \tau + dt)$ in element i. There are two conditions for this event to occur. The first condition is that there is no state transition during $(t_1, t_1 + \tau)$. The second condition is that a state transition occurs in element i during $(t_1 + \tau, t_1 + \tau + dt)$. Thus, $h_i(\tau, dt)$ can be written as

$$h_i(\tau, dt) = P[S(t_1 + \tau + dt) = M_S \,|S(t_1 + \tau) = N_S\,]Q(\tau). \tag{4.17}$$

Putting (4.9) and (4.16) in (4.17), we get

$$h_i(\tau, dt) = e^{-\lambda^*(t_1)\tau}\lambda_i(t_1)dt. \tag{4.18}$$

Let $H(\tau, dt)$ denote the probability that the next transition occurs in the time interval

$(t_1 + \tau, t_1 + \tau + dt)$, given $S(t_1) = N_S$. It is readily shown that

$$H(\tau, dt) = \sum_{i \in \Omega_0} h_i(\tau, dt) = \lambda^*(t_1) e^{-\lambda^*(t_1)\tau} d\tau. \tag{4.19}$$

Further, let τ denote the time interval between two adjacent network state transitions, and $f(\tau)$ denote the *state transition probability density function* (PDF):

$$f(\tau) = \lim_{dt \to 0} \frac{H(\tau, dt) - H(\tau, 0)}{dt} = \lambda^*(t_1) e^{-\lambda^*(t_1)\tau} \tag{4.20}$$

i.e.,

$$f(\tau) = \lambda^*(t_1) e^{-\lambda^*(t_1)\tau}. \tag{4.21}$$

The accumulative probability density function that the next transition occurs before time $t_1 + \tau$, given $S(t_1) = N_S$, can be written as

$$F(\tau) = \lambda^*(t_1) \int_0^\tau e^{-\lambda^*(t_1)t} dt = 1 - e^{-\lambda^*(t_1)\tau}. \tag{4.22}$$

Note that one can also get $F(\tau)$ from $F(\tau) = 1 - Q(\tau)$.

Equations (4.21) and (4.22) show that τ follows an exponential distribution and that the network transition rate is $\lambda^*(t_1)$. Here, $\lambda^*(t_1)$ is the sum of the element state transition rates of all the working elements in the network, and is determined by the sum of the extents of overloading of all the overloaded elements. The time interval τ is expected to be short when $\lambda^*(t_1)$ is large, i.e., the network state transition (cascading process) occurs very rapidly. Thus, the physical meaning of $\lambda^*(t_1)$ can be interpreted as the overloading stress of the entire power system.

In order to include this characteristic in our model, we take the following steps to determine the time of the next network state transition, given $S(t_1) = N_S$:

1. A random number z_1 is generated uniformly in (0,1).

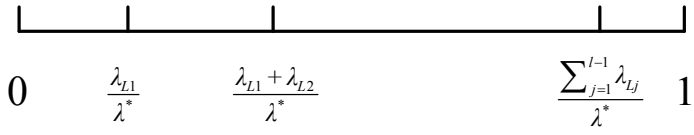


Figure 4.3: Relative probability for elements in Ω_0 to be first tripped given $S(t_1) = N_S$.

2. Let $F(\tau) = z_1$, and τ is derived as

$$\tau = \frac{ln(1 - z_1)}{-\lambda^*(t_1)}. \tag{4.23}$$

4.3.3 Order of State Transition

A number of working elements (elements in Ω_0) can possibly undergo state transition. In our analysis presented in Section 4.3.1, we allow only one element to be removed (tripped) at a time. Pfitzner *et al.* [108] pointed out that the order in which overloaded lines are tripped influences the cascade propagation significantly. In this section, we study the order in which element state transitions take place.

In our stochastic model, any overloaded element in Ω_0 may be tripped first. From a probabilistic viewpoint, the element with a higher $h_i(\tau, dt)$ will more likely be tripped first. Thus, we define the *relative probability* for element i ($i \in \Omega_0$) to be tripped first as:

$$rf_i = \frac{h_i(\tau, dt)}{H(\tau, dt)} = \frac{\lambda_i(t_1)}{\lambda^*(t_1)}. \tag{4.24}$$

where $\lambda^*(t_1) = \sum_{i\in\Omega_0} \lambda_i(t_1)$. Our model can incorporate this tripping order using the following steps:

1. A random number z_2 is generated uniformly in (0,1).

2. Suppose there are l overloaded elements in Ω_0. With no loss of generality and for ease of referral, let these overloaded elements be elements $L1, L2, \ldots, Lj, \ldots, Ll$.

Figure 4.3 shows the relative probability of an overloaded element in Ω_0 to be first tripped, given that $S(t_1) = N_S$.

3. The jth element in Ω_0 is selected to be tripped according to

$$\sum_{k=0}^{j-1} \frac{\lambda_{Lk}}{\lambda^*} \leqslant z_2 < \sum_{k=0}^{j} \frac{\lambda_{Lk}}{\lambda^*}, \tag{4.25}$$

where $\lambda_{L0} = 0$.

4.4 Cascading Failure Simulations and Parameters

In this section we describe the simulation algorithm and some important characterizing parameters of our model that are relevant to predicting the occurrence of power blackouts.

4.4.1 Simulation Algorithm

Figure 4.4 shows the flow chart for simulating the cascading failure process which can be summarized as follows:

1. *Initial Settings:* At the start of the simulation, all voltages at the power generation stations, currents flowing into the consumer nodes, admittances of the transmission lines, and capacities of elements are set.

2. *Initial Failure:* An initial failure is planted by removing one element from the network, which triggers the cascading failure process.

3. *Iterative Process:* Based on $S(t)$, we remove the tripped elements from the network, and keep all elements whose states is "0". The remaining network may be disconnected, forming so-called islands, due to the removal of the tripped elements. For a disconnected sub-network (island) containing no generator node,

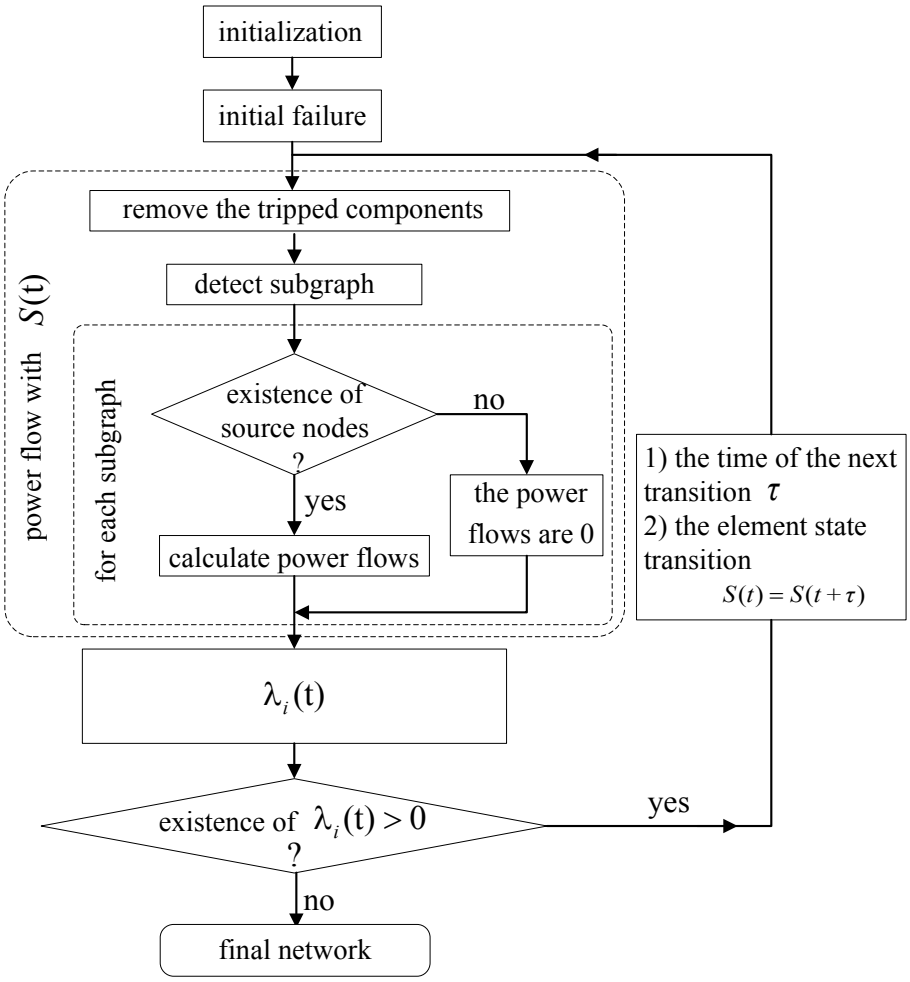


Figure 4.4: Flow chart for simulating the dynamic propagations of cascading failures.

all elements within it would have no access to power and all power flows become zero. All nodes in this sub-network are *unpowered*. Note that these elements are not tripped, and their states are still "0". Moreover, for a sub-network containing at least one generator node, equation (3.6) can be used to compute the power flow distribution in this sub-network. Power flows of all the "0"-state elements in G can be computed, and the tripping rate of each element λ_i can be obtained using (4.7). If all tripping rates are positive, we determine the next network state. Specifically, we first determine the time of the next network state transition using (4.23), and determine the element in Ω_0 that will be tripped next. The network state transition is determined using (4.25). Then, we update $S(t) = S(t+\tau)$, and

iterate the process until all the transition rates are found to be zero (i.e., no overloaded elements). With no more overloaded elements in the network, no state transition will occur and $S(t)$ is a stable state. We can then end the simulation and get the final network.

4.4.2 Parameter Settings and Metrics

The time of the initial failure is set as zero, and the time of the final network state transition (after which there are no overloaded elements in the network, and the network state enters a stable point) is t_{final}. Using the above algorithm, we can simulate the dynamic profile of $S(t)$ for power network G, from $t = 0$ to $t = t_{\text{final}}$. For $t > t_{\text{final}}$, $S(t)$ remains unchanged. The dynamic profile of $S(t)$ is thus the dynamic propagation of cascading failures in the network. In order to better represent and visualize the characteristics of the dynamics of a cascading failure, we use the following metrics, which are extracted from $S(t)$.

We propose several metrics to investigate the cascading failure in a power system.

First, to characterize the propagation profile of a cascading failure in a power system, the cumulative number of tripped elements at time t (NoTE(t)) is used. Here, we take NoTE(t) as the number of "1"-state elements in $S(t)$. Also, the number of elements not served is another important metric used to measure the blackout size. As the power grid's operation depends on the connection of the elements, the tripping of some elements in the network can disconnect the grid and island the consumer nodes from the power sources. These nodes are being deprived of power, and are labelled as *unpowered nodes* in our analysis. We use NoUN(t) to denote the number of cumulative unpowered nodes at t. To find NoUN(t), we remove the tripped elements in G, and identify all sub-networks in the remaining part of G. The consumer nodes that are isolated from generators are all unpowered nodes.

Furthermore, during a cascading failure process, it is particularly important to track

the growing rate of the number of failed or tripped elements, i.e., the frequency of removal or tripping of overloaded elements. Specifically, any rapid increase in the frequency of removal of overloaded elements is a precursor to an onset of a large blackout. Thus, a metric that effectively gives the critical time from which tripping begins to take place more rapidly is extremely relevant to prevention of power blackouts. This metric, called *onset time* (t_{onset}) here, can simply be defined as the time after which the propagation rate of the cascading failure increases rapidly, as depicted in Fig. 4.5. In other words, t_{onset} is a critical time point before which remedial control and protection actions should be applied to the power grid. After t_{onset}, the power grid undergoes a short phase of very rapid tripping of overloaded elements leading to large power blackout within a very short time. To compute the onset time, we identify the maximum rate of the growing profile by solving $d^2\text{NoTE}(t)/dt^2 = 0$, which gives $t = t_{\text{m}}$ as the time point where the growing rate is highest. Assuming that the value of $d\text{NoTE}(t)/dt$ at $t = t_m$ is g_m and the initial phase has a very slow growing rate, the onset time is simply given by

$$t_{\text{onset}} = t_m - \frac{\text{NoTE}(t_m)}{g_m} \tag{4.26}$$

In practice, we can use any handy algorithm to find t_{onset}, for instance, by locating the time instant where $d\text{NoTE}(t)/dt$ starts to increase rapidly. Section 4.5.2 offers one simple algorithm.

Finally, to characterize the general severity in the event of a possible blackout, we use the following statistical metric. Suppose a large number of cascading failure cases, initialized by failures of different elements in the network, are simulated. The probability that the blackout size of a randomly picked case is larger than a chosen threshold BS (Blackout Size) is given by

$$P[x(t) \geq \text{BS}] = \frac{n[x(t) \geq \text{BS}]}{n} \tag{4.27}$$

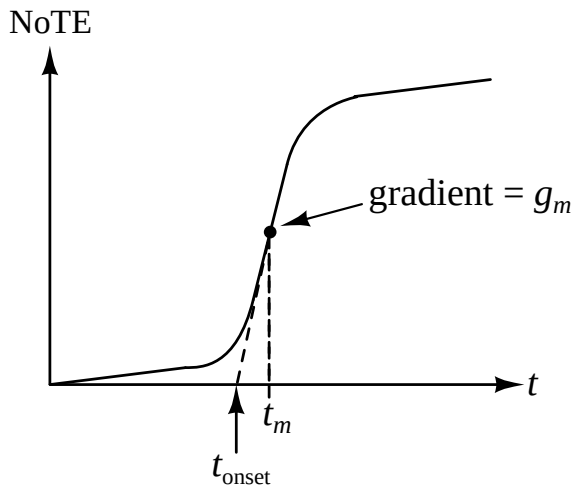


Figure 4.5: Typical propagation profile and onset time t_{onset}. Maximum propagation rate g_m occurs at $t = t_m$.

where $x(t)$ can be NoTE(t) or NoUN(t), n is number of the total blackout cases simulated, and $n[x(t) \geq \text{BS}]$ is the number of cases whose blackout size at t is larger than BS. Based on (4.27), we can evaluate the cumulative blackout size distribution of a network to reveal the probability (risk) of having a blackout of a specific level of severity in a given network.

4.5 Application Case Study

In this section, we simulate cascading failures in the UIUC 150 Bus System using the model proposed above. The UIUC 150 Bus is a power test case offered by Illinois Center for a Smarter Electric Grid at UIUC [109]. It contains 150 buses and 217 links that operate in 3 different voltage base values. We merge the parallel lines that connect the same two buses into one link, resulting in 203 links in our simulation. We assume that the current sinks of the consumer buses given in the UIUC 150 Bus are the normal load demands of these consumers. The voltages of generators are all 1.04 p.u. based on the data in the test case.

From the historical blackout reports [89, 90], one can find that the tripped elements

are mostly generators, transmission lines and transformers. Thus, in our simulation, we set current limits for the transmission lines, transformers and the generators according to $C_i = (1 + \alpha) * I_i(\text{normal})$, where $I_i(\text{normal})$ is the current flowing through a transformer or a transmission line, or the total current flowing out of a generator under normal load demand condition; α is the safety margin and is set to 0.2. The current limits of other elements (consumer buses and distribution buses) are set to values that are large enough to avoid tripping during a cascading failure.

4.5.1 Dynamics of Cascading Failure Propagation

We first study the failure spreading during a blackout process. Figure 4.6(a) shows the profile of cumulative tripped elements of the blackout in the Western North American system in July 1996 [89]. The blackout started from the failure of the 345 kV Jim Bridger-Kinport line (the time of that initial failure is 0 in the figure). As shown in the Fig. 4.6(a), NoTE grew very slowly, at the initial phase, until the failing of the 230 kV Brownlee-Boise Bench line at 1600 seconds after the initial failure. Then, the cascading failure speeded up abruptly, and within 380 seconds, NoTE reached 33 from 6 at the end of the initial phase. Finally, the cascading failure settled at a final state where 34 major elements were tripped, depriving 10% consumers of the Western interconnection area from access to electrical power. Figure 4.6(b) shows the profile of NoTE in another blackout of the same power system that occurred in August 1996. The cascading failure was triggered by the failure of the 500 kV Big Eddy-Ostrander line, and then continued with a sequence of tripping of elements. In almost the same fashion, the cascading failure propagated slowly at the beginning, but 6000 seconds later, the propagation rate accelerated sharply. The main propagation finished in 120 seconds. The 2003 American-Canada blackout [90] also showed a similar growing pattern, with NoTE growing very slowly for the initial 4 hours and then accelerating rapidly to its final state. The rapid increase in NoTE occurred in a few minutes, which

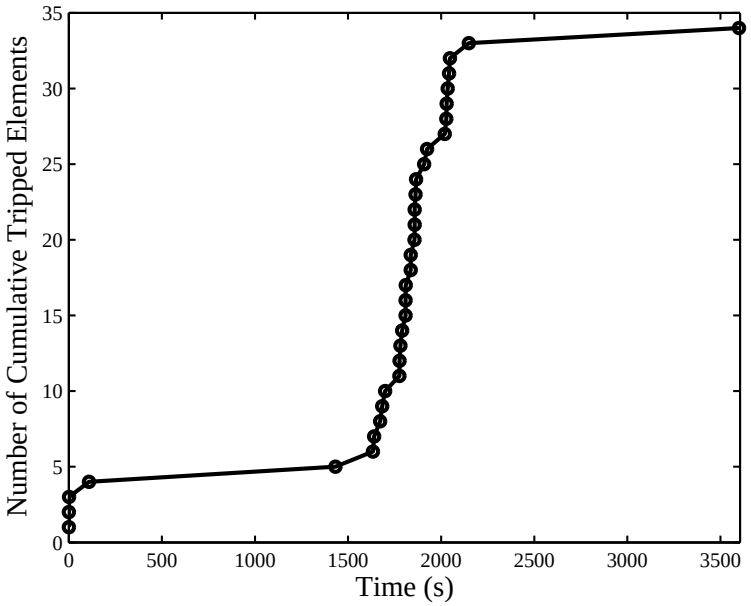
Table 4.1: Simulation results for the cascading failure triggered by the failure of line (2, 21)

Loading condition	NoTE(t_{final})	NoUN(t_{final})	t_{final} (s)
Normal loading	5	2	967
5% Load increase	25	36	3600

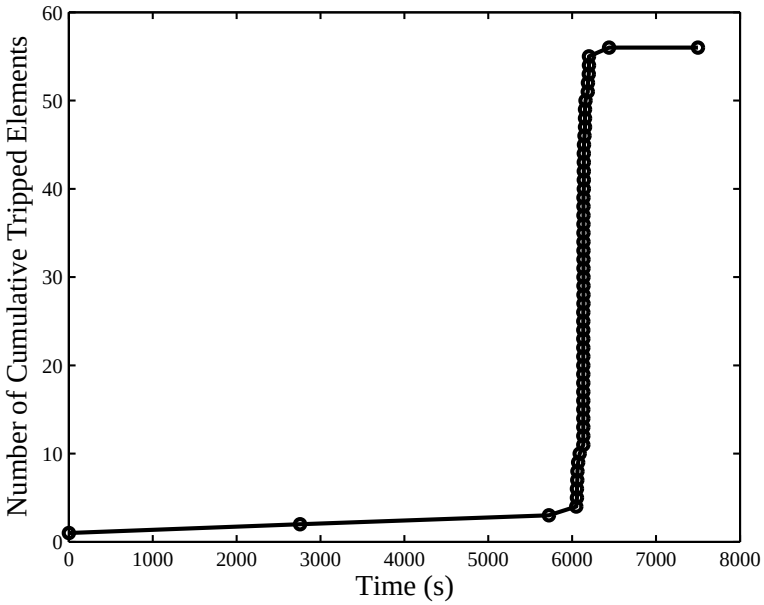
was a small fraction of the whole cascading period $(0, t_{\text{final}})$.

In the following, we use the proposed stochastic model to simulate the dynamic propagation of cascading failures triggered by the failure of one single line. First, we simulate 100 different propagation profiles of the cascading failure process triggered by the initial failure of line (2, 21), under a normal load demand condition and the condition with 5% increase in load demands. Note that when the loading of the power system is increased by 5% and $S(t = 0) = \mathbf{0}$, there are no overloaded elements, i.e., the 5% increase in load demands will not cause any outage in the power grid. From the data of historical blackouts, the time duration of the failure propagation is usually between 1 hour and 4 hours. In this simulation, we use a uniform a_i for all the elements in the UIUC 150 Bus system, and fit a_i to make the averaged t_{final} of the 100 simulated results under the condition of 5% increase in load demands to be 3600 s. Thus, a_i is set as 0.035 s^{-1} in our simulation. Table 4.1 lists the averaged simulated values of NoTE(t_{final}), NoUN(t_{final}) and t_{final}. From Table 4.1, we see that under a normal load demand condition, the failure of line (2, 21) will not cause severe disturbance to the power system. When the network is stressed by heavier loads, the failure of the same transmission line can lead to a large blackout in the power system.

Table 4.2 lists the sequence of the element tripping events in one simulated cascading failure process under the condition of 5% increase in load demand. We plot the profiles of NoTE and NoUN in Fig. 4.7(a), which display the same typical growing pattern as the historical blackout data. Using equation (4.21), the growth rate of the cascading failure is determined by $\lambda^*(t)$. Figure 4.7(b) shows the values of $\lambda^*(t)$

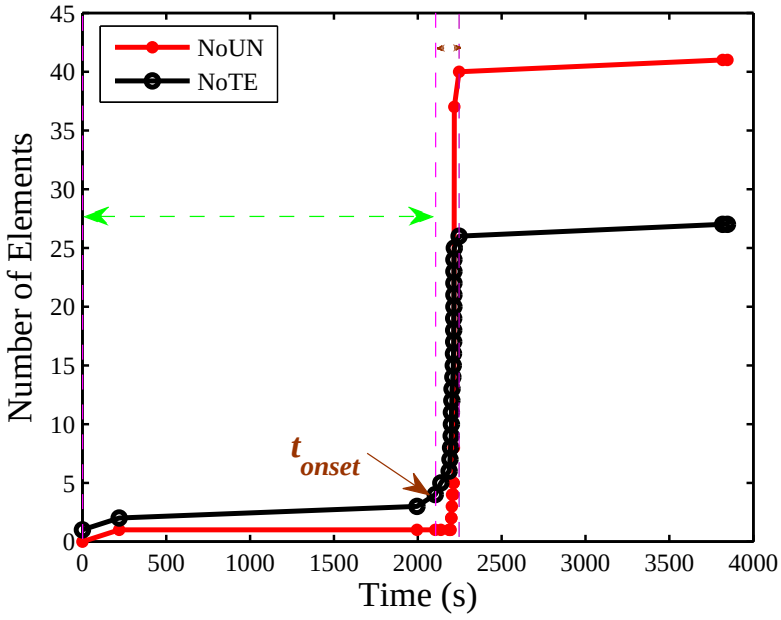


(a)

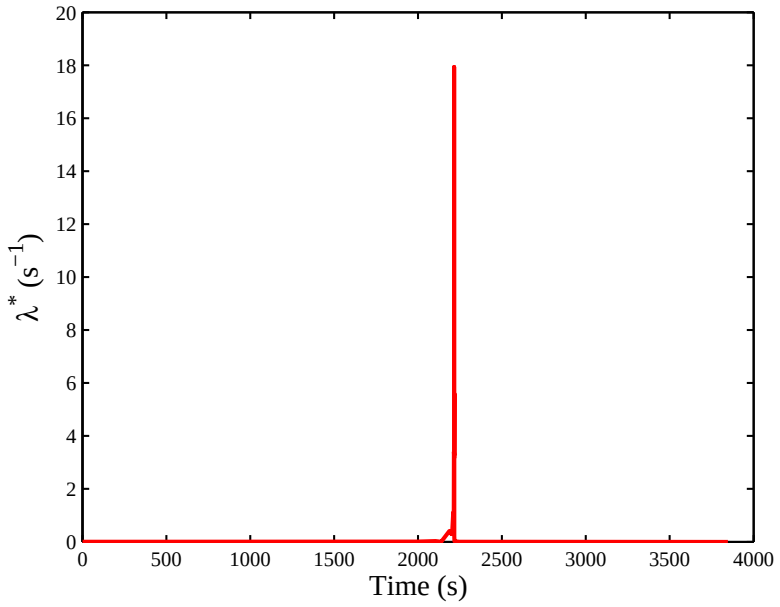


(b)

Figure 4.6: Propagation profile of the Western North America power blackout in (a) July 1996; (b) August 1996.



(a)



(b)

Figure 4.7: Simulation of the dynamics of a cascading failure event in the UIUC 150 Power System caused by an initial failure of line (2, 21). (a) NoTE and NoUN; (b) λ^*.

Table 4.2: Sequence of element tripping events

Sequence Number	Time	Unit/Line
1	0.000s	Line (2, 21) is tripped.
2	220.035s	Line (2, 14) is tripped.
3	1995.531s	Line (108, 101) is tripped.
4	2104.394s	Line (96, 102) is tripped.
5	2137.931s	Line (8, 23) is tripped.
6	2187.153s	Line (142, 101) is tripped.
7	2191.648s	Line (3, 19) is tripped.
8	2195.871s	Line (10, 25) is tripped.
9	2199.473s	Line (144, 116) is tripped.
10	2199.971s	Line (15, 17) is tripped.
11	2200.115s	Line (9, 39) is tripped.
12	2203.461s	Line (144,117) is tripped.
13	2204.694s	Generator 1 is tripped.
14	2209.551s	Line (88, 147) is tripped.
15	2211.713s	Line (16, 26) is tripped.
16	2212.815s	Generator 118 is tripped.
17	2213.497s	Line (89, 26) is tripped.
18	2217.194s	Line (114, 119) is tripped.
19	2214.603s	Line (68, 85) is tripped.
20	2214.909s	Line (137, 95) is tripped.
21	2215.02s	Line (148, 95) is tripped.
22	2215.073s	Line (65, 73) is tripped.
23	2215.649s	Line (22, 29) is tripped.
24	2215.669s	Line (6, 28) is tripped.
25	2217.261	Line (17, 21) is tripped.
26	2246.489s	Line (69, 87) is tripped.
27	3817.977s	Line (69, 70) is tripped.

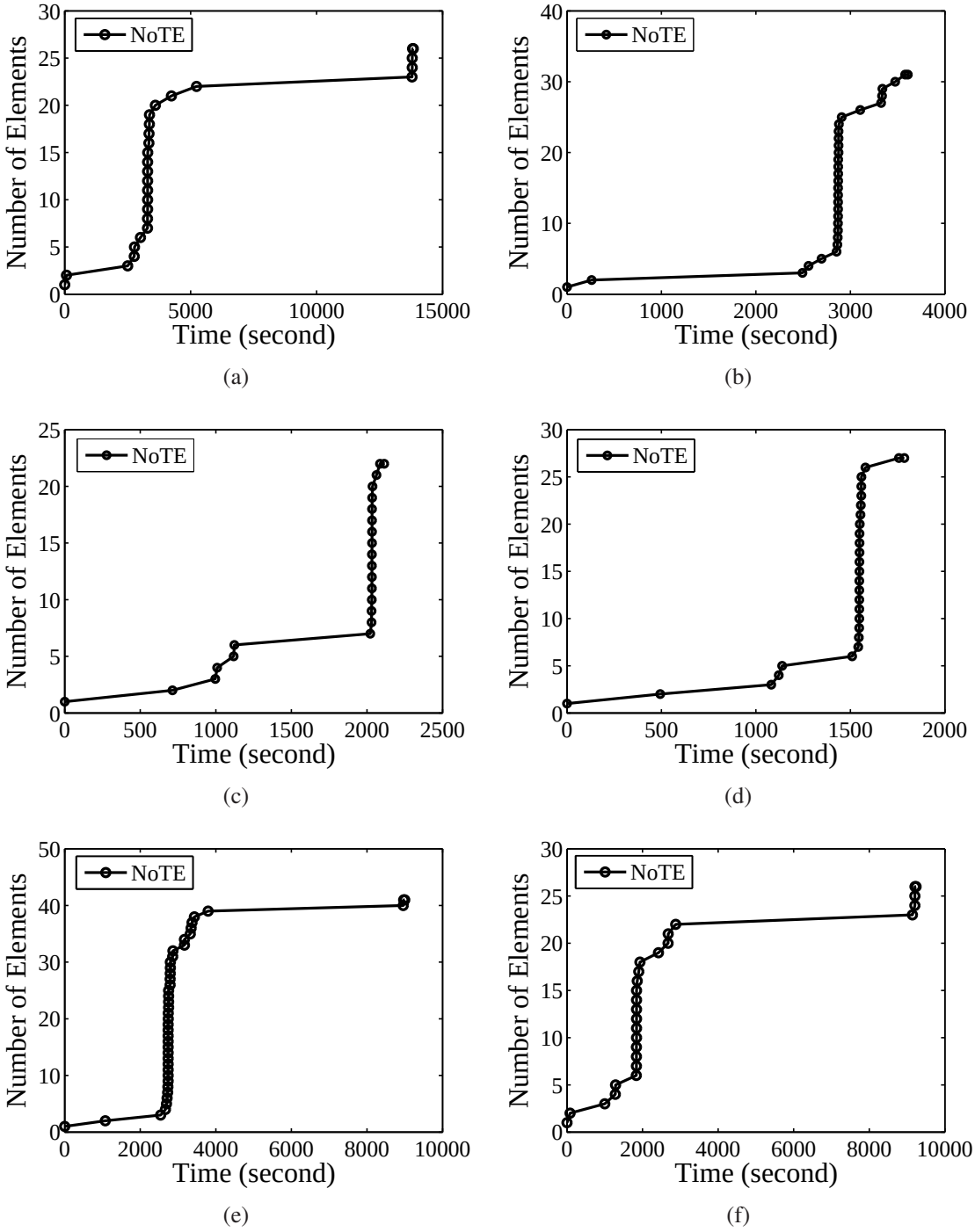
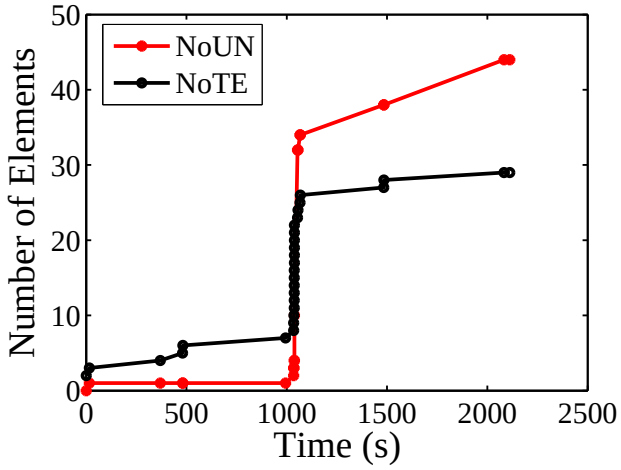
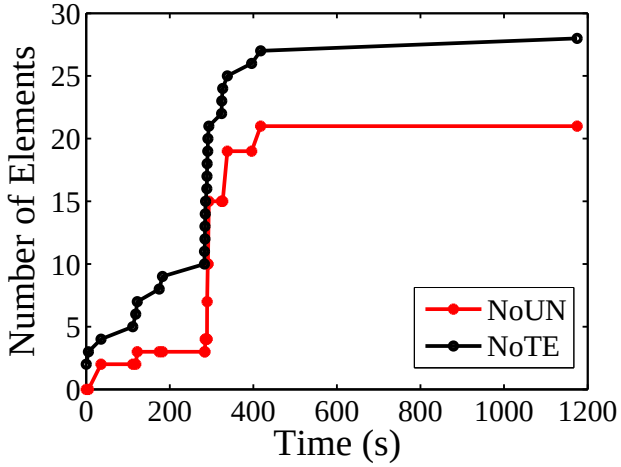


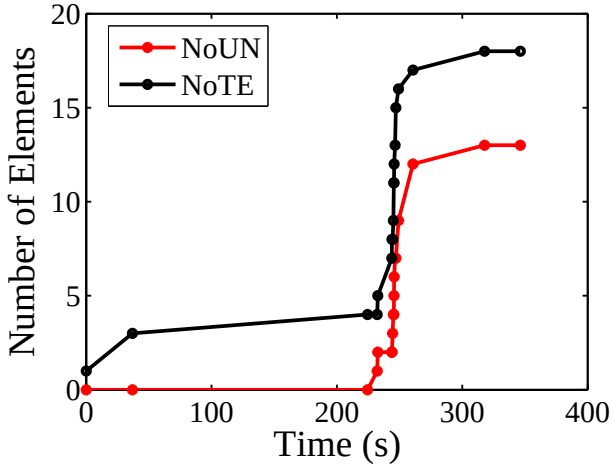
Figure 4.8: Simulation of failure propagations in UIUC 150 Bus power system with initial tripping of line $(2, 21)$ using the proposed model. (a)-(f) Six separate simulation runs.



(a)



(b)



(c)

Figure 4.9: Simulation of failure propagation initiated by (a) failure of line (2, 14) in UIUC 150 Bus; (b) failure of line (34, 35) in UIUC 150 Bus; (c) failure of line (103, 105) in IEEE 118 Bus.

throughout the simulated cascading process. Initially, the value of $\lambda^*(t)$ is relatively small, until the breakdown of some critical elements, its value increases very rapidly. This means that the power network operates under a high overloading stress. When the stress comes down again, the propagation slows down. The tripping of elements ceases when $\lambda^*(t)$ reduces to 0, and the network reaches its final condition. The consistency of our simulated cascading failure process with the historical data verifies the validity of our model in describing realistic blackout processes. The following two key issues should be noted.

(1) We use stochastic methods to investigate the cascading failure propagation. Our model takes into consideration the high complexities as well as uncertainties of the involving mechanisms which can be investigated with probabilistic methods. The tripping rates of the elements are related to the overloading extents of the corresponding elements and the more heavily overloaded ones will be more likely to be tripped first. Equations (4.23) and (4.25) incorporate these considerations. Thus, for the same system and same initial failure, different simulations may yield different results due to the stochastic nature of the model. Figure 4.7 is one particular simulation run of the UIUC 150 Bus with initial failure of line (2, 21). Furthermore, Figs. 4.8 (a)-(f) show results derived from 6 other simulation runs. From Fig. 4.8, we can see that these 6 sets of results share the same characteristic profile, where the growing rate of the blackout size is uneven and a relatively slow initial phase is followed by a sharp escalation of cascading failures.

(2) From our simulations, we observe cascading failure patterns as shown in Fig. 4.7. Figures 4.9 (a) and (b) show the simulated cascading failure propagation in the UIUC 150 Bus initiated by the failure of line (2, 14) and the failure of line (34, 35), respectively. Figure 4.9 (c) shows the simulated cascading failure propagation in the IEEE 118 Bus initiated by the failure of line (103, 105). It should be noted that not all initial failures will generate such cascading failure profiles. In fact, the initial failure of some elements will not cause further cascading failures at all. Another extreme case

Table 4.3: Confidence intervals of t_{onset}

Confidence Level	Confidence Interval (sec)
90%	(543, 3747)
95%	(451, 4327)
99%	(286, 5705)

is that initial failure of some crucially important element in the network will make all other elements to be unpowered instantly. For instance, the initial failure arises from a generator which is the only generating unit in its power network. Moreover, the failure propagation profile shown in Fig. 4.7 is unique for power systems, which is determined by the specific failure spreading mechanism. Such profile is not normally observed in other failure spreading mechanisms, such as disease propagations in human networks, rumor spreading on the Internet, and so on.

4.5.2 Blackout Onset Time

To evaluate t_{onset}, we adopt an intuitive algorithm that locates the time point at which NoTE begins to escalate rapidly. Suppose this time point is t_k which corresponds to the time when the kth element is tripped. The gradient of NoTE before this time point is $g_i = (k-1)/t_k$, and the gradient of NoTE after this time point is $g_m = w/(t_{k+w}-t_k)$, where w is an arbitrary additional number of elements tripped after the kth time point for the purpose of computing the gradient. We compare the two gradients, and if $g_m > \gamma g_i$, where $\gamma > 0$, we accept this kth time point as the onset time.

We perform 10,000 simulations of cascading failures triggered by removal of line (2, 21). In our algorithm, we use $w = 10$ and $\gamma = 50$ to find t_{onset} of these 10,000 simulation runs and analyze the probability density function of t_{onset}. From Fig. 4.10, we see that there is a peak in the interval (1200 s,1400 s), implying that t_{onset} is more likely to be around 1300 s. Also, Monte Carlo method is applied to derive the confidence interval of t_{onset} for three different confidence levels, as listed in Table 4.3. It should

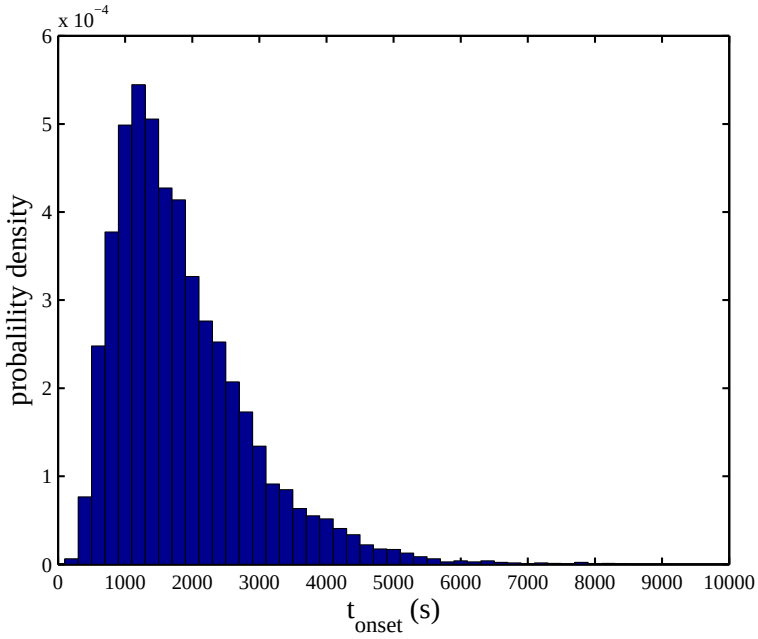


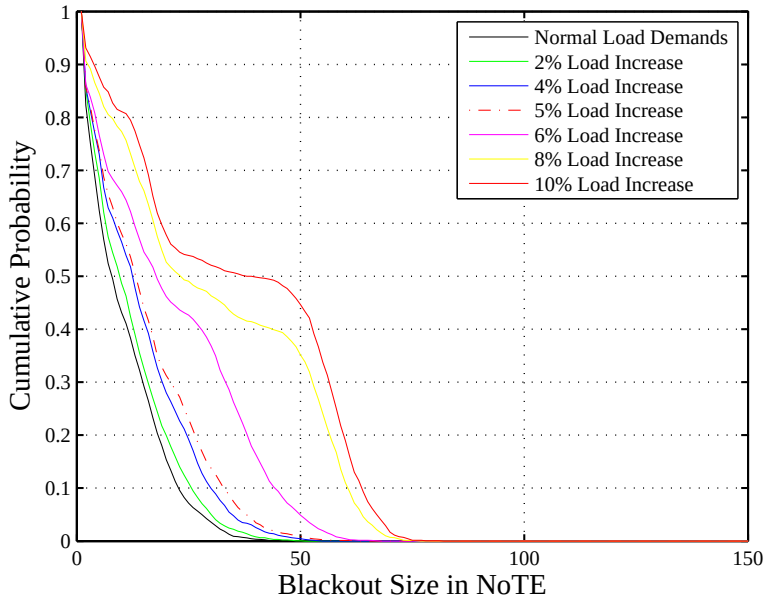
Figure 4.10: Probability density function of t_{onset}.

be noted that the t_{onset} distribution shown in Fig. 4.10 is only valid for the cascading failures in the UIUC 150 Bus power system with initial failure of line (2, 21). Different systems should have different t_{onset} distributions, which should be derived from computation on the specific power systems.

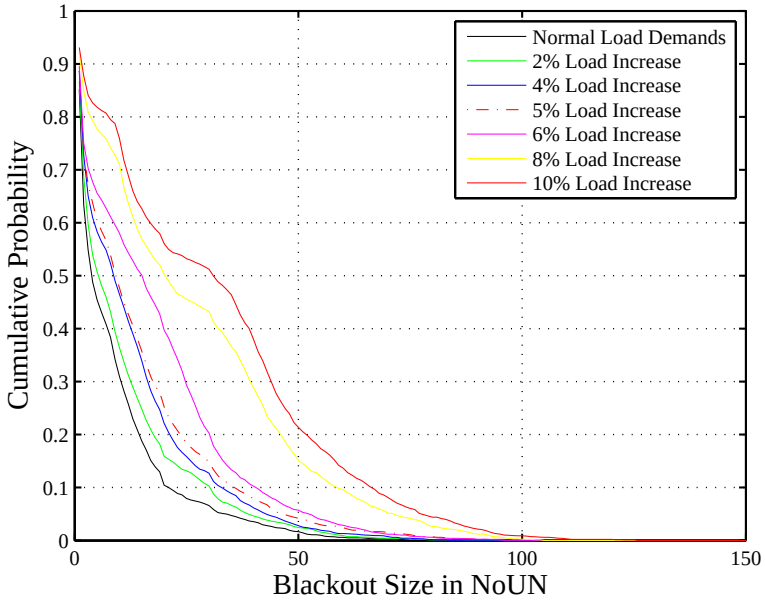
4.5.3 Effects of Heavy Load Demands

Another common characteristic of the three historical blackouts is that they all took place in the hot summer when the power demand is high. In this section, we investigate the overall influence of load demands on blackout risk of a power network. The cumulative blackout size distribution is used to indicate the risk of severe power blackouts of the power system.

Under a normal load demand condition, we simulate 10 profiles of cascading failure triggered by the failure of each line. Thus, we have altogether 2030 blackout cases for the UIUC 150 Bus System. Then, we analyze the profile data of these 2030 blackouts. The cumulative distributions of NoTE(t_{final}) and NoUN(t_{final}) are plotted us-



(a)



(b)

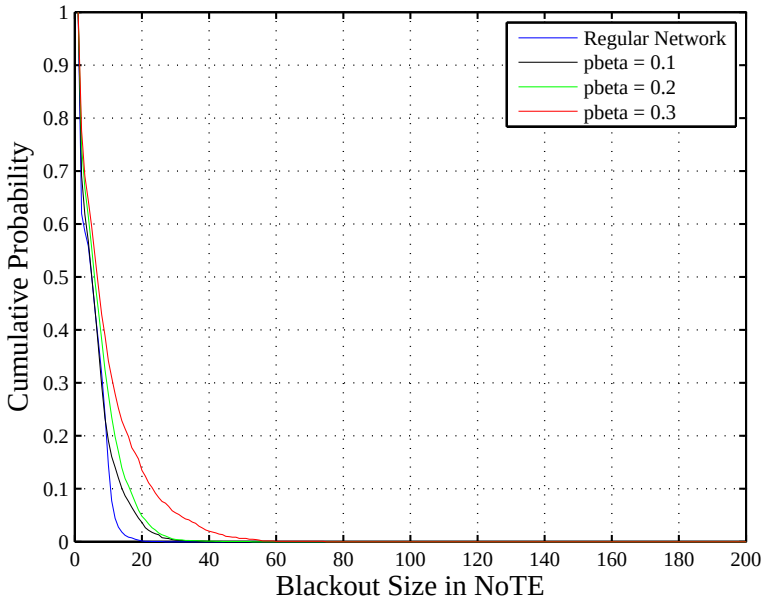
Figure 4.11: Cumulative blackout size distributions of UIUC 150 Power System. Blackout size measured in (a) NoTE; (b) NoUN.

ing equation (4.27). These simulations are repeated for the conditions that the load demands are increased by various percentages. Figures 4.11(a) and (b) show the cumulative distributions for NoTE(t_{final}) and NoUN(t_{final}) of the UIUC 150 Bus System under several different load demand conditions. Specifically, all simulated cascading failures will result in NoTE(t) > 0, as any cascading failure simulation has a tripped element as initial failure. Thus, for BS threshold = 0, $P[x(t) \geq 0] = 1$ where x(t) is NoTE(t). We see that under a normal load condition, the probability of large blackouts of the UIUC 150 Bus System is relatively low. However, when the load demands are increased, the probability of large blackouts increase significantly. We also observe that the probability of having severe blackouts does not grow in linearly with the growth of load demands. From Figs. 4.11(a) and (b), $P[x(t_{\text{final}}) \geq \text{BS}]$ grows relatively slowly relatively when the load demand increases by less than 5%, but more rapidly when the load demand increases by 5% to 10%.

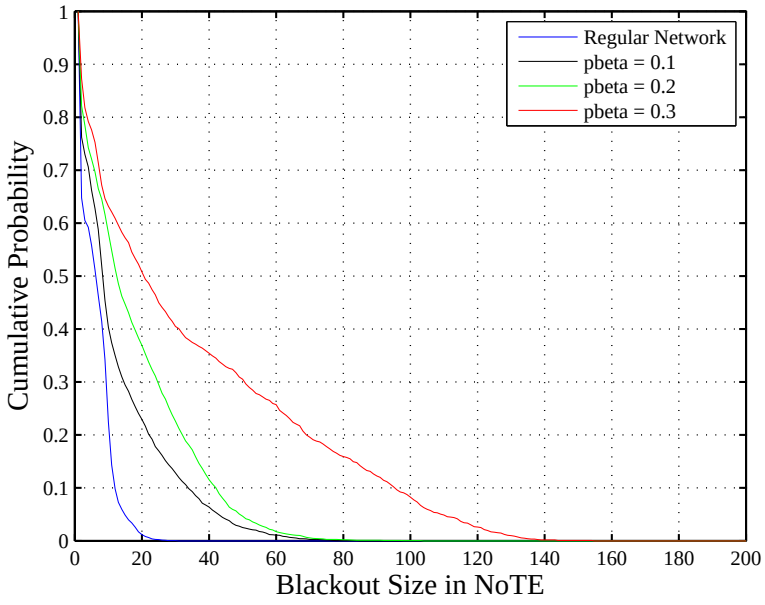
4.5.4 Effects of Network Structure

It has been shown that the network topology plays a significant role in determining the dynamics of propagation and spreading of disease or information in networks [5]. It is shown that the topological characteristics of many real-world power systems are not uniform [15]. Thus, it is meaningful to investigate the relationship between network structure and functional properties of power systems, and to identify better connectivity styles.

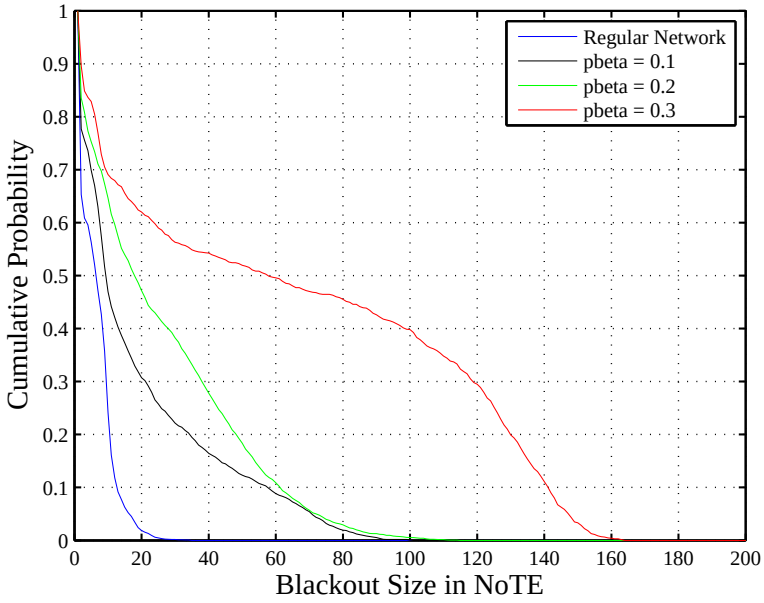
Regular networks and small-world networks are used as test power systems for comparison purposes. A regular network is generated with 150 nodes, each node's degree being 4. We allocate 30 generators in the regular network, whose voltages are set as 1.04 p.u. The remaining nodes are consumer nodes, each sinking 0.3 p.u. of current, and the admittances of all links in this network are set as 2×10^3 p.u. Then, we generate 3 small-world networks by rewiring the links in the regular network with


Regular Network
pbeta = 0.1
pbeta = 0.2
pbeta = 0.3
Cumulative Probability
Blackout Size in NoTE
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
20
40
60
80
100
120
140
160
180
200

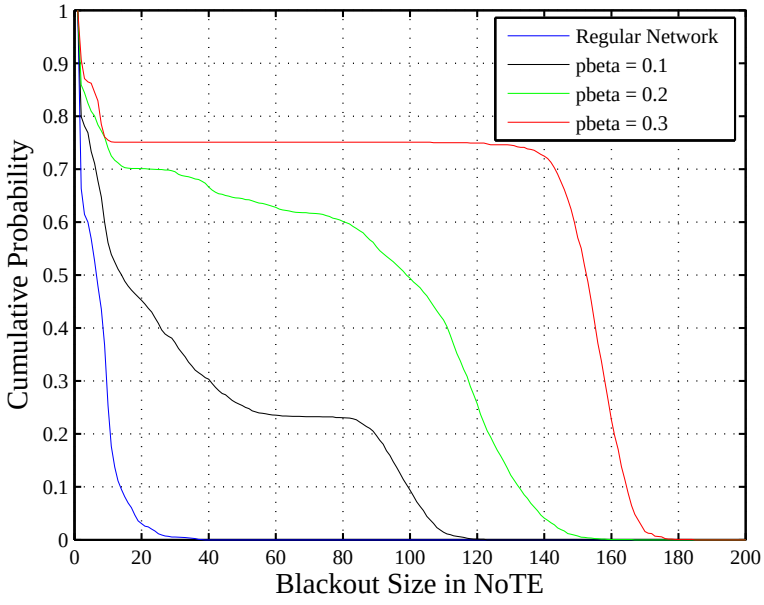
(a)


Regular Network
pbeta = 0.1
pbeta = 0.2
pbeta = 0.3
Cumulative Probability
Blackout Size in NoTE
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
20
40
60
80
100
120
140
160
180
200

(b)



(c)



(d)

Figure 4.12: Cumulative blackout size distributions. (a) t = 100 s; (b) t = 500 s; (c) t = 1000 s; (d) $t = t_{\text{final}}$. "pbeta" is rewiring probability for generating small-world networks.

rewiring probabilities 0.1, 0.2 and 0.3 [5].

For each test network, we increase the consumers' load demands by 5%, and then simulate 10 profiles of the cascading failure initiated by the failure (removal) of each line. We plot the cumulative blackout size distributions for the 4 networks based on equation (4.27). Figure 4.12(d) shows the cumulative distribution of NoTN(t_{final}), and we see that the risk of large final blackouts is higher for small-world networks than for regular ones. In order to show the speed of the propagations in these networks, we plot the accumulative distributions of NoTE at different time points. Figures 4.12(a), (b) and (c) show the cumulative distributions of NoTE at 100 s, 500 s and 1000 s, respectively. For the same duration $[0, t_0]$, a higher value of $P\{\text{NoTE}(t_0) \geq \text{BS}\}$ for the same BS indicates a faster speed of cascading. From Fig. 4.12, we can conclusion that the cascading failure propagates faster in small-world networks than in regular networks.

4.6 Summary

In this chapter, we develop a model to investigate the dynamics of the cascading failure processes in power systems, combining deterministic power flow equations and stochastic time duration descriptions. An extended chemical master equation method is adopted to analyze the network failure dynamics. It has been verified that the model produces propagation profiles that contain the key features displayed in historical blackout data. We studied the UIUC 150 Bus system and a few important representative network structures with the model, and identified the effects of heavy load demands and network structure on the rapidity of propagation of possible blackouts. We also develop metrics to evaluate the risk of large-scale blackouts in terms of cumulative blackout size distributions. The model described in this chapter thus provides predictive information for possible power blackout events in power systems.

Chapter 5

Modeling Cascading Failure in Cyber-Coupled Power Networks

In the previous two chapters, we investigated cascading failure in uncoupled power networks. In this chapter, we propose a model to investigate cascading failure propagation in a coupled system (smart grid) that comprises a power grid and a coupling cyber network. In this model, we take into consideration the effects of power overloading, contagion and interdependence between the power grid and the cyber network on failure propagations in the coupled system, and then use a stochastic method to generate the time intervals between failures, thus producing the dynamic profile of the failure cascade caused by the attack of cyber malwares. We study several coupled systems generated by coupling the UIUC 150 Bus System with cyber networks of different structures and coupling patterns. Simulation results show that the dynamic profile of the cascading failure in a coupled system displays a "staircase-like" pattern which can be interpreted as a combined feature of the typical step propagation profile triggered repeatedly by cyber attacks due to network coupling. Results also show that cyber coupling can intensify both the extent and rapidity of power blackouts. Moreover, the cyber network structure and the coupling patterns affect the propagation of the cascading failures in smart grids.

5.1 Introduction

Smart grids are defined as electrical networks with integration of information and communication technologies (ICT) to deliver electric power to the final consumers more efficiently and securely [110]. A smart grid is a typical cyber-physical system (CPS) [111], where the physical part is the power apparatus in the power grid and the cyber part is for state monitoring, communications, and control of the physical network. Coupling with cyber networks can make smart grids more efficient and intelligent, at the same time it may bring new challenges by making power systems more vulnerable to attacks from cyber networks [112–114].

As computers are in control of critical devices in today's power systems at every level [115], attacking power systems via spreading malware in computer networks may cause severe damages or even catastrophic consequences. The Aurora Generator Test conducted by Idaho National Laboratory demonstrated how a generator can be physically destroyed by a piece of codes [116]. Cyber malware can attack multiple points of the physical network and may jeopardize the CPS [115]. The latest demonstration of a severe blackout caused by cyber attacks took place on December 23, 2015 in Ukraine [21], which was planted by a computer malware (called BlackEnergy) that penetrated the computer network connected to the Ukrainian power system through an infected file downloaded by the operator. BlackEnergy silently infected workstations in the cyber network for several months, and then attacked the system by disconnecting breakers of several substations, making monitoring stations go blind and blocking the call centers. Finally, 80,000 customers were deprived of power for more than six hours.

In the past two decades, numerous studies were devoted to the cascading failure analysis in power systems, focusing mainly on the physical network. Having witnessed the threats from cyber coupled attacks, power engineers and researchers are becoming more aware of the importance of understanding the behavior of cyber coupled power

systems. Future smart grids will certainly be heavily dependent on safe and efficient operation of coupled power apparatus and communication networks. With this new motivation, researchers have recently diverted attention to the smart grids' vulnerability assessment and mitigation methods to cyber attacks [117–120].

Abstracting the substations as nodes and the transmission lines as edges, the power physical layer can be modeled as a network. Correspondingly, the cyber layer can also be represented as a complex network, in which computers are nodes and the cyber connections are edges. Considering the interdependence of these two networks (i.e., power nodes provide power to the nodes in cyber layer, and the cyber nodes control the operation of power nodes), the behavior of smart grids can be studied from a perspective of interdependent complex networks [121–123].

Buldyrev *et al.* in 2010 [124] studied failures in interdependent networks with percolation theory and concluded that networks with a broader degree distribution were more vulnerable. In percolation theory, all nodes in the network are deleted with a probability, which can fragment the network. The nodes that belong to a giant cluster are assumed to be able to function well, while the nodes in the remaining small clusters become malfunctioned. Cai *et al.* in 2016 [125] analyzed the cascading failures in power systems considering the interaction between power grids and communication networks. Failure of a power element is determined by the time when it is overloaded and the duration of data dispatching in the communication network. Rahnamay-Naeini *et al.* in 2016 [126] modeled the number of failures in a power grid and the number of failures in a communication network as two interdependent time series. Stochastic methods are adopted to analyze the dynamical profiles of these time series. It has been concluded in Rahnamay-Naeini *et al.*'s study that interdependence can make the individually reliable systems behave unreliably as a whole. Although these prior studies focused on interdependent networks composed by the power network and the cyber network, they fall short of taking into consideration the influence of computer malware on the operation of power systems. In the Ukrainian case, for instance, the malware

infection in the cyber network plays an important role in the cascading failure propagation in smart grids. Our previous work [94] showed that the mechanism of failure propagation in a power grid is very different from that of malware spreading in an individual cyber network [127]. However, for the smart grid where the physical layer and the cyber layer are highly mutual dependent, the cascading failures can be highly affected by the dynamics of computer malware spreading. Thus, the dynamic property of malware spreading should be considered in cascading failures in the case of smart grids.

In this chapter, we investigate the effects of cyber coupling on cascading failures in smart power grids. First, the mechanism of failure spreading in the power system (due to power overloading) and that in the cyber network (due to malware contagion) are considered in the model, with emphasis on the interdependence of these two networks. Then, based on the corresponding mechanisms, we combine the deterministic circuit-based model and a stochastic method to describe the failure processes of the two kinds of nodes in the coupled system in Section 5.2. Then, we introduce an algorithm to simulate the cascading failures in the coupled system in Section 5.3. We simulate several coupled systems and summarize key findings in Section 5.4. The coupled systems are generated by coupling the UIUC 150 Bus System with cyber networks of various structures and coupling patterns. Simulation results show that the failure propagation pattern in a coupled system displays characteristics of both the power network and the cyber network, and that cyber coupling can cause more severe damages to the power system. The cyber network structure as well as the coupling pattern play crucial roles in the propagation of the cascading failures in smart grids. Scale-free cyber networks promote the failure spreading in the coupled system, and a higher average node degree of the cyber network intensifies the spreading. Moreover, coupling of power nodes with high-degree cyber nodes makes failure propagate faster compared to coupling randomly or with low-degree nodes.

5.2 Model Description

In this chapter, we consider a smart grid composed of a set of power apparatus and its controlling network. The controlling network refers to the specific computer network for controlling power systems, which is normally isolated from the wide area network we use in other applications. In practice, firewalls and other security measures should be designed and applied in these important networks. For simplicity, we consider a coupled system A–B which is composed of two interdependent networks A and B, as shown in Fig. 5.1. Network A is the power grid, where solid rectangular nodes in Fig. 5.1 represent electrical buses in A and solid arcs represent transmission lines. Network B is the cyber network, where white circular nodes represent computers in the cyber network and dashed joining arcs represent the connections among the cyber nodes. Clearly, nodes in A and nodes in B are interdependent. Precisely, the cyber nodes control the operation of power nodes, while the power nodes provide power to the cyber nodes. The interdependent relationships are depicted by the horizontal lines in Fig. 5.1. In this chapter, we consider one-to-one coupling relation between the nodes in A and the nodes in B, i.e., $A_i \leftrightarrow B_i$. Each pair of coupled nodes (A_i and B_i) are called a *node pair* in the coupled system A–B. For the sake of maintaining generality, we also consider nodes without corresponding coupling nodes in the other network. For these nodes, there are no coupling effects. In Fig. 5.1, there are p power nodes, q cyber nodes and m *node pairs*, where $p \geq m$ and $q \geq m$. Usually the number of nodes in the cyber network is far bigger than that of the power network, i.e., $q \gg p$.

In this chapter, we study the cascading failures in the coupled system A–B, which is initiated by attacks of computer malwares. The cascading failure propagation in A–B can be viewed as a sequence of state transitions of the nodes in the coupled system. In the following subsections, we will define the states of nodes and describe their corresponding state transitions.

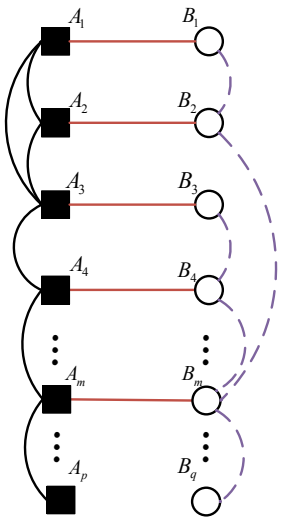


Figure 5.1: Coupled network consisting of a power network A and a cyber network B. Solid rectangles represent electrical buses and solid arcs represent transmission lines in A. White circles represent computers in the cyber network and dashed arcs represent connections among the cyber nodes in B. Horizontal lines represent interdependence between nodes in A and nodes in B.

5.2.1 Failure Mechanism of Power Elements

In this section, we introduce the mechanism of the electrical elements' failures. Previous works have analyzed cascading failures in individual power systems. Data fitting methods have been applied to study the failure propagation profiles in power systems in refs. [91, 93], regardless of the physical failure cascade mechanism in the network. Considering the effects of power flow distribution in the failure propagation, several models have been proposed to simulate the cascading failure propagations in power systems, which can be classified under two categories: *deterministic* models and *stochastic* models. In deterministic models [77,94], in each round of the cascading failure process, the power flow distribution in the network is computed, and overloaded electrical elements are removed at the same time. To show the dynamic profile, Eppstein *et al.* [66] made the simple deterministic assumption that the duration for an overloaded element to be tripped is equal to Δt which is given by $\int_t^{t+\Delta t}(f_j(\tau)-\bar{f}_j)d\tau = \Delta o_j$, where f_j is the power flow of overloaded element j, $\bar{f}_j$ is the flow limit and Δo_j is a

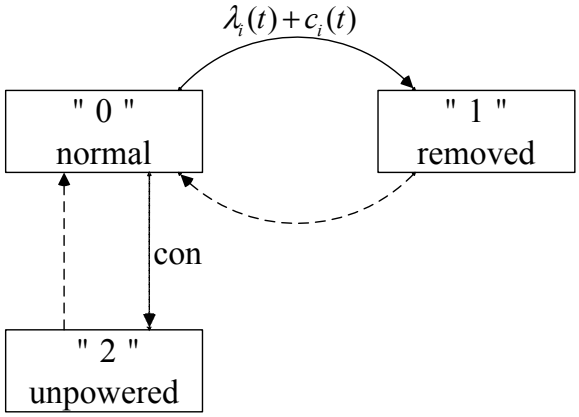


Figure 5.2: State transition diagram of a node in power network A. Transitions between state 0 and 2 are deterministic transitions, and those between 0 and 1 are stochastic transitions.

specific threshold of that element. Considering the high uncertainties and complexities in power systems, stochastic models are used to investigate cascading failures in power systems [68, 95, 98], but a mathematical formula that can describe the collective behavior of the power network has not been derived.

In modeling the failure cascading in a power grid in this chapter, we first apply *deterministic* power flow analysis to derive the power flow information and the overloading conditions of the electrical elements. Then, we adopt a stochastic method to obtain the time durations between failures to simulate the failure propagations in the network.

Let s_{A_i} denote the state of a power node A_i. In our model, we consider three possible states for a power node, i.e., $s_{A_i} \in \{0, 1, 2\}$. Specifically, $s_{A_i} = 0$ is the normal state, which corresponds to node A_i being connected and operating normally in the power network; $s_{A_i} = 1$ is the removed state, which corresponds to A_i being tripped by a circuit breaker and removed from the power network; and $s_{A_i} = 2$ is the unpowered or "islanded" state, which corresponds to A_i being inaccessible to power sources due to the removals of other failed elements in A. When A_i is in state 1 or 2, it is deprived of power. Possible state transitions of A_i are shown in Fig. 5.2.

Depending on the nature of the transitions, they are either deterministic transitions

or stochastic transitions, as shown in Fig. 5.2. The tripping (removal) of some elements in A can fragment the power network into several disconnected sub-networks. When a sub-network containing no power source is created, a condition "con" is said to be reached for all nodes in the sub-network. Under this condition, nodes in the sub-network change their states from 0 to 2. This state transition, namely $s_{Ai} = 0 \xrightarrow{\text{con}} s_{Ai} = 2$, is deterministic. Moreover, this state transition is caused by and always accompanying the state transition $(0 \rightarrow 1)$ of another element in A, and thus the transition time for this type of state transitions is not considered.

On the other hand, the time at which a stochastic state transition takes place is an important consideration that would affect the dynamic profile of the cascading failure propagation. Node A_i (in state 0) is tripped by its protective equipment with a certain probability value when A_i is overloaded or when its coupled node B_i is infected by a computer malware that can attack the power network by switching off circuit breakers of A_i. The stochastic state transition of node A_i from state 0 to state 1 is represented by a *state transition channel* T_1, and is represented as:

$$T_1 : s_{Ai} = 0 \rightarrow s_{Ai} = 1. \tag{5.1}$$

When node A_i has a coupled node B_i which works normally or does not have a coupled node in network B, the state transition $s_{Ai} = 0 \rightarrow s_{Ai} = 1$ is only caused by overloading. In much of the prior work on modeling the switching actions of the relays using Markov models [68] [95], transitions are determined by power loading conditions and elements' capacities. In real-time operation, as pointed out by Sun *et al.* [99], an electrical component's failure rate is not constant but varies with loading conditions, and that a component will experience more failures under heavy loading conditions. In order to incorporate these characteristics in our model, we describe the state transition $s_{Ai} = 0 \xrightarrow{\lambda_i(t)} s_{Ai} = 1$ as a stochastic process and define the tripping rate

λ_i as

$$\lambda_i(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \leq C_i \end{cases} \tag{5.2}$$

where $L_i(t)$ is the power loading of component i , C_i is the capacity of that component, and a_i is the basic unit rate (trippings per second). Using (5.2), the power flow analysis can be applied to derive $\lambda_i(t)$. In this chapter, we adopt the method introduced in Chapter 3 to compute the power flows in the power system, assuming that the power system will reach a new steady state after an element fails. In this chapter, we do not consider stability issues that have been studied in refs. [128, 129]. Thus, when A_i is in state 0, and on the condition that its coupling node B_i is working normally or it has no coupling nodes in network B, the probability that A_i transits from state 0 to 1 in an infinitesimal time interval dt can be written as

$$T_1 : P[s_{Ai}(t + dt) = 1 \mid s_{Ai}(t) = 0] = \lambda_i(t)dt. \tag{5.3}$$

When A_i has a coupling node B_i in network B and B_i is infected by a computer malware, A_i (in state 0) will have an extra chance to be removed from system due to the action of malware. Thus, we assume that the malware will add an additional rate $c_i(t)$ to the state transition rate λ_i. Thus, the probability that A_i transits from state 0 to 1 in an infinitesimal time interval dt when B_i is infected by computer malware can be written as

$$T_1 : P[s_{Ai}(t + dt) = 1 \mid s_{Ai}(t) = 0] = (\lambda_i(t) + c_i(t))dt, \tag{5.4}$$

where $c_i(t)$ represents the dependency of power node A_i on cyber node B_i.

State 1 and state 2 are fundamentally different states even though both correspond to an unserved node. For state 1, the power node is removed due to it being tripped by the protective relay upon power overloading. We use a stochastic method to describe this process. However, for state 2, the power node has no access (finds no path) to

power sources due to the tripping of other elements in the network. Though unserved, it is not tripped and is still well connected. We use a deterministic method to describe this process, and it depends on the tripping of other elements in the network. From the network's point of view, an element in state 1 is an open-circuit, changing the topology of the network, whereas an element in state 2 has no impact on the network topology.

In a fast cascading failure process, we do not consider repair and anti-malware actions. Thus, the corresponding transition rates are set as 0, i.e., dashed arrows in Fig. 5.2 are neglected.

5.2.2 Failure Mechanism of Cyber Nodes

Let s_{B_i} denote the state of node B_i. We consider three different states for a cyber node B_i, namely states 0, 1 and 2. Specifically, $s_{B_i} = 0$ is the normal state, in which B_i is working normally in the cyber network; $s_{B_i} = 1$ is the state of being infected by a computer malware; and $s_{B_i} = 2$ is the shutdown state corresponding to node B_i being shut down due to power outage. The difference between state 1 and state 2 is that when a computer is infected (in state 1), it is able to infect its neighboring nodes, whereas a shutdown computer (in state 2) is completely removed from the cyber network and does not infect others. Figure 5.3 shows the state transition diagram of cyber node B_i. All state transitions of B_i are stochastic transitions. Details of the transition process are as follows.

When node B_i is in state 0, it can be infected by a computer malware through connection with an infected neighbor. The malware diffusion can be modeled by a stochastic process [127]. Here, we use describe B_i's state transition as $s_{B_i} = 0 \xrightarrow{\mu_i} s_{B_i} = 1$, and refer to it as state transition channel T_2:

$$T_2 : s_{B_i} = 0 \xrightarrow{\mu_i} s_{B_i} = 1. \tag{5.5}$$

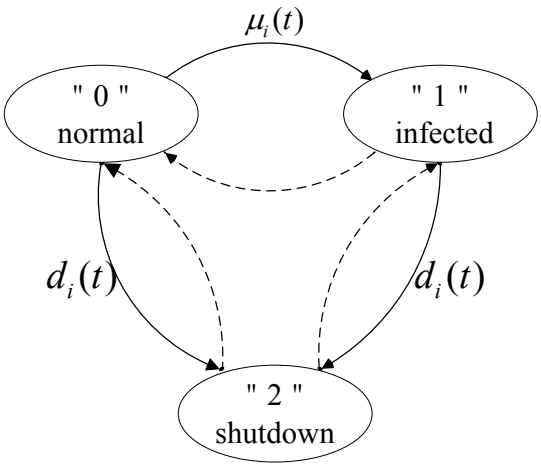


Figure 5.3: State transition diagram of a node in the cyber network B.

where μ_i is the rate of infection of node B_i and is defined as

$$\mu_i(t) = \sum_{j \in \Omega_{Bi}} \beta_{ij}, \tag{5.6}$$

where Ω_{B_i} is the set of all infected neighbors of node B_i and β_{ij} is the rate at which infected node B_j ($s_{B_j} = 1$) infects its neighbor B_i which is in state 0. For an infinitesimal time interval dt, the probability that a state transition occurs through T_2 can be written as

$$T_2 : P[s_{B_i}(t + dt) = 1 \mid s_{Bi}(t) = 0] = \mu_i(t)dt. \tag{5.7}$$

When node B_i has a corresponding coupled power node A_i and $s_{A_i} \in \{1, 2\}$, it can no longer provide power to its cyber node B_i, causing B_i to transit to state 2 (shutdown) due to power outage. In practice, usually there exists backup power for computers that perform crucial functions in controlling the power grid. Considering the limited supporting time of the backup power units, in our model, we use stochastic transitions to describe the state transitions for node A_i when $s_{A_i} \in \{1, 2\}$. Specific details are as follows.

When $s_{B_i} = 0$ and $s_{A_i} \in \{1, 2\}$, apart from state transition channel T_2, another state

transition channel T_3 exists:

$$T_3 : s_{B_i} = 0 \xrightarrow{d_i} s_{B_i} = 2, \tag{5.8}$$

where $d_i(t)$ is the state transition rate which is determined by the dependence of node B_i on its coupled power node A_i. In an infinitesimal time interval dt, the probability that a state transition occurs through T_3 can be written as

$$T_3 : P[s_{B_i}(t + dt) = 2 \mid s_{B_i}(t) = 0] = d_i(t)dt, \tag{5.9}$$

When $s_{B_i} = 1$ and $s_{A_i} \in \{1, 2\}$, there is another state transition channel T_4:

$$T_4 : s_{B_i} = 1 \xrightarrow{d_i} s_{B_i} = 2. \tag{5.10}$$

In time interval dt, the probability that a state transition occurs through T_4 can be written as

$$T_4 : P[s_{B_i}(t + dt) = 2 \mid s_{B_i}(t) = 1] = d_i(t)dt. \tag{5.11}$$

When $s_{A_i} = 0$, $d_i(t)$ is 0.

Finally, as repair or anti-malware actions are not considered in a fast cascading failure process, the corresponding transition rates can be set to 0, i.e., dashed arrows in Fig. 5.3 are neglected. For clarity of the figures, self-loop arrows are not displayed in Figs. 5.2 and 5.3.

5.3 Cascading Failure in Coupled Systems

The coupled system A–B contains p power nodes, q cyber nodes, and m node pairs in total. Let $S(t)$ denote the state of A–B, and $S(t) = [s_{A_1}, s_{A_2}, \cdots, s_{A_p}, s_{B_1}, s_{B_2}, \cdots, s_{B_q}]$. Suppose that there are m_S ($m_S \leq 3^{p+q}$) possible states for A–B. The cascading failure

Table 5.1: State transition channel list of the coupled system at time t given that $S(t) = N_S$. All the l nodes which may transit and their corresponding transition rates are listed.

Possible transition channel	$T^{(1)}$	$T^{(2)}$	$T^{(3)}$	...	$T^{(n)}$
Transition rate	r_1	r_2	r_3	...	r_n

process is the dynamic propagation profile of $S(t)$ as the system state transits in time among those m_S different states.

5.3.1 State Transition of the Coupled Network

Suppose, at time t, the coupled network is in state $S(t) = N_S$ (N_S is one specific system state of the 3^{p+q} possible states), and there are u nodes that may undergo a state transition. Each node of these u nodes can undergo a deterministic or stochastic transition, depending on the current node state and the transition rule. For a deterministic transition, the transition rule is triggered when condition "con" is met, while for a stochastic transition, the transition rule is described by a transition rate, as shown in Figs. 5.2 and 5.3. At time t, there are l ($l \leq u$) nodes that will undergo a stochastic transition, and each one will transit through a transition channel selected from T_1, T_2, T_3, T_4. For instance, if cyber node B_i is in state 0 (i.e., $s_{B_i} = 0$) at time t and is connected to an infected neighbor, and at the same time its coupled power node is removed or unpowered, then node B_i will have two state transition channels, namely, T_2 and T_3. Thus, the total number of transition channels (say n) can be larger than l. In our algorithm, we first identify condition "con", and transit all power nodes meeting "con" to state 2 instantly. Then, all possible stochastic state transition channels of the coupled system is listed in a *state transition channel list*, as shown in Table 5.1, where channel $T^{(i)} \in \{T_1, T_2, T_3, T_4\}$. Any node's state transition through any one of the n transition channels will lead to a state transition of the coupled network, i.e., change in $S(t)$.

The cascading failure process can be viewed as a sequence of state transitions. We only allow one element state transition at a time. That is, at most one state transition

channel is chosen at a time. See Section 4.3.1 for a rigorous argument. In order to simulate the dynamic propagation of $S(t)$, we need to

1. find the time at which a state transition occurs; and

2. identify the corresponding transition channel through which the transition occurs.

The following subsection explains the detailed process of finding transition time and identifying the transition channel.

5.3.2 Stochastic Transition Processes

Let $Q(\tau)$ denote the probability that no state transition occurs in time interval $(t, t+\tau)$, i.e., $Q(\tau) = P[S(t+\tau) = N_S \,|S(t) = N_S\,]$. Then, $Q(\tau + dt)$ can be written as

$$Q(\tau + dt) = P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,]Q(\tau). \tag{5.12}$$

Thus, we have

$$P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,] = (1 - r^* dt), \tag{5.13}$$

where $r^* = \sum_{i=1}^{n} r_i$. Note that equation (5.13) is only valid when dt is infinitesimally small (see Section 4.3.1). Substituting (5.13) into (5.12), we get

$$Q(\tau + dt) = Q(\tau)(1 - r^* dt). \tag{5.14}$$

Re-arranging (5.14), as $dt \to 0$ (i.e. dt is infinitesimal), we get

$$\lim_{dt\to 0} \frac{Q(\tau + dt) - Q(\tau)}{dt} = Q^{'}(\tau) = -r^* Q(\tau). \tag{5.15}$$

Thus, we can express $Q(\tau)$ as

$$Q^{'}(\tau) = -r^{*}Q(\tau).$$

Note that in equations (5.13) through (5.15), the above differential equation is derived by taking the limit $dt \rightarrow 0$ and is valid for any τ. Solving the above differential equation, we get

$$Q(\tau) = Q(0)e^{-r^{*}\tau}. \tag{5.16}$$

Since $Q(0) = P[S(t) = N_S \,|S(t) = N_S\,] = 1$, we can derive the expression of $Q(\tau)$ as

$$Q(\tau) = Q(0)e^{-r^{*}\tau} = e^{-r^{*}\tau}, \tag{5.17}$$

which is the general solution for $Q(\tau)$ and remains valid for all τ. Let $F(\tau)$ denote the probability that the next state transition occurs before time $t + \tau$. Then, we get

$$F(\tau) = 1 - Q(\tau) = 1 - e^{-r^{*}\tau}. \tag{5.18}$$

The probability density of τ can be found using equation (5.18) as

$$f(\tau) = r^{*}e^{-r^{*}\tau}. \tag{5.19}$$

From (5.18) and (5.19), we see that τ follows an exponential distribution. The state transition rate r^{*} of coupled system A–B is the sum of the transition rates of all the transition channels. As discussed in Section 5.2, r^{*} includes the effects of overloading in the power network, malware spreading in the cyber network, and the interdependence between of two networks.

Suppose the next state transition occurs at time τ through transition channel T_k. To include the property of exponential distribution of τ and the characteristic that the tran-

sition channel with a higher rate will be more likely chosen, the following procedure is used to determine the next state transition.

Two random numbers z_1 and z_2 are uniformly and independently generated in $(0, 1)$. Then, τ is generated from the following equation :

$$\tau = F^{-1}(z_1) = \frac{1}{r^*} \ln(\frac{1}{1 - z_1}). \tag{5.20}$$

And k is selected based on the following equation:

$$\sum_{j=0}^{k-1} \frac{r_j}{r^*} \leqslant z_2 \leqslant \sum_{j=0}^{k} \frac{r_j}{r^*}. \tag{5.21}$$

The dynamics of $S(t)$ is a series of the state transitions introduced above beginning with an initial failure (malware injection) until all state transition channels are exhausted. Figure 5.4 shows the flow chart used in simulating the cascading failures in the coupled system.

5.3.3 Simulation Flow Chart

- *Initialization:* The information of the coupled system A–B is set, including the network structure of A and B, and the coupling between the nodes in A and the nodes in B. In simulating the power failure propagation, the power flow calculation is necessary. Thus, for the power network, the admittance of the transmission lines, voltages of the generates, load demands of the consumers and winding ratios of transformers should be given.

- *Malware injection:* In this study, we assume the cascading failures are caused by cyber malware attacks. Thus, the initial trigger is the injection of a malware in the cyber network. The time of malware injection is set as 0.

- *Malware diffusion:* In the case of cyber attacks, the malware can be designed to

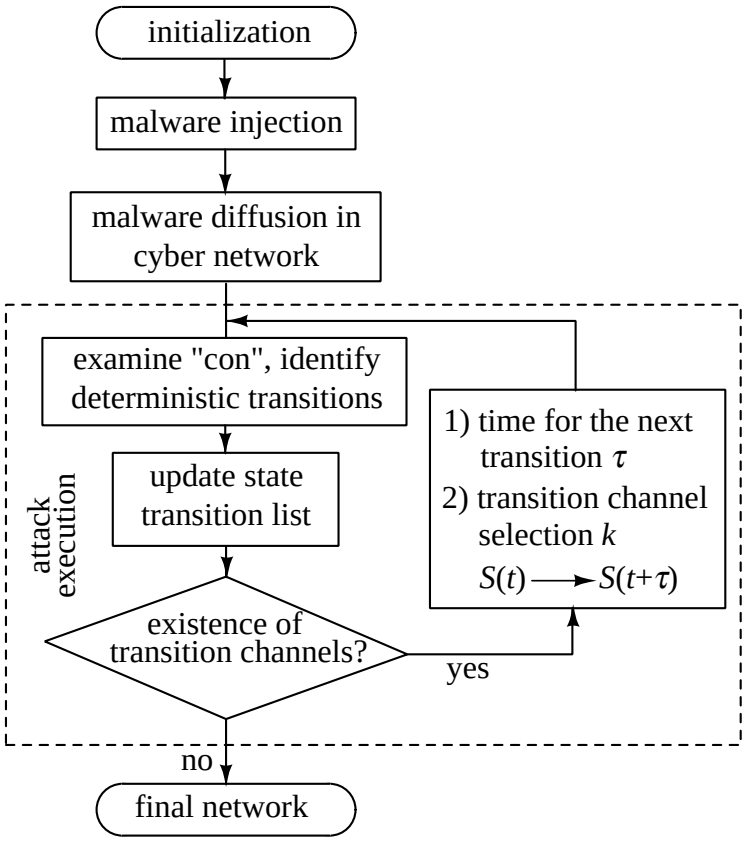


Figure 5.4: Simulation flow chart for cascading failures in the coupled system.

spread silently and harmlessly in the cyber network for a period of time in order to get enough nodes infected. Here, we set t_d as the time period for the malware diffusion before attack is launched to the power network, and in this time period, only transition channels applied to the cyber network are relevant.

- *Attack execution:* After t_d, the malware will launch attack to the power system. All possible transition channels may be selected. Iteration then proceeds as follows.

  (a) The condition "con" will be checked against $S(t)$, and the power nodes meeting "con" are marked as state 2, i.e., the deterministic state transition occurs. This kind of state transitions occurs instantly.

  (b) Based on $S(t)$ and equations (5.3)-(5.11), we update the list of possible

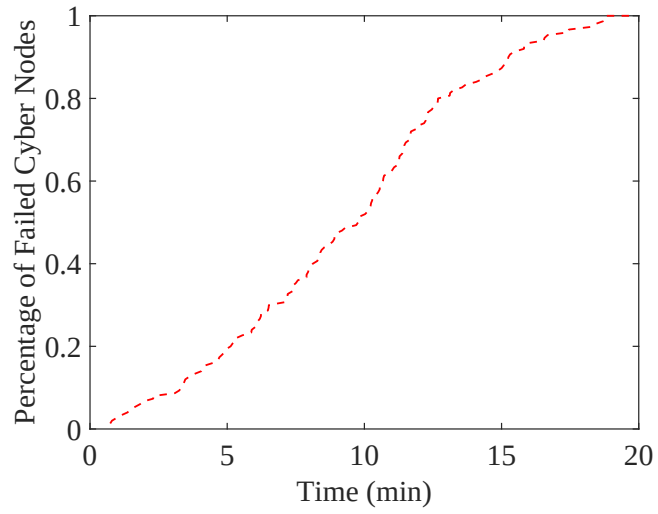
state transition channels. The list contains the rates contributed by all the failure spreading mechanisms in the coupled system, including power elements' failure due to power overloading based on equation (5.2) where the deterministic power flow analysis should be applied [94], cyber nodes' infection due to contagion based on equation (5.6), and the interdependencies between the two different networks.

(c) If there is a state transition channel in the list, we use equations (5.20) and (5.21) to select the next state of $S(t)$ and return to step (a). If there is no more transition channel in the list, cascading failure ceases to propagate and the system is said to enter an absorbing state. We end the iteration and record the time as t_{final}.

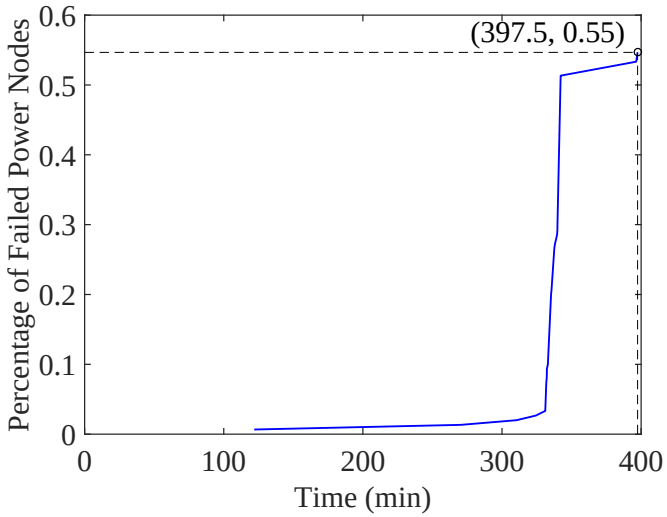
5.4 Simulation Results and Discussions

In this section, we perform simulation experiments with the proposed model to study the cascading failures in the coupled system and investigate the effects of cyber coupling on the failure propagation process. We specifically aim to identify the key factors and parameters that determine the extent and rapidity of power blackouts caused by cyber attacks. Test networks are generated by coupling the UIUC-150 Bus System [109] with cyber networks of different structures. The capacities of the generators, transformers and the transmission lines in the power network are set as 1.2 times of their respective current flows in normal operation. We also assume that the computer malware will execute attack once it infects a new cyber node, namely, $t_d = 0$. We introduce two essential metrics for characterizing the extent of the failure, namely, *percentage of failed power nodes* (PFPN) and *percentage of failed cyber nodes* (PFCN), which are defined as follows:

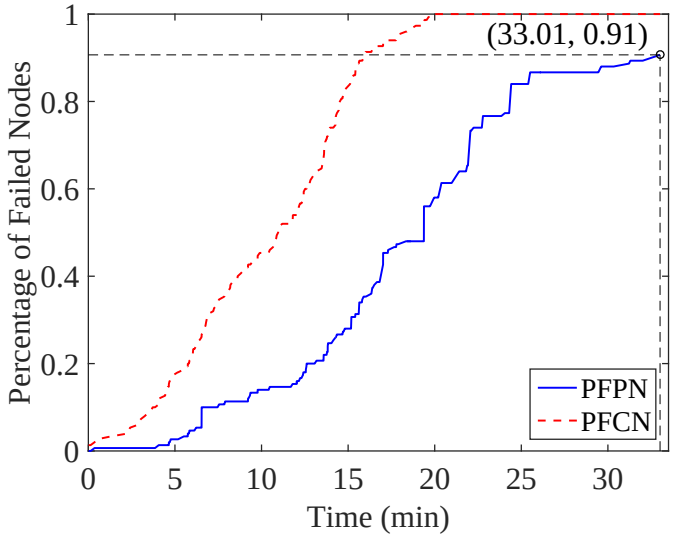
$$\text{PFPN}(t) = \frac{n_{\text{unpowered}}(t) + n_{\text{removed}}(t)}{p}, \tag{5.22}$$



(a)



(b)



(c)

Figure 5.5: Failure propagation in (a) cyber network showing smooth growth pattern; (b) uncoupled power grid showing "step jump" pattern; (c) coupled system.

$$\mathrm{PFCN}(t) = \frac{n_{\mathrm{infected}}(t) + n_{\mathrm{shutdown}}(t)}{q}, \tag{5.23}$$

where $n_{\mathrm{unpowered}}(t)$ and $n_{\mathrm{removed}}(t)$ represent the number of power nodes in state 1 and 2 at time t, respectively. Similarly, $n_{\mathrm{infected}}(t)$ and $n_{\mathrm{shutdown}}(t)$ are the number of cyber nodes in state 1 and 2 at time t, respectively. Note that a large PFPN(t) (PFCN(t)) means that a large total area of disconnected fragments of the power grid (cyber network) are out of operation.

5.4.1 Failure Propagation Patterns in the Coupled System

First, we examine the failure propagation patterns in the power network, cyber network and the coupled system. We first study the case where the coupled cyber network has the same structure as the power grid. This allows a close examination of the failure spreading patterns on the power network and the cyber network due to the different spreading mechanisms. The parameters of the coupled network are set as follows:

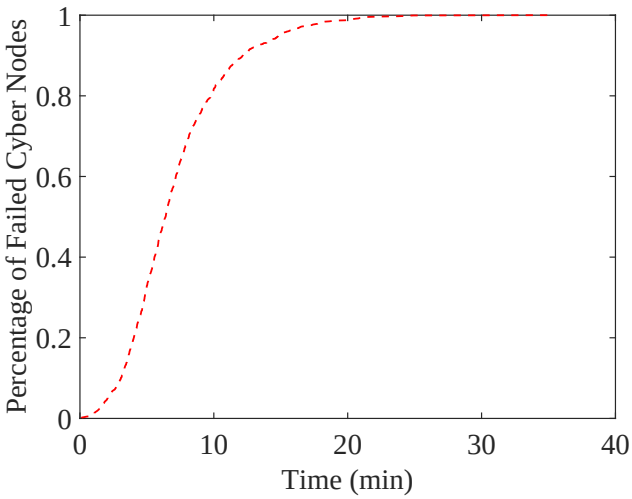
- The cyber network and the power grid have the same size, i.e., $p = q = 150$;
- The failure rate in power system a_i is 0.21 min^{-1}, and the infection rate in the cyber network β_{ij} is 0.5 min^{-1};
- Interaction relationship between the two networks are $c_i(t)$ and $d_i(t)$ that are set as

$$c_i(t) = \begin{cases} 0.05\ \mathrm{min}^{-1}, & \text{if } s_{B_1} = 1, \\ 0\ \mathrm{min}^{-1}, & \text{otherwise}, \end{cases}$$

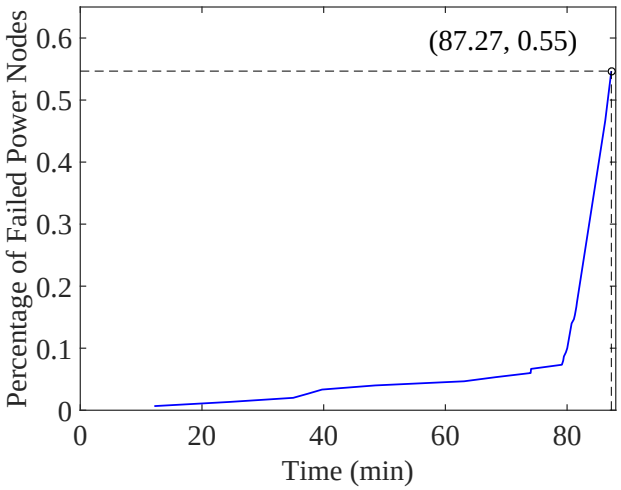
and

$$d_i(t) = \begin{cases} 0.01\ \mathrm{min}^{-1}, & \text{if } s_{A_1} = 1, 2, \\ 0\ \mathrm{min}^{-1}, & \text{otherwise}. \end{cases}$$

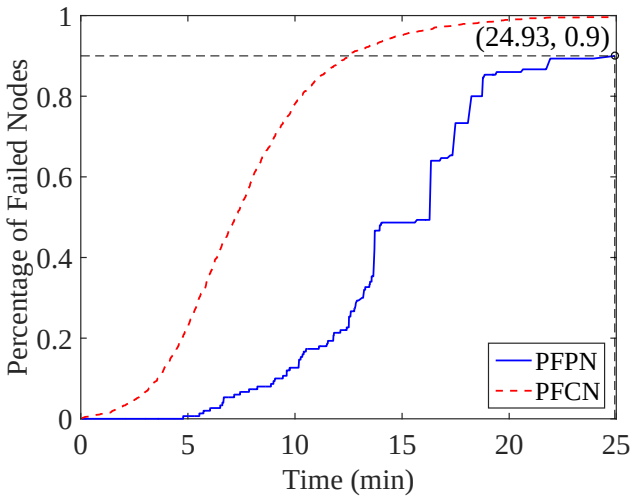
We obtain the values of a_i and β_{ij} through data fitting in this chapter. For a_i, we get the value through setting the averaged t_{final} of 100 simulations in the UIUC 150 Bus system as 5 hours, based on the practical observation that the durations of several


Percentage of Failed Cyber Nodes
Time (min)
0
0.2
0.4
0.6
0.8
1
0
10
20
30
40

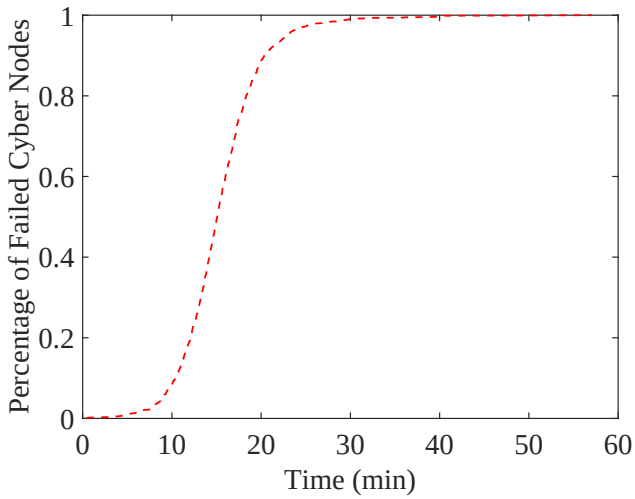
(a)


Percentage of Failed Power Nodes
Time (min)
(87.27, 0.55)
0
0.1
0.2
0.3
0.4
0.5
0.6
0
20
40
60
80

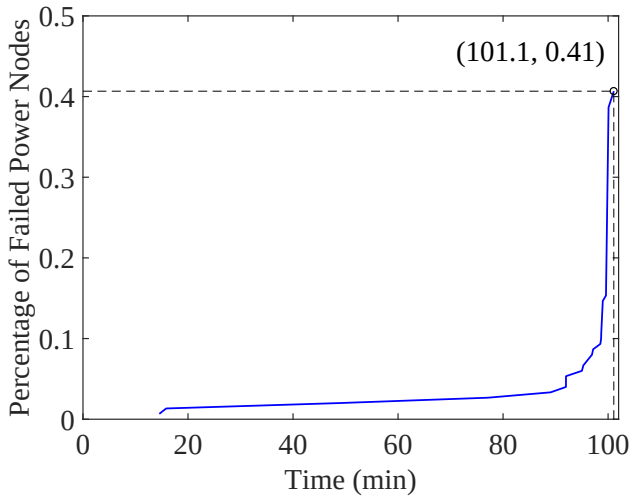
(b)


Percentage of Failed Nodes
Time (min)
(24.93, 0.9)
PFPN
PFCN
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25

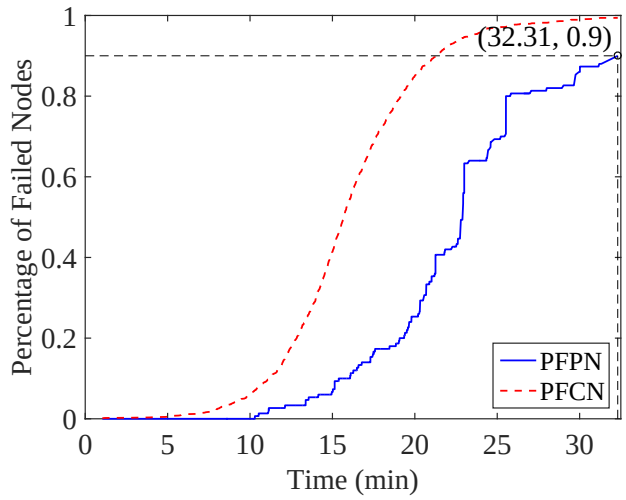
(c)


Percentage of Failed Cyber Nodes
Time (min)
0
0.2
0.4
0.6
0.8
1
0
10
20
30
40
50
60

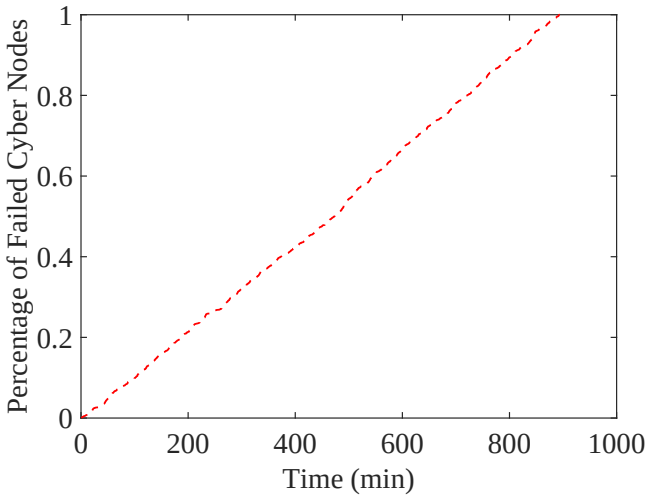
(d)


Percentage of Failed Power Nodes
Time (min)
(101.1, 0.41)
0
0.1
0.2
0.3
0.4
0.5
0
20
40
60
80
100

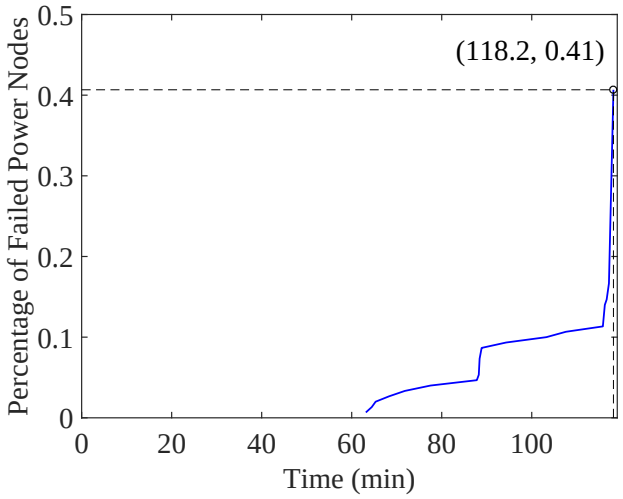
(e)


Percentage of Failed Nodes
Time (min)
(32.31, 0.9)
PFPN
PFCN
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30

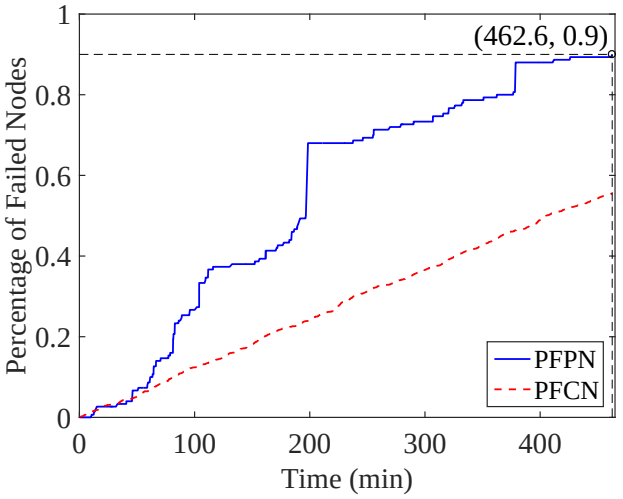
(f)



(g)



(h)



(i)

Figure 5.6: Failure propagation patterns. (a), (d), (g): malware spreading in cyber network with scale-free, random and regular structure, respectively; (b), (e), (h): power node failure propagation in (uncoupled) power grid; (c), (f), (i): failure cascading in the coupled system, with scale-free, random, regular cyber network, all showing "multiple-step staircase" pattern.

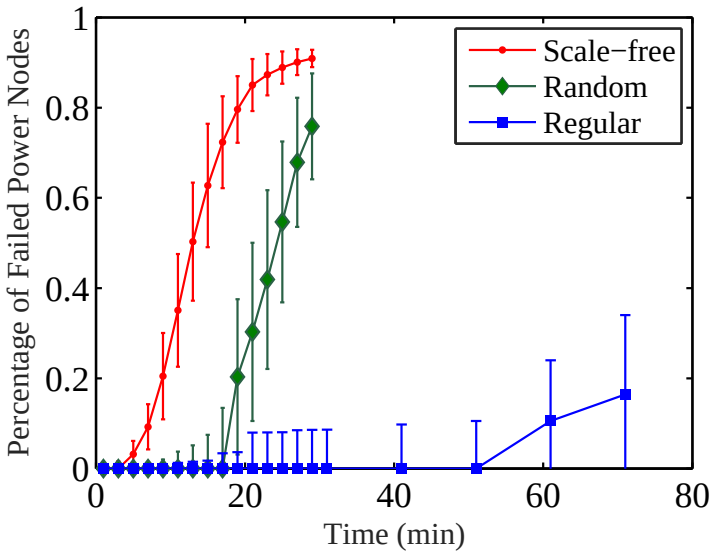


Figure 5.7: Comparison of the extents of cascading failures in power grid coupled with cyber network of different topological structures.

Table 5.2: Comparison on severity of cascading failures between the isolated power grid and the coupled system in terms of cascading failure extent denoted by PFPN(t_{final}) and average rate denoted by $\triangle t$.

Test case	PFPN(t_{final})	$\triangle t$ (min)
Individual power system	0.47	7.25
Coupled system	1	0.37

historical cascading failures were around 1 to 5 hours [89, 90]. For setting β_{ij} in the cyber network, we need to clarify that different malwares (viruses) can have very distinct infection rates. In this chapter we adopt the values used in a previous study [130], which models the combating virus spread in wireless sensor networks.

Figures 5.5 (a) and (b) show the dynamical profiles of cascading failures in the cyber network (a computer malware infected B_1 at $t = 0$) and the uncoupled power system (node A_1 removed at $t = 0$), respectively. From Fig. 5.5(b), we see that the failure propagates very slowly in the uncoupled power network before $t = 330$ min and that an abrupt increase of PFPN(t) occurs around $t = 330$ min, indicating that numerous power nodes failed in a short time during the failure cascading process.

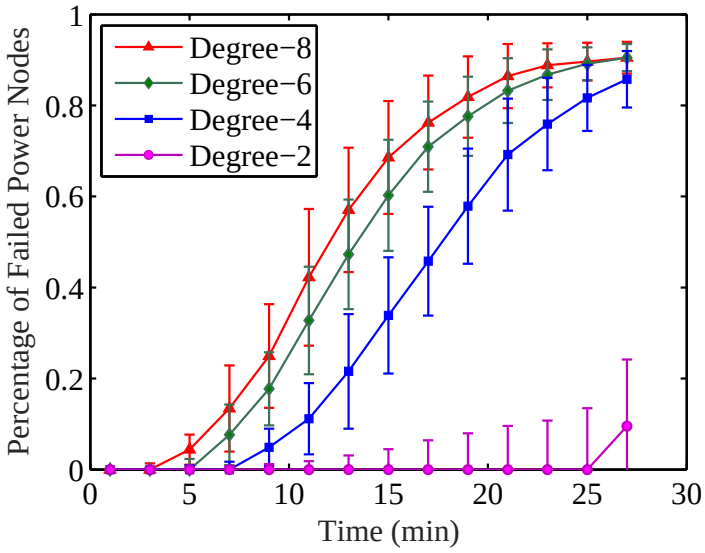
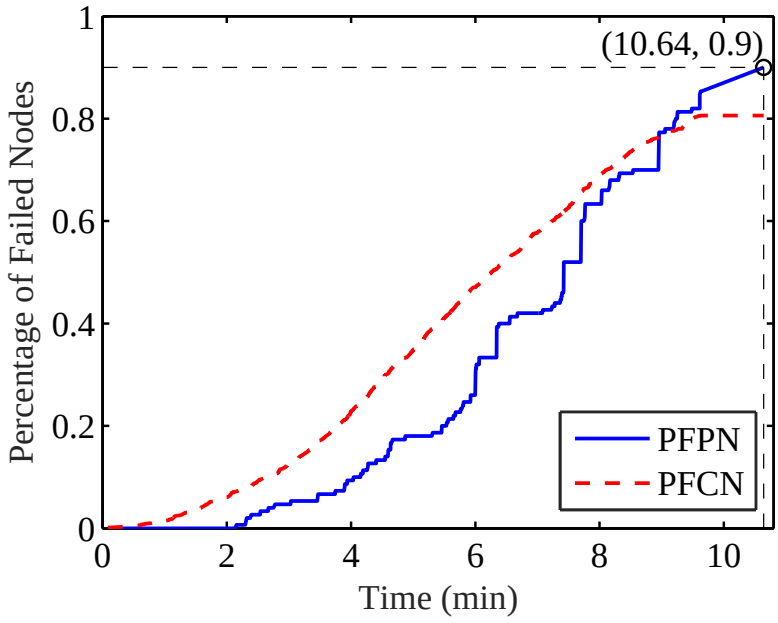


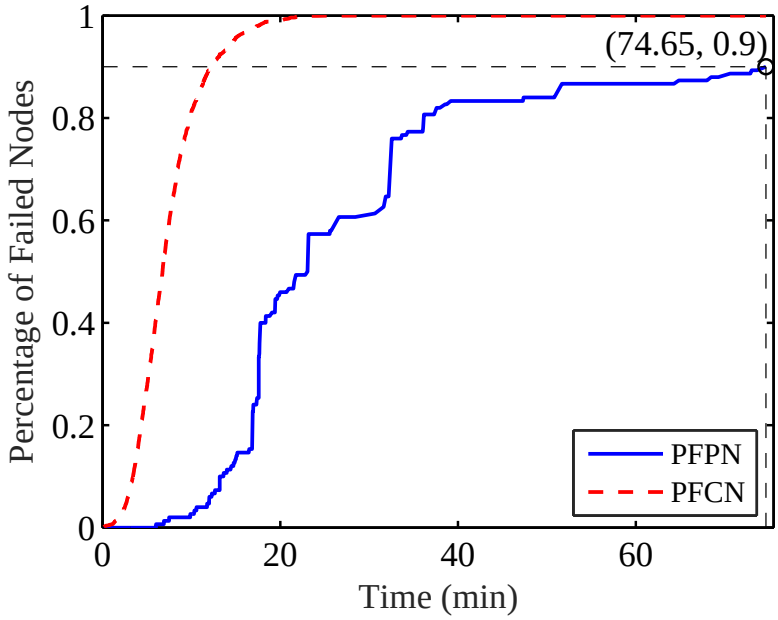
Figure 5.8: Comparison of the extents of cascading failures in power grid coupled with cyber network of different average node degrees.

Compared with the historical data recorded in the 2003 power blackout in the United States and Canada [90] and two blackouts in July and August 1996 of Western North America [89], the results in Fig. 5.5(b) show similar typical profiles of cascading failures. According to equation (5.19), the growth rate of PFPN(t) is related to the sum of the tripping rates, i.e., $r^* = \sum \lambda_i$ in this case. This abrupt change around $t = 330$ min is caused by the failure of some critical element in the power system leading to drastic power flow changes. We view the process where one element's state change causes redistribution of the overall power flows in the whole network as a *global* process, and this *global* process can cause a drastic increase of failure propagation rate in the system. Figure 5.5(a) shows that PFCN(t) grows smoothly. According to equation (5.19), the growth rate of PFCN(t) is related to the sum of the infection rates, i.e., $r^* = \sum \mu_i$ in this case. We view the process where the infected node only influences its neighboring nodes as a *local* process, which cannot cause any drastic change in r^*. Thus, PFCN(t) rises gradually. Clearly, the failure propagation patterns for the power network and the cyber network are dependent on the spreading mechanisms.

Figure 5.5(c) shows the failure propagation in the coupled system initiated by a



(a)



(b)

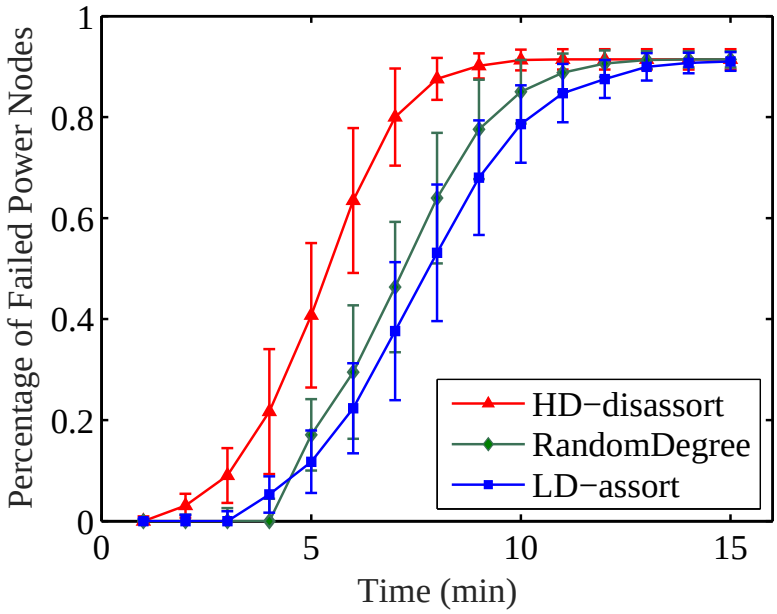
Figure 5.9: Spreading patterns in the coupled system under (a) strong attack with $c(t) = 0.3$ min^{-1}; and (b) weak attack with $c(t) = 0.01$ min^{-1}.

computer malware injected at cyber node B_1 at $t = 0$. The failure propagation in the coupled system is the combined effect of the above two mechanisms as well as the interactions between these two different networks. The propagation profile displays another interesting feature: PFPN(t) has a multiple-step staircase like growing pattern, clearly showing the typical step propagation pattern of cascading failures in the power network being repeatedly triggered by cyber attacks. Table 5.4.1 lists the averaged results of 100 repeated simulations of cascading failures in the individual power system and the coupled system, respectively. Here, PFPN(t_{final}) refers to the percentage of failed power nodes in the final state, and $\triangle t$ is the average time interval when PFPN(t) is increased by one per cent. It can be seen that the coupled system can have a larger area of blackouts as well as a much faster failure spreading rate than the standalone power network.

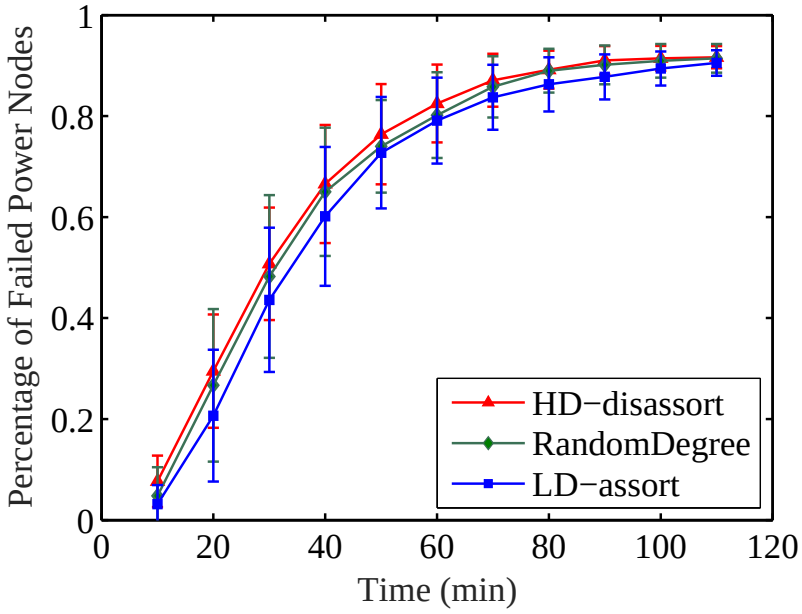
5.4.2 Effects of Cyber Network Structures

In this section, we investigate the influence of cyber network structure on the cascading failure propagation in the coupled system. We generate cyber networks of three classic typologies: *scale-free* (SF) network [6], *random* network [131] and *regular* network. The average node degree of all these cyber networks are fixed at 6. The size of the network is 1500. We use a random coupling pattern between the cyber network and the power grid in this section, i.e., 150 cyber nodes are chosen randomly from the cyber network to connect the power nodes. The infection rate β_{ij} is set as 0.1 min^{-1}.

Figure 5.6 shows the propagation profiles of cascading failures for three different cyber network structures, organized in three sets of charts, namely Figs. 5.6(a), (b), (c); Figs. 6(d), (e), (f); and Figs. 5.6(g), (h), (i). Specifically, Figs. 5.6(a), (d) and (g) show the malware spreading in the different types of cyber networks. We see that the regular cyber network has the slowest spreading rate with an almost linear growth profile. In terms of the spreading rate, the scalefree network is the fastest and the regular network



(a)



(b)

Figure 5.10: Extents of cascading failure in the coupled system under (a) strong attack with $c(t) = 0.3$ min^{-1}; and (b) weak attack with $c(t) = 0.01$ min^{-1}.

Table 5.3: Comparison on the effects of different cyber network topologies on cascading failures in the coupled networks.

Topology of synthesized cyber network	PFPN(t_{final})	$\triangle t$ (min)
Scale-free	1	0.32
Random	1	0.44
Regular	1	6.76

is the slowest. Figures 5.6(b), (e) and (f) show the growing profiles of PFPN(t) in the uncoupled power system, which are similar to the typical profile shown earlier in Section 5.4.1. Figures 5.6(c), (f) and (i) show the multiple-step staircase pattern in the failure propagation profile of the power network coupled with the cyber network. This again clearly shows the typical step propagation pattern of cascading failures in the power network being repeatedly triggered by cyber attacks.

Table 5.3 shows the averaged PFPN(t_{final}) and $\triangle t$ of 100 repeated simulations in the above three different coupled systems, respectively. Furthermore, Fig. 5.7 shows the averaged PFPN(t) and the deviations of a number of repeated simulations in the three coupled systems: UIUC-150 Bus System coupled with cyber network of different topological structures. Results show that when attacked by cyber malwares, the power system coupled with scale-free cyber network displays the most severe cascading failure.

It has been shown that most of the cyber networks in the real world have a scale-free structure. We evaluate the effect of the average node degree of the scale-free cyber network on the vulnerability of the power system coupled with it. We generate four scale-free networks of average node degree 2, 4, 6, and 8. Figure 5.8 reveals that if the average node degree of a scale-free cyber network is higher, the system is more vulnerable to attack with more failure transitions.

5.4.3 Effects of Coupling Patterns

Finally, we analyze how the coupling patterns between the two interdependent networks influence the dynamic propagation of cascading failures in power networks. Since the cyber network is normally much larger than the power network in terms of the number of nodes ($q \gg p$), we consider the coupling of all power nodes with 10% of cyber nodes in a one-to-one fashion. Three different coupling patterns are considered:

1. *High-degree cyber coupling:* Nodes in the cyber network are sorted in descending order of node degree, and the power nodes are sorted in ascending order (which is immaterial as all power nodes are coupled), namely, $\deg(A_1) \leq \deg(A_2) \leq \cdots \leq \deg(A_p)$ and $\deg(B_1) \geq \deg(B_2) \geq \cdots \geq \deg(B_q)$, where deg(.) denotes degree of the node. Then, coupling is established by connecting A_i and B_i ($i = 1, 2, \cdots p$).

2. *Random-degree-node coupling:* Randomly choose p nodes out of the q cyber nodes to connect the power nodes.

3. *Low-degree cyber coupling:* Similar to the first case, but with nodes in the cyber network sorted in ascending order of node degree such that the power nodes are coupled with low-degree cyber nodes.

Furthermore, in order to analyze how the coupling strength $c_i(t)$ influences the cascading failures, we study two cases: (1) strong attack with $c_i(t)$ set as 0.3 min^{-1}; (2) weak attack with $c_i(t)$ set as 0.01 min^{-1}.

Figures 5.9(a) and (b) show the failure propagation patterns under strong and weak attacks, respectively, for random-degree-node coupling. Under the strong attack condition, PFCN(t) is close to PFPN(t), meaning that an infected cyber node can lead to breakdown of power nodes very quickly (Fig. 5.9(a)). However, under weak attack condition, as shown in Fig. 5.9(b), PFCN(t) and PFPN(t) are farther apart. In terms of

failure spreading rates, we see that applying strong attack, the cascading failure incurs more severe damage and occurs more rapidly.

Figure 5.10 shows the averaged PFPN(t) profiles and their deviations of a number of repeated simulation runs at several specific time points for the three coupling patterns. From Fig. 5.10(a), under a strong attack condition (high coupling strength), high-degree dis-assortative coupling leads to a more vulnerable coupled system, while low-degree assortative coupling gives a more robust coupled system. However, under a weak attack condition, as shown in Fig. 5.10(b), the effect of coupling patterns is less significant.

5.5 Summary

The development of future smart grids is inevitably involving more computer control and communication technologies. The coupling of power networks with other networks of computers and even future IoT (Internet of Things) will have a significant impact on the safe and reliable operation of this important infrastructure. This chapter presents a novel stochastic model to investigate the characteristics of cascading failures in smart grids triggered by cyber malware attacks. Our study shows that cyber attacks could incur much more severe damages to power networks and power blackouts could occur much more rapidly when power networks are coupled with cyber networks. Our findings also demonstrate the importance of understanding how coupling weakens robustness and the various factors that affect the extent and rapidity of cascading failure propagation in coupled power networks.

Chapter 6

Conclusions and Suggestions for Future Work

In this chapter, we re-iterate the main contributions of the thesis and discuss some potential topics for future research.

6.1 Main Contributions of the Thesis

In the past decades, complex network theory has developed into a new discipline producing insightful results which are applicable to large real-world interconnected systems. From this newly emerged perspective, researchers have been inspired by the topological universalities observed in real systems which were once too complicated to handle. As one of the most critical man-made infrastructures, the power delivery system and its robustness have drawn much attention from the academic and engineering communities. Although much previous work studied the topological characteristics of real power grids, a clear link between the topology and the functional performance has not been fully established.

In this thesis, we apply complex network theory to the robustness analysis of power systems. The main objective is to investigate the relationship between the topology

and the robustness performance of power systems. The robustness of a power system is defined as the ability to sustain the initial failures of one or a few components in the network. As the initial failure of some elements in a power network can trigger a series of cascading failures, leading to a severe power outage, in this thesis, the robustness of a power system is defined to quantify the ability of the power system to withstand cascading failure. In order to make the analysis relevant to the practical properties of power systems, the use of appropriate models is crucially important. In this thesis, effective models have been built to study the cascading failure mechanism in power systems targeting several important aspects of the observed failure propagation profiles.

The main contributions of the thesis are summarized as follows.

1. A circuit-based model has been developed to simulate cascading failures in power systems.

Instead of merely using topological parameters to investigate cascading failure in a power system, a circuit-based power flow model has been introduced. The power flow in the network is effectively represented by electrical variables, i.e., current and voltage, and the power flow distribution algorithm is based on Kirchhoff's laws and the specific properties of network elements. The model is able to generate realistic power flow information of the elements in the power system. Based on the power flow information provided by this model, the cascading failure process can be simulated.

2. The robustness of a power system has been quantitatively studied.

The robustness performance refers to the ability of a system to tolerate disturbances. In a power system, some small initial disturbances at specific critical components can grow into a large-scale power blackout through a series of cascading failures. A power system could be more robust if there were fewer such critical components. The following two metrics have been defined to quantify a power system's robustness: the percentage of unserved nodes (PUN) caused by a failed component and the percentage of non-critical links (PNL) that will not cause severe damage. PUN and PNL

bridge the gap between the structure and the robustness of power networks. The effects of network structure and location of generators have been explored by assessing the robustness of the IEEE 118 Bus, Northern European Grid and some synthesized networks.

3. A model that can generate the dynamic propagation profiles of cascading failures in power systems has been developed.

Based on the power flow information provided by the circuit-based power flow model, a stochastic model has been used to describe the uncertain failure time instants. With the time instants of failures found, this model is able to give a complete dynamic profile of the cascading failure propagation beginning from a dysfunctioned component and developing eventually to a large-scale blackout. The use of stochastic processes here addresses the uncertainties in individual components' physical failure mechanism which may depend on manufacturing quality and environmental factors. Simulation results have shown that this model can reproduce similar failure propagation profiles with typical features displayed in historical blackout data. This consistency validates that the proposed model can reveal the mechanism of failure propagation and occurrence of large-scale blackouts in power systems.

4. The cascading failure patterns in cyber-coupled power networks have been studied.

Witnessing that the power blackout in the Ukrainian power grid was caused by a malware attack initiated from the cyber network, we have investigated the effects of cyber coupling on the robustness of power systems. Considering the effects of power overload, contagion, and interdependence between power grids and cyber networks, a model for simulating cascading failures in the coupled system (smart grid) that comprises a power grid and a coupling cyber network has been proposed. We have shown that cyber attacks can cause more extensive and rapid power blackouts. The specific effects of the cyber network structure and the coupling patterns have also been discussed.

6.2 Suggestions for Future Work

6.2.1 Consideration of the Oscillatory Process

In the cascading failure model proposed in Chapter 4, we assume that after the failure of one element in the network, the power flow will converge to a new steady state very rapidly. The time of the convergence process can be ignored and no failure is caused by the oscillations during this period. However, in the real system, a host of possible events can happen during this convergence period. For example, transients with high-frequency oscillations can trigger the actions of the relays in the protection equipment causing some elements to trip unexpectedly.

To take into full consideration the oscillatory process, the dynamics of the generators in a power grid should be described with appropriate differential equations. A model that considers both the effects of power overloading in the steady state and the effects of the transients during the convergence process can be established to better characterize the cascading failure mechanism in power systems.

Further, the dynamic descriptions for renewable energy sources are quite different from those for traditional ones. Thus, the effects of intermittent renewable energy sources on cascading failure in large-scale networks can be investigated with specific dynamic equations used for renewable generators in the model.

6.2.2 Detection of the Critical Elements

In Chapter 4, it has been shown that many real cascading failure cases share a propagation profile where an initial slow failure growth phase is followed by an abrupt acceleration phase and most of the component failures occur in a small fraction of the time of the entire failure cascade process. The element that fails in the acceleration point and the onset instant are critical. If the failure propagates to this point, a catastrophic cascading failure will soon occur. Thus, to detect the critical elements and to

predict the onset time will be very meaningful for the purpose of system protection. Before the onset time, the system operator still has enough time to take appropriate actions to halt the failure cascade, for instance, to repair the previous failures that are still in a small number or to island the network to mitigate the power overloading. The detection of the critical elements deserves in-depth research.

6.2.3 Optimization of the Coupling Patterns

From the simulation results of cascading failures in the cyber-coupled network reported in Chapter 5, it is clear that the coupling patterns between the nodes in the power network and the nodes in the cyber network can have profound influences on cascading failure. It will be meaningful to optimize the coupling pattern that helps resist the failure propagating between the two networks.

6.2.4 Comparison of Different Failure Spreading Patterns

In Chapter 5, it has been shown that the propagation profile of the cascading failure in a power system is quite different from that of malware spreading in a cyber network. Our first explanation for the difference is that the failure spreading mechanisms in the two kinds of networks are very different [132, 133]. For the power grid, failures are caused by power overloading. Obeying Kirchhoff's laws, the power flow distribution is globally determined, and the failure of one element in the network can influence the power flows of all the other elements. Thus, there exist critical nodes whose removal can change the power flow distribution drastically and cause an abrupt jump of the failure growth. Such kind of mechanism also exists in other delivery networks. For example, in a communication network with a shortest-path-based routing algorithm, removing one node from the network can change the shortest path distribution in the whole network, thus influencing the traffic load of a large number of nodes. However, for the malware spreading in a cyber network, one infected node can only influence its

neighboring nodes, termed as local effects. The failure under the local effects grows smoothly. We can also find many other similar examples, like rumor spreading in an online social network, evolutionary dynamics in the field of game theory, and so on. Thus, it is of fundamental importance to verify the above hypothesis regarding the global and local effects on spreading profiles and to examine whether these phenomena also exist in other similar networks by performing in-depth analytical and empirical studies.

Bibliography

[1] J. Travers and S. Milgram, "An experimental study of the small world problem," *Sociometry*, vol. 32, no. 4, pp. 425–443, Dec. 1969.

[2] R. Albert, H. Jeong, and A.-L. Barabási, "Diameter of the world-wide web," *Nature*, vol. 401, no. 6749, pp. 130–131, Sept. 1999.

[3] B. A. Huberman and L. A. Adamic, "Growth dynamics of the world-wide web," *Nature*, vol. 401, no. 6749, pp. 131–131, Sept. 1999.

[4] M. E. Newman, "Power laws, pareto distributions and zipf's law," *Contemporary Physics*, vol. 46, no. 5, pp. 323–351, Feb. 2007.

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

[6] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

[7] A. L. Barabási, *Network Science*. UK: Cambridge University Press, 2016.

[8] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, p. 3200, Apr. 2001.

[9] X. F. Wang and G. Chen, "Synchronization in small-world dynamical networks," *International Journal of Bifurcation and Chaos*, vol. 12, no. 01, pp. 187–192, Jan. 2002.

[10] A. Vazquez, A. Flammini, A. Maritan, and A. Vespignani, "Global protein function prediction from protein-protein interaction networks," *Nature Biotechnology*, vol. 21, no. 6, pp. 697–700, May 2003.

[11] C. K. Tse, J. Liu, and F. C. Lau, "A network perspective of the stock market," *Journal of Empirical Finance*, vol. 17, no. 4, pp. 659–667, Sept. 2010.

[12] X. F. Liu, C. K. Tse, and M. Small, "Complex network structure of musical compositions: Algorithmic generation of appealing music," *Physica A*, vol. 389, no. 1, pp. 126–132, Jan. 2010.

[13] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, no. 2, pp. 25–103, Feb. 2004.

[14] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 7, pp. 2465–2475, Jul. 2007.

[15] G. A. Pagani and M. Aiello, "The power grid as a complex network: a survey," *Physica A*, vol. 392, no. 11, pp. 2688–2700, Jun. 2013.

[16] V. Rosato, S. Bologna, and F. Tiriticco, "Topological properties of high-voltage electrical transmission networks," *Electric Power Systems Research*, vol. 77, no. 2, pp. 99–105, Feb. 2007.

[17] J. Ding, X. Bai, W. Zhao, Z. Fang, Z. Li, and M. Liu, "The improvement of the small-world network model and its application research in bulk power system," in *Proc. IEEE International Conference on Power System Technology*, Chongqing, China, 2006, pp. 1–5.

[18] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the Italian electric power grid," *Physica A*, vol. 338, no. 1, pp. 92–97, Jul. 2004.

[19] P. Hines, E. Cotilla Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, pp. 33–122, Sept. 2010.

[20] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[21] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS ICS and Electricity Information Sharing and Analysis Center, 2016.

[22] M. E. J. Newman, "Assortative mixing in networks," *Physical Review Letters*, vol. 89, no. 20, p. 208701, Oct. 2002.

[23] J. Wu, C. K. Tse, F. C. Lau, and I. W. Ho, "Analysis of communication network performance from a complex network perspective," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 12, pp. 3303–3316, Jun. 2013.

[24] D. Z. Chen, "Developing algorithms and software for geometric path planning problems," *ACM Computing Surveys (CSUR)*, vol. 28, no. 4es, p. 18, Dec. 1996.

[25] WikiPedia. Shortest path problem. [Online]. Available: https://en.wikipedia.org/wiki/Shortest_path_problem#cite_note-2

[26] L. Backstrom, P. Boldi, M. Rosa, J. Ugander, and S. Vigna, "Four degrees of separation," in *Proc. 4th Annual ACM Web Science Conference*, Evanston, USA, 2012, pp. 33–42.

[27] S. Bhagat, M. Burke, C. Diuk, I. O. Filiz, and S. Edunov. Three and a half degrees of separation. [Online]. Available: https://research.fb.com/three-and-a-half-degrees-of-separation/

[28] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, Mar. 1977.

[29] M. E. Newman and M. Girvan, "Finding and evaluating community structure in networks," *Physical Review E*, vol. 69, no. 2, p. 026113, Feb. 2004.

[30] S.-H. Yook, H. Jeong, and A.-L. Barabási, "Modeling the internet's large-scale topology," *Proceedings of the National Academy of Sciences*, vol. 99, no. 21, pp. 13 382–13 386, Oct. 2002.

[31] X. F. Wang and G. Chen, "Complex networks: small-world, scale-free and beyond," *IEEE Circuits and Systems Magazine*, vol. 3, no. 1, pp. 6–20, Sept. 2003.

[32] P. Erdös and A. Rényi, "On random graphs," *Publicationes Mathematicae*, vol. 6, no. 26, pp. 290–297, 1959.

[33] A. Fronczak, P. Fronczak, and J. A. Hołyst, "Average path length in random networks," *Physical Review E*, vol. 70, no. 5, p. 056110, Nov. 2004.

[34] N. Rubido, C. Grebogi, and M. S. Baptista, "Resiliently evolving supply-demand networks," *Physical Review E*, vol. 89, no. 1, p. 012801, Jan. 2014.

[35] M. Rosas-Casals and B. Corominas-Murtra, "Assessing european power grid reliability by means of topological measures," *WIT Transactions on Ecology and the Environment*, vol. 121, pp. 527–537, 2009.

[36] K. Sun, "Complex networks theory: A new method of research in power grid," in *Proc. IEEE Transmission and Distribution Conference and Exhibition: Asia and Pacific*, Dalian, China, 2005, pp. 1–6.

[37] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos*, vol. 19, no. 1, p. 013119, Feb. 2009.

[38] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the european power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, p. 026102, Feb. 2008.

[39] D. P. Chassin and C. Posse, "Evaluating north american electric grid reliability using the barabási–albert network model," *Physica A*, vol. 355, no. 2, pp. 667–677, Sept. 2005.

[40] G. A. Pagani and M. Aiello, "Towards decentralization: A topological investigation of the medium and low voltage grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 538–547, Jun. 2011.

[41] Z. Wang, A. Scaglione, and R. J. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 28–39, Jun. 2010.

[42] E. Cotilla-Sanchez, P. D. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the north american electric power infrastructure," *IEEE Systems Journal*, vol. 6, no. 4, pp. 616–626, Feb 2012.

[43] L. A. N. Amaral, A. Scala, M. Barthelemy, and H. E. Stanley, "Classes of small-world networks," *Proceedings of the National Academy of Sciences*, vol. 97, no. 21, pp. 11 149–11 152, Oct. 2000.

[44] P. H. Nardelli, N. Rubido, C. Wang, M. S. Baptista, C. Pomalaza-Raez, P. Cardieri, and M. Latva-aho, "Models for the modern power grid," *arXiv preprint arXiv:1401.0260*, 2014.

[45] M. E. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167–256, Aug. 2003.

[46] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4, pp. 175–308, Feb. 2006.

[47] S. H. Strogatz, "Exploring complex networks," *Nature*, vol. 410, no. 6825, pp. 268–276, Mar. 2001.

[48] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, p. 47, Jan. 2002.

[49] WikiPedia. List of major power outages. [Online]. Available: https://en.wikipedia.org/wiki/List_of_major_power_outages

[50] T. G. Lewis, *Network Science: Theory and Applications*. Hoboken, NJ, USA: John Wiley & Sons, 2011.

[51] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, Dec. 2017.

[52] P. Crucitti, V. Latora, and M. Marchiori, "Locating critical lines in high-voltage electrical power grids," *Fluctuation and Noise Letters*, vol. 5, no. 02, pp. L201–L208, Jun. 2005.

[53] R. Baldick *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–8.

[54] P. S. Georgilakis and N. D. Hatziargyriou, "A review of power distribution planning in the modern power systems era: Models, methods and future research," *Electric Power Systems Research*, vol. 121, pp. 89–100, Apr. 2015.

[55] J. Bialek *et al.*, "Benchmarking and validation of cascading failure analysis tools," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4887–4900, 2016.

[56] A. Dwivedi, X. Yu, and P. Sokolowski, "Analyzing power network vulnerability with maximum flow based centrality approach," in *Proc. 8th IEEE International Conference on Industrial Informatics*, Osaka, Japan, 2010, pp. 336–341.

[57] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, Dec. 2002.

[58] J. W. Wang and L. L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, Dec. 2009.

[59] O. Yağan, "Robustness of power systems under a democratic-fiber-bundle-like model," *Physical Review E*, vol. 91, no. 6, p. 062811, Jun. 2015.

[60] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. Englewood Cliff, NJ, USA: McGraw Hill, 1994.

[61] WikiPedia. Power-flow study. [Online]. Available: https://en.wikipedia.org/wiki/Power-flow_study

[62] B. Stott, J. Jardim, and O. Alsaç, "DC power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, Aug. 2009.

[63] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. New York, NY, USA: Springer Science & Business Media, 2011.

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

[65] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts," in *Proc. 34th IEEE Hawaii International Conference on System Sciences*, Hawaii, USA, 2001, p. 51.

[66] M. J. Eppstein and P. D. Hines, "A random chemistry algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, Mar. 2012.

[67] B. Stott, J. Jardim, and O. Alsac, "DC Power Flow Revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, Jul. 2009.

[68] Z. Wang, A. Scaglione, and R. J. Thomas, "A markov-transition model for cascading failures in power grids," in *Proc. 45th IEEE Hawaii International Conference on System Sciences*, Hawaii, USA, 2012, pp. 2115–2124.

[69] F. Dörfler, M. Chertkov, and F. Bullo, "Synchronization in complex oscillator networks and smart grids," *Proceedings of the National Academy of Sciences*, vol. 110, no. 6, pp. 2005–2010, Feb. 2013.

[70] P. J. Menck, J. Heitzig, J. Kurths, and H. J. Schellnhuber, "How dead ends undermine power grid stability," *Nature Communications*, vol. 5, pp. 1–8, Jun. 2014.

[71] F. Dörfler and F. Bullo, "Synchronization in complex networks of phase oscillators: A survey," *Automatica*, vol. 50, no. 6, pp. 1539–1564, Jun. 2014.

[72] M. Rohden, A. Sorge, M. Timme, and D. Witthaut, "Self-organized synchronization in decentralized power grids," *Physical Review Letters*, vol. 109, no. 6, p. 064101, Aug. 2012.

[73] D. Witthaut and M. Timme, "Braess's paradox in oscillator networks, desynchronization and power outage," *New Journal of Physics*, vol. 14, no. 8, p. 083036, Aug. 2012.

[74] A. E. Motter, S. A. Myers, M. Anghel, and T. Nishikawa, "Spontaneous synchrony in power-grid networks," *Nature Physics*, vol. 9, no. 3, pp. 191–197, Feb. 2013.

[75] T. Nishikawa and A. E. Motter, "Comparative analysis of existing models for power-grid synchronization," *New Journal of Physics*, vol. 17, no. 1, p. 015012, Jan. 2015.

[76] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, Jan. 2014.

[77] S. Pahwa, C. Scoglio, and A. Scala, "Abruptness of cascade failures in power grids," *Scientific Reports*, vol. 4, pp. 1–9, Jan. 2014.

[78] M. Anghel, K. A. Werley, and A. E. Motter, "Stochastic model for power grid dynamics," in *Proc. 44th IEEE Hawaii International Conference on System Sciences*, Hawaii, USA, 2007, pp. 113–113.

[79] D. J. Klein and M. Randić, "Resistance distance," *Journal of Mathematical Chemistry*, vol. 12, no. 1, pp. 81–95, Dec. 1993.

[80] M. Youssef, C. Scoglio, and S. Pahwa, "Robustness measure for power grids with respect to cascading failures," in *Proc. International Workshop on Modeling, Analysis, and Control of Complex Networks*, San Francisco, USA, 2011, pp. 45–49.

[81] A. Scala, S. Pahwa, and C. Scoglio, "Cascade failures and distributed generation in power grids," *International Journal of Critical Infrastructures*, vol. 11, no. 1, pp. 27–35, 2015.

[82] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Transactions on Circuits and Systems I, Regular Papers*, vol. 51, no. 9, pp. 1733–1740, Sept. 2004.

[83] R. Christie. 118 bus power flow test case. [Online]. Available: https://www.ee.washington.edu/research/pstca/pg_tcaintro.htm

[84] L. Muchnik. Complex networks package for matlab. [Online]. Available: http://www.levmuchnik.net/Content/Networks/ComplexNetworksPackage.html

[85] A. G. Phadke and J. S. Thorp, *Computer Relaying for Power Systems*. Chichester, West Sussex, UK: John Wiley & Sons, 2009.

[86] W. Quattrociocchi, G. Caldarelli, and A. Scala, "Self-healing networks: redundancy and structure," *PloS one*, vol. 9, no. 2, p. e87986, Feb. 2014.

[87] S. H. Horowitz and A. G. Phadke, *Power System Relaying*. New York, USA: Wiley, 2008.

[88] M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*. New York, USA: Wiley, 2004.

[89] "1996 system disturbances," North American Electric Reliability Council, USA, Tech. Rep., 2002.

[90] U.S.-Canada System Outage Task Force, "Final report on the August 14th blackout in the United States and Canada," US Dept. Energy and National Res. Canada, Tech. Rep., 2004.

[91] Q. Chen, C. Jiang, W. Qiu, and J. D. McCalley, "Probability models for estimating the probabilities of cascading outages in high-voltage transmission network," *IEEE Transactions on Power Systems*, vol. 21, no. 3, pp. 1423–1431, Mar. 2006.

[92] I. Dobson, B. A. Carreras, and D. E. Newman, "Branching process models for the exponentially increasing portions of cascading failure blackouts," in *Proc. 39th IEEE Hawaii International Conference on System Sciences*, Hawaii, USA, 2005, p. 64.

[93] I. Dobson, "Estimating the propagation and extent of cascading line outages from utility data with a branching process," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 2146–2155, Feb. 2012.

[94] X. Zhang and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 456–464, Sept. 2015.

[95] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, Apr. 2014.

[96] P. Rezaei, P. D. Hines, and M. J. Eppstein, "Estimating cascading failure risk with random chemistry," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2726–2735, May 2015.

[97] H. M. Merrill and A. J. Wood, "Risk and uncertainty in power system planning," *International Journal of Electrical Power & Energy Systems*, vol. 13, no. 2, pp. 81–90, Feb. 1991.

[98] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, S. Mei, W. Wei, and L. Ding, "Risk assessment of multi-timescale cascading outages based on markovian tree

search," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2887–2900, Oct. 2016.

[99] Y. Sun, P. Wang, L. Cheng, and H. Liu, "Operational reliability assessment of power systems considering condition-dependent failure rate," *IET Generation, Transmission & Distribution*, vol. 4, no. 1, pp. 60–72, Jan. 2010.

[100] D. T. Gillespie, "A general method for numerically simulating the stochastic time evolution of coupled chemical reactions," *Journal of Computational Physics*, vol. 22, no. 4, pp. 403–434, Apr. 1976.

[101] D. T. Gillespie, "Exact stochastic simulation of coupled chemical reactions," *Journal of Computational Physics*, vol. 81, no. 25, pp. 2340–2361, Dec. 1977.

[102] K. Bae and J. S. Thorp, "A stochastic study of hidden failures in power system protection," *Decision Support Systems*, vol. 24, no. 3, pp. 259–268, Mar. 1999.

[103] F. Yang, A. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of protection system hidden failures on bulk power system reliability," in *Proc. 38th IEEE North American Power Symposium*, Carbondale, USA, 2006, pp. 517–523.

[104] J. Chen, J. S. Thorp, and M. Parashar, "Analysis of electric power system disturbance data," in *Proc. 34th IEEE Hawaii International Conference on System Sciences*, Hawaii, USA, 2001, p. 13.

[105] A. R. Bergen and V. Vittal, *Systems Analysis*. New York, USA: Tom Robbins, 2000.

[106] F. Milano, L. Vanfretti, and J. C. Morataya, "An open source power system virtual laboratory: The psat case and experience," *IEEE Transactions on Education*, vol. 51, no. 1, pp. 17–23, Jan. 2008.

[107] C. Zhan, C. K. Tse, and M. Small, "A general stochastic model for studying time evolution of transition networks," *Physica A*, vol. 464, pp. 198–210, Dec. 2016.

[108] R. Pfitzner, K. Turitsyn, and M. Chertkov, "Controlled tripping of overheated lines mitigates power outages," *arXiv preprint:1104.4558*, 2011.

[109] UIUC 150-bus system. [Online]. Available: http://icseg.iti.illinois.edu/synthetic-power-cases/uiuc-150-bus-system/

[110] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

[111] R. Baheti and H. Gill, "Impact of control technology," IEEE Control Systems Society, Tech. Rep., Mar. 2011.

[112] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[113] C. Lu, R. Rajkumar, and E. Tovar, "Guest editorial special section on cyber-physical systems and cooperating objects," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 2, pp. 378–378, May 2012.

[114] H. Gharavi, H.-H. R. Chen, and C. Wietfeld, "Guest editorial special section on cyber-physical systems and security for smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2405–2408, Sept. 2015.

[115] D. M. Nicol, "Hacking the lights out," *Scientific American: Science News, Articles and Information*, vol. 305, no. 1, pp. 70–75, Jul. 2011.

[116] M. Zeller, "Myth or reality – Does the Aurora vulnerability pose a risk to my generator?" in *Proc. 64th Annual Conference for Protective Relay Engineers*, College Station, USA, 2011, pp. 130–136.

[117] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[118] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sept. 2015.

[119] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[120] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sept. 2015.

[121] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, p. 631, May 2012.

[122] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliability Engineering & System Safety*, vol. 95, no. 12, pp. 1335–1344, 2010.

[123] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.

[124] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[125] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

[126] M. Rahnamay-Naeini and M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent markov-chain approach," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1997–2006, Mar. 2016.

[127] V. Karyotis and M. Khouzani, *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*. San Francisco, California, USA: Morgan Kaufmann, 2016.

[128] Y. Li, Y. Zhou, F. Liu, Y. Cao, and C. Rehtanz, "Design and implementation of delay-dependent wide area damping control for stability enhancement of power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1831–1842, Jul. 2017.

[129] Y. Li, F. Liu, and Y. Cao, "Delay-dependent wide-area damping control for stability enhancement of HVDC/AC interconnected power systems," *Control Engineering Practice*, vol. 37, pp. 43–54, Apr. 2015.

[130] S. Tang, "A modified SI epidemic model for combating virus spread in wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 18, no. 4, pp. 319–326, Apr. 2011.

[131] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publication of the Mathematical Institute of the Hungarian Academy Sciences*, vol. 5, pp. 17–61, 1960.

[132] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 9, pp. 5766–5771, Apr. 2002.

[133] P. D. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 958–967, Mar. 2017.