STUDY OF ROBUSTNESS OF CYBER-COUPLED POWER SYSTEMS FROM A COMPLEX NETWORK PERSPECTIVE

DONG LIU

PhD

The Hong Kong Polytechnic University

2019

The Hong Kong Polytechnic University

Department of Electronic and Information Engineering

Study of Robustness of Cyber-coupled Power Systems from A Complex Network Perspective

Dong LIU

A thesis submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

June 2019

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)

Dong Liu (Name of student)

Abstract

This thesis studies the robustness of smart grids from a complex network perspective. A power system can be modeled as a network consisting of nodes representing power substations and links representing power transmission lines. To study the cascading failure in power systems, we develop a network-based model combining a circuit-based power flow model with a stochastic model. Considering the effect of cyber coupling, a smart grid can be modeled as a cyber-coupled power system in which a power network is connected to a cyber network. To produce the propagation profile of the cascading failure caused by cyber attack, we further introduce a model by considering power overloading, contagion, and interdependence between power and cyber networks. The main objective of this thesis is to enhance the robustness of standalone power systems and power systems that are coupled with cyber networks by taking network-based approaches.

First, by examining the propagation profile of the failure cascade of power systems, we define the onset time as the time after which the propagation rate of the cascading failure increases rapidly. Based on the onset time and the scale of the failed grid in a cascading failure event, each component in a power network can be categorized into three types, corresponding to three levels of severity of the failed grid upon the initial failure of that component. Moreover, we propose a decision-tree-based learning model to enhance the robustness of power networks. The resulting decision tree identifies three network features in a power network, including average shortest path length, average clustering coefficient, and average effective resistance (distance) to the nearest

generator, which are highly correlated with the network robustness and can effectively contribute to robustness enhancement of the power network.

Then, we aim to find an effective interpretation of the interdependence between power and cyber networks in studying the cascading failure in cyber-coupled power systems. We consider the interaction between two processes, one aiming to attack and the other aiming to defend the components in the power network. Through evaluating the effectiveness of different attack and defense strategies by examining the actual propagation process of cascading failure events, it has been found that the tit-for-tat defense strategy, in which the defender adopts the same strategy as the attacker, is the preferred defense strategy. Moreover, allocating defense strength in terms of capacity-based distribution can most effectively suppress cascading failure.

Finally, we introduce a parameter, called relative coupling correlation coefficient, to quantify the coupling pattern of a cyber-coupled power system. In modeling coupled systems, coupling patterns, which are determined by some node criticality metrics, can describe how power and cyber nodes are connected. Simulation results show that a coupled system of lower relative coupling correlation coefficient has better robustness. Moreover, when optimizing the coupling pattern for robustness improvement, the adoption of node capability and node degree as node criticality metrics for power and cyber networks, respectively, would result in a much more robust network compared to the adoption of other node criticality metrics for robustness enhancement.

Publications

Journal papers

- **D. Liu** and C. K. Tse, "Effect of coupling patterns on robustness of cyber-coupled power systems," in preparation.
- **D. Liu** and C. K. Tse, "Cascading failure of cyber-coupled power systems considering interactions between attack and defense," *IEEE Transactions on Circuits and Systems I: Regular Papers*, to appear.
- **D. Liu**, C. K. Tse, and X. Zhang, "Robustness assessment and enhancement of power grids from a complex networks perspective using decision trees," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 5, pp. 833–837, Apr. 2019.
- 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.

Conference papers

- **D. Liu**, X. Zhang, and C. K. Tse, "Enhancing robustness of power grids using a complex network approach," in *Proc. IEEE International Symposium on Circuits and Systems, (ISCAS 2019)*, Sapporo, Japan, May 2019. **(Nominated**

as Best Student Paper Award and recommended to be published in the IS-CAS special issue in *IEEE Transactions on Circuits and Systems II: Express Briefs*)

- **D. Liu**, X. Zhang, and C. K. Tse, "Effect of malware spreading on propagation of cascading failure in cyber-coupled power systems," in *Proc. IEEE International Symposium on Circuits and Systems, (ISCAS 2018)*, Florence, Italy, May 2018.

- **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 (IFEEC 2017)*, 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 (ISCAS 2017)*, Baltimore, USA, 2017.

Acknowledgments

Foremost, I would like to express my sincere gratitude to my advisor Prof. C. K. Michael Tse for his continuous support of my Ph.D. study, for his patience, inspiration, enthusiasm, and immense knowledge. His guidance helped me at all times of my research including the writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study. He is a role model that I will keep learning from for a lifetime.

My special thanks are extended to Prof. Francis C. M. Lau, Prof. Guanrong Chen and Prof. Chao Lu, for encouraging me to pursue significant and challenging research.

I am particularly grateful to Dr Zhang Xi for his assistance and many constructive discussions. Our close collaboration has produced lots of ideas on the topic of complex network applications.

I am proud to be a member in the Nonlinear Circuit and Systems Group. In this group, I always feel we are a family and everyone here, current or former members, helps each other a lot. I would like to express my appreciation for their company that makes my four-year study more enjoyable.

I would like to thank the Research Committee of the Hong Kong Polytechnic University for the provision of financial sponsorship during the entire period of my Ph.D. study. I also appreciate the Office of Student Resources and Residential Life for offering me a great chance to become a hall tutor during my Ph.D. study period.

Last but not least, I would like to thank my parents for supporting me spiritually throughout my life.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

A complex system is a system consisting of a large number of interacting components. Complex systems are around us and examples of complex systems include power grids, communication systems, human brains and so on. The emergence of network science leads to a network representation of a complex system. Basically, in a complex system, components are modeled as nodes and the interactions among the elements are modeled as links, and these edges and nodes form a *network* or *graph* [3]. Network-based approaches provide powerful tools to study the structure and the dynamics of complex networks which can be applied to the real-life complex systems.

Network science has been originated from a branch of mathematics called *graph theory*. In 1736, network science was first applied to solve real-life problems, when the Swiss mathematician Euler published a solution to the historically notable problem, Seven Bridges of Königsberg, based on *graph theory*. Königsberg, a city in Prussia, contains four lands (including two islands and two mainland portions) separated by the river named Pregel while four lands are connected by seven bridges. A question is raised whether there is a solution to arrange a walk through the city that would cross each of the seven bridges once and only once. Euler proved that the problem cannot be

addressed by formulating the problem in an abstract mathematical term. In particular, four landmasses were abstracted as four nodes and seven bridges were abstracted as seven links. The resulting mathematical structure is characterized as a *graph* and it is found that the problem can only be addressed if each node in the graph has an even number of links.

Graph theory has been developed and then widely applied to studying real-life systems since Euler's analysis of the problem of Seven Bridges of Königsberg. Furthermore, with the increasing scale of the *graph*, the study of *complex network* has developed as a new direction of research interest.

In 1959, two Hungarian mathematicians Paul Erdös and Alfréd Rényi, first introduced an algorithm of generating a random graph [4], which is recognized as a milestone in the history of graph theory. The generation of an Erdös and Rényi (ER) random graph is simple. A network is constructed by adding m links between pairs of nodes randomly selected from n nodes. In ER random networks, a Possion node degree distribution is observed. Because of the simplicity of the network generation process, ER random networks have become major network models to be studied.

The ER random network model is not enough to comprehend and analyze real-world systems, which are not fully randomly constructed. In the late 1990s, two main significant network models were published, namely, small-world networks and scale-free networks.

The small-world phenomenon was first discovered in the "six degrees of separation" experiment led by Stanley Milgram in 1967 [4]. The objective of this experiment was to figure out the average shortest path length of the American social networks. In the experiment, two persons randomly invited from Sharon and Boston were selected as two target points and two groups of peoples from Kansas and Nebraska volunteered as start points. Each of the volunteers from the start points was asked to send a letter to his/her friend until the letter reaches one of the persons in two target points. The experiment showed that the average path length was 5.2 hops, meaning the letter can be

forwarded from one person to another person via 5.2 intermediate friends on average, which is characterized as a small-world phenomenon in a social network.

In 1998, Watts and Strogatz identified *the small-world network* [1], by analogy with the small-world phenomenon. In their study, a rewired procedure was developed to rewire edges in a ring lattice (regular network) with n nodes and k links with a probability p. It is found that for an intermediate value of p, the rewired graph is a small-world network, which is highly clustered like a regular graph and has a small shortest path length, similar to a random graph.

In 1999, Albert *et al*. [5] discovered a power-law degree distribution in the World Wide Web, in which web resources are identified by Uniform Resource Locators (URLs) and interconnected by hypertext links. By considering the URLs as nodes and the hypertext links as links, the resulting network showed that the distribution of the number of both incoming and outgoing hypertext links of URLs follow a power law [6]. The network whose degree distribution follows a power-law is characterized as a *scale-free network*, where a large majority of nodes have a low degree and only a small number of nodes have a relatively high degree. Barabási and Albert introduced a growth model to generate a scale-free network using a preferential attachment mechanism [7].

Since then, the small-world and scale-free network models have inspired more and more researchers to broaden the field of network science [8]. The structures and dynamics of various complex systems have been investigated from a network science perspective [9] and a series of applications to real networks include the analysis of metabolic and genetic regulatory networks [10], the study of infrastructure stability and robustness [11], the performance of communication systems [12], the model of epidemic spreading for the control of disease [13] and so on.

Power systems, being critical infrastructures in modern society, have been studied using a complex network approach to assess and enhance their robustness. A highly robust power system generally means it can survive without large-scale power outage

after a cascading failure. To answer the question concerning which kind of topology can achieve high robustness, the initial phase of modeling power systems using network-based approaches mainly focuses on the analysis of some general topological properties [14]. Then, the physical processes of cascading failure have been considered, which improve the effectiveness and practicality of the network-based approaches used for revealing the robustness of power systems and also for identifying the critical components [15].

Complex systems in the Industry 4.0 era are highly interactive and thus should be modeled as interdependent networks or coupled networks. For instance, power systems nowadays are coupled with communication networks, and have evolved as smart grids [16]. Because of the interactions in interdependent networks, the failure of a component in one network can cause the failure of other components in other networks [17]. The proposed interdependent network model has attracted a great deal of attention from researchers to explore the network property of interdependent systems.

Cyber-physical systems have emerged as essential networked systems that enable the incorporation of computational and intelligent management capabilities provided by sophisticated computer networks in critical applications for residential, commercial, industrial and military uses [18]. A cyber-physical system is a physical system integrated with cyber networks. The cyber part of the system provides intelligent and efficient monitoring, control, computing and communication functions [19]. Real-world examples of cyber-physical systems are numerous, and the smart grid is one particularly important example. A smart grid is an electric power distribution network supported by advanced cyber networks, and is a critical infrastructure delivering power to a large population of users [20]. Cyber security has become a key challenge to power delivery systems due to the involvement of cyber networks that makes smart grids vulnerable to attacks via cyber coupling [21]. For instance, in December 2015, the attack of computer malware from cyber networks caused a severe outage of the Ukrainian power grid, demonstrating that the cyber attack on power grids was no longer a fic-

tional event. Modeling smart grids as interdependent networks, the robustness of smart grids considering cyber attack can be assessed and further improved.

1.2 Motivation

Complex network theory provides effective bias for analyzing the robustness of power grids. By abstracting power substations as nodes and transmission lines as links, a bond is constructed between the structural vulnerability and the connectivity of power grids. Moreover, to review a blackout event, cascading failure of power systems should be studied, which corresponds to a sequence of tripping events of power components, eventually resulting in a large-size power outage. Various models have been developed to understand the cascading failure process for the purpose of enhancing the reliability and performance of power systems. However, some difficult challenges are to be addressed.

First, although the highly abstracted and generalized network-based model offers a convenient framework permitting the use of statistical physics, it is inadequate to implement these high-level models to real-world power systems without considering the underlying physical processes. In the cascading failure process, one of the main reasons of component failure is the power flow overloading. Therefore, Kirchhoff's laws and electrical properties of components are crucial in generating the necessary power flow information in a power network.

Second, the coupling of cyber networks can increase the efficiency and intelligence of smart grids while it may bring new challenges by making power systems more vulnerable to attacks from cyber networks. A smart grid can be modeled by a cyber-coupled power system consisting of a power grid and a coupling cyber network. Due to the coupling between the cyber network and the power system, a cyber attack can be launched by computer malware to power components while the malware can continue to spread over the cyber network. Thus, the dynamic property of malware spreading

should be considered in the propagation of cascading failure in the case of smart grids by using an interdependent network model.

Third, the interpretation of the interdependence between cyber networks and power networks plays an important role in the study of cascading failure in cyber-coupled power systems. Attacker can access the power network and cause damage to power components by infecting malware to cyber networks. At the same time, a defender can protect the components from being tripped due to power flow overloading and cyber attack. Therefore, the interaction between attack and defense is relevant to the study of the cascading failure of cyber-coupled power systems. This offers a novel perspective to interpreting the interdependence of power and cyber networks.

Fourth, coupling patterns, which reveal how a power node and a cyber node is connected based on the node criticality metrics in coupled networks, have a considerable impact on the robustness of cyber-coupled power systems. The coupling pattern is a critical topological property in the interdependent network model. By using the network-based model with consideration of physical power flow processes and the coupling pattern, we aim to investigate the effect of coupling patterns on the robustness assessment and enhancement cyber-coupled power systems.

The main objective of this thesis is to develop a network-based model to study cascading failure in cyber-coupled power systems, with emphasis on the robustness assessment and enhancement of power systems.

1.3 Thesis Organization

The remainder of this thesis is organized as follows.

Chapter 2 provides a literature review. A brief introduction of complex network theory, robustness assessment of power systems, cascading failure models in power systems and cascading failure in cyber-coupled power systems are reviewed.

Chapter 3 introduces a model that combines a circuit-based power flow model with

a stochastic model to describe the uncertain failure time instants, aiming to generate a complete dynamic profile of the cascading failure propagation beginning from a failure of component and developing eventually to a large-scale blackout in power networks. Then, considering the effect of power overloading, contagion, and interdependence between power grids and cyber networks on failure propagations in the coupled system, another model is proposed to investigate the cascading failures in a coupled system (smart grid) consisting of a power grid and a coupling cyber network.

Chapter 4 offers an alternative approach to assess and enhance the robustness of power grids. We identify the onset time, which is the time after which the propagation rate of a cascading failure increases rapidly. Based on the onset time and the scale of the failed grid in a cascading failure event, we categorize each component in a power network into three types, corresponding to three levels of severity of the failed grid upon the initial failure of that component. Moreover, to investigate robustness enhancement of power networks, we propose a decision-tree-based learning model to extract significant network-based features. Notably, the characterization of the criticality of power components is able to provide a novel perspective to further explore robustness enhancement of cyber-coupled power systems.

Chapter 5 further discusses the robustness of cyber-coupled power systems emphasizing the interdependence between power and cyber networks. A network-based model with consideration of the physical power flow process is developed to study the cascading failure in cyber-coupled power systems. Interaction between two processes, one aiming to attack (cause damage) and the other aiming to defend (protect) the components in the power network, is considered in the model. The failure propagation profile is investigated by detailed time series analysis of four critical time points, and the effectiveness of different attack and defense strategies are analyzed and evaluated.

Chapter 6 studies the effect of coupling patterns on the robustness of cyber-coupled power systems. A crucial parameter called relative coupling correlation coefficient is introduced to quantify the coupling patterns of coupled systems. Different classes of

coupling patterns with consideration of node criticality metrics in the cyber and power networks are proposed to examine how they affect the robustness of coupled systems.

Chapter 7 concludes the thesis with a summary of the major findings of the project and a presentation of some thoughts on future works.

The overall framework of this thesis is depicted in the schematic diagram shown in Fig. 1.1

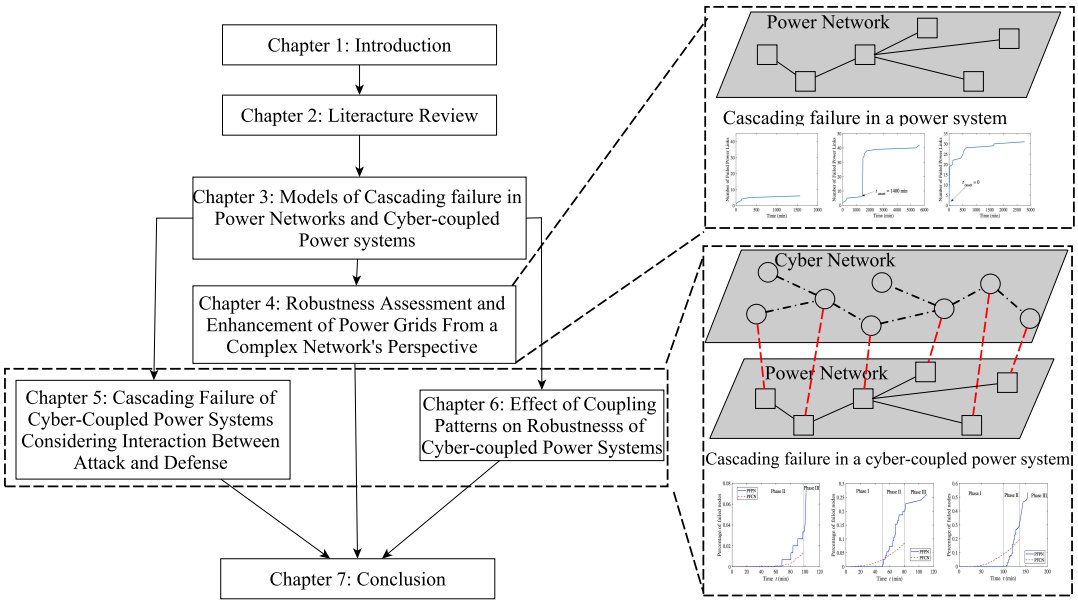


Figure 1.1: Illustration of the overall structure of this thesis.

Chapter 2

Literature Review

In this chapter, a brief introduction of complex networks, covering measures of network topology, models of networked systems, and interdependent networks, is given. Then, two main classes of approaches, namely, analysis of pure structural vulnerabilities with and without consideration of electrical properties, are discussed for the purpose of assessing the robustness of power systems. To gain a comprehensive understanding of the vulnerability of power systems to cascading failure, the main research directions aiming to develop models of cascading failure in power systems with and without the coupling of cyber networks are reviewed.

2.1 A Brief Introduction to Complex Networks

Complex network theory has become one of the mainstream methodologies for modeling real-world complex systems. The main contribution of applying complex network theory is the provision of an effective analytical basis for studying how network structure influences the functional behavior of network-based systems. This section introduces some measures of network topology, models of networked systems, and interdependent networks.

2.1.1 Measures of Network Topology

To explore the topological properties of complex networks, some important measures that are most widely used are reviewed, including node degree, degree distribution, shortest path length, clustering coefficient and so on.

Node Degree

A network is constructed by a bunch of nodes which are connected by edges. The *degree*, being a simple and basic metric, is used to measure the topological criticality of a node in a network. In an undirected network where the edges have no direction, the degree k_i of node i refers to the number of edges incident with the node i. In a directed network where the edges are unidirectional, the *out-degree* of a node refers to the number of outgoing edges from this node, and the *in-degree* refers to the number of incoming edges to this node.

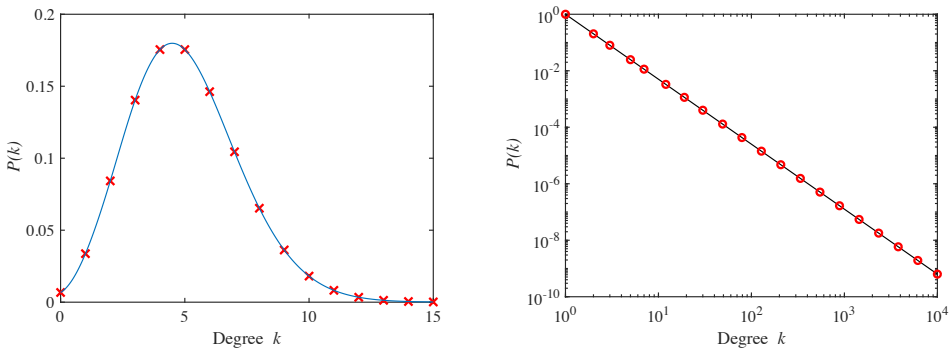
Node degree takes a crucial role in analyzing the real-world network. The nodes with higher degree can be characterized as *hubs* in a network which exhibit a greater importance in the analysis of the network structural vulnerability. Degree-based attack involving removal of a fraction of the nodes with higher degree has been identified as an effective strategy to cause a severe destruction of the network connectivity [22]. In other words, removing nodes with higher degree fragments the network more efficiently than removing the same number of nodes with lower degree.

Average Node Degree

To statistically overview the connection density of a network, the *average node degree* $\langle k \rangle$, representing the mean value of the degrees of all the nodes of the network, can be expressed 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. A higher $\langle k \rangle$ implies that the nodes in the network are more densely connected with each other.



(a) (b)

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

Node Degree Distribution

One more statistical metric describing the collective topological feature involving node degree is called *node degree distribution*, which refers to the probability that a node selected randomly has degree k. Node degree distribution, denoted by $P(k)$, can be written as

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

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

Two popular node degree distributions, namely, the Poisson distribution and power-law distribution, are demonstrated in Fig. 2.1(a) and Fig. 2.1(b), respectively. The Poisson distribution can be expressed in the form of $P(k) \sim e^{-\lambda}\lambda^{-k}/k!$, where λ is the average node degree of the network. According to Fig. 2.1(a), the peak of the curve is normally found when k is around the average node degree. Also, the network exhibiting a Poisson distribution of node degree is usually characterized as a homogeneous network. But many empirical studies have shown that the degree distribution in most large-scale real networks does not follow the Poission distribution. Most real networks have the node degree distribution obeying the power-law distribution, denoted as the form of $P(k) \sim k^{-\gamma}$, where γ is the degree exponent. As shown in Fig. 2.1(b), if a

network has a power-law degree distribution, it can be described as a heterogeneous network. Generally, for this kind of networks, most of the nodes have a few edges while only a small fraction of nodes have very large degree.

Degree-Degree Correlation

Another topological property relevant to the node degree is *degree-degree correlation*, which reveals the mixing way in which nodes with different degrees are connected. A measurement is provided to quantify the degree-degree correlation called *assortativity coefficient*, which is defined as

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

where k_i and k_j are the degrees of nodes i and j, respectively, M is the set of edges in the network, and m is the number of edges in M. Here, $r > 0$ means that high-degree nodes are more likely to connect to high-degree nodes in the network exhibiting assortativity. On the contrary, $r < 0$ implies that high-degree nodes tend to connect to low-degree nodes in the network which is regarded as a disassortative network. It has been found from empirical studies [23] that most social networks are assortative while most technical networks, such as power grids and biological networks, are disassortative.

Shortest Path

The *shortest path* between nodes i and j in a network is the path with the fewest number of edges between nodes i and j. The distance between nodes i and j, denoted by d_{ij}, is defined as the number of edges contained in the shortest path connecting these two nodes. There can be multiple shortest paths of the same distance between a pair of nodes. Shortest path takes an essential role in characterizing the internal structure of a network. There are many applications of the shortest path. For example, the shortest

path can be used to optimize efficiency in the data transmission of a communication network and delivery of payloads in a transportation network. An efficient algorithm to find the shortest path has become a classical problem in computer science [24]. The largest distance between any pair of nodes, which is the maximum distance among all distances in a network, is termed *diameter*.

Average shortest path length is a typical metric used for measuring the separation between two nodes in a network. Denoted by L, *average shortest path length* is defined as the mean distance between all pairs of nodes in the network with N nodes, which is given by

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

It has been found that in a large-scale social network, the value of L is small, and is equal to 4 and 3.5 based on the the study of the online social network Facebook in the year 2012 [25] and the year 2016 [26], respectively. In other words, with the rapid development of Internet, distance between people in this world becomes shorter and shorter.

Betweenness Centrality

Betweenness centralities of a node and an edge in a network have been proposed to account for the importance of the nodes and edges contained in the shortest path. The betweenness of node i is the number of the shortest path passing through it, which is expressed by

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

where σ_{st} is the number of all the shortest paths from node s to node t, and $\sigma_{st}(i)$ is the number of the shortest paths that pass through node i.

The similar concept of betweenness can be extended to an edge (i, j) connecting nodes i and j. The edge betweenness denoted by B_{ij}, is the number of shortest paths

between any pair of nodes that pass through edge (i, j), which can be expressed 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 pass through edge (i, j).

Both betweenness of nodes and edges serve to measure the frequency of the nodes and edges contained in the shortest path between any pair of nodes in a network. The node betweenness, regarded as a metric of node importance, takes an essential role in communication networks because a node with larger betweenness usually implies that it carries heavier traffic load when taking the shortest path routing strategy for performing data transmission. The edge betweenness can be used for identifying the community structure, where the nodes are tightly connected with each other. The edge with larger betweenness is usually considered to be the interconnection between two different communities. An effective approach based on the removal of the large-betweenness edges is proposed to effectively split the network into different communities [27].

Clustering Coefficient

The *clustering coefficient* is a measure of the extent to which the neighbors of a given node connect to each other in a network. At most $k_i(k_i - 2)/2$ edges can be connected among the neighbors of node i with degree k_i. The clustering coefficient of node i, denoted by Γ_i, is determined by the ratio of the number of existing edges E_i connecting the neighbors of node i, i.e.,

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

To capture the extent of clustering from a whole network's perspective, *average clustering coefficient* is found by averaging the Γ_i over all N nodes in the network, i.e.,

$$\Gamma = \frac{1}{N}\sum_{i=1}^{N} \Gamma_i. \tag{2.8}$$

The concept of the clustering coefficient comes from a question that how many of your friends are also friends themselves, which indicates the extent of the existence of clusters. Empirical studies have found that the clustering coefficients of real-world social networks are usually high because friends of an individual are more likely friends of each other as well. For hierarchical networks, the clustering coefficient is relatively low like the Internet and power grids [28].

2.1.2 Models of Network Topology

Also, three elegant network models, including the Erdös-Rényi (ER) random network models, the Watts-Strogatz (WS) small-world network model, and the Barabási-Albert (BA) scale-free network model, are developed to categorize networks with similar topological properties. The network models provide a platform permitting the statistical analysis of the dynamics and the structures of networks.

ER Random Network

The ER random network model is applied to generate a random network, where an edge is assigned to connect each node pair with a given probability. This model is initially proposed by Erdös and Rényi in 1959 [4] to provide a mechanism to construct a random network in two steps. The first step is to fix N isolated nodes and the second step is to connect each pair of nodes by an edge with a given probability p. An ER random network with a large N has totally $pN(N-1)/2$ edges and its average node degree is given by $\langle k \rangle = (N-1)p \approx Np$.

The node degree distribution of an ER random network follows a Poission distribution, which can be expressed as

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

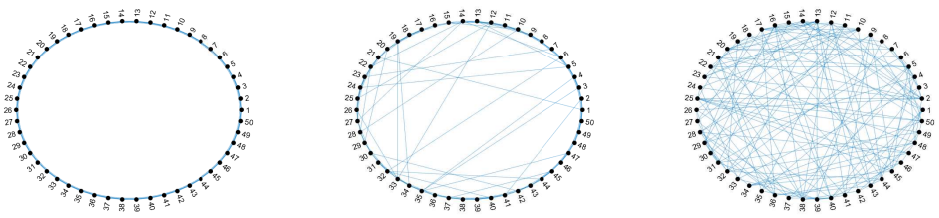
The ER network can be regarded as a homogeneous network and usually has relatively small average path length denoted by $L_{\text{random}} \sim \ln(N)/\ln(\langle k \rangle)$ and low clustering

coefficient denoted by $\Gamma_{\text{random}} \sim \langle k \rangle / N$. The ER network offers a baseline for comparison with other types of networks. However, the ER network can hardly describe a real-world network due to the very different network characteristics.

WS Small-world Network Model

The WS small-world network model was proposed by Watts and Strogatz [1] in 1998, which is used to produce a network exhibiting the small-world effect. The networks generated by WS small-world network model have short average path length and relatively high clustering coefficient, which mimic most of real-world networks in empirical studies and demonstrate very different network properties from those of random networks and regular networks.

The generation of a WS small-world network is based on a rewiring process which rearranges the links in a regular network exhibiting a large average path length and high clustering coefficient to a random network with a small average path length and a low clustering coefficient. Starting with a regular network which has N nodes with the same degree k, an edge in the network is rewired with a probability p by randomly selecting another node to replace one of its terminal nodes. Fig. 2.2 depicts a random rewiring procedure for interpolating between a regular ring lattice and a random network with a given probability p. During the process of rewiring, both of the average path length $L(p)$ and the clustering coefficient $\Gamma(p)$ are characterized as functions of probability p which represent the likelihood of transition of the rewired network features, as shown in Fig. 2.3. The initial regular network, when $p = 0$, is characterized as a highly clustered network with a large average path length, where $\Gamma(0) \approx 3/4, L(0) \approx N/2\langle k \rangle$. Considering $p = 1$, the rewired network becomes a random network, where $\Gamma(0) \approx \langle k \rangle / N$ and $L(0) \approx \ln(N)/\ln(\langle k \rangle)$, showing a relatively small average path length and low clustering coefficient compared with the original regular network. When p is tuned from 0 to 1, one typical rewired network emerges which has the shortest path length close to that of the random network and the clustering coefficient similar to that of the regular network. The rewired network is called SW small-world network.



(a) (b) (c)

Figure 2.2: Random rewiring procedure for interpolating between a regular ring lattice and a random network with a given probability p: (a) $p = 0$, (b) $p = 0.15$, (c) $p = 1$.

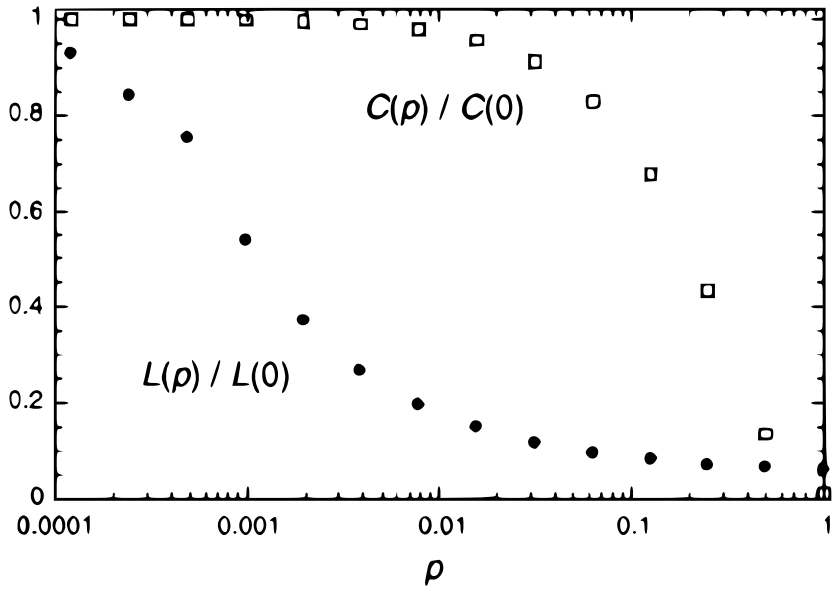


Figure 2.3: Average path length and clustering coefficient of the randomly rewired networks between a regular ring lattice and a random network with a given probability p. $C(p)/C(0)$ and $L(p)/L(0)$ decrease at different rates as p increases. The interim networks exhibit small-world properties. This figure is extracted from *Nature* [1].

The characteristics of an SW small-world network reassemble many large-scale social networks. Many clusters are usually formed in social networks indicating that the friends of one individual are usually also friends of others. Moreover, the average shortest path length of a social network is small because most people know each other through a few common friends of them.

BA scale-free Network Model

A large number of networks in reality display a power-law degree distribution while

networks with a Poission degree distribution is hard to found. Such class of networks are defined as scale-free networks where a few nodes with a high degree serve as a hub and most of the nodes have low degree.

Barabási and Albert [7] introduced a network generation model to reproduce scale-free networks based on two main ingredients, one being the growth and the other being preferential attachment. The algorithm of creating a BA scale-free network consists of two rules:

(1) One new node at each time step will be added to the network with the connection of the existing nodes in the network.

(2) The probability Π_i that a new edge between the newly added node and the existing node i will be connected is given by $\Pi_i = k_i / \sum_j k_j$, where k_i is the degree of node i.

Based on the two rules, the degree distribution follows a power law with the growth of the network. The power law, i.e., $P(k) \sim k^{-3}$, implies that the probability that a node with degree k is found is proportional to k^{-3}, regardless of the network scale.

The BA scale-free network captures the topological characteristics of many real-world networks such as the online social network Wikipedia [29] and the Protein-protein interaction network [30]. The scheme of preferential attachment mimics the evolution of many real-world networks. In all these networks, new nodes are more likely to link with the nodes having more connections. For example, in a citation network, if one paper has more citations, it is more likely to be read and then cited again. Such a highly cited paper is exactly represented by a node with higher degree in the citation network.

2.1.3 Interdependent Networks

A single and isolated network can not adequately describe many real-world complex systems which interact with and rely on other systems. For example, a power grid

nowadays is connected with a cyber network in order to make the power grid more efficient and intelligent by inserting advanced sensing and control functions.

The emergence of the study of interdependent networks (coupled networks) has provided a convenient framework to assess the robustness of interdependent networks. In particular, the robustness assessment of interdependent networks focuses on the influence of interdependency among the comprised networks.

Buldyrev *et al*. [17] developed a mathematical framework to study cascading failure in interdependent networks aiming to assess their vulnerabilities to attacks. The model consists of two networks A and B. Either network A or B has the same number of nodes N. The connection style between nodes of network A and network B is one-to-one, meaning that there only exists one edge connecting node A_i in network A and node B_i in network B. For the interdependency between the coupled nodes A_i and B_i, a simple assumption is made that the normal operation of node A_i relies on the support of node B_i and vice versa. In other words, the failure of node B_i leads to the failure of node A_i, and the malfunction of node A_i may cause the malfunction of B_i as well.

The cascading failure of such interdependent networks is modeled by an iterative process, as illustrated in the Fig. 2.4. Starting with removing one node a_5 from network A, the interdependent network is fragmented. In the first stage, the node connected to the removed node is also taken away from network B. Also, network A is split into three isolated clusters due to the removal of the links connecting the initially removed node a_1 to other nodes in network A. In the second stage, the links within network B of that connect nodes having connections with cluster A_{C1} are eliminated, and thus network B decomposes into four clusters. In the final stage, similarly, the links within network A that connect nodes having connections with cluster B_{C1} are eliminated, and thus network A decomposes into four clusters. Eventually, there is no more decomposition in both networks A and B. Here, both clusters A_{C1} and B_{C1} are regarded as giant mutually connected clusters which function normally and their sizes are used to evaluate the extent of survival of the interdependent networks after the iterative process of

cascading failure. In this work, an analytical solution based on the percolation theory is presented to point out that a broader degree distribution makes interdependent networks more vulnerable to random attack. This remarkable conclusion offers a crucial insight of how to design more robust interdependent networks.

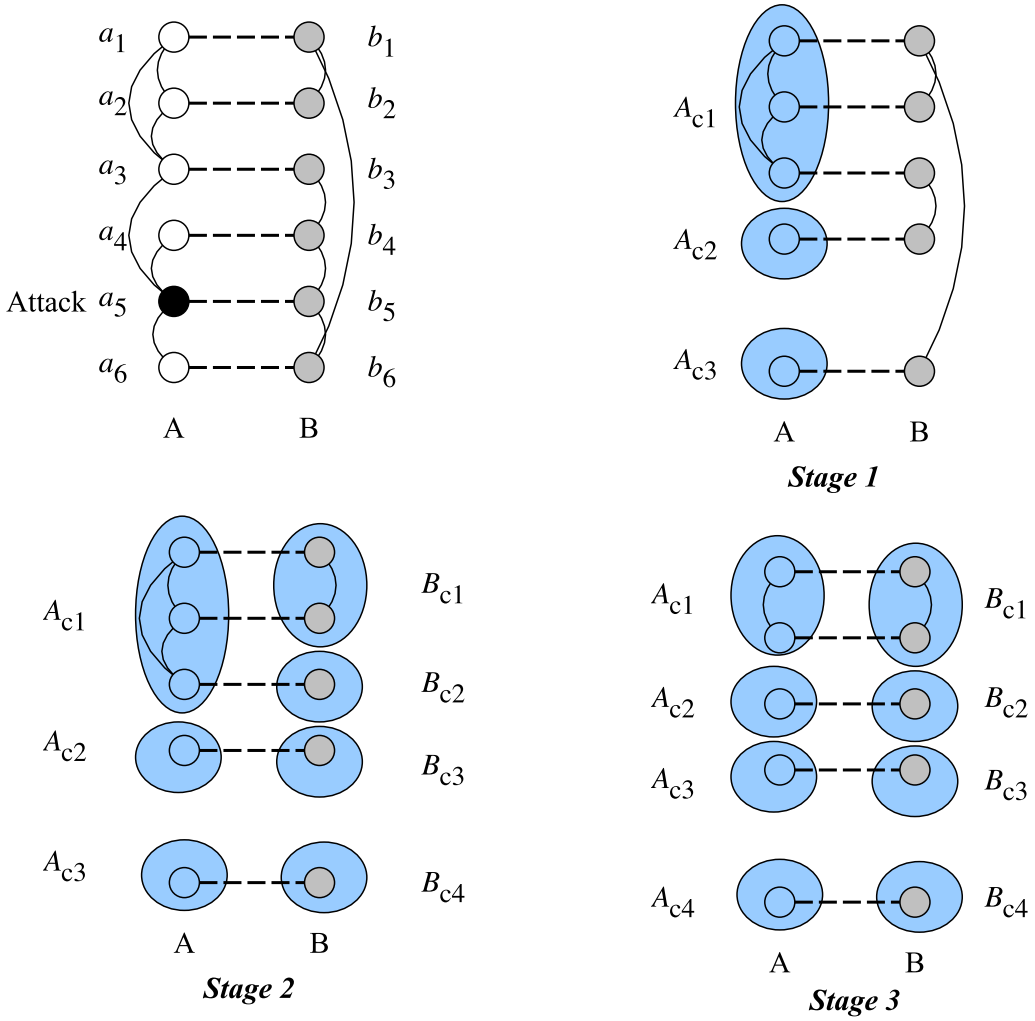


Figure 2.4: Modeling an iterative process of cascading failure of interdependent networks.

An increasing number of studies following this initial work [17] have been published, which have improved our understanding of the robustness of interdependent networks. As the initial failure can be chosen randomly or might be targeted by selecting among a set critical nodes such as nodes with high degree, Huang *et al*. [31] devel-

oped a mathematical framework to examine the robustness of interdependent networks under an initial targeted attack. Using a general technique which maps the targeted-attack problem in interdependent networks to the random-attack problem, it is found that strategies dedicated to defend an interdependent network such as protecting the high degree nodes can not improve the robustness of an interdependent network.

Different from the interdependent networks studied in [17], where all the nodes in networks *A* and *B* are coupled, Parshani *et al*. [32] developed a model to study the iterative cascade of failures in interdependent networks where a fraction of nodes in network *A* and network *B* are interconnected. The analytical and numerical results show that reducing the coupling strength between the networks, i.e., the fraction of the interdependent nodes, leads to a change from a first order percolation phase transition to a second order percolation transition at a critical point.

The observation of many interdependent systems has pointed out that the dependent pairs of nodes in both networks might not be chosen randomly. Instead, it has been found that a high-degree node in one network is more likely to connect a high-degree node in the other network. To quantify the coupling pattern, which is the way in which node pairs are coupled between the two networks, two metrics are proposed in Parshnani *et al*.'s work [33] and both of them serve to measure the level of inter-similarity between the networks. The first metric is called inter degree-degree correlation (IDDC) and a high value of this metric indicates that the nodes with similar numbers of edge connections in both networks tend to be interdependent. The second metric is inter-clustering coefficient (ICC), a value of which indicates that the neighbors of interdependent nodes in the two networks are more likely to be coupled. The results based on both a simulation model and the analysis of real port-airport system suggest that the interdependent networks are more robust if they have a higher inter-similarity level. Consistent findings are witnessed in the study of cooperation between layered networks [34]. A special case [35] where all coupled pairs of nodes are of the same degree was studied by formulating and solving an analytical problem and the

findings of this study are consistent with the aforementioned work [34].

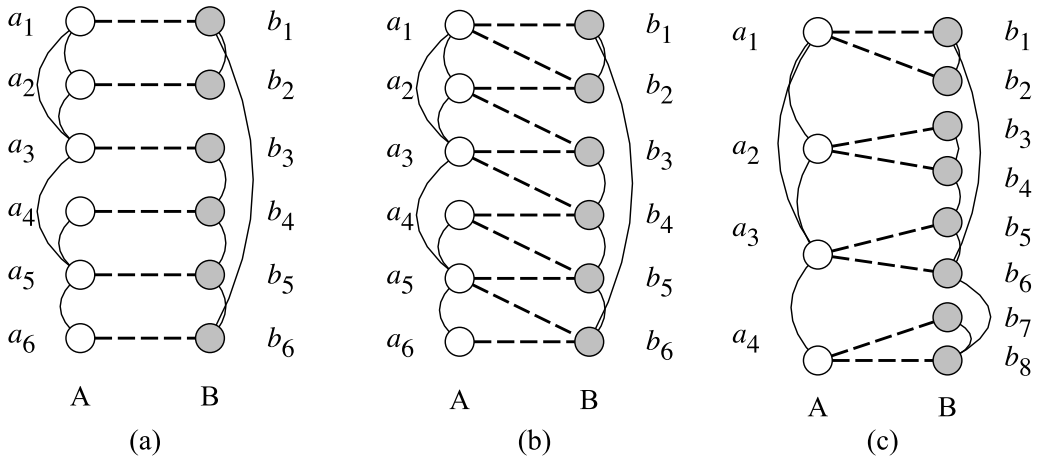


Figure 2.5: Coupling styles of interdependent networks: (a) one-to-one correspondence, (b) one-to-multiple correspondence and (c) multiple-to-multiple correspondence.

Considering an interdependent network consisting two networks A and B, Shao *et al*. [36] pointed out another restriction that a node in network A might not depend on only one node in network B, and vice versa. Two more models of interdependent networks are thus introduced, namely, the multiple-to-multiple correspondence and one-to-multiple correspondence, as shown in Fig. 2.5. For a multiple-to-multiple correspondence, it is assumed that one node in network A can provide support to multiple nodes in network B, while one node in network B can provide support to multiple nodes in network A. Based on this coupling style, failure of one node in network A may not lead to failure of its coupled node in network B and vice versa. In Huang *et al*.'s study [37], the robustness of a real-world interdependent system, namely, a modern smart grid consisting of a communication network and a power network, was studied by considering the interdependency between a communication network and a power network as a one-to-multiple correspondence. For each communication station, only one inter link is connected from the power grid because the communication nodes receive power from one specific power station. Each power station has multiple dependent communication nodes since normally it provides power to many communication

devices.

Improving network robustness is an essential topic not only for single networks but also for interdependent networks. Brummitta *at al*. [38] applied the BakTang-Wiesenfeld sandpile model to study the effect of interdependence on the cascading behavior of interdependent networks. The main finding of this work is that adding some connectivity between two networks is beneficial for suppressing the largest cascades while too much interconnectivity intensifies the cascades of failure. Methods for recovering an interdependent network before it totally collapses have been studied [39]. Specially, for a given initial failure of a fraction of nodes, a critical probability of recovery exists. Below this criticality probability of recovery, the cascade can be suppressed and the system can be restored back to its initial state.

2.2 Network Robustness of Power Systems

Power systems are complex systems serving as key components in vital infrastructures of today's society. One of the main concerns in the study of power systems is the assessment of their robustness, which is an essential indicator of how much damage would result from an unexpected event. Complex network theory provides an accessible tool to reveal the relationship between the robustness and the topological characteristics of power systems [14, 40]. To abstract a power grid as a network, generators, loads and substations are represented as nodes and these nodes are interconnected by edges used for representing transmission lines.

A first glance of power grids from a network topological viewpoint considers the basic information of power network, including the size of the network (i.e. the number of nodes and the number of links), the average node degree, the clustering coefficient and the average shorter path length. Table 2.1 summarizes the basic topological properties of different power networks from different regions [8]. In terms of the number of nodes and links, the scale of power network is relatively small compared with some

other kinds of large-scale networks like Internet [8]. The fourth column shows the average node degrees of six power networks being in the range from two to three, indicating that the stations in power networks are not connected very densely.

Table 2.1: Basic topological properties of different power networks including the number of nodes, the number of links, average node degree ($\langle k \rangle$), clustering coefficient (Γ) and average shortest path length (L) of different power networks.

Region	Number of nodes	Number of links	$\langle k \rangle$	Γ	$\Gamma/\Gamma_{\text{random}}$	L	L/L_{random}
West America [41]	4941	6594	2.67	0.080	148.045	18.7	2.159
North China [42]	8092	9018	2.23	0.002	6.169	32	2.852
Center China [42]	2379	2739	2.32	0.004	4.512	21.08	2.282
Italy [43]	127	171	2.69	0.156	7.365	8.47	1.730
France [43]	146	223	3.05	0.279	13.355	6.61	1.479
Spain [43]	98	175	3.57	0.316	8.675	4.92	1.366

The clustering coefficient and average shortest path length given in Table 2.1 are used to characterize the small-world property of power networks. A small-world network has its average path length similar to that of a random network of the same scale, and its clustering coefficient much larger than that of a random network [1]. It has been found that the size for a power grid might be optimized to reach an appropriate balance between vulnerability and efficiency [44]. For each power network given in Table 2.1, the clustering coefficient Γ and the average shortest path length L are compared with those of an ER random network of having the same number of nodes as the power network, denoted by $\Gamma/\Gamma_{\text{random}}$ and L/L_{random}. The power grid is regarded as a typical small-world network exhibiting the small-world network property if both conditions are met, i.e., $\Gamma/\Gamma_{\text{random}} \gg 1$ and $L/L_{\text{random}} \approx 1$. From Table 2.1, it is found that Western American and French power grids can be characterized as small-world networks and the other four power grids do not exhibit the small-world property.

One main aim in the study of robustness assessment of power grids from a complex

network's perspective is the discovery of network structures of power grids exhibiting high robustness. Previous work [41, 45] has indicated that the Western American power grids exhibits the small-world property. In Holmgren's work [45], it has been found that the analyzed electric power grids are more sensitive to attacks than the random graph. Focusing on the European power grids, it has been found [46] that the appearance of motif, characterized as some local patterns in the network such as stars and triangles, increases the vulnerability of power grids.

However, it is difficult to identify a predominant network topology which can abstract the structure of real-world power grids. In Albert *et al*.'s work [47], the exponential cumulative degree function was found in the North American power grid while Chassin *et al*.'s work [48] demonstrated the node degree distribution of North American power grid followed a power-law distribution. The small-world property can be identified in the Shanghai power grid [49] and some European power grids including [43, 45], Italian, French, Spanish and Nordic power grids. But in Rosas-Casals *et al*.'s work [50], power grids from a dataset containing 33 European power grids show an exponential degree distribution and most of them have insignificant small-world property. No consistent result has been obtained to suggest that the real-world power grid can be generalized as a small-world network or scale-free network. Analyzing the network robustness from real-world power grids instead of synthesized networks with general network topology offers more practical and meaningful results.

Another main goal of using network-based approaches to assess the robustness of power networks is the identification of the critical elements of power networks. The critical power elements are regarded as the nodes or links in a power network which, being removed, will lead to an unacceptable damage to the power network. Removal strategies are applied to evaluate the importance of the power elements in vulnerability analysis of power networks. Through sequentially or concurrently removing nodes or links in power networks [51, 52], the vulnerabilities of power networks are assessed according to the comparison of indicators such as the relative size of the largest con-

nected components [53] and the efficiency [54] recorded before and after a process of cascading failure.

Motter *et al*. [55] were among the earliest researchers who studied the cascading failure in the Westen American power grid. The results shown in this work indicated that more severe cascading failure in power grids could be triggered by the load-based intentional attacks than the random and degree-based removal of nodes. Albert *et al*. [47] examined the structural vulnerability of power grids by introducing another metric, i.e., the connectivity loss, which is used to measure the degradation of the capability of distribution nodes to take power from the generator. The main finding here is that for a given power network, intentionally attacking nodes with higher degree or higher load leads to a higher connectivity loss. Both of these studies offer an evidence that nodes or links with higher topological centrality like degree of nodes and links might not be sufficient to reflect their higher criticality in power networks.

Different from the pure topological metrics, the so-called electrical metrics are proposed as promising measures for identifying critical components in power grids. Such measures consider the inherent power flow parameters combined with the network-based approaches [40]. Thus, electric metrics offer effective information to examine the vulnerabilities of power grids.

Arianos *et al*. [56] developed a complex network approach to estimate the vulnerability of power networks. The newly proposed net-ability which considers the electrical properties, is capable of locating the most critical links in a power network. Similarly, an extended betweenness has been introduced [56] and it exhibits its superior performance of identifying critical lines in power grids. Although the electric metrics have extended the topological metrics and achieved a better performance for the detection of the criticality of power components, the correlation is still not high between these electric metrics and real malfunction data obtained from an engineering setting [41].

2.3 Cascading Failure in Power Systems

Cascading failure, usually leading to large-scale power outage, is defined as a sequence of dependent events in which initial failure of one or a set of components in a power system triggers the sequent failure of other dependent components [57]. The initial failure of power components might be caused by varied reasons such as human errors and natural disasters [58]. The subsequent failure of power components can be triggered by the previous failure via different mechanisms. Overloading of power components is considered as one of the dominant triggering dynamics in the process of cascading failure. In this process, power components will be tripped by protection schemes when their loads exceed their capacities by a certain extent.

To model the cascading failure propagation in power systems, a step by step process has been proposed by Motter and Lai [55], which takes the overloading mechanism into consideration. For a power network, it has been assumed that the energy flow passes along the shortest path between each pair of nodes. The load at node i, denoted by L_i, is calculated by counting the number of shortest paths passing through the node i. The capacity of each node is defined as the maximum load that can be carried by the node. The capacity C_i of node i is assumed to be proportional to its initial load $L_i(0)$, which is given by

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

where $\alpha \geq 0$ represents the tolerance parameter. Once the load of a node exceeds its capacity at time t, i.e., $L_i(t) > C_i(t)$, the node is regarded as being out of function and will then be removed from the network. The process of cascading failure starts by removing a single node in a network. The removal leads to a change of the network topology and a redistribution of loads along the renewal shortest paths. The redistribution may lead to more failure of nodes whose loads exceed the capacities. The cascading failure is complete when there is no more overloaded node in the network. The relative size

of the largest connected components serves as a metric to evaluate the extent of the cascading failure. By simulating the Western American power grid, the results show that attacking the node with the largest load initially can lead to a larger scale of failure compared to attacking the node with the largest degree or a random node.

In Wang and Rong's model [59], the initial load of a node is formulated by a function of the product of the node degree and the summation of the degrees of the node's neighboring nodes instead of node degree or node betweenness. When a node is removed from the power network, its load will be redistributed to its neighboring nodes proportionally according to the initial load of the neighboring nodes. This study offered an intuitive understanding of how power flow is redistributed in the power network after the network topology is changed due to the removal of nodes. This work thus differs from the flow redistribution based on the shortest path [55].

However, the dynamics of flow redistribution based only on the topological characteristics cannot adequately model cascading failure in power networks because they omit the actual power flow mechanism. Specifically, power flow is governed by electrical principles like Kirchhoff's law rather than along shortest path length in a power network. The omission of physical laws in the power flow model might lead to results which are of less significance and even inconsistent with practical power systems. Hines *et al*. [60] pointed out the fact that the failure of a new power component at the next time step can be very far away from the current failure in a power network, which draws an inconsistent conclusion with that of the Wang and Rong's study [59]. Thus, power flow calculation should be taken into consideration in studying the cascading failure in power networks in order to have an accurate and practical understanding of the robustness of power systems.

The objective of using an AC or DC power flow model is to calculate the steady-state solutions of power systems including the voltage at each bus and the current through each transmission line. The determination of power flow using these electrical engineering approaches offers a meaningful and reliable solution to the modeling flow

distribution in power networks and thus leads to a realistic study of cascading failure in power systems.

AC Power Flow Model

The AC power flow model [61] is used to calculate the voltage and current for a power network at steady-state conditions. Given a power network having N nodes, the voltage at node i is given by $V_i = |V_i| \angle\theta_i$, where $|V_i|$ is the voltage amplitude and θ_i is the phase angle at node i. Likewise, for another node k, the voltage is denoted by $V_k = |V_k| \angle\theta_k$. The current passing through the transmission line (i, k) between nodes i and k is calculated based on Ohm's Law, i.e., $I_{ik} = (V_i - V_k)(G_{ik} + jB_{ik})$, where B_{ik} and G_{ik} are the susceptance and the conductance of line (i, k), respectively. Then, considering the power flow passing through transmission line (i, k), the power S_{ik} injected to node i is given by

$$S_{ik} = V_k I_{ik} = P_{ik} + jQ_{ik}, \tag{2.11}$$

where P_{ik} and Q_{ik} are the active and reactive power respectively. Here, P_{ik} and Q_{ik} can be further derived in the form of:

$$P_{ik} = |V_i|^2 G_{ik} - |V_i||V_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}). \tag{2.12}$$

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

The power externally injected at node i is expressed by $S_i = P_i - jQ_i$, where P_i is the active power and Q_i is the reactive power. Since the sum of the power externally injected to node i and the power injected to node i through the transmission line is zero, the active and reactive power can be given as

$$P_i = -\sum_{k=1}^{N} P_{ik} = \sum_{i=1}^{N} |V_i|\,|V_k|\,(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}), \tag{2.14}$$

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

where $G_{ii} = -\sum_{k\neq i} G_{ik}$ and $B_{ii} = -\sum_{k\neq i} B_{ik}$. Here, G_{ik} and B_{ik} are both zero if there is no transmission line between nodes i and k. Also, the phase difference between nodes i and k is denoted as $\theta_{ik} = \theta_i - \theta_k$. These two equations contain four variables: P_i, Q_i, θ_i and V_i. Thus, there are $2N$ equations and $4N$ variables for a power network with N nodes. To solve these $2N$ equations, at least $2N$ variables need to be specified. In the AC power flow analysis, the nodes (buses) in a power network are classified into three types, i.e slack node, load node and generator node. For each type of nodes, some variables are known, and the unknown variables are to be found by solving the equations.

These $2N$ equations are non-linear, with no closed form solution. Thus, the solution must resort to suitable numerical iterative techniques including the Gauss-Seidel method, Newton-Raphson method, Fast-decoupled-load-flow method, and so on [61].

Dey *et al*. [62] studied the effect of the network topology on the propagation of cascading failure in power systems. The average rate of propagation of failure events, calculated as a branching process parameter, is studied by evaluating cascade phenomena under varying topological conditions. In this study, the AC load flow analysis is performed for modeling cascading failure in different test power grids. The cascading failure is modeled as a sequential tripping of transmission lines in a power network. During the process of cascading failure, the power flow is redistributed after any line is removed from the power network. By using the AC power flow model, the power flow passing through each line is calculated and if it is over its capacity, the line will be tripped. The line tripping time is determined by the extent of overloading. In particular, greater overload leads to a faster line tripping. Based on the simulation results, it has

been found that the variations in topological parameters have qualitative correlation with the failure propagation rate in the cascading failure analysis.

Liu *et al*. [63] applied a network approach incorporating an AC power flow model to analyze the vulnerability of the power network and to identify key nodes in power grids. The node electrical centrality, defined by considering network topological characteristics and electrical properties, is used to identify the key nodes in power systems. This study also introduced a vulnerability index based on the concept of net-ability to evaluate the degradation of the transferability and comparative performance of power systems under normal and cascading failure conditions. It has been verified from the simulation results that the key nodes exhibit high electrical centrality and their removal can effectively lead to a severe damage to power systems.

The effectiveness of incorporating the AC power flow model has been well recognized. In addition, other models built for studying the cascading failure in power systems which adopt the AC power flow model includes the Manchester model [64] which is based on load shedding, AC OPA model [65] and so on.

DC Power Flow Model

Due to the high complexity of the AC power flow model, a large quantity of computation resources are required to obtain the numerical solution. For a large power network, the time taken for solving these nonlinear equations is unacceptably long. Thus, DC power flow model is proposed as an alternative method to calculate the power flow in power networks. To derive the DC power flow equations, the following three assumptions are made:

(1) The voltage magnitude at each bus is assigned to be 1 p.u.;

(2) The resistance is much smaller than the reactance of each transmission line, and hence it can be neglected;

(3) The phase difference θ_{ik} between node i and node k of a transmission line (i, k) is very small. Thus, $\sin\theta_{ik} \approx \theta_{ik}$ and $\cos\theta_{ik} \approx 0$.

Then, equation (2.12) can be rewritten as

$$P_{ik} \approx -B_{ik} \sin(\theta_i - \theta_k) \approx -B_{ik}(\theta_i - \theta_k). \tag{2.16}$$

The active power for each node is given by

$$P_i = -\sum P_{ik} = \sum_{k=1}^{N} B_{ik}(\theta_i - \theta_k). \tag{2.17}$$

For node i, equation (2.17) is regarded as a nodal equation. The nodal equations of all nodes in a power network can be expressed in matrix form, i.e.,

$$\mathbf{P} = \mathbf{B}\boldsymbol{\theta}, \tag{2.18}$$

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

The DC power flow model has been adopted in an increasing number of studies aiming to simulate cascading failure in power grids. Wang *et al*. [66] developed a stochastic Markov model to capture the behavior of failure propagation in power systems within a continuous time span. This model not only considers the uncertainties in both generation and load setting in power systems, but also incorporates the line flow distribution based on the network equations and the DC power flow equations. The simulation results demonstrate the ability of this model for the identification and prediction of the critical paths of the possible cascading failure.

Rahnamay-Naeini *et al*. [67] proposed a scalable and analytically tractable probabilistic model for the purpose of describing the dynamics of cascading failure events. In the model, the state transition is used to describe the events occurring in power grids, like lines being tripped, for which the rate is found from the DC power flow model. This model provides an alternative way to predict the evolution of the blackout probability and achieves the analytical characterization of the probability function of the

blackout size.

To study the robustness of power systems from a network perspective, Zhang and Tse [68] developed a deterministic model by incorporating Kirchhoff's laws, the properties of network elements and a complex network structure. By utilizing this model, two critical metrics, namely, the percentage of unserved nodes (PUN) caused by a failed component and the percentage of noncritical links (PNL) that will not cause severe damage, are introduced to quantitatively assess the robustness of power systems. It has been found that two factors are strongly correlated with the power systems' robustness: one being the average shortest path length, and the other one being the consumers' accessibility to generators. Combined with a stochastic model to describe the uncertain failure time instants, an extended model [69] was developed to describe the propagation of cascading failure in power systems. Based on this model, the simulated dynamic profiles of cascading failures contain all salient features that are consistent with those found in historical blackout data.

The models adopting DC power flow model in the aforementioned studies fall short of taking into consideration of the effect of transient stability analysis on cascading failure in power systems. Yan *et al*.'s work [70] offers a reference by comparing the models based on DC power flow-based analysis and transient stability analysis, for the purpose of identifying a more appropriate model for the analysis of power grid cascading failures under different scenarios.

Recently, Cetinay *et al*. [71] compared the AC power flow model with the DC power flow model when they are adopted to model the cascading failure in power systems. It has been found that the results are consistent using either AC or DC power flow model for operations with no cascading failure or just a single line failure. However, modeling cascading failure using the DC power flow model fails to achieve approximative results as given by AC power flow model. Thus, trade-off of using the DC power flow model exists between its simplification and poor precision in describing cascading failure. More models adopting either AC or DC power flow model can be

found in a recent review paper [72].

2.4 Cascading Failure in Cyber-Coupled Power Systems

The modern power grids have been evolving into smart grids with the integration of advanced monitoring, control, and communication technologies. A smart grid, characterized as a cyber-coupled power system, is a typical cyber physical system where a power system is coupled with one or multiple cyber systems. On the one hand, the coupling of cyber systems makes power systems more intelligent and efficient for power generation and delivery. One the other hand, the cyber security issues are raised due to the threat of cyber attack targeting smart grids. Different from the traditional physical attack on power systems, cyber attack can be launched distantly as long as attackers can access the power systems through their coupled cyber systems. Such attack may lead to a more severe power outage.

The interdependent network model provides an appropriate framework to examine the cascading failure in cyber-coupled power systems, especially in respect of how failure in one network affects failure in other mutual networks. Although an increasing number of studies offer a network topological perspective to assessing vulnerabilities of cyber-coupled power systems, the network approaches used to model cascading failure often omits the underlying physical process such as the power flow distribution in power systems. Moreover, the interdependency between cyber systems and power systems is oversimplified, resulting in partial or inconsistent interpretations.

Cai *et al*. [73] developed a model to describe the dependencies between power systems and dispatching data networks, aiming to examine the intricate impacts on cascading failure. Regarding the influence of power networks on dispatching data networks, the tripped lines cause the malfunction of the power nodes and thus may lead to the failure of communication nodes. Different tripping rates of communication nodes have been considered in terms of the failure of different types of power nodes.

In terms of the influence of dispatching data networks on power networks, the failure of the communication nodes changes the topology of dispatching data networks, and thus the data transmission is affected. If the abnormal data is received by the control center with time delay and the protection action is taken late, the overloaded will be tripped. It has been found from this study that for the topology of the coupled data dispatching network, the double star structure is better than the mesh, which makes the power network more robust against cascading failure.

In Wang *et al*.'s work [74], it has been assumed that every node in the communication network is connected to a corresponding physical node in a transmission grid by bidirectional links that represents data uploading channels and command downloading channels. For a power network coupled with a communication network, bidirectional interdependencies between these two networks can be modeled from two aspects: 1) the failure of power nodes makes communication nodes lose information and thus the communication nodes are considered to be useless; 2) losing information in communication networks leads to an abnormal control to the power network making the line tripping is hard to avoid. Moreover, this study has also introduced different classes of information channels that characterize the interdependency of interconnected networks.

The modeling of the interdependencies between power networks and the coupled cyber networks plays an essential role in the analysis of cascading failure in the cyber-coupled power systems. A comprehensive review paper [75] offers an overview of various interdependencies between power systems and information technology systems. Another problem in the study of the cascading failure in cyber-coupled power systems is related to coupling pattern of power and cyber systems, particularly in terms of the structural connectivity [75].

In Parandehgheibi *et al*.'s model [76], the robustness of interdependent networks is studied under the assumption that every router in the cyber network is powered by at least on a power substation, and every substation sends and receives information

via multiple coupling links with the cyber network. Moreover, the direction of the coupling links is defined by classifying the interdependencies between power networks and communication networks into unidirectional and bidirectional ones.

Huang *et al*. [77] introduced a practical interdependent network model aiming to offer a method of characterization of the cascading failure in a cyber physical system. In the model, different from a one-to-one connection style in [17] and multiple-to-multiple connection fashion in [76, 36], each node in the computational-resource network is assumed to obtain support from only one node in the physical-resource network, while each node in the physical-resource network is assumed to have multiple interconnections with the computational nodes. This connection style is termed "one-to-multiple" correspondence. Although this connection style has its practical meaning in modeling cyber-coupled power systems, the study [77] has adopted the percolation theory instead of the underlining physical process to simulate cascading failure events. Thus, the results from this study require further verification.

Retaining the one-to-one connection style between a power network and its coupled cyber network, Kang *et al*. [78] divided the coupling links between cyber nodes and power nodes into two categories, i.e., the top-down coupling links representing the impact of cyber networks on power networks and the bottom-up coupling links abstracting the influence of power networks on cyber networks. It has been found that to enhance the robustness of cyber-coupled power systems, *Assortative Coupling*, i.e., nodes with similar degrees in both interconnected networks are coupled, is suitable for implementation of the bottom-up coupling links. For the implementation of the top-down coupling links, *Disassortative Coupling* is adopted, which connects the high degree nodes in one network with the low degree nodes in the other network.

To summarize, three main challenges in studying cascading failure in cyber-coupled power systems can be identified: 1) the necessary incorporation of physical processes; 2) the effective interpretations of interdependencies; 3) the underlying effect of coupling patterns.

Chapter 3

Modeling the Dynamic Propagation of Cascading Failure

In the previous chapter, we have reviewed the complex network theory and its application to power systems and cyber-coupled power systems, with emphasis on the robustness of these systems. In this chapter, we introduce two models. The first model is for simulation of the cascading failure propagation in power systems. With the consideration of the power network being coupled with a cyber network, the second model is used to generate the dynamic profile of cascading failure events caused by the attack of cyber malware.

3.1 Model of Cascading Failure in Power Systems

Our model has two key features. First, we apply circuit-based power flow equations to determine the sequence of failure events in accordance to the extent of overloading 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 pro-

cesses 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. 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.

3.1.1 Failure Mechanisms of Components

A power system is composed of various electrical stations connected by transmission lines, and each station or transmission line is protected by protective equipment. Here, we model electrical stations as nodes and transmission lines as links, with nodes being connected by links forming a power network. 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.

3.1.1.1 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. 3.1.

Here, $\lambda_i(t)$ 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

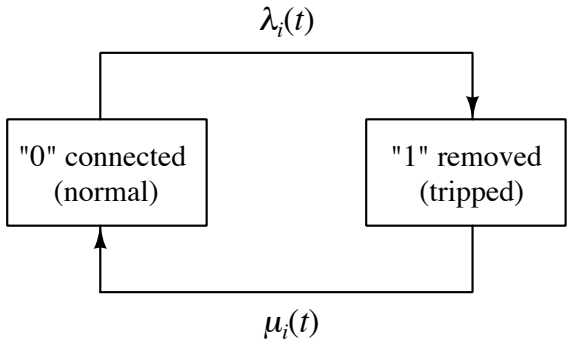


Figure 3.1: Dynamic description of failure in terms of state transitions. State "0" is the normal connected state; state "1" is the removed or tripped state. Arrows represent transitions between different states while self-loop arrows are not displayed in the figure.

$P[s_i(t+dt)=0]$ can be written as

$$\begin{aligned} P[s_i(t+dt)=1] &= P[s_i(t+dt)=1\,|s_i(t)=0\,]P[s_i(t)=0] \\ &\quad + P[s_i(t+dt)=1\,|s_i(t)=1\,]P[s_i(t)=1] \\ P[s_i(t+dt)=0] &= P[s_i(t+dt)=0\,|s_i(t_1)=0\,]P[s_i(t)=0] \\ &\quad + P[s_i(t+dt)=0\,|s_i(t)=1\,]P[s_i(t)=1] \end{aligned} \tag{3.1}$$

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. 3.1, $P[s_i(t+dt)=1\,|s_i(t)=0)\,]$ can be written as

$$P[s_i(t+dt)=1\,|s_i(t)=0\,]=\lambda_i(t)dt. \tag{3.2}$$

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

$$P[s_i(t+dt)=0\,|s_i(t)=0\,]=1-\lambda_i(t)dt. \tag{3.3}$$

Likewise, we have

$$P[s_i(t+dt)=0\,|s_i(t)=1\,] = \mu_i(t)dt, \tag{3.4}$$

$$P[s_i(t+dt)=1\,|s_i(t)=1\,] = 1-\mu_i(t)dt. \tag{3.5}$$

3.1.1.2 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.,

$$\lambda_i(t)=\lambda_i^0(t)+\lambda_i^1(i) \tag{3.6}$$

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 [79]; 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 [80, 81], power overloading is a dominant one. Here, 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 [82]. Based on this assumption, we can write $\lambda_i^1(t)$ as

$$\lambda_i^1(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \leq C_i \end{cases} \tag{3.7}$$

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, $\lambda_i^1 \gg \lambda_i^0$ [83]. 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. Here, 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.

3.1.1.3 Power Flow Calculation

Our model for the power system is based on the admittance model proposed by Grainger and Stevenson [61]. For a power system with n buses, the admittance model is written as

$$\begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n} \\ Y_{21} & Y_{22} & \cdots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \cdots & Y_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix}, \tag{3.8}$$

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 3.8 at any point of time. A time series of values of V_n and I_n describe dynamic behaviors of a power system. Equation 3.8 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 3.8.

In addition to equation (3.7), power flow calculation is still needed for the analysis of cascading failures. Several algorithms and tools are available for computing power flows [84, 85]. 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 [86]. 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. Here, 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. Here, we introduce a comprehensive model for the calculating of power flow. 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 current value is negative as the node consumes power, i.e.,

$$\begin{bmatrix} -Y_{i1} & \cdots & Y_{ii} & \cdots & -Y_{in} \end{bmatrix} * V = I_i \tag{3.9}$$

where $V = \begin{bmatrix} \cdots & v_i & v_j & v_k & v_h & \cdots \end{bmatrix}^T$.

(ii) Distribution Nodes

A distribution node j is a connecting node that nether produces nor consumes power. Thus, we set $I_j = 0$, i.e.,

$$\begin{bmatrix} -Y_{i1} & \cdots & Y_{ii} & \cdots & -Y_{in} \end{bmatrix} * V = 0 \tag{3.10}$$

(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

$$\begin{bmatrix} 0 & \cdots & y_k & \cdots & 0 \end{bmatrix} * V = v_k \tag{3.11}$$

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. 3.2. Here, a is the winding turns ratio; v_{hL} and v_{hR} are the voltages at node h's input side and output side. Here, 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

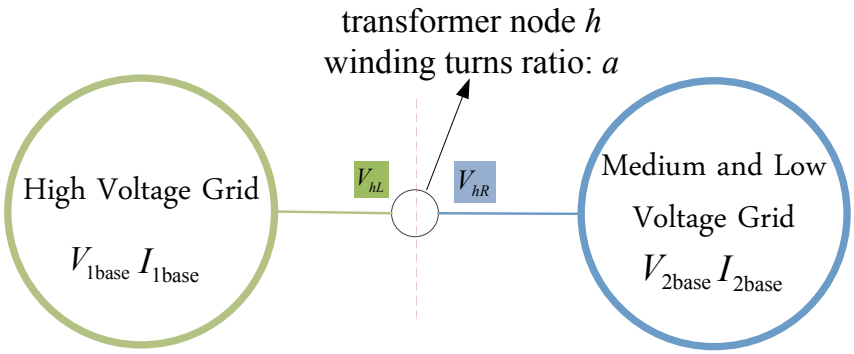


Figure 3.2: Transformer h connecting grids of varying voltages.

$v_{hL} = v_{hR} = v_h$.

The nodal equation of node h is

$$\begin{bmatrix} Y_{h1} & \cdots & Y_{hh} & \cdots & Y_{hn} \end{bmatrix} * V = 0 \tag{3.12}$$

Combining equations (3.9)–(3.12), we get the following power system equation:

$$A * V = B \tag{3.13}$$

where

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

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

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

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

$$I_{ij} = (v_i - v_j) * Y_{ij} \tag{3.14}$$

3.1.2 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).

3.1.2.1 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

$$\begin{aligned} P[S(t+dt) = N_S \,|S(t) = N_S\,] &= \prod_{i\in\Omega_0}[1-\lambda_i(t)dt)] \\ &= 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt + \sum_{x_1,x_2\in\Omega_0}\lambda_{x_1}(t)\lambda_{x_2}(t)(dt)^2 \\ &\quad - \sum_{x_1,x_2,x_3\in\Omega_0}\lambda_{x_1}(t)\lambda_{x_2}(t)\lambda_{x_3}(t)(dt)^3 + \cdots \\ &= 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt + o(dt) \approx 1 - \sum_{i\in\Omega_0}\lambda_i(t)dt \end{aligned} \tag{3.15}$$

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

$$\begin{aligned} P[S(t+dt) = M_S \,|S(t) = N_S\,] &= \lambda_k(t)dt \prod_{i\in\Omega_0\setminus\{k\}}[1-\lambda_i(t)dt] \\ &= \lambda_k(t)dt - \sum_{x_1\in\Omega_0\setminus\{k\}}\lambda_k(t)\lambda_{x_1}(t)(dt)^2 \\ &\quad + \sum_{x_1,x_2\in\Omega_0\setminus\{k\}}\lambda_k(t)\lambda_{x_1}(t)\lambda_{x_2}(t)(dt)^3 + \cdots \\ &= \lambda_k(t)dt + o(dt) \approx \lambda_k(t)dt \end{aligned} \tag{3.16}$$

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

$$P[S(t+dt) = R_S \,|S(t) = N_S\,] = 0 \tag{3.17}$$

where R_S denotes the network state that two or more of the "0"-state elements in N_S become "1". From equation (3.17), there is at most one element state transition at a time.

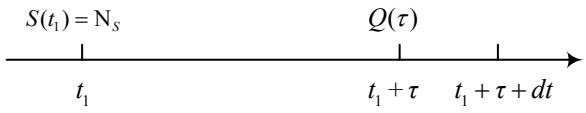


Figure 3.3: Time line of network state transitions.

3.1.2.2 Extended Gillespie Method

In this section, we derive $S(t)$ using an extended Gillespie method [87], which was used for analyzing coupled chemical reactions [88, 89].

As shown in Fig. 3.3, 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.,

$$Q(\tau) = P[S(t_1 + \tau) = N_S \,|S(t_1) = N_S\,]. \tag{3.18}$$

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

$$\begin{aligned} Q(\tau + dt) &= P[S(t_1 + \tau + dt) = N_S \,|S(t_1) = N_S\,] \\ &= P[S(t_1 + \tau + dt) = N_S \,|S(t_1 + \tau) = N_S\,]Q(\tau). \end{aligned} \tag{3.19}$$

Given $S(t_1) = N_S$, power flow calculation can be performed, as described in Section 3.1.1.3, and $\lambda_i(t_1)$ can be derived based on the settings in Section 3.1.1.2. 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 (3.15), we get

$$P[S(t_1 + \tau + dt) = N_S \,|S(t_1 + \tau) = N_S\,] = 1 - \sum_{i \in \Omega_0} \lambda_i(t_1)dt. \tag{3.20}$$

Thus, by putting (3.20) in (3.19), we get

$$Q(\tau + dt) = Q(\tau)(1 - \lambda^*(t_1)dt), \tag{3.21}$$

where $\lambda^*(t_1) = \sum_{i \in \Omega_0} \lambda_i(t_1)$. Furthermore, re-arranging (3.21) and taking the limit $dt \rightarrow$

0, we get

$$\begin{aligned} &\frac{dQ(\tau)}{d\tau} = \lim_{dt\to 0} \frac{Q(\tau+dt) - Q(\tau)}{dt} = -\lambda^*(t_1)Q(\tau), \\ &\Rightarrow Q'(\tau) = -\lambda^*(t_1)Q(\tau). \end{aligned} \tag{3.22}$$

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 (3.22) is

$$Q(\tau) = e^{-\lambda^*(t_1)\tau}. \tag{3.23}$$

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

$$h_i(\tau, dt) = P[S(t_1 + \tau + dt) = M_S \,|S(t_1 + \tau) = N_S\,]Q(\tau). \tag{3.24}$$

Putting (3.16) and (3.23) in (3.24), we get

$$h_i(\tau, dt) = e^{-\lambda^*(t_1)\tau}\lambda_i(t_1)dt. \tag{3.25}$$

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

$$H(\tau, dt) = \sum_{i\in\Omega_0} h_i(\tau, dt) = \lambda^*(t_1)e^{-\lambda^*(t_1)\tau}dt. \tag{3.26}$$

Further, let τ denote the time interval between two adjacent network state transitions,

and $f(\tau)$ denote the *state transition probability density function* (PDF):

$$f(\tau) = \lim_{dt \to 0} \frac{H(\tau, dt) - H(\tau, 0)}{dt} = \lambda^*(t_1) e^{-\lambda^*(t_1)\tau} \tag{3.27}$$

i.e.,

$$f(\tau) = \lambda^*(t_1) e^{-\lambda^*(t_1)\tau}. \tag{3.28}$$

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

$$F(\tau) = \lambda^*(t_1) \int_0^\tau e^{-\lambda^*(t_1)t} dt = 1 - e^{-\lambda^*(t_1)\tau}. \tag{3.29}$$

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

Equations (3.28) and (3.29) 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).

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

$$\tau = \frac{ln(1 - z_1)}{-\lambda^*(t_1)}. \tag{3.30}$$

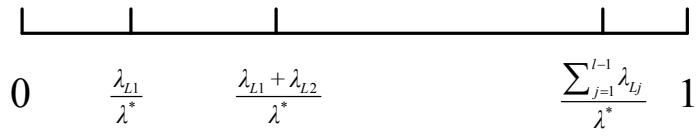


Figure 3.4: Relative probability for elements in Ω_0 to be first tripped given $S(t_1) = N_S$.

3.1.2.3 Order of State Transition

A number of working elements (elements in Ω_0) can possibly undergo state transition. In our analysis presented in Section 3.1.2.1, we allow only one element to be removed (tripped) at a time. Pfitzner *et al*. [90] 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:

$$rf_i = \frac{h_i(\tau, dt)}{H(\tau, dt)} = \frac{\lambda_i(t_1)}{\lambda^*(t_1)}. \tag{3.31}$$

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 3.4 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

$$\sum_{k=0}^{j-1} \frac{\lambda_{Lk}}{\lambda^*} \leqslant z_2 < \sum_{k=0}^{j} \frac{\lambda_{Lk}}{\lambda^*}, \tag{3.32}$$

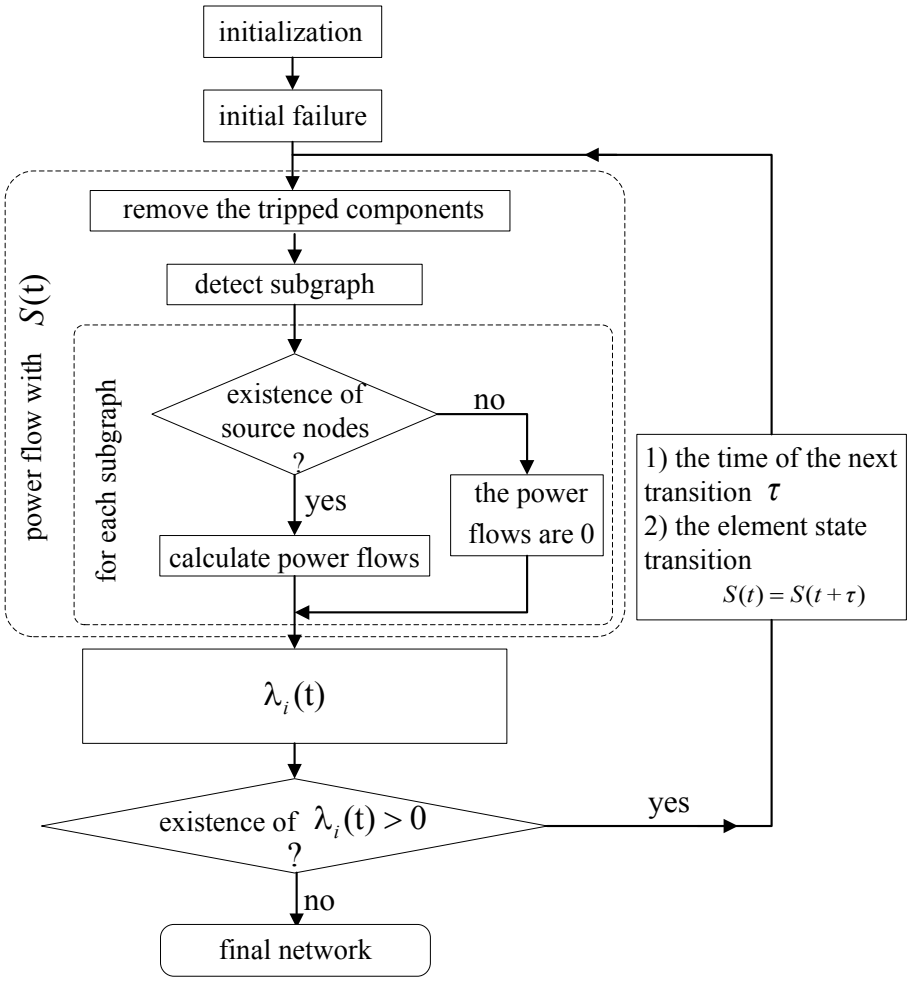


Figure 3.5: Flow chart for simulating the dynamic propagations of cascading failure.

where $\lambda_{L0} = 0$.

3.1.2.4 Simulation Algorithm

Figure 3.5 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, 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 (3.13) 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 (3.7). 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 (3.30), and determine the element in Ω_0 that will be tripped next. The network state transition is determined using (3.32). 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.

3.2 Model of Cascading Failure in Cyber-coupled Power Systems

In this model, we take into consideration the effects of power overloading, contagion, and interdependence between power grids and cyber networks 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 cascading failures caused by the attack of cyber malwares.

3.2.1 Model Description

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. 3.6. Network A is the power grid, where solid rectangular nodes in Fig. 3.6 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. 3.6. Here, 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. 3.6, 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., $q \gg p$.

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

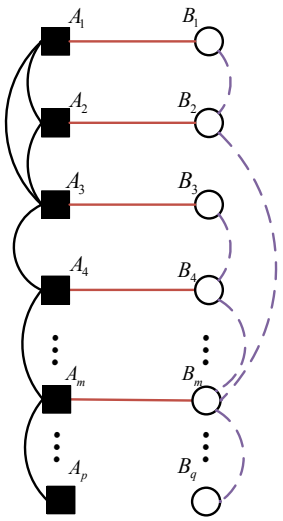


Figure 3.6: Coupled network consisting of a power network A and a cyber network B. Solid rectangles represent electrical buses and solid arcs represent transmission lines in A. White circles represent computers in the cyber network and dashed arcs represent connections among the cyber nodes in B. Horizontal lines represent interdependence between nodes in A and nodes in B.

subsections, we will define the states of nodes and describe their corresponding state transitions.

3.2.1.1 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, 92], 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 [68, 93], 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*. [94] made the simple deterministic assumption that the duration for an over-

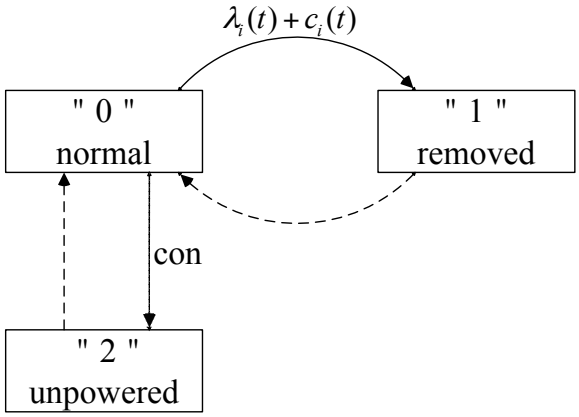


Figure 3.7: State transition diagram of a node in power network A. Transitions between state 0 and 2 are deterministic transitions, and those between 0 and 1 are stochastic transitions.

loaded 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. Considering the high uncertainties and complexities in power systems, stochastic models are used to investigate cascading failures in power systems [58, 66, 67], 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, 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. 3.7.

Depending on the nature of the transitions, they are either deterministic transitions or stochastic transitions, as shown in Fig. 3.7. 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:

$$T_1 : s_{Ai} = 0 \rightarrow s_{Ai} = 1. \tag{3.33}$$

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 [66] [67], transitions are determined by power loading conditions and elements' capacities. In real-time operation, as pointed out by Sun *et al*. [82], 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

$$\lambda_i(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \le C_i \end{cases} \tag{3.34}$$

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 (3.34), the power flow analysis can be applied to derive $\lambda_i(t)$. Here, we adopt the method introduced in Section 3.1.1.3 to compute the power flows in the power system, assuming that the power system will reach a new steady state after an element fails. Moreover, we do not consider stability issues that have been studied in refs. [95, 96]. 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

$$T_1 : P[s_{Ai}(t + dt) = 1 \mid s_{Ai}(t) = 0] = \lambda_i(t)dt. \tag{3.35}$$

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

$$T_1 : P[s_{Ai}(t + dt) = 1 \mid s_{Ai}(t) = 0] = (\lambda_i(t) + c_i(t))dt, \tag{3.36}$$

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. 3.7 are neglected.

3.2.1.2 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 3.8 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 [97]. 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:

$$T_2 : s_{B_i} = 0 \xrightarrow{\mu_i} s_{B_i} = 1. \tag{3.37}$$

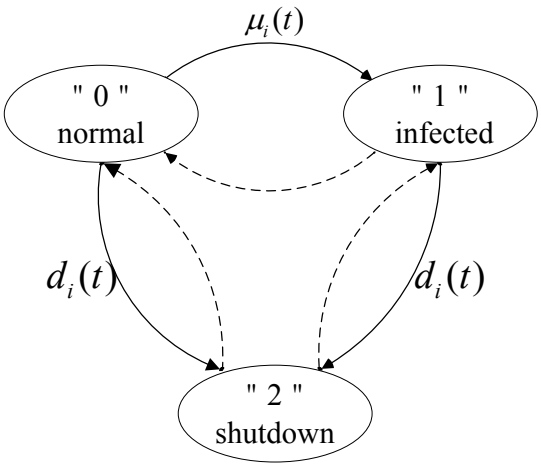


Figure 3.8: State transition diagram of a node in cyber network B.

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

$$\mu_i(t) = \sum_{j \in \Omega_{Bi}} \beta_{ij}, \tag{3.38}$$

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

$$T_2 : P[s_{B_i}(t + dt) = 1 \mid s_{Bi}(t) = 0] = \mu_i(t)dt. \tag{3.39}$$

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:

$$T_3 : s_{B_i} = 0 \xrightarrow{d_i} s_{B_i} = 2, \tag{3.40}$$

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

$$T_3 : P[s_{B_i}(t + dt) = 2 \mid s_{B_i}(t) = 0] = d_i(t)dt, \tag{3.41}$$

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

$$T_4 : s_{B_i} = 1 \xrightarrow{d_i} s_{B_i} = 2. \tag{3.42}$$

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

$$T_4 : P[s_{B_i}(t + dt) = 2 \mid s_{B_i}(t) = 1] = d_i(t)dt. \tag{3.43}$$

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. 3.8 are neglected. For clarity of the figures, self-loop arrows are not displayed in Figs. 3.7 and 3.8.

3.2.2 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 process is the dynamic propagation profile of $S(t)$ as the system state transits in time

Table 3.1: 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

among those m_S different states.

3.2.2.1 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. 3.7 and 3.8. 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 3.1, 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 3.1.2.1 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.

3.2.2.2 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

$$Q(\tau + dt) = P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,]Q(\tau). \tag{3.44}$$

Thus, we have

$$P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,] = (1 - r^* dt), \tag{3.45}$$

where $r^* = \sum_{i=1}^{n} r_i$. Note that equation (3.45) is only valid when dt is infinitesimally small (see Section 3.1.2.1). Substituting (3.45) into (3.44), we get

$$Q(\tau + dt) = Q(\tau)(1 - r^* dt). \tag{3.46}$$

Re-arranging (3.46), as $dt \to 0$ (i.e. dt is infinitesimal), we get

$$\lim_{dt \to 0} \frac{Q(\tau + dt) - Q(\tau)}{dt} = Q^{'}(\tau) = -r^* Q(\tau). \tag{3.47}$$

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

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

Note that in equations (3.45) through (3.47), 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

$$Q(\tau) = Q(0)e^{-r^{*}\tau}. \tag{3.48}$$

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

$$Q(\tau) = Q(0)e^{-r^{*}\tau} = e^{-r^{*}\tau}, \tag{3.49}$$

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

$$F(\tau) = 1 - Q(\tau) = 1 - e^{-r^{*}\tau}. \tag{3.50}$$

The probability density of τ can be found using equation (3.50) as

$$f(\tau) = r^{*}e^{-r^{*}\tau}. \tag{3.51}$$

From (3.50) and (3.51), 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 3.2.1, 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 :

$$\tau = F^{-1}(z_1) = \frac{1}{r^*} \ln(\frac{1}{1 - z_1}). \tag{3.52}$$

And k is selected based on the following equation:

$$\sum_{j=0}^{k-1} \frac{r_j}{r^*} \leqslant z_2 \leqslant \sum_{j=0}^{k} \frac{r_j}{r^*}. \tag{3.53}$$

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 3.9 shows the flow chart used in simulating the cascading failures in the coupled system.

3.2.2.3 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:* Here, 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

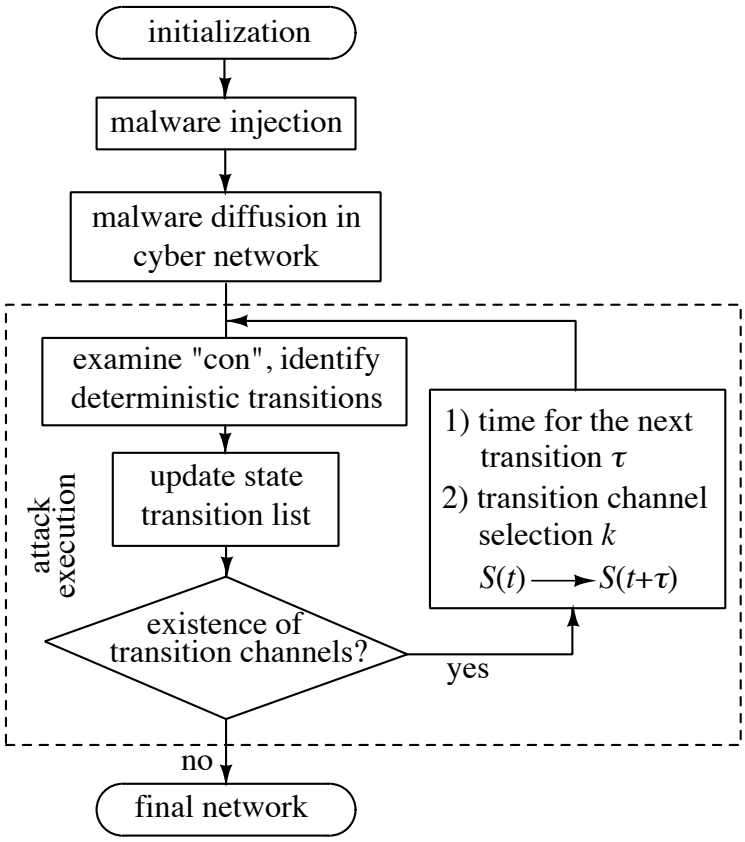


Figure 3.9: Simulation flow chart for cascading failures in the coupled system.

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 (3.35)-(3.43), 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 (3.34) where the deterministic power flow analysis introduced in Section 3.1.1.3 should be applied, cyber nodes' infection due to contagion based on equation (3.38), and the interdependencies between the two different networks.

(c) If there is a state transition channel in the list, we use equations (3.52) and (3.53) 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}.

Chapter 4

Robustness Assessment and Enhancement of Power Grids From a Complex Network's Perspective

In the previous chapter, two models have been introduced to model the cascading failure in power systems and cyber-coupled power systems respectively. In this chapter, we develop a system-level method to assess the robustness of power grids. By focusing on the dynamics of failure cascade, we identify a critical observable parameter, namely *onset time*, which is the time after which the propagation rate of a cascading failure increases rapidly. Based on the *onset time* and the scale of the failed grid in a cascading failure event, we categorize each component in a power network into three types, corresponding to three levels of severity of the failed grid upon the initial failure of that component. In particular, the most concerned category of components is the one that makes the power network more vulnerable to failure because their initial failure would result in a dramatically fast and large-scale cascading failure. Through extensive simulations, we analyze the robustness of five selected power networks by assessing the proportion of the three types of components. Moreover, to investigate robustness enhancement of power networks, we propose a decision-tree-based learning

model to extract significant network-based features. By utilizing a number of power networks generated by means of edge re-arrangement targeting topology improvement of the original power system, a decision tree is generated. This tree identifies three features for all nodes, including average shortest path length, average clustering coefficient and average effective resistance (distance) to the nearest generator, which exhibit strong correlation with the robustness of the power network. Experiments show that coordinating multiple network-based features leads to an effective enhancement of the robustness of power networks.

4.1 Introduction

Power systems, regarded as vital infrastructures in modern society, provide energy for all sectors of society, industry and government, e.g., data centers, city lighting, transportation, and public services. Therefore, power systems of high vulnerability and a relatively high likelihood of outage over a large area would not only affect our daily life, but also incur large economic loss upon failure. For instance, the power outage in Northeastern United States and Canada in 2003 was widely known as a serious event depriving 50 million people from power supply for up to four days [98]. The Indian blackout in 2012 and Taiwan blackout in 2017 also raised concerns about the robustness of power systems.

Numerous studies have been devoted to modeling the dynamics of cascading failure in power systems, aiming to assess power outage risks [58]. On the one hand, research based on the data fitting methods utilizes historical data to statistically analyze the propagation of cascading failures in power systems [92, 91]. On the other hand, according to the overloading effect involved in real networks [99], the propagation process is treated as a sequential tripping of electrical elements including stations or transmission lines. Basically, through power flow calculation, either adopting a DC model or AC model, one may determine whether the load carried in a power element

(e.g., power flowing through a transmission line) is over its maximum capacity, increasing the likelihood of failure of that element [66, 67, 100, 101]. Notably, Zhang *et al*. [101] proposed an effective model from a complex network perspective incorporating physical power flow equations. In particular, the simulation results showed a universal growing pattern which was found consistent with historical data of power outage.

An increasing number of studies have assessed the robustness of power systems considering cascading failure. Different from the traditional dynamical stability analysis of power systems [102, 103, 104], recent studies have investigated the robustness of power systems from a complex network perspective [14, 40]. In such studies, a power transmission network is abstracted as a network consisting of "nodes" representing power substations and "links" representing transmission lines. By adopting network-based approaches, researchers have attached a great deal of importance to identifying the kind of topology that optimizes the robustness of power networks.

The development of assessing the robustness of power grids from the network science's point of view can be divided into three main phases. In the initial phase, researchers focused on examining the effect of network topology on the robustness of power systems [59, 105, 106]. In the second phase, the focus was shifted to studying extended network properties that directly contribute to enhancing robustness of power systems [107, 108, 109] after realizing that pure topological analysis has limited capability in capturing the essential characteristics of power grids [110]. Basically, a power network was represented by a weighted and directed network [107]. The distance in a power network was associated with the impedance and the direction of power flow passing from generators to loads was considered. This type of networks was much different from other categories of networks like social networks conventionally modeled by an influence graph [60]. However, such network-based models have ignored the physical power flow distribution in power networks, thus generating results that might not be consistent with realistic scenarios of cascading failure in power grids. We have

now entered the third phase of study, with emphasis on incorporating the physical processes and component characteristics in network-based models. In Zhang and Tse's work [68], the DC power flow model was used to address the power flow re-balancing process in the propagation of cascading failure and point out the importance of considering the global mechanism. This has changed the path of study significantly from previous works that assumed the failure propagation being driven by a local mechanism similar to classical spreading or diffusion. Consistently, Hines *et al*. [60] also pointed out that two consecutively failed power elements might be located very far from each other due to the global power re-distribution effect.

The use of complex network concepts has offered new insights in robustness assessment of power grids. Inspired by the concept of betweenness from network science, Bompard *et al*. [111] introduced an extended betweenness parameter which is superior to topological betweenness for identification of critical components in power grids. Dwivedi *et al*. [112] developed an approach using maximum-flow-based complex networks to identify vulnerable lines through evaluating the capacity in power systems. Moreover, by using a realistic large-scale modeling and analysis method, Yang *et al*. [113] found that small vulnerable sets in power systems dominate the cascading failure process. It is now generally agreed [114] that the vulnerability assessments become more reliable if the electrical characteristics of power grids can be captured, although the complexity of the network-based analysis would be increased. Moreover, network topology is still central to robustness assessment as it determines power flow distribution in the system, although the physical power flow process involving electrical properties of all components remains indispensable. Thus, from the foregoing review, a system-level analysis involving network structure and physical properties of components is necessary for realistic robustness assessment [115, 116, 117].

The main objective of this chapter is to offer a system-level method to assess the robustness of power systems using a network-based model. Most robustness assessment strategies studied so far have emphasized on the final status when cascading failure

propagation is completed. For instance, the number of failed elements or eventual power loss are used as the key metrics for evaluating vulnerability of power systems. Our previous model [101], however, captures an abrupt increase in the number of failed links in a power system during the failure propagation process, which is fully consistent with real historical data. We define a time point called *onset time* as the time after which the propagation rate increases rapidly. It is found that the *onset time* plays an essential role in the analysis of cascading failure. Before this *onset time*, the cascading failure occurs very slowly and protective action may be taken in time to reduce the risk of a fast and large-scale power blackout. A recent study [118] also suggested that operators can manage a contingency plan before the failures increase rapidly if they have sufficient time to react to the cascading failure. However, a short onset time would make protective actions very challenging. Therefore, in this chapter, based on the onset time and blackout scale (final number of failed components in a power network) captured from each simulated scenario of cascading failure, we classify the links in a power network into three types, denoted as Type I, Type II and Type III power lines. A Type I power line is a power line which, upon failure, does not lead to cascading failure of the system. A Type II or III power line, however, upon failure, will lead to cascading failure of the system. Moreover, the cascading failure caused by failure of a Type II line has a relatively long onset time. Thus, the most concerned ones are Type III power lines which make the system more vulnerable to failure because their initial failure would result in a dramatically fast and large-scale cascading failure. Through implementing the proposed method which requires extensive simulations, we have a qualitative view of the vulnerability of a few selected power systems of different scales.

Moreover, we introduce a decision tree-based learning procedure to extract significant network-based features relevant to the robustness of power networks. In this chapter, we consider one particular solution to reducing the vulnerability of power networks to cascading failure. This procedure involves minor rearrangements of the topology of the grid. Specifically, a rewiring scheme is implemented by reconnecting a small quan-

tity of edges in the power network while the network size and degree distribution are unchanged. As demonstrated in a previous study [119], small changes in the network structure may effectively improve the robustness of power grids. In this chapter, a number of rewired power networks originated from the UIUC-150 bus power system are collected as the input of the learning algorithm and then a decision tree is generated. It is demonstrated that the tree involves three significant network-based features, including *average shortest path length*, *average clustering coefficient* and *average effective resistance (distance) to nearest generator* of all consumer nodes, which define the tree forming rules. The rules are applied to generate a power network of lower vulnerability. Experiments show that a power network has higher robustness against cascading failure if its topology exhibits fewer random network properties, namely, longer average shortest path length and more decentralized generator distribution.

4.2 Model of Cascading Failure Propagation in Power Systems

In this chapter, we adopt the model introduced in Section 3.1, which aims to simulate propagation process of cascading failure in power systems. The model combines a circuit-based power flow model and a stochastic model. In particular, the objective of the former model is to determine the failure sequence according to the extent of overloadings of individual power elements while the later model is to describe the dynamic changes in power systems such as the uncertain time instants of failure. To generate a dynamic propagation profile of cascading failure initializing from a dysfunctioned power element and developing eventually to a large-scale power outage, the simulation is run by following the steps given in the flow chart in Fig. 3.5. The key steps include the DC power flow calculation, the overloading effect of power elements and the stochastic process of failure.

4.3 Methodology of Vulnerability Assessment Based on Cascading Failure in Power Systems

In a prior work [68], two robustness parameters, namely, *percentage of unserved nodes* (PUN) and *percentage of noncritical links* (PNL), were proposed to assess the robustness of power system. In this chapter, witnessing the existence of a critical parameter called *onset time* in the profile of failure propagation, both from simulations [101] and historical data, we extend the methodology to quantitatively assess the vulnerability which takes robustness from a reciprocal perspective. In other words, a highly vulnerable power system is not robust.

The extended method consists of three main steps: 1) detecting *onset time* in the failure propagation process, 2) mapping *onset time* to a vulnerability index, and 3) assessing the systematic vulnerability of a power grid. Vulnerabilities of five selected power systems will be presented and analyzed.

4.3.1 Detection of Onset Time

The *onset time* is defined as the time when the number of failed nodes in a power grid begins to increase sharply during the propagation process. To identify the *onset time*, we apply the method developed by Goswami *et al*. [2], aiming to detect the abrupt transition in time series.

An illustration of the detection of the *onset time* is shown in Fig. 4.1. Fig. 4.1(a) plots the number of power elements (here, transmission lines are considered) being removed as time elapses. Here, the number of removed power links is denoted as NFL(t). Also, we characterize one complete propagation process of cascading failure as a *cascading failure scenario*, which is like an analog blackout event as shown in Fig. 4.1(a). From Fig. 4.1(a), we see that $t_{\text{onset}} \approx 2044$ min. In other words, in this cascading failure scenario, a fast cascading failure occurs after $t = 2044$ min,

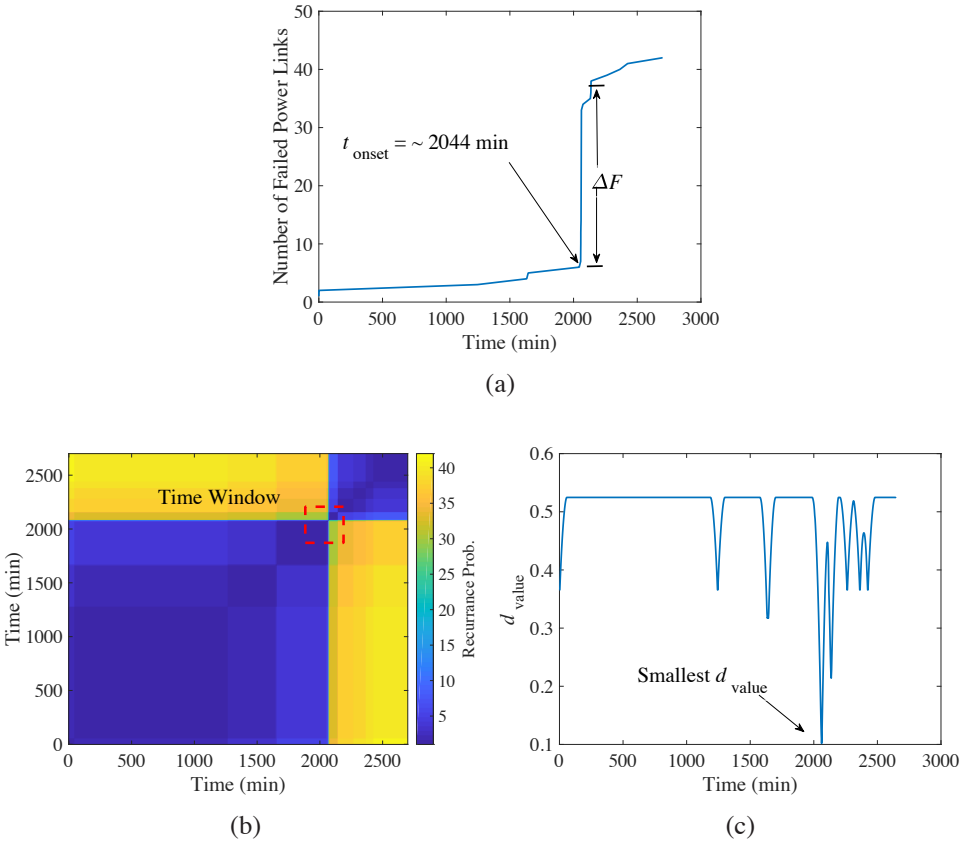


Figure 4.1: Detection of onset time using Goswami *et al.*'s method [2]. (a) Propagation profile of cascading failure; (b) recurrence matrix as heat map; (c) differential value indicating locations of large increments.

The occurrence of a dramatic increase in the number of failed power components is a typical kind of abrupt transmission in time series. Using Goswami *et al.*'s method [2], the first step to detect abrupt transmission is to transform the time series data NFL(t) into a recurrence matrix [120], which effectively quantifies the temporal evolution of the observable. The recurrence matrix $\mathbf{R}$ is a symmetric matrix consisting of recurrence probabilities [120]. Basically, each element $\mathbf{R}(i, j)$ represents the difference between time series data NFL(t_i) and NFL(t_j). Based on the recurrence matrix presented as a heat map as shown in Fig. 4.1(b), we derive a statistical value called *differential value*, denoted as d_{value}. By using a sliding window from t_1 to t_2, d_{value} is used to evaluate how similar the recurrence probabilities are within a sliding window. In particular, d_{value} is given by

$$d_{\text{value}} = \frac{\sum_{i,j=t_1}^{t_m} \mathbf{R_{ij}} + \sum_{i,j=t_m}^{t_2} \mathbf{R_{ij}}}{\sum_{i,j=t_1}^{t_2} \mathbf{R_{ij}}} \tag{4.1}$$

where t_m is the mid-point between t_1 and t_2 of the current sliding window, i.e., $t_m = (t_1 + t_2)/2$. Specifically, the numerator includes two sums of the elements in two recurrence matrices, namely, one is within the time duration $[t_1, t_m]$ and the other one is within the time duration $[t_m, t_2]$. In the denominator, the summation includes all elements in the recurrence matrix within $[t_1, t_2]$. One extreme case is that if elements in $\mathbf{R}$ within the sliding time window are all the same, then d_{value} is equal to 0.5.

If there are different densities of colors displayed in the heat map within a time window as shown in Fig. 4.1(b), the value of d_{value} is smaller than 0.5. For instance, from Fig. 4.1(b), when t_m is around 2000 min, the densities of colors show that both recurrence matrices corresponding to two time slots $[t_1, t_m]$ and $[t_{\text{m}}, t_2]$ are having smaller recurrence probabilities compared with the other recurrence probabilities outside the two recurrence matrices in the time window $[t_1, t_2]$. Thus, by plotting d_{value} versus time t_m, and as the sliding window moves along the diagonal of the entire $\mathbf{R}$ as shown in Fig. 4.1(b), we identify the smallest value of d_{value}, which corresponds to an abrupt transition. In this example, $t_{\text{m}} \approx 2050$ min. In summary, t_{m} is identified as the indicative time where d_{value} is smallest, and hence provides a reference for finding the *onset time* in a cascading failure scenario.

4.3.2 Mapping Onset Time to Vulnerability

In this section, we introduce an empirical *vulnerability index* based on the *onset time* observed in a cascading failure scenario. Here, we also define *rescue time*, denoted as T_{rescue}, which is the minimum acceptable duration taken by the system to recover the power system from serious cascading failure. Thus, when there are sufficient resources such as monitoring and restoration systems that can be utilized to protect the power grid [121], T_{rescue} should be small. Typically, a smaller T_{rescue} indicates a faster

response for protection, hence greater tolerance to cascading failure. Thus, T_{rescue} can be regarded as the critical value of t_{onset}, distinguishing safe and vulnerable scenarios. When $t_{\text{onset}} \geq T_{\text{rescue}}$, the power system is considered *safe*. Moreover, when $t_{\text{onset}} < T_{\text{rescue}}$, the power system will exhibit an inevitable cascading failure, which corresponds to a *vulnerable scenario*.

To assess the vulnerability of the power system, we simulate a large number of *cascading failure scenarios* for each power component chosen as an initial failed component and removed from the power network. Then, the vulnerability of power component i is evaluated based on the relative frequencies of safe and vulnerable scenarios resulted from initial failure of this component, i.e.,

$$V_i = \frac{N_{\text{sim}}\,|_{t_{\text{onset}}<T_{\text{rescue}}}}{N_{\text{sim}}} \tag{4.2}$$

where component i is initially tripped in one *cascading failure scenario* and a total of N_{sim} simulations are run. Basically, the vulnerability index V_i of component i is the percentage of cascading failure scenarios with $t_{\text{onset}} < T_{\text{rescue}}$. Furthermore, a threshold denoted as V_{critical} can be set to find out whether the selected component would likely result in a vulnerable scenario when it is initially tripped. In particular, if $V_i \geq V_{\text{critical}}$, a vulnerable scenario is expected when component i fails.

The final size of the blackout marked by the number of the failed links NFL(t_{final}) at the end of one *cascading failure scenario* is another key parameter reflecting the severity of a power outage. Thus, setting a threshold called $\text{NFL}_{\text{critical}}$, we expect a large-scale power outage if $\text{NFL}(t_{\text{final}}) \geq \text{NFL}_{\text{critical}}$. Specifically, a *fast* and *large-scale* cascading failure scenario can be identified by checking, respectively, $t_{\text{onset}} \geq T_{\text{rescue}}$ and $\text{NFL}(t_{\text{final}}) \geq \text{NFL}(t_{\text{critical}})$.

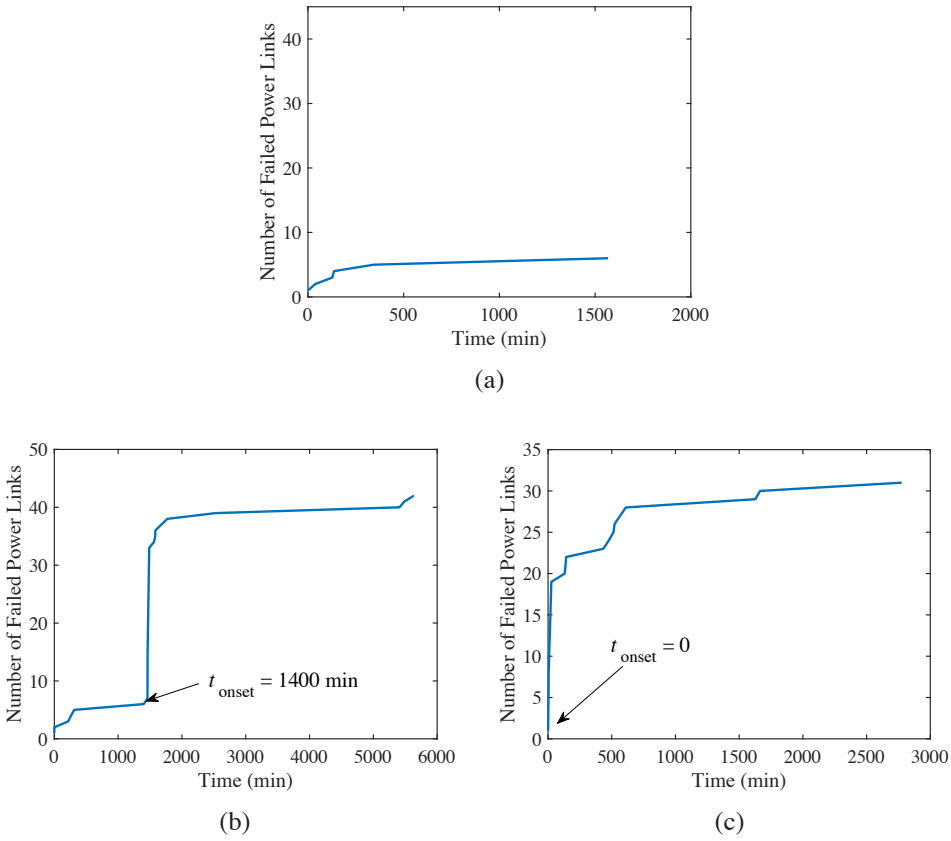


Figure 4.2: Three types of power lines observed in failure propagation in power networks. (a) Type I: no significant number of failed links; (b) Type II: significant number of failed links but relatively long onset time; (c) Type III: significant number of failed links and relatively short *onset time*.

4.3.3 Systematic Vulnerability Assessment

In order to gain a practical understanding of how vulnerable a power network is, we classify the power components in the power network into three types.

1. **Type I components**: A Type I power component is a power component which, upon failure, does not lead to cascading failure of a significant scale. Here, failure of power components leading to $\mathrm{NFL}(t_{\mathrm{final}}) < \mathrm{NFL}_{\mathrm{critical}}$ is regarded as insignificant, as shown in Fig. 4.2(a).

2. **Type II components**: A Type II power component, upon failure, will lead to cascading failure of the system, meeting the criteria $\mathrm{NFL}(t_{\mathrm{final}}) \geq \mathrm{NFL}_{\mathrm{critical}}$. Moreover, the *onset time* is longer than T_{rescue}, thus allowing recovery in time. An

example is shown in Fig. 4.2(b).

3. **Type III components**: A Type III power component, upon failure, will lead to cascading failure of the system with a significant number of subsequent failed components, i.e., $\text{NFL}(t_{\text{final}}) \geq \text{NFL}_{\text{critical}}$. Moreover, the *onset time* is shorter than T_{rescue}, making recovery difficult, as shown in Fig. 4.2(c).

4.3.4 Assessment Results

We run simulations according to the aforementioned method to assess the vulnerability of five selected power systems, including UIUC 150-Bus power system (UIUC150), South Carolina 500-Bus power system (SC500), SouthChina 612-Bus power system (GD612), European 1354-Bus power system (EURO1354) and Texas 2000-Bus power system (TEXAS2000). We launch a possible *cascading failure scenario* by setting an initial fault in a power line. For each initial line failure, we perform 1000 simulations, i.e., $N_{\text{sim}} = 1000$. Furthermore, V_{critical} and $\text{NFL}_{\text{critical}}$ are set to 0.75 and 10, respectively, to provide a specific condition for the vulnerability assessment of the five selected power networks based on the three categories of power lines. In other words, a power line is classified as Type III when 75% or more of vulnerable scenarios are generated from the 1000 simulations. Moreover, a cascading failure is significant when ten or more power lines fail eventually.

Table 4.1: Assessment results of selected power systems.

	UIUC150	SC500	GD612	EURO1354	TEXAS2000
N_{node}	150	500	612	1354	2000
N_{link}	203	584	852	1710	2667
$N_{\text{T1}}/P_{\text{T1}}$	90 / 44%	269 / 46%	344 / 40%	1123 / 66%	827 / 31%
$N_{\text{T2}}/P_{\text{T2}}$	50 / 25%	170 / 29%	112 / 13%	192 / 11%	327 / 12%
$N_{\text{T3}}/P_{\text{T3}}$	63 / 31%	145 / 25%	396 / 47%	395 / 23%	1513 / 57%

Table 4.1 shows the assessment results for the five selected power networks. The

first two rows give topological information of the power networks including the number of nodes N_{node} and the number of links N_{link} . We intentionally select five power systems with different scales. In rows 3, 4 and 5, the quantities and percentages of three different types of links are presented, as denoted to $N_{\text{T1}}/P_{\text{T1}}$, $N_{\text{T2}}/P_{\text{T2}}$ and $N_{\text{T3}}/P_{\text{T3}}$. Specifically, the percentages of Type III power lines shown in the 5th row are the indicative values for vulnerability since failure of Type III power lines induces fast and large-scale cascading failure [58].

In GD612 and TEXAS2000, around 50% of the power lines are Type III, and in other three power networks, less than a third are Type III. In other words, GD612 and TEXAS2000 are more prone to a fast and large-scale cascading failure. The above simulation-based assessment of robustness of a power network clearly points to the importance of reducing the number of Type III power lines for improvement of robustness. In the following we will investigate how fewer Type III power lines can be achieved through altering topology and other properties.

4.4 Network-Based Feature Extraction

Network topology plays an important role in determining the vulnerability of power grids to cascading failure. In most of the previous work surveyed in [14, 40], a network approach utilizing a single network feature, such as degree distribution or small-world property, has been considered for robustness enhancement. To further forecast the robustness of power grids from a complex network's perspective, we present here a decision tree-based learning model to generate rules in terms of a set of network-based features. Specifically, three network-based features are considered, namely, *average shortest path length*, *average clustering coefficient* and *average effective resistance (distance) to a nearest generator of all consumer nodes*.

4.4.1 Decision Tree Learning Model

Decision tree-based learning models are widely used in the field of machine learning, especially for data regression and classification [122]. In particular, a decision tree exhibits the capability of predicting the relationship between a criterion variable and one or more independent variables. It can also perform classification on a set of observations. In addition, the results obtained from decision trees are easy to understand and interpret because of their visual representations.

The main objective of adopting a decision tree-based learning model is to extract relevant network-based features that enhance robustness of power networks by changing the network topologies. In other words, via the decision tree, we learn how a power grid can be made less vulnerable through adjusting the network-based features. Basically, we formulate the networks' robustness enhancement as a classification problem. The given power network is being "updated" by changing its topology. The updated power networks denoted as G_{ud} are classified into either "safe" or "fragile" power networks, which serve as two assessors. When the value of P_{III} representing the percentage of Type III power lines in the updated power network is smaller than that of the original power network, we assign a "1" to the assessor of this updated power network, indicating a "safe" power network. Otherwise, a "0" is assigned to the assessor. The predictors in this decision tree model are the network-based features.

A typical decision tree consists of a number of decision nodes, one being a root node and others being leaf nodes. The production of a decision tree starts from the root node and finishes when no more decision node can be split into leaf nodes. At each decision node, one of the predictors is selected [123]. The split criterion used here is the node error, which is defined as the fraction of misclassified networks at a node. According to the split criterion, in a leaf node labeled as a set of "safe" power networks, there are actually 10% "fragile" power networks, which are viewed as the misclassified networks, and the node error is 0.1. For example, in the root node, if a

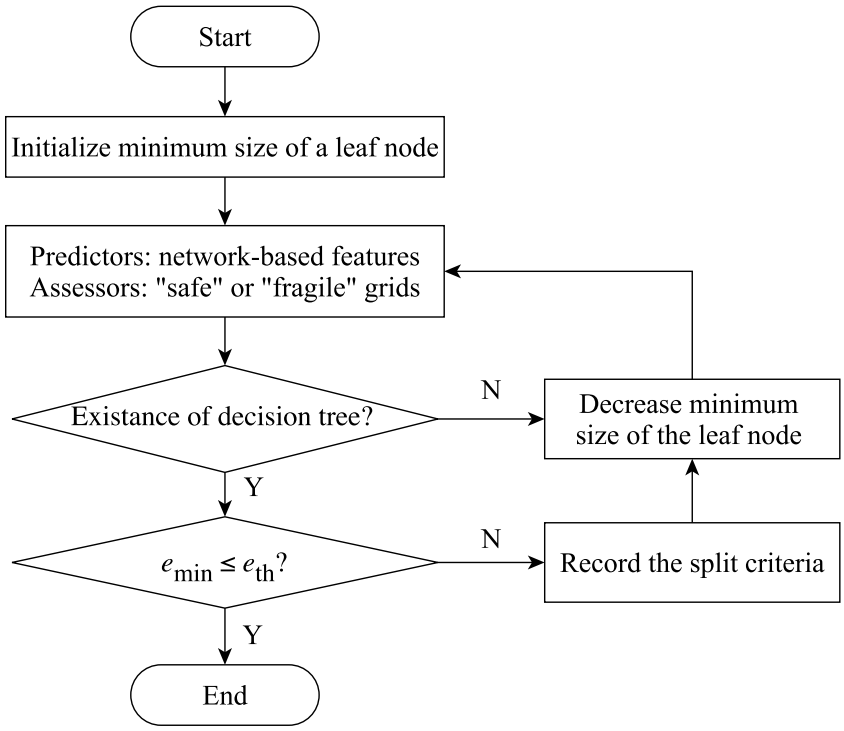


Figure 4.3: Flow chart for generating an appropriate decision tree.

smaller node error can be achieved by choosing Predictor A (a network feature) to split the data, Predictor A is the appropriate attribute for the root node.

A decision tree can be generated from the dataset including predictors and assessors. However, relevant features may not be readily extracted unless the predictors chosen are positively or negatively correlated with the assessors, thus clearly indicating how network features should be modified to achieve more robust power networks. Thus, in order to get more practical predictors, we design the following algorithm to generate a sound decision tree.

The algorithm presented by the flow chat shown in Fig. 4.3 takes the following steps,

- *Step 1*: The minimum number of branches in a leaf node, which represents the minimum number of power networks being observed in a leaf node, is set. A larger minimum number of leaf nodes gives a simpler decision tree.

- *Step 2*: Feeding the input dataset (predictors and assessors) into the learning model, a decision tree is initially generated. Then, by reducing the minimum number of branches in a leaf node, the decision tree is formed by iteration until a standard tree consisting of at least one decision node and two leaf nodes is generated.

- *Step 3*: For a generated standard tree, the node error e in classifying power networks as "safe" power networks is found for all the leaf nodes. For instance, for a leaf node of power networks classified as "safe", if 25% are actually "fragile", then e is equal to 0.25. Furthermore, if the minimum value of e (denoted as $e_{\min}$) among all the leaf nodes is less than a given threshold e_{th}, the split criterion in terms of increasing or decreasing the values of predictors will achieve more robust power networks is determined. Otherwise, the iteration resumes at Step 2.

4.4.2 Network-Based Features

Significant network-based features of a power grid are used in this chapter for enhancing the robustness of power grids. We have tested the significance of more than 10 network-based features and eventually selected the following three.

1. *Average Shortest Path Length (L)*: the mean value of the shortest paths between each pair of nodes in the network [124], i.e.,

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij}. \tag{4.3}$$

   where N is the total number of nodes and d_{ij} is the shortest path between nodes i and j.

2. *Average Clustering Coefficient (Γ)*: a local metric to measure the density of triangles in a network. A triangle is formed if two nodes that are connected to a

third node are also connected to each other. Thus, for each node i in a network, there is one corresponding clustering coefficient Γ_i [124]. For the entire network, the average clustering coefficient is

$$\Gamma = \frac{1}{N} \sum_i \Gamma_i. \tag{4.4}$$

3. *Average Effective Resistance (Distance) to a Nearest Generator of All Consumer Nodes (D)*: a measure of the accessibility to generators of all power consuming loads in a power network, i.e.,

$$D = \frac{1}{(N-g)} \sum_{i \in \mathcal{N} \setminus \mathcal{G}} d(i) \tag{4.5}$$

where $\mathcal{N} \setminus \mathcal{G}$ is the set of nodes excluding the generator nodes, N is the total number of nodes, and g is the number of generators, $d(i)$ represents resistance distance of node i to its nearest generator introduced in the previous study [68].

Both *Average Shortest Path Length* and *Average Clustering Coefficient* reveal the major characteristic of the network structure of a power grid. A network exhibiting a short L and a large Γ is classified as a small-world network from the network science's viewpoint [1]. Recent studies have found that power grids displaying the small-world property have higher robustness [40]. Moreover, *Average Effective Resistance (distance) to a Nearest Generator of All Consumer Nodes* reveals the location information of generators in a power network. A smaller D implies that generator distribution is more decentralized in a power network. It has been found [68] that decentralized power source nodes exhibiting a smaller D reduces the vulnerability of the power network to cascading failure.

4.5 Results and Discussion

Experiments have been conducted to demonstrate the effectiveness of the decision tree learning method for improving power grid's robustness against cascading failure. Based on the UIUC 150-bus power system, a number of updated power networks (modified topologies) are acquired by edge modification. By implementing the learning model, we derive a set of rules using three network-based features to predict whether the updated power network is more robust, and then compare with the ratio of Type III power lines in a power network found from simulations.

4.5.1 Enhancing Robustness via Topology Modification

The goal of improving the robustness of a power network is to reduce the number of Type III power components. In this chapter, we consider lowering the vulnerability of power networks by changing the topology. Once a large power network is established (evolved over time), redesigning a new power network seems rather difficult. Thus, the initial planning (design) of a power grid has traditionally incorporated robustness consideration [125, 126]. However, allowing transmission switching [127] in existing grids is a feasible means of improving robustness via topology modification, as demonstrated by Beygelzimer *et al*. [128]. Here, to modify the structure of an available power network, we propose a rewiring scheme, based on the work of Wang *et al*. [129], with several practical constraints imposed. Basically, a fraction p of the edges in the power network are rewired while keeping the total number of edges for maintaining consistency of the network size [44]. Moreover, we impose two practical constraints. First, after rewiring an edge, we preserve the admittance of the power line. Second, since excessive modification of the grid's topology is economically infeasible, we perform less than 10% edge rewiring, i.e., $p < 0.1$. By using the rewiring scheme, we generate updated power grids or *candidate networks* which might be more robust compared with the original one. After rewiring, the numbers of nodes and edges keep

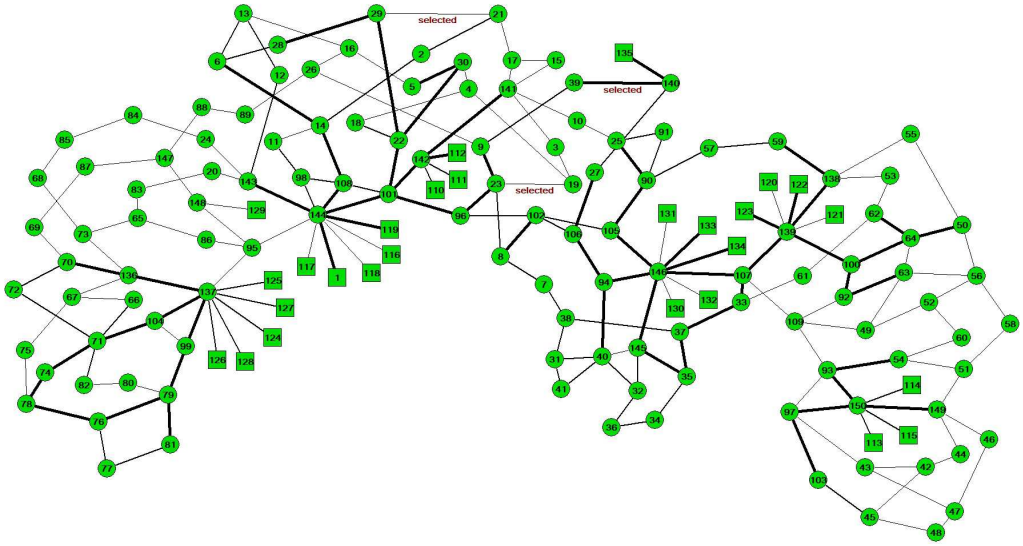


Figure 4.4: UIUC 150-bus power system before edge modification. Numbers of Types I, II and III (thickest edges) power lines are 90, 63, and 50. Edge modification involves removing edges (19, 23), (21, 29) and (39, 140).

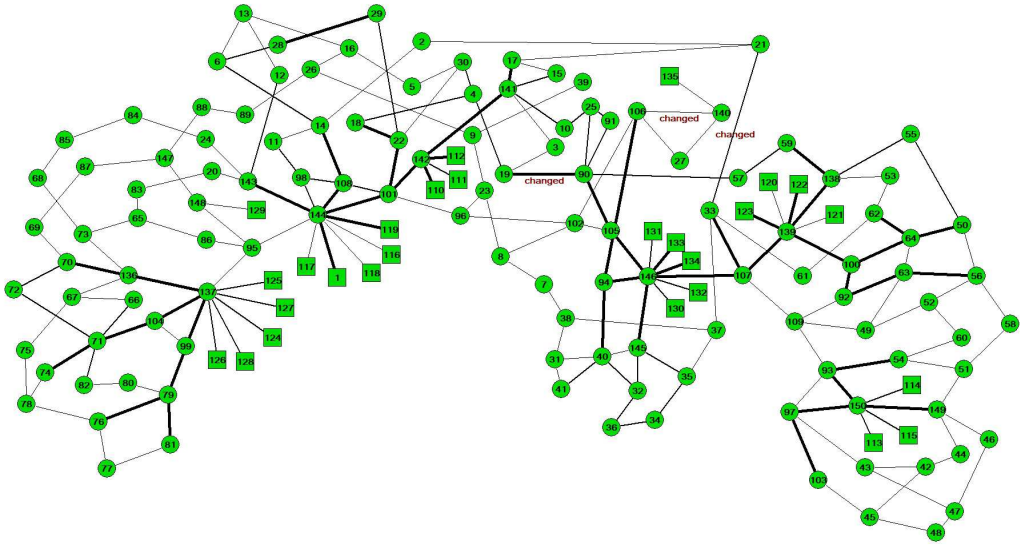


Figure 4.5: UIUC 150-bus power system after edge modification. Numbers of Types I, II and III power lines (thickest edges) are 107, 51, and 45. Edge modification involves adding edges (19, 90), (21, 33) and (106, 140).

unchanged.

An example of enhancing the robustness of UIUC 150-bus power system is illustrated in Figs. 4.4 and 4.5. Three edges are removed, as shown in Fig. 4.4, and then three new edges are added, as shown in Fig. 4.5. It is found that after edge modifi-

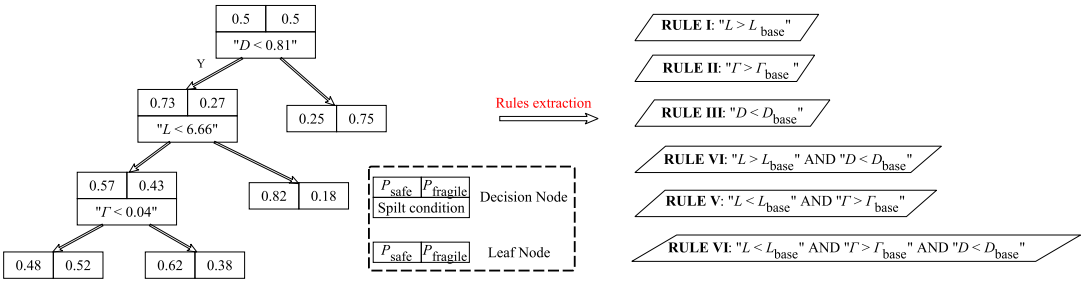


Figure 4.6: Rules derived by comparing the original and updated networks. Updated network is generated by decision tree with $e_{\text{th}} = 0.25$. Split condition at decision node uses either network-based feature L, Γ or D.

cation, the number of Type III power lines are reduced in the updated power network indicating am improved robustness of the updated power network. In particular, most of the Type III power lines near the three removed edges have become either Type I or Type II lines while very few new Type III lines are created by adding the new edges. In the following subsection, we demonstrate how the robustness of a power grid can be enhanced by rewiring edges in a power network according to some network-based features.

4.5.2 Rules Construction

A decision tree is generated by implementing the algorithm given in Section 4.4.1. Referring to the example shown in Fig. 4.6, the tree contains three decision nodes and four leaf nodes. Both decision nodes and leaf nodes display the percentages of "safe" power networks P_{safe} and "fragile" power networks P_{frag}. Furthermore, the split condition based on a network-based feature is given in each decision node. For example, in the root node (the top decision node), the split condition is $D \leq 0.81$, satisfing which will give more "safe" power networks. Otherwise, $D > 0.81$ results in more "fragile" power networks among the updated power networks.

Suppose L_{u}, Γ_{u} and D_{u} denote the Average Shortest Path Length, Average Clustering Coefficient and Average Effective Resistance (distance) to a Nearest Generator of All Consumer Nodes of the updated network, respectively. Also, L_{base}, Γ_{base} and

D_{base} denote the corresponding attributes of the original network. A set of six rules is proposed for enhancing the robustness of the network against cascading failure. These rules are:

Rule I: $L_{\text{u}} > L_{\text{base}}$

Rule II: $\Gamma_{\text{u}} > \Gamma_{\text{base}}$

Rule III: $D_{\text{u}} < D_{\text{base}}$

Rule IV: $L_{\text{u}} > L_{\text{base}}$ and $D_{\text{u}} < D_{\text{base}}$

Rule V: $L_{\text{u}} < L_{\text{base}}$ and $\Gamma_{\text{u}} > \Gamma_{\text{base}}$

Rule VI: $L_{\text{u}} < L_{\text{base}}$ and $\Gamma_{\text{u}} < \Gamma_{\text{base}}$ and $D_{\text{u}} < D_{\text{base}}$

The aim is to generate networks via iterative topology updates involving rewiring of links that complies with these rules.

4.5.3 Effectiveness Verification of Enhancement Rules

To verify the effective of the aforedescribed enhancement rules, we compare the rule compliant and non-compliant networks using the test algorithm summarized in the following three steps and illustrated by the flow chart shown in the Fig. 4.7.

- *Step 1*: An updated power network is generated by implementing the rewiring scheme mentioned in Section 4.5.1.
- *Step 2*: The network-based features of the updated power network are checked for compliance with a chosen rule. For example, if Rule I is chosen, then the *Average Shortest Path Length* of the updated power network is compared with the original network's. On compliance, go to Step 3. Otherwise, return to Step 1.
- *Step 3*: The vulnerability of the updated power network is assessed by calculating the percentage of each type of power lines. The iteration ends until a minimum number of "safe" power networks N_{th} are obtained.

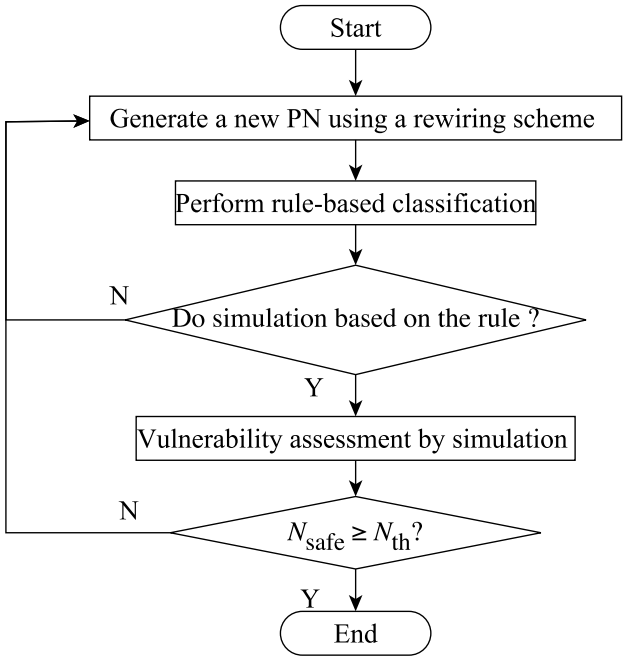


Figure 4.7: Flowchart for verifying the effectiveness of the rules for enhancement of robustness of the rewired power grid.

To evaluate the effectiveness of each rule used for enhancing the robustness of an updated power network, we find the number of successful generations of "safe" power networks denoted as N_{safe} and the total number of power networks simulated for assessment of the robustness of power systems, which is given by N_{ast}. Basically, since at least N_{th} "safe" power networks are required, a smaller N_{ast} reveals a higher effectiveness of the corresponding rule, which gives more updated power networks exhibiting lower vulnerability to cascading failure.

The values of N_{ast}, N_{safe} and N_{frag} (the number of "fragile" power networks assessed by simulation) are shown in Fig. 4.8. Rule VI makes the largest contribution to filtering more "safe" power networks in terms of the ratio N_{safe}/N_{ast}. Although Rule I and Rule II based on one single feasible remove at least 50% of "fragile" power networks, the better performance of Rule VI demonstrates the combined use of L and D in reducing Type III power lines. In particular, updating the network topology of the original power network by increasing L and reducing D results in updated power networks having enhanced robustness. This finding shows the superiority of the decision tree-based

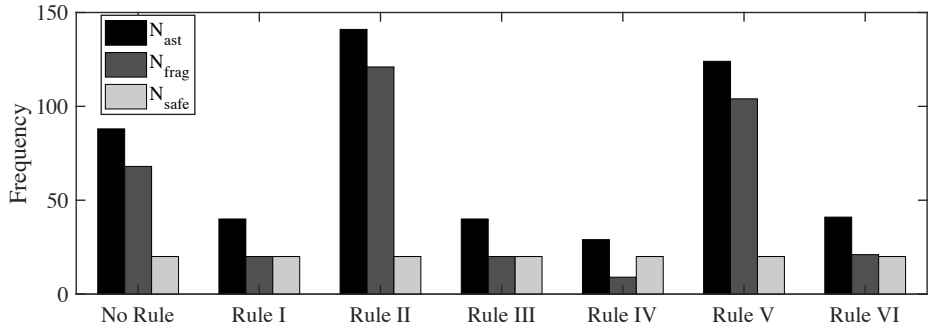


Figure 4.8: Effectiveness of rules on robustness enhancement of power networks

learning model in providing an understanding of the use of multiple network-based features in enhancing robustness of power networks.

The results also have two remarkable implications about the effect of network topologies on the robustness of power grids. First, increasing L of a power network, which implies weakening the small-world property, can improve robustness against cascading failure [40]. Second, reducing D, which means more decentralized power source distribution, can lower the vulnerability of a power network to cascading failure, which is consistent with the early study [68].

4.6 Summary

Enhancing the robustness of power systems plays an essential role in maintaining reliable electricity supply that is needed for almost all residential, industrial, business and governmental activities. In particular, the risk of a fast and large-scale blackout should be kept to minimum. In this chapter, we develop a system-level method to assess the vulnerability of power systems. Specifically, the vulnerability is evaluated through examining a parameter called *onset time* that can be detected in a failure cascade profile, which reveals the rapidity of cascading failure. Moreover, we propose a decision tree-based learning model to extract significant network-based features which can become effective indicators for enhancing the robustness of power networks. One

way to reduce the vulnerability of a power network to fast and large-scale cascading failure is to perform minor rewiring of edges. Numerous rewired power networks are collected as the input for the learning model. A decision tree that uses some significant network-based features, together with a set of rules, provides an effective procedure for reducing network vulnerability. Experimental results reveal that a power network has higher robustness against cascading failure if its topology exhibits less random features and more decentralized generator distribution. It is expected that future study employing the decision tree-based learning model will discover more crucial network-based attributes that guarantee reduced vulnerability of power systems.

Chapter 5

Cascading Failure of Cyber-Coupled Power Systems Considering Interaction Between Attack and Defense

In the previous chapter, we have proposed a system-level method to assess the vulnerability of power systems from a complex network's perspective using decision trees. In this chapter, we develop a network-based model with consideration of the physical power flow process to study the cascading failure in cyber-coupled power systems. We take the coupling between power and cyber networks as being resulted from the interdependence of power nodes and cyber nodes. Interaction between two processes, one aiming to attack (cause damage) and the other aiming to defend (protect) the components in the power network, is considered in the model. This interaction offers a novel perspective to interpreting the interdependence of power and cyber networks. To study how an attacker or defender deploys resources to attack or protect a power component, four strategies in distributing the attack and defense strengths are considered, namely, even distribution, degree-based distribution, capacity-based distribution, and random

distribution. To probe into the actual propagation process of a blackout, we define four critical time points, namely, start time, attack time, isolation time and end time, and use these time points to analyze and evaluate the effectiveness of different attack and defense strategies. The tit-for-tat defense strategy, in which defender adopts the same strategy as the attacker, is found to be the preferred defense strategy under most conditions. Moreover, allocating defense strength in terms of capacity-based distribution can most effectively suppress cascading failure. This finding was not obtainable without due consideration of the physical power flow process in network-based models.

5.1 Introduction

Cyber-physical systems have emerged as essential networked systems that enable the incorporation of computational and intelligent management capabilities provided by sophisticated computer networks in critical applications for residential, commercial, industrial and military uses [18]. A cyber-physical system is a physical system integrated with cyber networks. The cyber part of the system provides intelligent and efficient monitoring, control, computing and communication functions [19]. Real-world examples of cyber-physical systems are numerous, and the smart grid is one particularly important example. A smart grid is an electric power distribution network supported by advanced cyber networks, which is a critical infrastructure delivering power to a large population of users [20]. Cyber security has become a key challenge to power delivery systems due to the involvement of cyber networks that makes smart grids vulnerable to attacks via cyber coupling [21]. For instance, in December 2015, the attack of computer malware from cyber networks severely caused the outage of the Ukrainian power grid, demonstrating that the cyber attack on power grids was no longer a fictional event.

The modeling of cascading failure has taken either a network science's or an electrical engineering perspective, and the aim is to investigate the vulnerability of power

systems and reduce the likelihood of occurrence of power outage. By applying the methodology of complex networks, which is effective for analyzing large-scale and real-world networks [8, 130, 12], cascading failure in a power network can be examined in terms of a series of nodes' or links' failure, where nodes represent power substations and links are the transmission lines. On the other hand, researchers in the area of power systems pay more attention to the stability of power grids such as the problem of voltage collapse [103]. Moreover, recently, combined models have been considered, incorporating the actual operational processes into the network-based models [114].

As modern smart grids become increasingly reliance on cyber assets such as smart power meters, intelligent sensors and controllers, cyber attacks have become real threats to power grids. Moreover, SCADA (Supervisory Control and Data Acquisition) systems that facilitate maintenance of smart grids are themselves vulnerable to cyber attacks. In particular, an attacker may try to gain access to SCADA systems and perform malicious actions on power systems [131], for instance, by causing de-synchronization [132] or erroneous state estimation [133].

Network-based studies have recently been shifted to cascading failure in interdependent networks. Here, *interdependent networks*, or coupled networks, refer to one or more networks coupled together. Buldyrev *et al*. [17] initially studied cascading failure in interdependent networks for the purpose of assessing their vulnerabilities to attacks. In their work, an interdependent (coupled) network consists of a communication network and a power grid with the description of an iterative process of cascading failure. Although the highly abstracted and generalized network-based model offers a convenient framework permitting the use of statistical physics, it is challenging to implement these high-level models to real-world cyber-physical systems. The main reason is the omission of the underlying physical processes in these high-level network-based models. For instance, Kirchhoff's laws and electrical properties of components are crucial in generating the necessary power flow distribution in a power network, and the protocols for traffic control play a crucial role in data transmissions in communication

networks. Ignoring these physical processes and properties often lead to unrealistic models and sometimes inconsistent results. Thus, this is one of the main concerns to be addressed here in this chapter. Accordingly, by incorporating physical processes in modeling cyber-coupled power systems, consistent results and useful insights can be obtained in relation to the practical operation and performance of the coupled system. Through using a network-based model, node electrical centrality can be effectively identified by adopting an AC power flow model [63], and the robustness of interdependent power grids and communication networks can be effectively assessed by using a DC power flow model [134].

One central challenge in modeling cyber-coupled power systems is the interpretation of the interdependence between cyber networks and power networks. The interdependence can be modeled by adopting percolation theory in the aforementioned pure network-based models, which is, however, not readily applicable to practical systems. Thus, the modeling of interdependence in coupled networks, being another main concern, has been widely carried out with realistic engineering considerations. For instance, Cai *et al*. [73] developed an interactive model to analyze cascading failure in interdependent systems by considering the interdependence between power systems and the dispatching data networks. In Cai *et al*.'s model, the tripped power components in power grids may cause abnormal function of data centers in cyber networks, while failure of any component in cyber networks may cause overloading of some power lines. To understand the various forms of practical interdependence between power systems and cyber networks, Wang *et al*. [74] investigated the effect of multiple cyber attacks including denial-of-service (DoS) attacks, replay attacks, and false data injection attacks on cascading failure in electrical cyber-physical systems. Despite the increased complexity of the problem when technical details are included in the network-based model, identification of the parameters affecting networks' robustness is still of highest practical significance.

In the previous studies of cascading failure in cyber-coupled power systems, mal-

ware propagation is assumed to be completed at the time of attack and the attacker has full knowledge of the power grid. However, in reality, cyber attack can also be launched under incomplete information of power grids [135]. Also, the effect of continuous spreading of the malware on the cyber network has not been considered while power grids are being attacked. Thus, another main concern is the lack of proper models for investigating the cascading failure in a power grid coupled with the cyber network while the malware spreading is still proceeding on the cyber network. The model introducted in Section 3.2 was developed to study the effect of cyber coupling on cascading failure, and significant difference has been found in the cascading failure in cyber-coupled power systems compared to the propagation process of malware spreading on the cyber network and cascading failure in the uncoupled power system. This model provides an engineering perspective to assessing the vulnerability of cyber-coupled power systems, which can be viewed as a practical extension of the network-based model proposed earlier [17]. However, up to now, the essential interaction between attack and defense strategies has still been omitted in the study of cyber-coupled power networks. Ma *et al*. [136] developed a Markov security game model to offer an insight into how the attacker and defender decide to deploy finite resources to attack and defend the power components during the processes of sequential and intentional attack [51, 112].

In this study, we aim to develop one network-based model to comprehensively address the above-mentioned three concerns, namely, the incorporation of the power flow model, the interdependence between attack and defense, and the effect of malware spreading while cascading failure proceeds over the power network. Moreover, we examine four types of attack and defense strategies targeting power components, and study their interactions. The attacker aims to cause dysfunction of critical components in order to intensify the severity of power outage, while the defender attempts to protect the components of high vulnerability to reduce the risk of cascading failure. The attack and defense resources are allocated according to four strategic distributions: 1)

Even Distribution, 2) Degree-based Distribution, 3) Capacity-based Distribution, and 4) Random Distribution. The main contributions are summarized as follows:

1. With the incorporation of the physical process for modeling the cascading failure in power systems, our study offers consistent and practical insights into the choice of defense strategies that can reduce the severity of cascading failure under various circumstances of attack strategies and resource availabilities.

2. We consider the interdependence between the power network and the cyber network in terms of interactions between attack and defense. From a complex network's perspective, we provide an analytical basis for studying the essential interaction between the two processes, one aiming to attack and the other aiming to defend the components in the power network.

3. By probing into the propagation profiles of malware spreading and failure propagation in the coupled power system, our study provides a complete mural describing the various combinations of attack and defense strategies under various coupling conditions, and how they affect the severity of cascading failure.

5.2 Model

In this section, we describe the model used in studying cascading failure in cyber-coupled power systems introduced in Section 3.2. Moreover, in this chapter, we complete the model by incorporating the process of malware attacks from the cyber network. The model is implemented to simulate the propagation patterns of cascading failure under various combinations of attack and defense strategies.

5.2.1 Cyber-Coupled Power Systems

We consider a cyber-coupled power system consisting of a power grid and a cyber network. The mechanism of cascading failure in this coupled system is governed by two

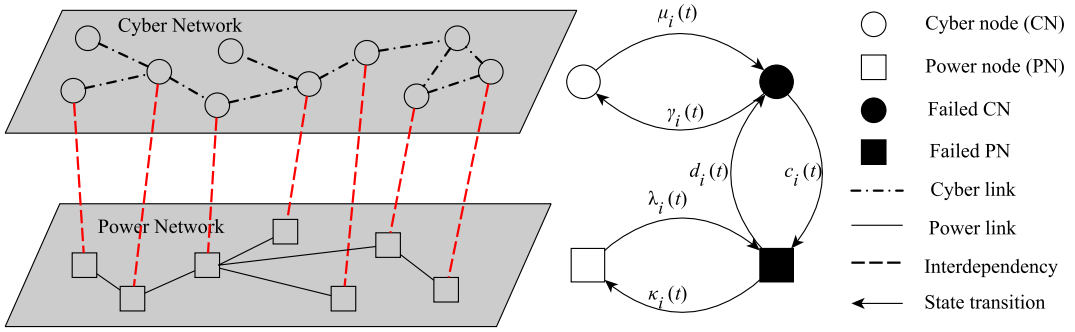


Figure 5.1: Coupled network consisting of a cyber network and a power network, with state transitions showing infection of a cyber node, overload tripping of a power node and attack to a power node from a cyber node.

main processes. First, the power flow distribution of the power grid is determined by the network connectivity (topology) and the physical laws that govern the voltage and current distribution in the network. Second, combined with a stochastic process that describes the necessary state transitions in the coupled network, the process is completed to include the effect of cyber coupling on the failure propagation in the network. In Fig. 5.1, the coupled system is abstracted as a coupled network which consists of a power network A with N_A nodes (shown in the bottom layer) and a cyber network B with N_B nodes (shown in the top layer). The cyber network provides sensing and control functions, while the power network powers the cyber network. Thus, there exists an interdependency between these two networks, as denoted by the vertical dashed connections between nodes in networks A and B.

To practically describe the interconnection between networks A and B, we adopt the definition of coupling strength [32]. Basically, since not all the nodes in the power network need to be connected to the cyber network and vice versa, we assume that a fraction q_A of the nodes in network A are affected by the nodes in network B and a fraction q_B of the nodes in network B are affected by the nodes in network A. Here, we consider one-to-one connection style so that the number of connections N_{A-B} is equal to $q_A N_A = q_B N_B$, with the model extendable to investigate other kinds of connection

styles.

5.2.2 Dynamics of Cascading Failure

We assume that a cyber node is able to take malicious actions on its coupled power node when it is infected by a malware. This corresponds to an interdiction attack pointed out in a recent review work [137]. Thus, in Fig. 5.1, a normal cyber node, represented by a white circle, can become infected and be represented by a solid black circle. Following the malware contagion mechanism [97], the infection rate on the cyber network is given by

$$\mu_i(t) = \sum_{j \in \Omega} \beta_{ij}, \tag{5.1}$$

where Ω is the set of all infected neighbors of cyber node i and β_{ij} is the rate at which infected cyber node j infects its neighbor node i. Note that a recovery process may exist in a real cyber node, which may contribute to suppressing the cascading failure in cyber-coupled power system. Here, for scenarios of fast cascading failure, we may take the recovery rate $\gamma_i(t)$ as zero. For an infinitesimal time interval dt, the probability that a state transition occurs under the condition that a cyber node transits from normal state (represented by 0) to failure state (represented by 1) can be written as

$$T_1 : P[s_{B_i}(t + dt) = 1 \mid s_{B_i}(t) = 0] = \mu_i(t)dt. \tag{5.2}$$

In a power system, a power node, represented by a square in Fig. 5.1, fails to serve its function either when it is tripped due to power overloading or when it is unserved because of losing access to any power generator. It is noted that the failure under the second condition occurs instantly. On the other hand, we represent the tripping process as a state transition based a stochastic model shown in Fig. 5.1, where a white square becomes a black solid square. For practical purposes, it suffices to take power overloading as the dominant tripping mechanism on a power node, which is explained

in detail in Section 3.1.1.2. 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 $\lambda_i(t) = 0$. Instead, when the element exceeds its capacity, there will be a short delay before it is finally removed. The tripping rate is related to the extent of overloading. Specifically, if element i is heavily overloaded, it will be tripped more rapidly compared to the case of slight overloading. Based on this assumption, the tripping rate in the process, λ_i, is given by

$$\lambda_i(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \leq C_i \end{cases} \tag{5.3}$$

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 tripping rate. In this chapter, the method used for determining the power loading in the power system is based on a deterministic DC-based flow model introduced in Section 3.1.1.3. We assume that cascading failure occurs very fast so that any restoration action is still not taken. Correspondingly, the restoration rate κ is zero in this model. Thus, when a power node is in normal state, and on the condition that its coupling cyber node is working normally or it has no coupling nodes, the probability that a power node transits from normal state (represented by 0) to failure state (represented by 1) in an infinitesimal time interval dt can be written as

$$T_2 : P[s_{A_i}(t + dt) = 1 \mid s_{A_i}(t) = 0] = \lambda_i(t)dt. \tag{5.4}$$

From Fig. 5.1, the vertical dash line connecting a cyber node and a power node represents the interdependence between the two systems. In particular, we assume that the cyber component in the cyber network has control over its coupled power component (or substation), while the power node supplies power to the cyber network. Thus, based on the existing coupling structure, when a power node has a coupled cyber node

which is infected by a computer malware, the power node (in normal state) will be more prone to failure due to the malicious action of the malware. Thus, we may formulate that the malware infection will increase the state transition rate λ_i mentioned in equation (5.3) by an additional term $c_i(t)$. The probability that a power node transits from normal state (represented by 0) to failure state (represented by 1) in an infinitesimal time interval dt when B_i is infected by computer malware can thus be written as

$$T_3 : P[s_{A_i}(t + dt) = 1 \mid s_{A_i}(t) = 0] = (\lambda_i(t) + c_i(t))dt, \tag{5.5}$$

where $c_i(t)$ represents the dependence of a cyber node on a power node. Furthermore, assuming that all cyber components are adequately powered by backup power supply during cascading failure, the coupling strength of power network to cyber network, denoted by $d_i(t)$, is zero. Thus, cascading failure induced by the coupling between cyber and power networks is unidirectional in the current study. In other words, the failure of cyber nodes might cause the failure of power nodes while the failure of power nodes does not affect cyber nodes. Also, instead of drilling into stability or synchronization [138] in communication networks from a control viewpoint, our study assumes that the controllers in cyber networks are accessed by the attacker once infected by a malware.

5.3 Attack and Defense Strategies

We consider the interaction between attack and defense to probe further into the way in which the cyber network interferes the power network. In particular, based on a one-to-one coupling style, if the power node is coupled with a cyber node, we consider the power node as a cyber-coupled power node $A'_i \in A'$, where A' is the full set of power nodes coupled with cyber nodes. Each A'_i is influenced by its coupled cyber node in two distinct ways. The first one is the attack on the power nodes launched by malware

on the cyber nodes, and the second one is due to the defense action taken through intelligent control implemented in the cyber nodes. Thus, equation (5.5) becomes

$$T_3' : P[s_{A_i}(t+dt) = 1 \mid s_{A_i}(t) = 0] = \min\{(\lambda_i(t) + c_i(t))dt, 0\}, \tag{5.6}$$

where $\min\{(\lambda_i(t) + c_i(t))dt, 0\}$ indicates that the probability should be a non-negative value even when $|c_i(t)| > |\lambda_i(t)|$. By considering the interaction between attack and defense in state transition T_3', $c_i(t)$ is given as

$$c_i(t) = \begin{cases} \chi_i(t) - \psi_i(t), & \text{if } A_i \in A' \\ 0, & \text{if } A_i \notin A' \end{cases} \tag{5.7}$$

where $\chi_i(t)$ and $\psi_i(t)$ represent the attack rate and the defense rate, respectively, with the same unit of λ. To determine these two rates, in this study, we propose four types of attack and defense strategies, as described in the next two subsections.

5.3.1 Attack Strategies

From a attacker's point of view, when a power node A_i is coupled with a cyber node B_i which is infected by the malware, the power node V_i is said to be a vulnerable power node, where V represents the entire set of vulnerable power nodes which is a subset of the entire power network. In other words, only when a power node A_i becomes a vulnerable power node, the attack rate $\chi_i(t)$ becomes valid.

Two factors determine the value of $\chi_i(t)$. The first one is the average strength, denoted by X, which represents the resource available for launching attack on a power component. In this chapter, X is assumed constant. It is noted that here $N_A = N_V$. The second factor is the attack allocation strategy on V, which may take the following options:

1. *Strategy I – Even distribution* S_{A1}: In this case, the attack strength is distributed

evenly to all V_i evenly. Thus, the attack rate of A_i is given by

$$\chi_i(t) = \begin{cases} X, & \text{if } A_i \in V \\ 0, & \text{if } A_i \notin V \end{cases} \tag{5.8}$$

2. *Strategy II – Degree-based distribution* S_{A2}: The degree k_{A_i} of each power node is taken as a measure of its criticality. In particular, the attack rate is allocated according to the node degree, i.e.,

$$\chi_i(t) = \begin{cases} \dfrac{k_{A_i} X}{\frac{1}{N_A} \sum\limits_{A_i} k_{A_i}}, & \text{if } A_i \in V \\ 0, & \text{if } A_i \notin V \end{cases} \tag{5.9}$$

3. *Strategy III – Capacity-based distribution* S_{A3}: The capacity C_{A_i} of each power node is taken as a measure of its criticality. Here, capacity C_{A_i} is actually C_i given in (3) for the particular node A_i, where $C_i = (1 + \alpha) \times I_i(\text{normal})$, and $I_i(\text{normal})$ is the total current flowing out of a power node under normal load demand condition. Thus, the attack rate is set according to C_{A_i} for A_i, i.e.,

$$\chi_i(t) = \begin{cases} \dfrac{C_{A_i} X}{\frac{1}{N_A} \sum\limits_{A_i} C_{A_i}}, & \text{if } A_i \in V \\ 0, & \text{if } A_i \notin V \end{cases} \tag{5.10}$$

4. *Strategy IV – Random distribution* S_{A4}: For comparison's sake, a random allocation strategy is considered. For each vulnerable power node V_i, the attack rate is randomly assigned. It is noted that $\sum\limits_i \chi_i(t) = N_V X$.

5.3.2 Defense Strategies

In a likewise fashion, we introduce four allocation schemes for the defense rate $\psi_i(t)$. However, unlike the attack rate which is only relevant to vulnerable power nodes v_n,

the defense rate exists on each power node whenever the power node is coupled with a cyber node. It is noted that here $N_A = N_{A'}$. Specifically, the value of $\psi_i(t)$ is assigned according to the following strategies:

1. *Strategy I – Even distribution* S_{D1}: In this case, the defense strength is evenly distributed to each A'_i. Thus, the defense rate of A_i is given by

$$\psi_i(t) = \begin{cases} \Psi, & \text{if } A_i \in A' \\ 0, & \text{if } A_i \notin A' \end{cases} \tag{5.11}$$

2. *Strategy II – Degree-based distribution* S_{D2}: The degree k_{A_i} of each cyber-coupled power node is taken as a measure of its criticality. Thus, the defense rate of A_i is designed according to

$$\psi_i(t) = \begin{cases} \dfrac{k_{A_i}\Psi}{\frac{1}{N_A}\sum\limits_{A_i} k_{A_i}}, & \text{if } A_i \in A' \\ 0, & \text{if } A_i \notin A' \end{cases} \tag{5.12}$$

3. *Strategy III – Capacity-based distribution* S_{D3}: The capacity C_{A_i} of each cyber-coupled power node is taken as a measure of its criticality, similar to the attack cases. Thus, the value of $\psi_i(t)$ is assigned according to C_{A_i}, i.e.,

$$\psi_i(t) = \begin{cases} \dfrac{C_{A_i}\Psi}{\frac{1}{N_A}\sum\limits_{A_i} C_{A_i}}, & \text{if } A_i \in A' \\ 0, & \text{if } A_i \notin A' \end{cases} \tag{5.13}$$

4. *Strategy IV – Random distribution* S_{D4}: For comparison's sake, a random allocation scheme is also considered. For each cyber-coupled power node A'_i, the value of the defense rate $\psi_i(t)$ is randomly assigned. It is noted that $\sum\limits_i \psi_i(t) = N_{A'_i}\Psi$.

5.4 Analysis of Failure Propagation

5.4.1 Indicative Time Points

In this subsection, we introduce four critical time points to permit detailed time series analysis. The aim of the time series analysis is to investigate the effect of the launch time determined by the attacker on the severity of the cascading failure in coupled systems. The Ukrainian blackout report has highlighted two important points [139, 140]. First, the attacker started shutting down the power grid by action of a malware which has intruded and diffused over then cyber network for a certain period of time. Second, the operator of the power system switched from automatic mode to manual mode of the control operation. This operation was executed to stop the spreading of failure in the power network caused by cyber coupling. In other words, the switching to the manual control isolates the infected cyber network from the power system. When the cyber network carrying malware is disconnected, the power network cannot be controlled by the attacker. Correspondingly, we define four critical time points to construct a failure propagation profile.

1. *Intrusion time (t_{init})* is the time when the malware begins to infect the cyber network.

2. *Attack launch time* or *launch time (t_{att})* is the time when the attacker launches the attack. Before $t = t_{\text{att}}$, the malware can diffuse to more cyber nodes and the attacker may obtain more information to effectively impair the power grid. It is noted that $t_{\text{att}} \geq t_{\text{int}}$ and t_{att} will serve as a variable for examining cascading failure in coupled systems.

3. *Isolation time (t_{iso})* is the time when the cyber network is isolated from the power system, making the power grid unaffected by the malware. Thus, $c_i(t)$ in equation (5.6) is equal to zero after $t = t_{\text{iso}}$. The value of t_{iso} is determined after

confirming that the failure is caused by cyber attacks. There are a number of approaches in the detection of cyber attacks [141, 142]. Here, we implement one feasible solution, and specifically, we assume that the cyber security scheme starts to determine whether an attack has been originated from the cyber network when the first failure of a power network occurs at $t = t_{\text{fail}}(m)$ where m indicates the number of failed power nodes. Here, according to SCADA-specific intrusion detection applied in power grids [143], if more cyber nodes are infected when the detection is initialized, the probability that the data containing abnormal activity can be captured is higher. Thus, it is appropriate to assume that the detection time is inversely proportional to the number of infected nodes in the cyber network at the time when an action of detection is taken. Here, the t_{iso} is given in the basic form of

$$t_{\text{iso}} = \frac{T_{\text{ISO}}}{P_{\text{ICN}}} \tag{5.14}$$

where T_{ISO} is a constant determined by the amount of resource available to the defender for detecting the intrusion and P_{ICN} is the percentage of the infected cyber nodes at the time when the first power node fails.

4. *End time (t_{end})* is the time at which the cascading failure ends. In practice the power system has its own protection scheme to stop cascading failure within a period of time. Moreover, if there is no protection scheme terminating a cascading failure, then the propagation failure should end at t_{end}, which is the time when there is no more power overloading either in nodes or links.

5.4.2 Study of Cascading Failure in Coupled Systems

Simulations of failure propagation in a coupled system can be performed according to flow chart as shown in Fig. 5.2, which comprises three main processes, namely, malware spreading on the cyber network, cascading failure in the cyber-coupled power

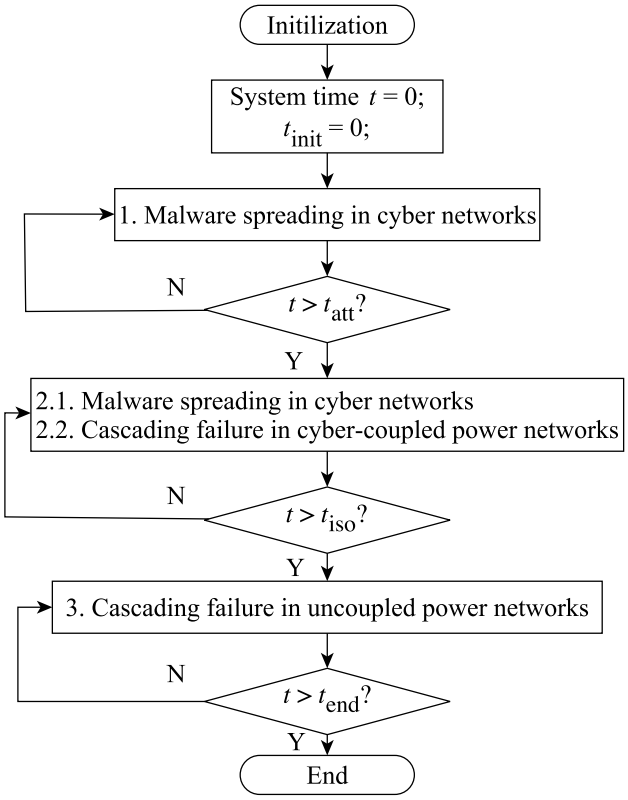


Figure 5.2: Flow chart of simulation of failure propagation in a coupled system.

system, and cascading failure in the uncoupled power grid (after isolation is effected).

As a preliminary study, in this subsection, we specifically examine the effect of launch time on the possible scenarios of cascading failure in the coupled system. We consider the coupled system comprising the UIUC-150 Bus power system [144] and a cyber system realized by a Gnutella peer-to-peer network containing 6301 nodes and 20777 edges [145]. We randomly select $q_A N_A$, where $q_A = 1$ power nodes to connect with the same number of cyber nodes in one-to-one connection style. In particular, we consider the entire power network being fully coupled with the cyber network. Furthermore, in the simulations, we set the current limits as $C_i = (1 + \alpha) \times I_i(\text{normal})$, where $I_i(\text{normal})$ is the total current flowing out of a power node under the normal load demand condition. In particular, the tolerance index α is set as 0.2, which implies that the capacity of each power node is 1.2 times larger than its load.

To launch the simulation study, the default parameter settings are set as follows:

1. The failure rate in power system a_i is 0.21 min^{-1} and the infection rate β_{ij} is one-tenth of a_i.

2. The attack and defense strengths are assumed to be the same, with the assumption that the attacker and defender have the same amount of resources to attack and defense one power node. Thus, the ratio between two strengths is one, i.e., $X/\Psi = 1$.

3. According to prior reports on malware analysis [146, 147], if a cyber network is fully infected within several tens of minutes, the malware can be detected and then the potential cascading failure originated from cyber attacks can be confirmed. Here, T_{ISO} is set as 10 min.

We observe three distinct phases in a full propagation process of cascading failure in the coupled system. Fig. 5.3 shows three propagation scenarios of the growth in the number of failure nodes in both power grids and cyber networks. In these three propagation scenarios, we plot the percentage of failed nodes in the cyber network and the power network against time. Note that the first malware injection starts at $t = 0$, i.e., $t_{\text{init}} = 0$. The three phases are described as follows,

1. *Phase I ($t_{\text{init}} \leq t < t_{\text{att}}$)*: In this phase, the malware is being spread in the cyber network and continues to obtain information of the power grid. At the same time the attacker gains access to more control assets. The growing dash line shown in Fig. 5.3(c) before $t < 100$ min shows the steadily rising percentage of infected cyber nodes. Note that there is no Phase I in Fig. 5.3(a) because $t_{\text{att}} = 0$.

2. *Phase II ($t_{\text{att}} \leq t < t_{\text{iso}}$)*: In this phase, the attacker begins to launch the attack on the power system through the invading malware. On the one hand, the malware continues to infect more cyber nodes. On the other hand, cascading failure of the cyber-coupled power system starts, and power nodes fail due to both cyber attack and power overloading. Thus, the solid curve shown in Fig. 5.3(b) between $t =$

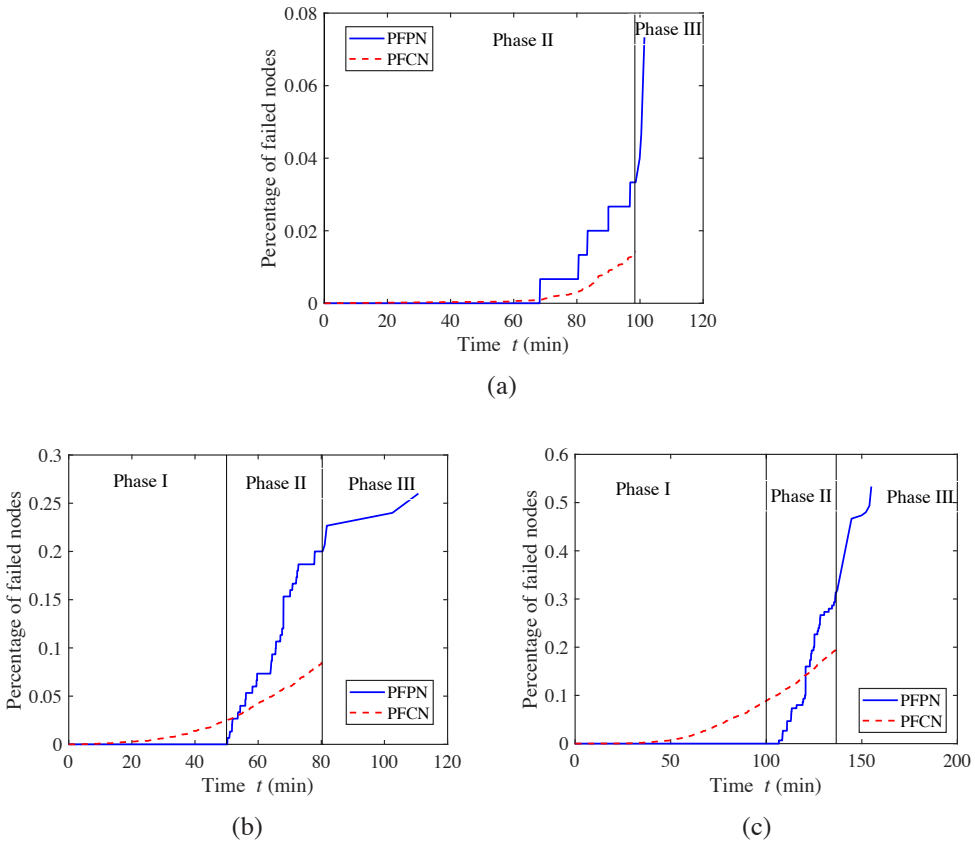


Figure 5.3: Failure propagation in coupled systems under the condition of random coupling with (a) $t_{\text{att}} = 0$; (b) $t_{\text{att}} = 50$ min; (c) $t_{\text{att}} = 100$ min.

50 and 80 min displays the rapid growth of failed power nodes. Moreover, a "staircase-like" pattern is apparent in this phase which can be interpreted as a combined feature of the typical step propagation profile triggered repeatedly by cyber attacks due to the network coupling. Moreover, the malware can only attack the power network in this phase. Thus, this phase can be regarded as *active attack phase*.

3. *Phase III* ($t_{\text{iso}} \leq t \leq t_{\text{end}}$): In this phase, since the cyber network is disconnected from the cyber network, cascading failure is caused only by overloading, corresponding to transition T_1. In particular, as shown in Figs. 5.3(b) and 5.3(c), the percentage of failed power nodes still increases, consistent with the previous study [101]. When no more overloading occurs in the power network, cascading

failure ends at t_{end}.

There are two key observations when different values of t_{att} are assigned. First, a larger t_{att} results in a shorter *active attack phase*. Second, significant destruction would be observed in the power system when a sufficiently large number of cyber nodes are infected by malware. Therefore, we observe over 50% of the power nodes have failed in the case where 10% of cyber nodes are infected at $t = t_{\text{att}}$ (Fig. 5.3(c)), whereas the power outage in other cases are far less significant when cyber infection is relatively smaller at $t = t_{\text{att}}$ (Figs. 5.3(a) and 5.3(b)).

By considering four proposed critical time points, the analysis of the failure propagation broadens the understanding of the cascading failure in cyber-coupled power systems in two respects: 1) the determination of the launch time has significant impact on the extent and rapidity of the cascading failure in coupled systems; and 2) the detailed failure propagation process induced by different failure mechanisms including cyber attacks and overload-triggered trippings show distinct failure propagation profiles. Note that these findings offer a complete picture of the cascading failure in cyber-coupled power systems. Moreover, compared with the work omitting the effect of the malware spreading process [73], our model here provides a practically consistent approach to assessing the robustness of cyber-coupled power systems.

In the next section, extensive simulations will be performed to probe into a few important observations related to cascading failure in coupled systems under different scenarios of attack-defense interaction.

5.5 Results

In this section, using the aforedescribed model, a large number of numerical experiments are carried out to capture full propagation profiles of cascading failure in the cyber-coupled power system. The main objective is to gain a comprehensive under-

standing of how different combinations of attack and defense strategies affect cascading failure of coupled systems. To fairly assess the extent and severity of cascading failure in the coupled system under cyber attack, we introduce a metric called *Average Failure Rate* (AFR), which is defined as

$$\mathrm{AFR}(t_{\min}, t_{\max}) = \frac{N_{\mathrm{FPN}}(t_{\max}) - N_{\mathrm{FPN}}(t_{\min})}{t_{\max} - t_{\min}} \tag{5.15}$$

where $N_{\mathrm{FPN}}(t_{\max})$ and $N_{\mathrm{FPN}}(t_{\min})$ are the numbers of failed power nodes at the start time $t_{\min}$ and the stop time $t_{\max}$, respectively. Our purpose is to reveal the propagation process of cascading failure. Clearly, the value of AFR depends on the choice of $t_{\min}$, assuming $t_{\max}$ is always the final time. If $t_{\min}$ is chosen as 0, the computed AFR is the average failure rate over the entire period beginning from the time of launching the cyber malware. Moreover, if $t_{\min}$ is taken as t_{att} (i.e., the time when cyber attack is launched on the power network), the computed AFR is actually the average failure rate of the power network itself. Therefore, $\mathrm{AFR}(0, t_{\max}) < \mathrm{AFR}(t_{\mathrm{att}}, t_{\max})$, and the appropriate use of AFR will provide useful information on the rapidity and severity of the cascading failure for the specific application in question.

It should be noted that $\mathrm{AFR}(t_{\min}, t_{\max})$ does not capture the transient of cascading failure in different phases. In fact, the main focus here is the full process of the cascading failure. Therefore, for a complete event of cascading failure, the start time of time window is set as $t_{\min} = 0$ and the stop time is the time when the cascading failure ends, namely, $t_{\max} = t_{\mathrm{end}}$, which varies among simulation runs. Note that in the sequel, the values of both $\mathrm{AFR}(0, t_{\mathrm{end}})$ and $\mathrm{AFR}(t_{\mathrm{att}}, t_{\mathrm{end}})$ are the average values of $\mathrm{AFR}(0, t_{\mathrm{end}})$ and $\mathrm{AFR}(t_{\mathrm{att}}, t_{\mathrm{end}})$ over all simulation runs.

5.5.1 Attack and Defense Interactions

When the attacker and the defender adopt different strategies, the cascading failure propagation can be quite different. To understand the influence of the attacker-defender

interaction, we organize a set of games in which the attacker and the defender take different attack and defense strategies. The full set of games contains $2^4 = 16$ single games. Specifically, in each single game, one scenario of the battle between the defender and attacker corresponds to one specific pair of defense and attack strategies. In addition, the attacker launches the attack from the cyber network to the power network at varying t_{att} (with t_{att} being sampled from 0 to 2000 min). For each sampled t_{att}, the cascading failure of the coupled system is simulated, and then the values of AFR$(0, t_{\text{end}})$ and AFR$(t_{\text{att}}, t_{\text{end}})$ are calculated.

Each of Figs. 5.4 and 5.5 presents 16 interaction game scenarios. Figs. 5.4(a) and 5.4(e) show, respectively, AFR$(0, t_{\text{end}})$ and AFR$(t_{\text{att}}, t_{\text{end}})$ for 4 game scenarios corresponding to Attack Strategy I versus the 4 different defense strategies. Likewise, other figures show either AFR$(0, t_{\text{end}})$ or AFR$(t_{\text{att}}, t_{\text{end}})$ for 4 game scenarios corresponding a given attack strategy versus the 4 different defense strategies. Two findings can be concluded from Fig. 5.4:

- There is an optimal selection of t_{att} that gives the most effective attack on the power network. Thus, it is not true that a larger t_{att} would favor the attacker and make the cascading failure more severe, despite more information of the power network can be obtained with a larger t_{att}. The reason for this is that the duration of the *active attack phase* (defined in Section 5.4.2) will be limited if the attack is launched too late, thus allowing the action of isolating the power network from the cyber network be taken to save the power network. In this respect, our model is in full agreement with the events occurred in the Ukrainian power outage.

- From each set of game scenarios, when the attacker adopts one strategy (except random strategy), the best defense strategy is always the same corresponding strategy, in terms of the metric AFR. For instance, from Fig. 5.4(a), when Attack Strategy I is adopted, the most effective defense strategy is Defense Strategy I. This scenario of having the defender implement the same strategy as the

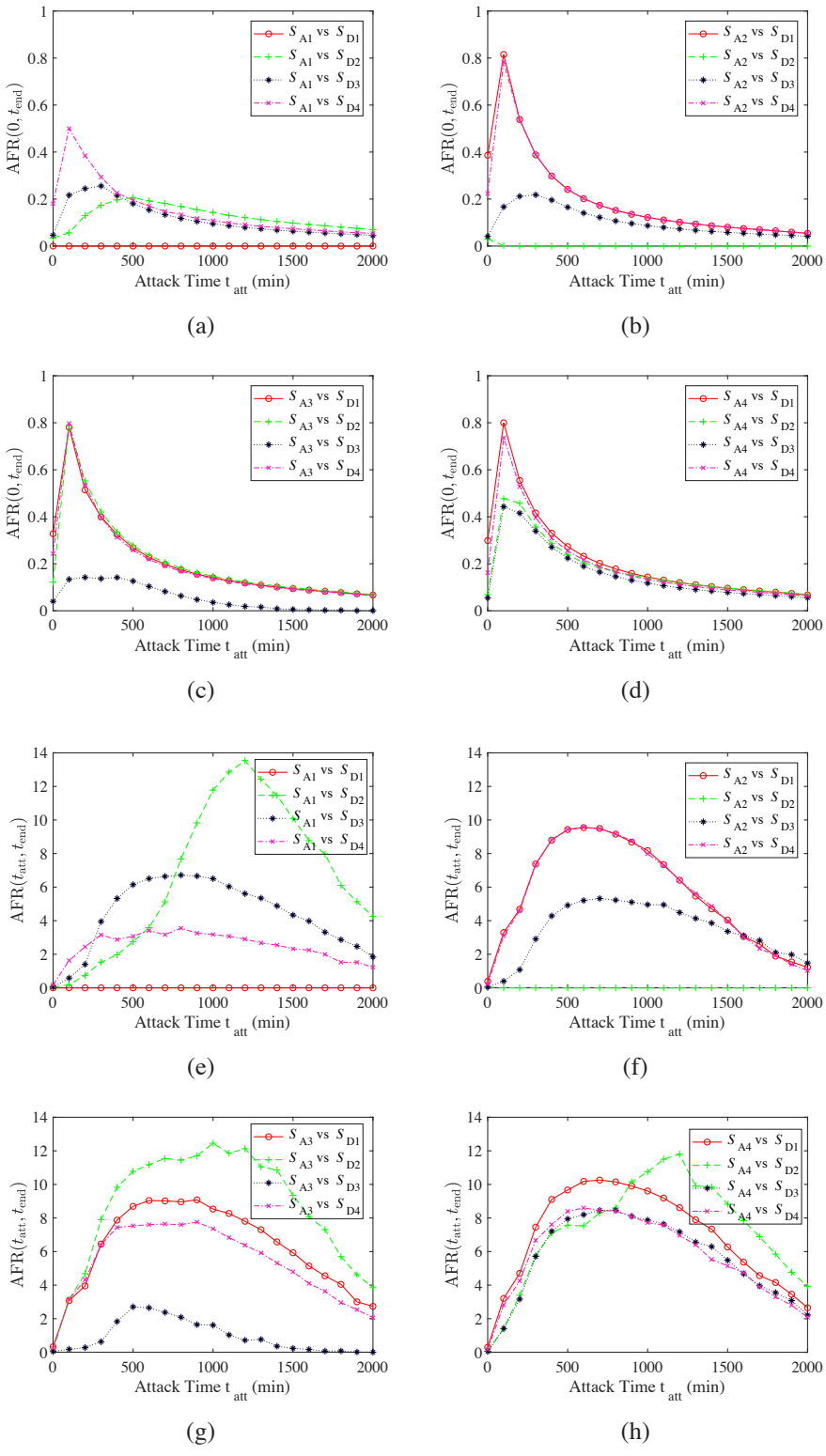


Figure 5.4: Comparison of attack-defense interaction for two Average Failure Rates, i.e., AFR$(0, t_{\text{end}})$ and AFR$(t_{\text{att}}, t_{\text{end}})$. (a) & (e) Attack strategy I versus defense strategy I, II, III or IV, (b) & (f) attack strategy II versus defense strategy I, II, III or IV, (c) & (g) attack strategy III versus defense strategy I, II, III or IV, (d) & (h) attack strategy IV versus defense strategy I, II, III or IV. All graphs plot the mean value of AFR over 500 simulation runs.

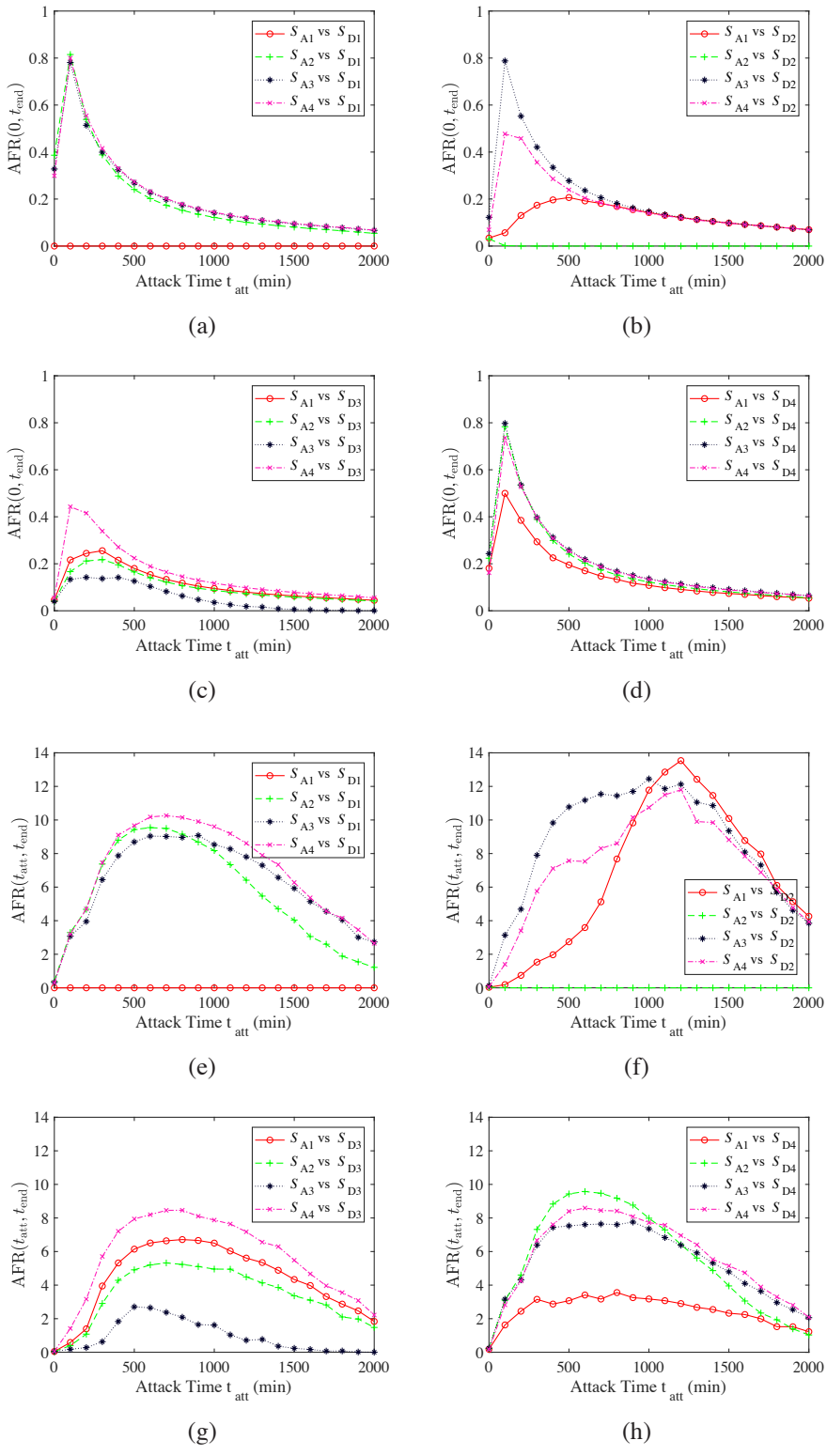


Figure 5.5: Comparison of attack-defense interaction for two Average Failure Rates, i.e., AFR$(0, t_{\text{end}})$ and AFR$(t_{\text{att}}, t_{\text{end}})$. (a) & (e) Attack strategy I, II III or IV versus defense strategy I, (b) & (f) attack strategy I, II III or IV versus defense strategy II, (c) & (g) attack strategy I, II, III or IV versus defense strategy III, (d) & (h) attack strategy I, II, III or IV versus defense strategy IV. All graphs plot the mean value of AFR over 500 simulation runs.

attacker is a typical example of "tit-for-tat", which is found to be the most effective defense strategy, as witnessed in Figs. 5.4(a), 5.4(b), 5.4(c), 5.4(e), 5.4(f) and 5.4(h). However, when a random attack strategy is adopted, as shown in Figs. 5.4(d) and 5.4(h), the tit-for-tat strategy does not show any obvious advantage because a random distribution of defense strength on the power network is surely not the same as another random distribution of attack strength on the power network.

Fig. 5.5 shows another set of 16 interaction game scenarios with defender strategy being the preset condition. Specifically, each figure corresponds to one of the four different attack strategies versus one given defense strategy. Here, the tit-for-tat strategy does not result in the most effective attack, while Attack Strategy III appears to be universally effective.

From the results presented in Figs. 5.4 and 5.5, we see that although AFR$(0, t_{\text{end}})$ and AFR$(t_{\text{att}}, t_{\text{end}})$ are not identical, they consistently display similar characteristics and give the same qualitative conclusion regarding the attack-defense interactions.

5.5.2 Preferred Strategies

To quantitatively evaluate the effectiveness of different attack and defense strategies, we attempt to find the *preferred* strategy in each set of game scenarios. In particular, the *preferred* defense strategy refers to the one that gives the smallest value of AFR$(0, t_{\text{end}})$, whereas the *preferred* attack strategy is the one that causes the most severe power outage corresponding to the largest value of AFR$(0, t_{\text{end}})$. In addition, we perform a large number of simulations for each scenario and examine the distribution of AFR$(0, t_{\text{end}})$.

Figs. 5.6(a) and 5.6(b) show the distributions of the preferred strategies from attacker's and defender's perspective, respectively. In this chapter, we rank the preference under varying t_{att}. For instance, for all simulations corresponding to one at-

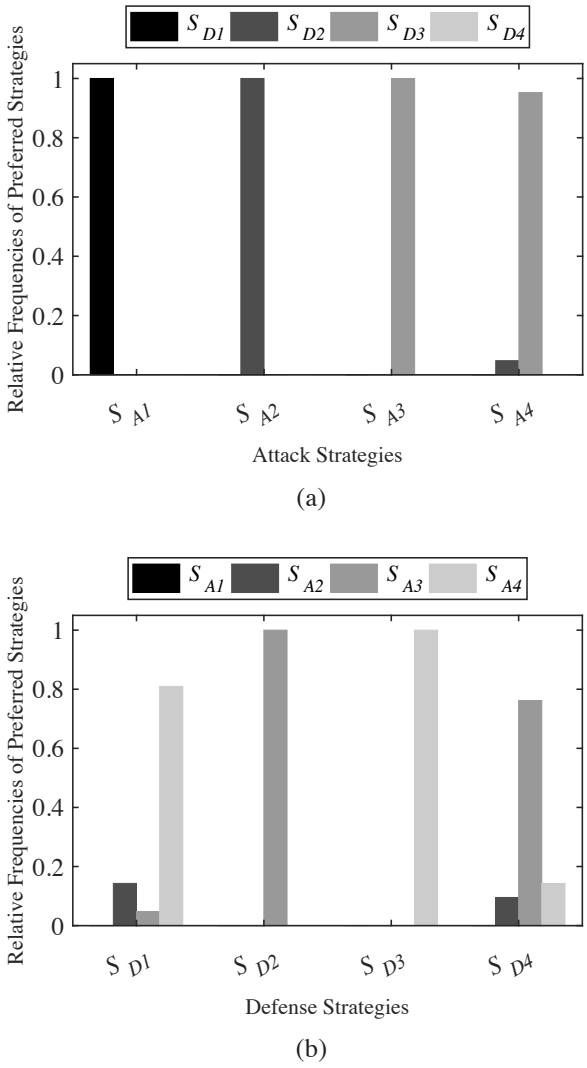


Figure 5.6: Distribution of (a) *preferred* defense strategies from defender's perspective showing the "tit-for-tat" strategy being a preferred defense strategy; (b) *preferred* attack strategies from attacker's perspective showing different interactions of strategies.

tack strategy, we count the number of each defense strategy that gives the smallest $\mathrm{AFR}(0, t_{\mathrm{end}})$ for the same t_{att} (being a preferred strategy). The distribution can thus be plotted. The tallest bar in each game shown in Fig. 5.6 means that the particular strategy has the highest probability of being the preferred strategy. It is noted that the sampled attack time t_{att} is given in the range from 0 to 2000 min. For a larger attack time, the difference of the effectiveness of varied attack and defense strategies become less significant.

In Fig. 5.6(a), for each attack strategy adopted, almost all preferred defense strategies follow the tit-for-tat rule. Thus, from the defender's viewpoint, the preferred strategy is to apply the same strategy as the attacker. However, from the attacker's point of view, the distributions shown in Fig. 5.6(b) suggest that regardless of the defense strategy used, Attack Strategy III is preferred. Although it has been found that Attack Strategy IV is preferred in some cases, it is impractical for attackers to implement a random allocation scheme.

Our findings initially highlight the superiority of defending the cyber-coupled power nodes with large capacity (load) to enhance the robustness of the cyber-coupled power system. In other words, preventing the power nodes with large capacity from being tripped can effectively alleviate overloading stress induced by power flow redistribution during the cascading failure propagation. Furthermore, these findings are not obtainable without due consideration of the physical power flow process in network-based models.

It should now be apparent that the incorporation of the physical power flow process in the model is vital to the study of cascading failure in power systems. The above finding of Attack Strategy III being the preferred attack strategy reflects the importance of taking power capacity into consideration. Thus, network-based models which only consider topology and assume an unrealistic power flow process will not give practically relevant findings. This is precisely the key merit of our present study.

5.5.3 Effects of Coupling Patterns

The way in which the power and cyber networks are coupled plays an important role in determining the relative merits of different attack and defense strategies in suppressing or aggravating cascading failure. In this study, we build coupled networks with various coupling patterns. In particular, we focus on the following 6 common coupling patterns: Assortative Coupling (ACP), Dissortative (DCP), High Cyber Node Degree

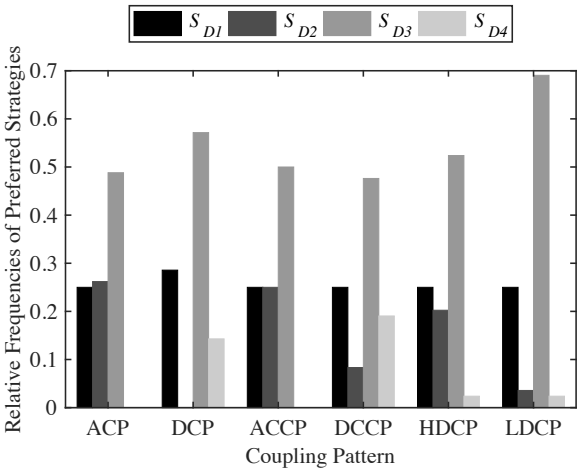
Coupling (HDCP), Low Cyber Node Degree Coupling (LDCP), Assortative Capacity Coupling (ACCP) and Dissortative Capacity Coupling (DCCP). Moreover, we also take 10 Random Coupling Patterns (RCP) for comparison purposes.

In constructing the coupled networks, we first sort the nodes in the cyber network according to the node degree, and sort the power nodes according to degree or power capacity, as appropriate. For ACP, DCP, ACCP and DCCP, we select N_A cyber nodes from the entire cyber network, which have a scale-free degree distribution, i.e., very few high-degree cyber nodes and more low-degree cyber nodes. For HDCP (and LDCP), we select N_A cyber nodes with high (and low) degree to connect to the power network. Moreover, we sort the power nodes with the capacity of the nodes when implementing ACCP and DCCP. For RCP, cyber nodes are randomly connected to the power nodes. Also, one-to-one coupling is adopted.

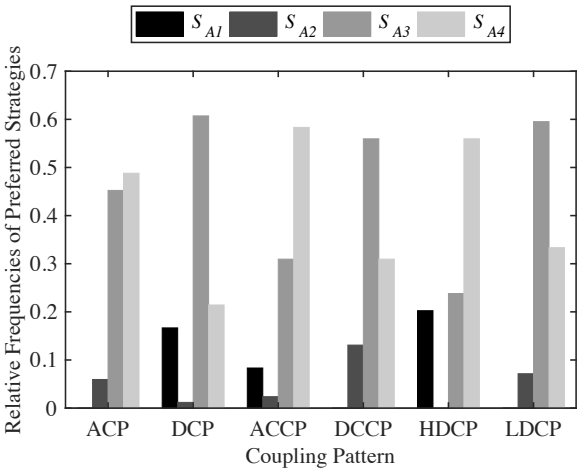
Figs. 5.7(a) and 5.7(b) show the distributions of preferred strategies from defender's and attacker's perspective, respectively, for the 6 coupling patterns. For the 10 Random Coupling Patterns, the distributions of preferred strategies from defender's and attacker's perspective are shown in Figs. 5.7(c) and 5.7(d). For each coupled network, we count the number of times each of four strategies is ranked as the most preferred strategy in a set of games. We are particularly interested in the effectiveness of the defense strategies in resisting varied attack strategies under various coupling methods.

It has been found that from the defender's viewpoint, Defense Strategy III is the most preferred defense strategy among all strategies under study and for all 16 coupled networks. Moreover, from the attacker's viewpoint, Attack Strategy III takes a superior position in the coupling cases of DCP, DCCP, LDCP and all studied RCPs, and is still a preferred strategy to cause fast and large-scale cascading failure for the coupling cases of ACP, ACCP and HDCP, irrespective of the defense strategy used by the defender. For RCP, cyber nodes are randomly connected to the power nodes by random in a one-to-one fashion.

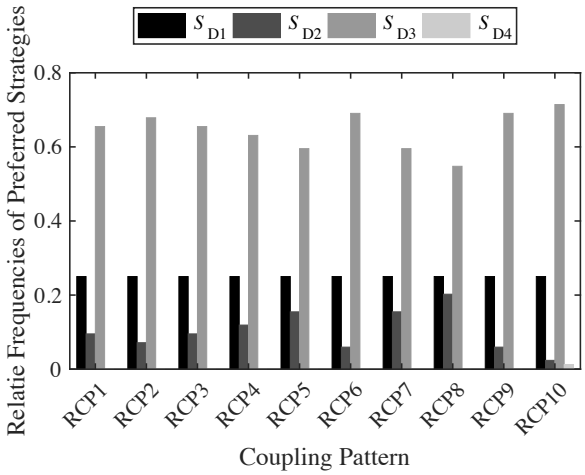
Again, our model, having taken into consideration of the physical power flow pro-


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
ACP DCP ACCP DCCP HDCP LDCP
Coupling Pattern

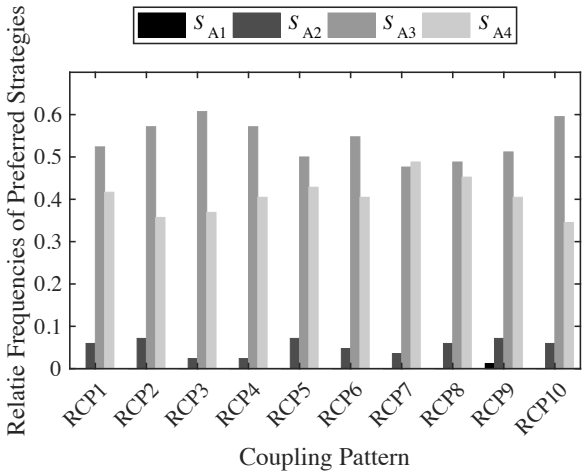
(a)


S_{A1} S_{A2} S_{A3} S_{A4}
Relative Frequencies of Preferred Strategies
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
ACP DCP ACCP DCCP HDCP LDCP
Coupling Pattern

(b)



(c)



(d)

Figure 5.7: Distribution of (a) *preferred* strategies from defender's perspective; and (b) *preferred* strategies from attacker's perspective, for various coupling patterns. ACP: assortative coupling, DCP: dissortative coupling, HDCP: high cyber node degree coupling, LDCP: low cyber node degree coupling, ACCP: assortative capacity coupling, DCCP: dissortative capacity couplingm, RCP: random coupling pattern.

cess, is able to assess the capacity-based attack strategy, as explained earlier. Moreover, our experiments with different coupled systems constructed by considering various coupling patterns provide more empirical evidences of the superior performance of Attack or Defense Strategy III either from the attacker or defender's perspective.

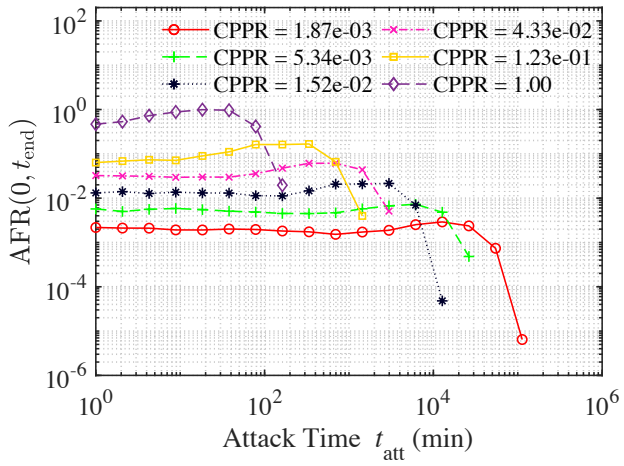
5.5.4 Effects of Propagation Rate Disparity in Cyber and Power Networks

From the foregoing results, we see that there exists an optimal t_{att} that results in the most severe outage, as shown in Figs. 5.4 and 5.5. Obviously, this choice of t_{att} is affected by the rate at which malware spreads on the cyber network relative to the rate of failure propagation on the power network.

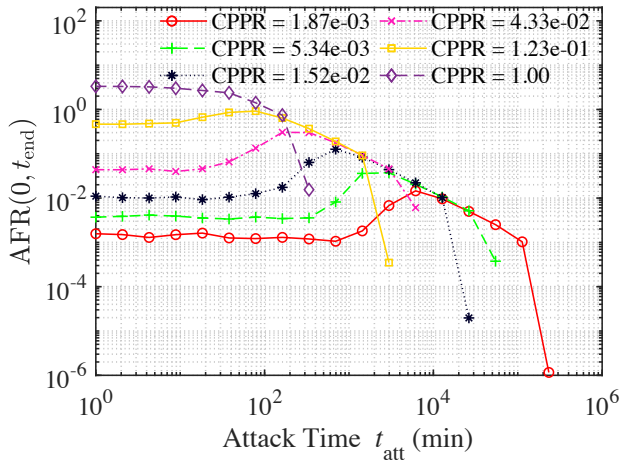
In the cyber-coupled power system, two distinct propagation mechanisms, namely, one for malware spreading and one for failure propagation on the power network, can be identified. These spreading and propagation rates are used to calculate the probabilities for the specific stochastic state transitions. Specifically, the infection rate of cyber node i from infected node j is β_{ij}, and the tripping rate of power node i is a_i. To investigate the effects contributed by these two rates on the cascading failure in a cyber-coupled power system, we use the *cyber-physical propagation ratio* (CPPR), which is defined, for homogeneous networks, as

$$\text{CPPR} = \frac{\beta_{\text{global}}}{a_{\text{global}}} \tag{5.16}$$

where β_{global} is the value of β_{ij} of all cyber nodes, and a_{global} is equal to a_i of all power nodes, assuming homogeneity of the power network. Varying the value of CPPR results in different profiles of cascading failure propagation in the coupled power system. Also, the type of cyber attack and the spreading rate of cyber malware affect the dependence of cascading failure profile on cyber coupling. Fig. 5.8 offers a broad view of the



(a)



(b)

Figure 5.8: Effect of cyber-physical propagation ratio (CPPR) on the dependence of average failure rate (AFR) upon attack time t_{att} when (a) Attack Strategy III and Defense Strategy III are adopted; and (b) Attack Strategy IV and Defense Strategy IV are adopted. All graphs plot the mean value of AFR over 500 simulation runs.

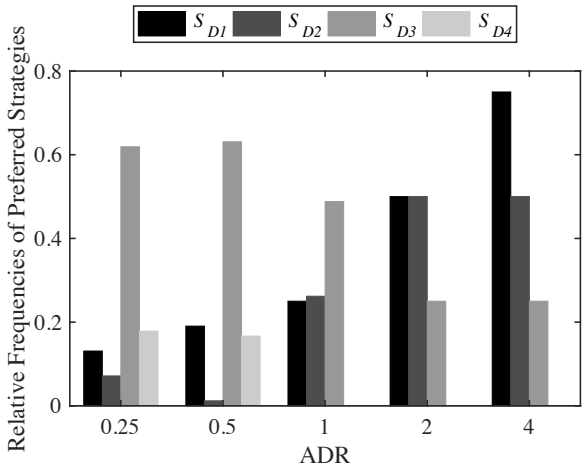
trend of AFR$(0, t_{\text{end}})$ as t_{att} varies, for two sets of attack and defense strategies. It is observed that the value of AFR$(0, t_{\text{end}})$ rises gradually as t_{att} increases, and after reaching a peak value, falls rapidly with increasing t_{att}. Moreover, the peak value of AFR$(0, t_{\text{end}})$ indicates the most severe cascading failure, which corresponds to the optimal t_{att} mentioned earlier. It is also found that a higher CPPR gives a smaller optimal t_{att}, i.e., an earlier attack time will give rise to more severe cascading failure for a higher CPPR. In particular, a higher CPPR implies that malware spreads faster in cyber networks so that attackers can obtain more effective network information within a shorter period of time. Thus, the attack time becomes shorter under the condition of a higher CPPR.

5.5.5 Effects of Relative Strengths of Attack and Defense

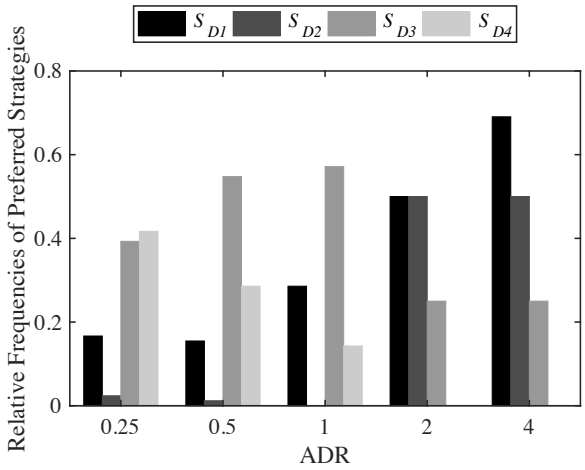
Results in the foregoing sections are obtained under the assumption that the magnitudes of attack and defense strength, X and Ψ, are identical. In order to study the effects of varied strengths of attack and defense, we introduce a parameter *attack-to-defense strength ratio* (ADR), which is given by

$$\text{ADR} = \frac{\Psi}{X} \tag{5.17}$$

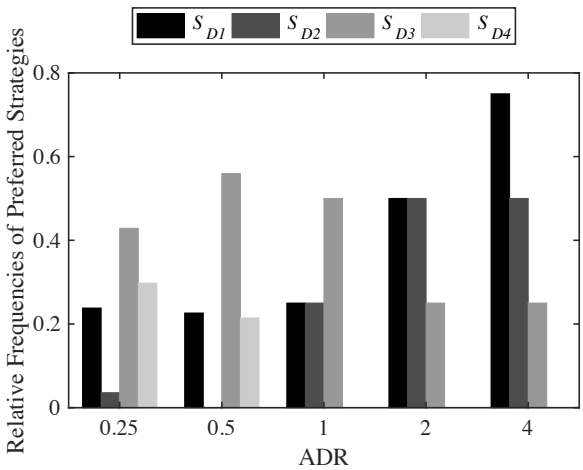
Fig. 5.9 presents the distributions of preferred strategies from defender's perspective for the 6 dedicated coupling patterns and 3 random coupling patterns described earlier, with ADR varied from 0.25 to 4. It is found that as ADR increases, the most preferred defense strategy has shifted from Strategy III to Strategy I. In particular, when the defense resource is limited, adopting Defense Strategy III (i.e., distributing the defense strengths according to the capacity of power nodes) achieves the greatest protection of the coupled system from cascading failure, irrespective of the attacker strategy or coupling pattern. However, when the defense resource is abundant for securing the the entire power grid, adopting Defense Strategy I (i.e., evenly distributing the defense strengths over the power network) can effectively resist attacks. This is


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0.8
0.6
0.4
0.2
0
0.25
0.5
1
2
4
ADR

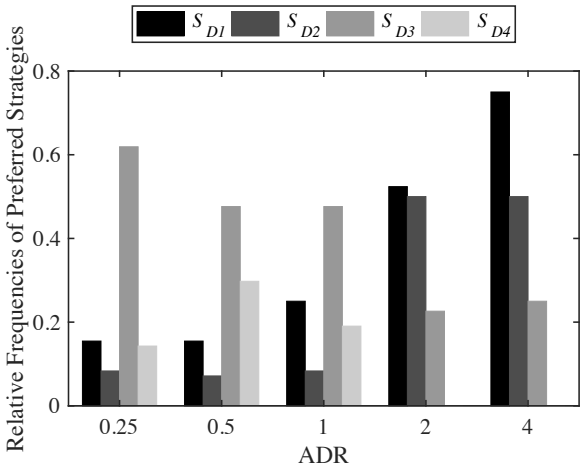
(a)


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0.8
0.6
0.4
0.2
0
0.25
0.5
1
2
4
ADR

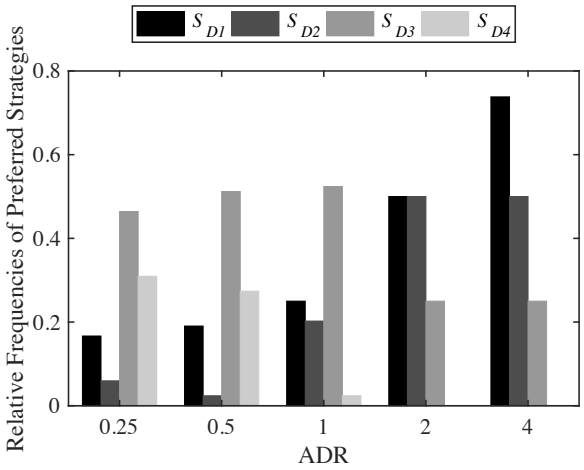
(b)


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0.8
0.6
0.4
0.2
0
0.25
0.5
1
2
4
ADR

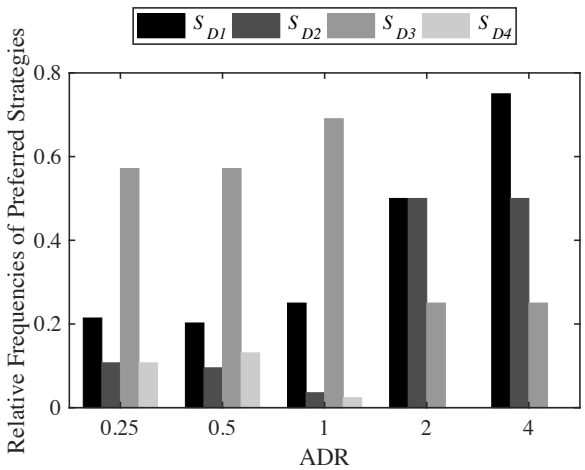
(c)


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0
0.2
0.4
0.6
0.8
0.25
0.5
1
2
4
ADR

(d)


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0
0.2
0.4
0.6
0.8
0.25
0.5
1
2
4
ADR

(e)


S_{D1} S_{D2} S_{D3} S_{D4}
Relative Frequencies of Preferred Strategies
0
0.2
0.4
0.6
0.8
0.25
0.5
1
2
4
ADR

(f)

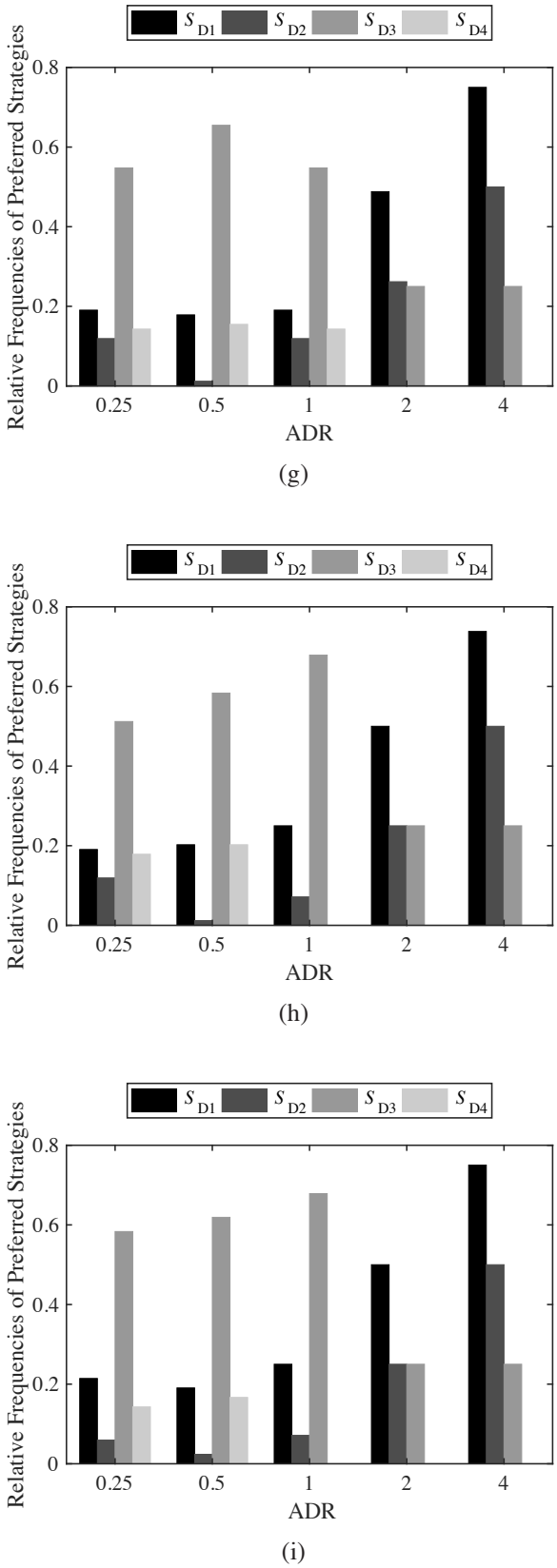


Figure 5.9: Distributions of preferred defense strategies for different coupling patterns. (a) ACP, (b) DCP, (c) ACCP, (d) DCCP, (e) HDCP, (e) LDCP, (f) RCP1, (g) RCP2 and (h) RCP3, with attack-to-defense strength ratio (ADR) varied from 0.25 to 4.

because when defense resource is abundant, consideration of prioritization of power components to be protected becomes unnecessary or non-critical. In this chapter we emphasize the incorporation of an appropriate modeling of the coupling process that is essential to capturing the interdependence of the physical and cyber networks.

5.6 Summary

Modern smart grids are critical infrastructure requiring high level of security to prevent attacks and failures that would cause severe power blackout. It is thus important that models for studying failure of power networks provide realistic description of the essential processes that govern the propagation of failure events on the power grid. The key features of the developed network-based method include: (i) the incorporation of the physical power flow process in studying cascading failure in power grids, (ii) the interpretation of the interdependence between attack and defense of power components in a cyber-coupled power network, and (iii) the effect of malware spreading in the cyber network on the extent of cascading failure in power grids. Moreover, in our study, an attacker and defender perspective has been taken to examine the cyber-coupled power network under different coupling patterns. Besides, key relevant parameters must be appropriately defined and their effects on the cascading failure profiles be revealed. Our study has pinpointed the preferred defense strategies for protecting a cyber-coupled power network, and highlighted the factors affecting the propagation profiles of cascading failure of power networks. Much enhanced understanding of the key parameters and their roles in controlling failure propagation have been gained in this study through the attack-defense interaction viewpoint and the incorporation of essential physical processes in the model for analysis and possible prediction. It is expected that future study along this direction will result in comprehensive understanding of cascading failure in large-scale cyber-coupled physical systems, and hence offer effective protection strategies to minimize the severity of failure propagation in

vital cyber-coupled infrastructures.

Chapter 6

Effects of Coupling Patterns on Robustnesss of Cyber-Coupled Power Systems

In the previous chapter, to study the cascading failure in cyber-coupled power systems, we have developed a network-based model incorporating the physical power flow process and the interaction between attack and defense on the components in the power network is considered. In this chapter, we introduce a parameter, called *relative coupling correlation coefficient*, to quantify the coupling pattern of a cyber-coupled power system. We model the coupled system as a coupled network consisting of a power network and a cyber network. Coupling patterns, which are determined by some node criticality metrics, reveal how power nodes and cyber nodes are connected. To understand the effect of coupling patterns on the robustness of coupled systems, we classify coupling patterns according to two node criticality metrics of the cyber network, i.e., node degree and node betweenness, and two node criticality metrics of the power network, i.e., node degree and node capability. Simulation results show that a coupled system of lower relative coupling correlation coefficient has better robustness. Moreover, when optimizing the coupling pattern for robustness improvement, the adoption

of node capability and node degree as node criticality metrics for power and cyber networks, respectively, would result in a much more robust network compared to the adoption of other node criticality metrics. The finding offers a practical comprehension of the effect of coupling patterns on robustness of cyber-coupled power systems with the adoption of network approaches incorporated with the physical power flow process.

6.1 Introduction

Cyber Physical Systems (CPS), comprising intelligent cyber facilities and functional physical systems, have emerged as a crucial and challenging research theme requiring cross-disciplinary efforts. The integration of smart devices like sensors and intelligent computational algorithms supports traditional physical systems with significant upgrade of adaptability, autonomy and efficiency [148]. Smart Grids, which are specific implementations of CPS, consist of power apparatus such as generators, transformers and transmission lines, connected with cyber parts like phasor measurement units (PMU), wide area measurement systems and advanced metering infrastructures (AMI) [21]. The use of cyber system facilities offers efficient monitoring and control of power systems, but at the same time arouses security concerns.

Cyber security is of growing concern as smart grids are rapidly developing. The coupling with a cyber system creates loopholes that permit access by attackers who aim to disrupt the power system [20]. In the Ukrainian Blackout event that occurred in December 2015 [139], a computer malware (called BlackEnergy) had penetrated to the computer networks that were connected to the power grid. Through infecting more computers and gaining unauthorized access, the hackers launched their attack by disconnecting circuit breakers in the power substations, resulting in an eight-hour long power outage.

The robustness of power systems coupled with cyber systems has been extensively

studied. Using a complex network approach, a cyber-coupled power system [149] is composed of a cyber network and a power network. The former consists of interconnected cyber nodes, and the latter contains power substations connected by transmission lines. Buldyrev *et al*. [17] initially modeled cascading failure in a power network coupled with an Internet network from the perspective of interdependent networks. Since then, there have been an increasing number of studies devoted to examining the effect of various topological and coupling characteristics on the robustness of interdependent networks [150], including the inter-edge effects [36], the inter-similarity features [33], optimization of interconnectivity [38] and effects of coupling strengths [32].

It should be noted that much of the prior work adopted percolation theory to model failure spreading in interdependent networks, which omits the underlying physical processes. Without considering physical processes, the conclusions drawn from these studies may not provide practically relevant suggestions to enhance the robustness of a cyber-coupled power system. To overcome the limitation of the network-based models developed by network scientists, numerous studies were devoted to assessing the robustness of cyber-coupled power systems by taking into consideration the physical processes of power systems. Cai *et al*. [73] developed a model to analyze the failure propagation in a power system connected with a dispatching data network. By considering the interdependence between two interacting networks, the power system has been shown to become more vulnerable when coupled with a double-star network. Moreover, it has been shown [151] that cyber coupling has significantly effects on the cascading failure of cyber-coupled power systems and demonstrated that cyber coupling could intensify both the extent and rapidity of power outages.

The main advantage of applying a complex network approach to accessing the robustness of cyber-coupled power systems is the convenient extraction of network-based features that affect robustness. Inter-similarity is one of the key areas investigated in Parshani *et al*.'s work [32]. Through evaluating two measures, namely, inter degree-degree correlation (IDDC) and inter-clustering coefficient (ICC), it can be concluded

that more inter-similar networks would significantly lower the vulnerability of systems to random failure. Moreover, Tan *et al*. [152] proposed three kinds of coupling methodologies based on the heterogeneity of load in the two individual networks including assortative coupling, dissortative coupling and random coupling. It has been pointed out that the assortative coupling can make interconnected networks, such as interconnected communication networks, more robust to traffic congestion. Specifically, assortative coupling corresponds to the coupling pattern realized by two steps. Step 1 sorts nodes in the two interconnected networks in descending order of load, and step 2 connects the nodes of the two networks following the sorted order. In other words, the assortative coupling exhibits the highest level of inter-similarity measured using Parshani *et al*.'s method [32].

Previous studies have shown that coupling patterns play a crucial role in determining the robustness of coupled systems. The coupling pattern defines the way a node or link pair is connected between two individual networks based on the sorting of node or link metrics. However, few studies have focused on the systematic exploration of coupling patterns for lowering the vulnerability of coupled systems. It is known that various kinds of coupling patterns can be realized by adopting different network-based metrics as the node or link criticality measurement in the individual networks. For instance, Parshani *et al*.'s work chose node degree as the node criticality metric and introduced an inter degree-degree correlation (IDDC) for evaluating the robustness of the port-airport coupled system [32]. In a power network, it has also been found that power capacity can be used to measure the criticality of a power component [153].

In this chapter, we introduce a *relative coupling correlation coefficient* ρ to quantify coupling patterns and to investigate the effect of parameter ρ on the robustness of coupled systems. In particular, we propose four classes of coupling patterns with the consideration of two cyber node criticality metrics, i.e., node degree and node betweenness, and two power node criticality metrics, i.e., node degree, and node capacity. The cascading failure in a cyber-coupled power system can be simulated by taking a

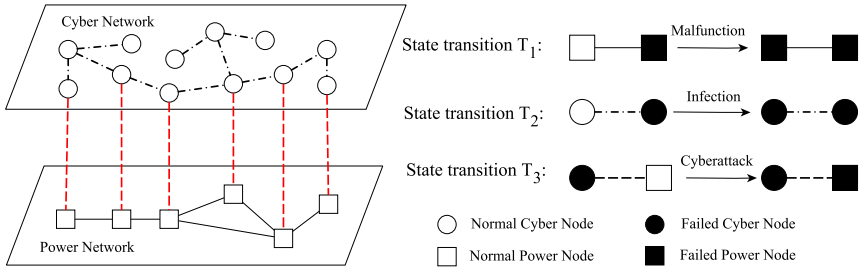


Figure 6.1: A coupled network consisting of a cyber network and a power network, with state transitions showing infection of a cyber node, malfunction (overload tripping) of a power node and attack to a power node from a cyber node.

network approach with combination of the physical process, The simulation results show that a high coefficient ρ always indicates a higher vulnerability of the coupled system. Moreover, the vulnerability of the coupled system can be lowered by adopting node capability and node degree as the node criticality metrics for power and cyber networks, respectively, rather than considering other node criticality metrics. In particular, such reduction of vulnerability is more significant when the relative coupling correlation coefficient ρ is relatively small.

6.2 Modeling Cascading Failure in Cyber-coupled Power Systems

A cyber-coupled power system consists of a power network and a cyber network, as shown in Fig. 6.1. The power network, denoted as network *A* and shown as the bottom layer in Fig. 6.1, comprises a set of nodes (white squares) representing power substantiations and a set of links (solid lines) representing power transmission lines. A cyber network, denoted as network *B* in the upper layer, is composed of nodes (white circles) representing the cyber components, and links (dot-dash lines) representing the connections among cyber components. Moreover, the nodes in the power network and cyber network are also connected and their connection are shown by the vertical dash lines. In practice, a cyber node can assess and control a power node when they are

connected. In this chapter, the one-to-one connection style between power and cyber nodes is considered and each pair of coupled nodes are a "node pair" in the coupled network. Also, the scale of the cyber network is much larger than that of the power network, namely, the number of nodes in the cyber network is much larger than that in the power network. Thus, some nodes in the cyber network are selected to construct node pairs in the coupled network.

In this chapter, we take the cascading failure in the coupled system as a sequence of state transitions of node pairs. In particular, the cascading failure of the coupled system is initialized by a malware attack from the cyber network to the power network. Three kinds of state transition are depicted in Fig. 6.1, including the malfunction of a power component, the infection process of cyber malware and the effect of cyber attack on a power node.

Two main reasons for a power component to fail are considered in this model. First, a power component fails when it is in a subnetwork where there is no power generator. Second, a power component is prone to failure when it carries load that exceeds its capacity, and the probability of failure is given in the following state transition T_1:

$$T_1 : P[s_{A_i}(t+dt) = 1 \mid s_{A_i}(t) = 0] = \lambda_i(t)dt \tag{6.1}$$

where $\lambda_i(t)$ is the tripping rate which is given by $\lambda_i(t) = a_i(L_i(t)/C(i) - 1)$ if the loading $L_i(t)$ is larger than the capacity $C_i(t)$ in the power component i, and is 0 otherwise. Moreover, the loading $L_i(t)$ is obtained from the DC power flow calculation model given in Section 3.1.1.3.

The malware diffusion in the cyber network is modeled by a stochastic process. In particular, a cyber node may be infected when its neighbor is infected, as described by state transition T_2:

$$T_2 : P[s_{B_i}(t+dt) = 1 \mid s_{B_i}(t) = 0] = \mu_i(t)dt. \tag{6.2}$$

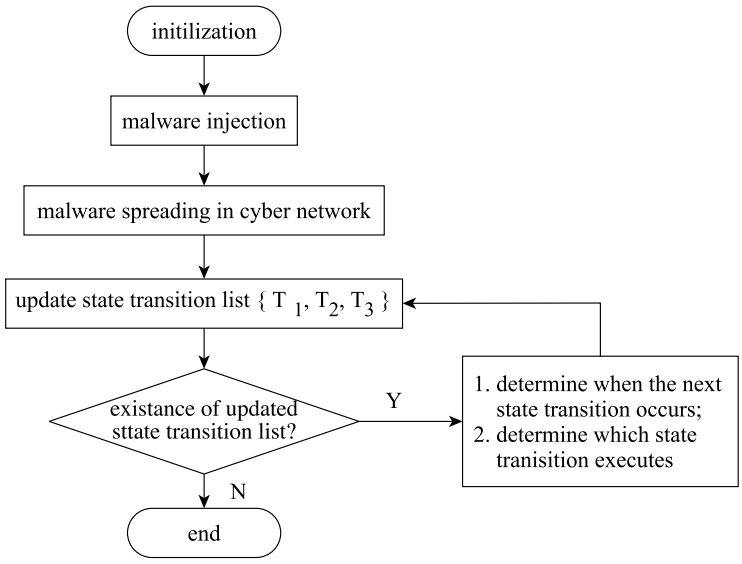


Figure 6.2: Flow chart of simulation of failure propagation in the coupled system.

where $\mu_i(t)$ is the infection rate on the cyber network which is given by $\mu_i(t) = \sum_{j\in\Omega_{Bi}} \beta_{ij}$. Specifically, Ω_{Bi} is the set of all infected neighbors of cyber node i and β_{ij} is the rate at which the infected cyber node j infects its neighbor node i.

For the failure of a power node due to cyber attack, we augment the above failure probability by adding a fixed term. Specifically, when a power node is attacked by cyber malware, the probability of the power node being removed from the power network increases by a value $c_i(t)$ which corresponds to the attack strength. Moreover, if the effect of defense (protection) is considered, the probability of removing a power node due to its failure is reduced by a value $d_i(t)$. Thus, the state transition T_3 for failure due to cyber attack is given by

$$T_3 : P[s_{A_i}(t+dt) = 1 \mid s_{A_i}(t) = 0] = (\lambda_i(t) + c_i(t) - d_i(t))dt. \tag{6.3}$$

In this study, both $c_i(t)$ and $d_i(t)$ are constants and we assume that the attack strength is larger than the defense strength, i.e., $c_i(t) > d_i(t)$.

The cascading failure in a coupled system is simulated according to the flow chart shown in Fig. 6.2. After the initialization step, the process begins from a malware

injection, which then spreads in the cyber network. In this stage, only state transition T_2 is executed. Once a cyber attack is launched, one of the three state transitions T_1, T_2 or T_3 is selected to be executed through determining (1) the instant when the next state transition occurs; and (2) the particular state transition to be executed in the current iteration. These two decisions are made by the stochastic method developed in a previous study [151]. It is noted that after each iteration, the states of all nodes will be updated, and the iteration continues until there is no further state transition. Moreover, if all the power elements have failed, the program stops.

6.3 Relative Coupling Correlation Coefficient

A problem with assessing the robustness of coupled networks is associated with the determination of the coupling pattern. In particular, it has been found that higher inter-similarity increases the robustness of the coupled network. One of the inter-similarity metrics is the *inter degree-degree correlation* [33], which is a form of associative mixing coefficient, can be written as

$$r = \frac{M^{-1}\sum_i j_i k_i - [M^{-1}\sum_i \frac{1}{2}(j_i + k_i)]^2}{M^{-1}\sum_i \frac{1}{2}(j_i^2 + k_i^2) - [M^{-1}\sum_i \frac{1}{2}(j_i + k_i)]^2} \tag{6.4}$$

where j_i and k_i are the degrees of the nodes in two individual networks at the end of the ith interdependent link, with $i = 1, 2, ..., M$. Moreover, if networks A and B have the same degree distribution, r is in the range from –1 to 1. Also, the largest value of r corresponds to an associative coupling pattern, i.e., the highest-degree node in A is connected to the the highest-degree node in B, the second highest-degree node in A is connected to the second highest-degree node in B, and so on. On the other hand, the smallest value of r corresponds to a disassortative coupling pattern, i.e., the highest-degree node in A is connected to the the lowest-degree node in B, the second highest-degree node in A is connected to the second lowest-degree node in B, and so

forth.

In a cyber-coupled power system, apart from using node degrees, we consider a few other network-based metrics for describing node criticality. These metrics include the node betweenness in the cyber network, the node betweenness in the power network, and the node capacities in the power network. Here, we characterize the coupling pattern by extending the inter degree-degree correlation coefficient to an inter criticality-criticality correlation coefficient. This new metric, called *relative coupling correlation coefficient*, is defined as

$$\rho = \frac{M^{-1}\sum_m I'_{Am}I'_{Bm} - [M^{-1}\sum_m \frac{1}{2}(I'_{Am} + I'_{Bm})]^2}{M^{-1}\sum_m \frac{1}{2}(I'^2_{Am} + I'^2_{Bm}) - [M^{-1}\sum_m \frac{1}{2}(I'_{Am} + I'_{Bm})]^2} \tag{6.5}$$

where I'_{Am} and I'_{Bm} are the normalized node criticality metrics of two nodes in the two interconnected networks, respectively, when they are connected by edge m. As aforedescribed, the existence of interconnected edge m connecting cyber and power nodes implies that the cyber node can take a malicious action against the power node.

Specifically, the normalized node criticality metrics for network A is

$$I'_A = \frac{I_A - \min(I_A)}{\max(I_A) - \min(I_A)} \tag{6.6}$$

where I_A is a node criticality metric in the power network, which can be either node degree or node capability. Likewise, the normalized node criticality metrics for network B is

$$I'_B = \frac{I_B - \min(I_B)}{\max(I_B) - \min(I_B)} \tag{6.7}$$

where I_B is a node criticality metric in the cyber network which can be either node degree or node betweenness.

Several classes of coupling patterns corresponding to different combinations of node criticality metrics in power and cyber networks can be considered. In particular, we consider four classes, i.e., degree-to-degree (d2d), degree-to-betweenness (d2b),

capacity-to-degree (c2d) and capacity-to-betweenness (c2b).

6.4 Results and Discussions

In this section, we first construct a few cyber-coupled power systems using various implementations of coupling patterns. Then, two major sets of results are shown to highlight the effects of changing the relative coupling correlation coefficient ρ on the robustness by considering four different classes of coupling patterns.

6.4.1 Realization of Cyber-coupled Power Systems

We consider a cyber system realized by a Gnutella peer-to-peer network [145] containing 6301 nodes. This network is coupled with the UIUC-150 power system [144], forming a cyber-coupled system. The power and cyber nodes are connected in a one-to-one fashion. Thus, the initial step is to select 150 cyber nodes for connection to the 150 power nodes. In particular, the cyber nodes are selected according to the distribution of a chosen normalized node criticality metric. For example, if we choose the degree-to-degree coupling pattern, the aim is to identify the cyber nodes which have a similar degree distribution to that of the power nodes. In other words, a higher similarity of two chosen normalized node criticality metrics can offer a broader range of the coefficient ρ.

Fig. 6.3(a) and Fig. 6.3(d) show the distributions of two normalized node criticality metrics, namely, node degree and node capacity, respectively, in the UIUC150 power network. Then, the cyber nodes having similar distribution of a normalized node criticality metric are extracted, as shown in Fig. 6.3(b), Fig. 6.3(c), Fig. 6.3(e) and Fig. 6.3(f), under four different combinations of classes of coupling patterns. For instance, when considering the degree-to-degree coupling pattern, the distribution of the normalized node degree of the extracted cyber nodes depicted in Fig. 6.3(b) shows

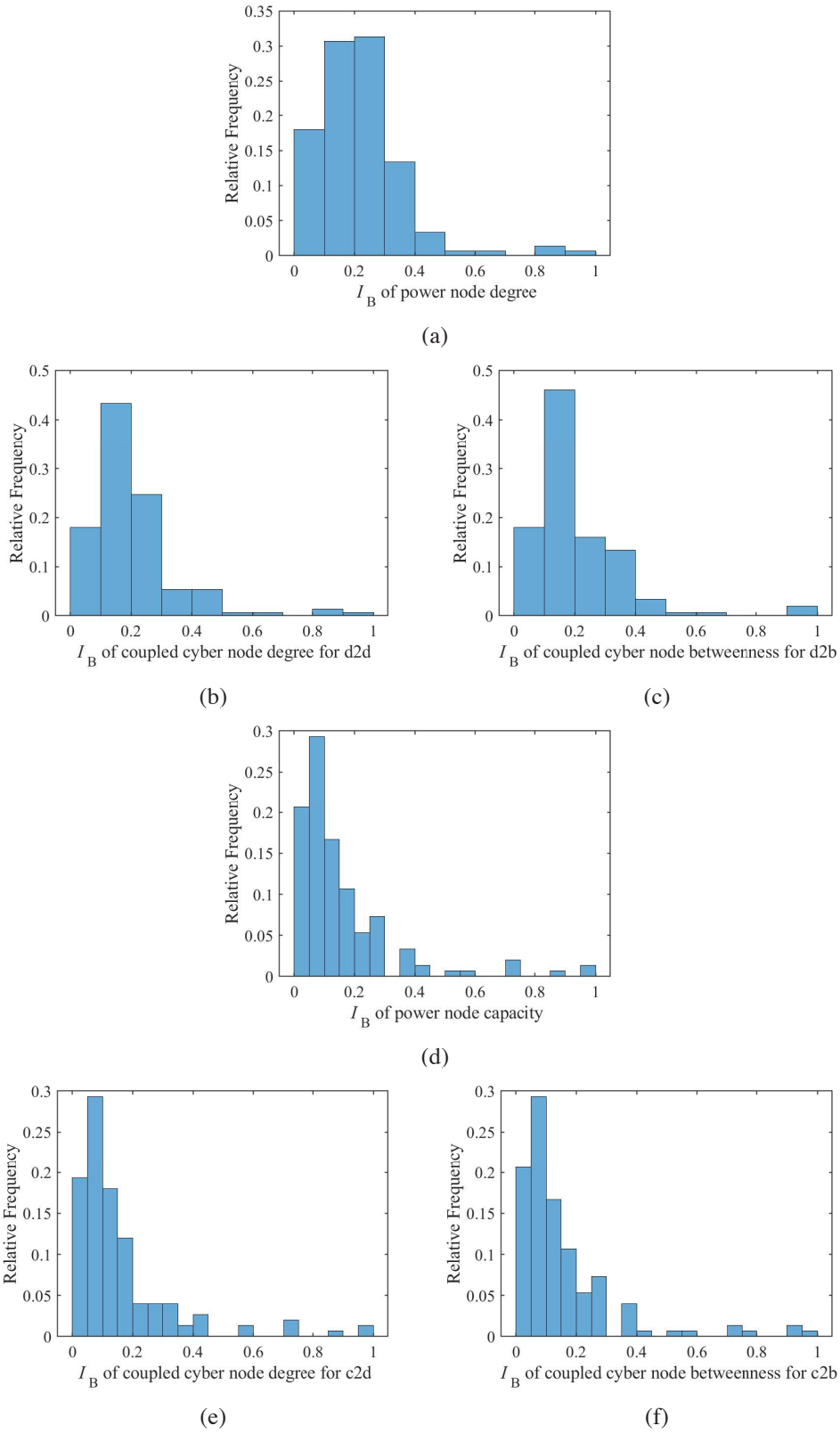


Figure 6.3: Distributions of two normalized criticality metrics. (a) Node degree; (d) node capacity for the UIUC150 power system. Distributions of normalized criticality metrics of the extracted cyber nodes when realizing the coupling patterns including (b) degree-to-degree (d2d), (c) degree-to-betweenness (d2b), (e) capacity-to-degree (c2d) and (f) capacity-to-betweenness (c2b).

a high similarity with the distribution of the normalized node degree of the power node depicted in Fig. 6.3(a). By coupling the power nodes with the extracted cyber nodes based on different combinations of node criticality metrics, the ranges of the values of coefficient ρ are given in Table 6.1. In the following experiments, the coefficient ρ for different classes of coupling patterns are considered, corresponding to various coupling patterns between the cyber and power networks. In particular, a larger maximum value of ρ gives a coupled network having highly similar distributions of the node criticality metric of the power network and the cyber network.

Table 6.1: The range of the values of the relative coupling correlation coefficient ρ for different classes of coupling patterns (d2d: degree-to-degree, d2b: degree-to-betweenness, c2d: capacity-to-degree and c2b: capacity-to-betweenness).

	ρ_{d2d}	ρ_{d2b}	ρ_{c2d}	ρ_{c2b}
Minimum Value	-0.60	-0.60	-0.40	-0.40
Maximum Value	0.80	0.80	0.80	0.80

The cascading failure of a power network is triggered by two types of events. First, an infected cyber node can trip a power node that is coupled with it. Second, the failure of a power node may induce overloading on other nodes in the power network, causing subsequent cascading failure events. To evaluate the extent and rapidity of a cascading failure in a cyber-coupled power system, we measure the percentage of failed power nodes in the power network, denoted by p_{FPN}, when a certain percentage of cyber nodes are infected and become failed nodes, which is denoted by p_{FCN}. In particular, under the same value of p_{FCN}, a larger p_{FPN} implies that more power nodes fail in the cascading failure process. In particular, for two given coupled systems having the same number of infected cyber nodes (the same value of p_{FCN}), the system which exhibits a larger value of p_{FPN} is less robust. In the following experiments, in order to assess the vulnerability of coupled systems, the value of p_{FPN} is plotted for different sampled values of p_{FCN} ranging from zero to one.

6.4.2 Effects of the Relative Coupling Correlation Coefficients

To examine the effect of varying the relative coupling correlation coefficient on the robustness of cyber-coupled power systems, an experiment is designed as follows:

1. **Network Preparation:** A number of coupled systems are implemented, each by coupling a cyber network and a power network using the aforementioned four classes of coupling patterns. For the implementation of each class of coupling patterns, coupled systems with varied values of relative coupling correlation coefficients are realized by reconnecting the interconnection links between the cyber-power node pairs. Note that a number of coupled systems might be obtained which have approximately the same relative coupling correlation coefficient.

2. **Result Assessment:** For each coupled system, simulation is performed using the cascading failure propagation model and the results including the numbers of failed power nodes and cyber nodes in the propagation process of cascading failure are obtained for the robustness assessment of the coupled system.

Fig. 6.4 shows the vulnerability assessment of cyber-coupled systems for different values of relative coupling correlation coefficient, corresponding to four classes of coupling patterns. In each figure, p_{FCN} versus p_{FPN} is plotted for the coupled system for different values of relative coupling correlation coefficient.

From the four plots shown in Fig. 6.4, it can be found that with the increasing number of infected cyber nodes, more power nodes fail. Also, from Fig. 6.4, a larger ρ might increase the vulnerability of the coupled system, that is, a larger ρ leads to a faster cascading failure propagation. In particular, for a given coupled system, a larger ρ indicates that the nodes with higher criticality in the power network tend to couple with the nodes with higher criticality in the cyber network, which can be described as a high-to-high coupling pattern. Specifically, regardless of the class of coupling patterns,

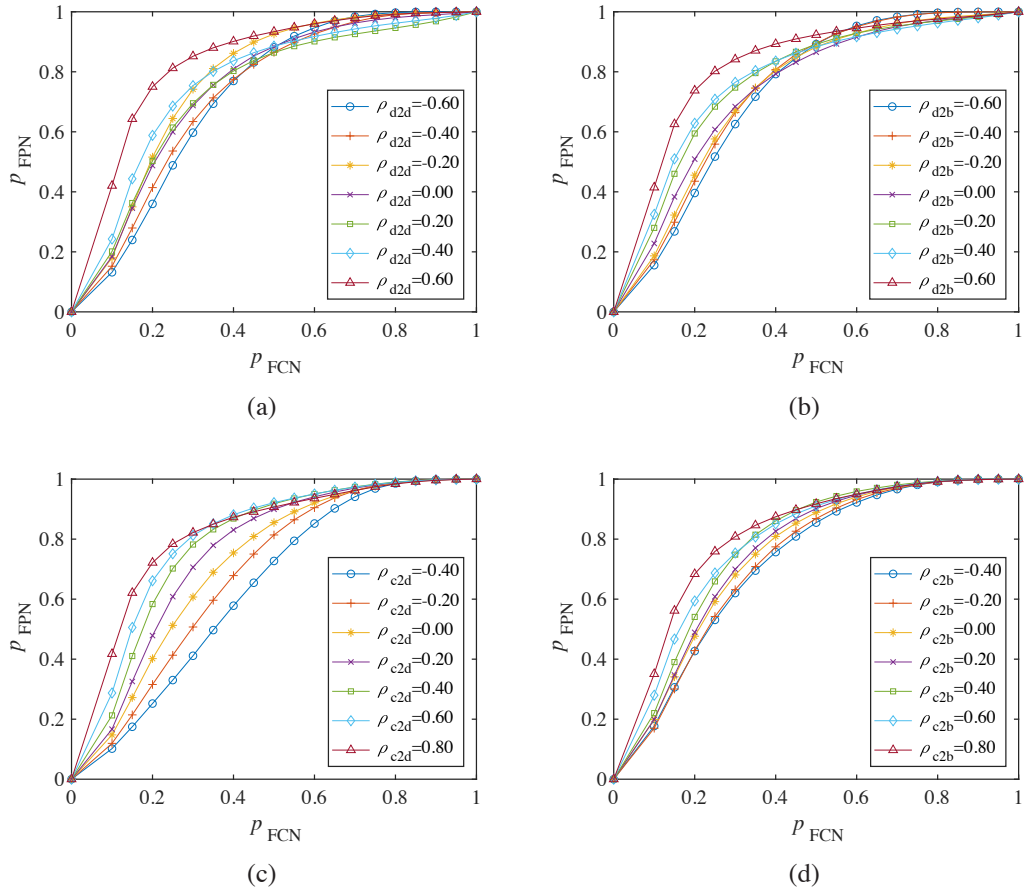


Figure 6.4: The vulnerability assessment of cyber-coupled coupled systems at varying relative coupling correlation coefficients for four classes of coupling patterns based on different combinations of node criticality metrics in power and cyber networks, namely, (a) degree-to-degree (d2d), (b) degree-to-betweenness (d2b), (c) capacity-to-degree (c2d) and (d) degree-to-betweenness (d2b).

when ρ reaches the highest value, i.e., $\rho = 0.8$, the cyber-coupled power system fails at the highest rate. Moreover, the cascading failure in the coupled systems proceeds slowly when the value of ρ is low.

The increased vulnerability brought from the increasing relative coupling correlation coefficient can be readily identified for the capacity-to-degree coupling patterns shown in Fig. 6.4(c). Specifically, when the value of ρ_{c2d} increases from -0.40 to 0.80, it is witnessed that at a certain value of p_{FCN}, a larger value of ρ_{c2d} leads to a higher value of p_{FPN}. This implies that for the same number of infected cyber nodes, the coupled system becomes more vulnerable to cyber attack when the high-capacity power nodes tend to connect to the high-degree power nodes and the low-capacity power nodes tend to connect to the low degree-cyber nodes.

The major reason why a large value of ρ corresponding to a high-to-high coupling pattern gives a cyber-coupled power system of poor robustness is twofold. First, coupling power nodes of higher node criticality with cyber nodes of higher node criticality makes the power network more prone to cyber attack. Second, the failure of more power nodes of high node criticality leads to a faster and more severe cascading failure in the power system.

6.4.3 Effects of Choice of Criticality in Coupling Patterns

Different classes of coupling patterns are built based on different combinations of node criticality metrics in power and cyber networks. In particular, if the node degree is taken as the node criticality metric for both power and cyber nodes, the interconnections between power and cyber networks are constructed in terms of the similarity between the degrees of both power and cyber nodes. In particular, the similarity level is quantified by the proposed relative coupling correlation coefficient ρ. This section aims to examine how different classes of coupling patterns affect the robustness of cyber-coupled power systems.

Fig. 6.5(a) shows the relationship between p_{FCN} and p_{FPN} for four different classes of coupling patterns under the condition that $\rho = -0.4$. Likewise, Fig. 6.5(b), Fig. 6.5(c) and Fig. 6.5(d) are also plotted with a fixed value of ρ, namely, $\rho = 0$, $\rho = 0.4$ and $\rho = 0.8$, respectively. It has been found that when the relative coupling correlation coefficient stays at a relatively low value, e.g. $\rho = -0.4$, $\rho = 0$, adopting the capacity-to-degree coupling patterns can achieve an enhancement of the robustness of coupled systems where the cascading failure propagation proceeds more slowly compared with those systems implemented by adopting other classes of coupling patterns. The capacity-to-degree coupling pattern corresponds to the node capacity being chosen as node criticality metric in the power network and node degree being chosen as node criticality metric in the cyber network. But when the relative coupling correlation coefficient is relatively high, the achievement for enhancing the robustness of coupled systems based on the preference of capacity-to-degree coupling patterns is of weak significance.

Here, it should be noted from our point of view that node capacity and node degree have significant impact on evaluating the criticality of nodes in power and cyber networks, respectively. Thus, for a given coupled system, if power nodes of high node degree are coupled with cyber nodes of low node degree, cascading failure can be suppressed in two ways. First, the power nodes with large capacity can be protected from being tripped by cyber attack because they are connected to the cyber nodes with low degree. Basically, the cyber nodes with low degree are less likely to be infected. Then, the effective defense of large capacity power nodes can bring about small extent of cascading failure in the power system.

In summary, the results offer a broad understanding of the effect of coupling patterns, quantified by a parameter called relative coupling correlation coefficient ρ, on the robustness of cyber-coupled power systems. On the one hand, the coupled system having a larger value of coefficient ρ is more vulnerable to cascading failure. This finding is consistent with the suggestion given a previous study [154], but other re-

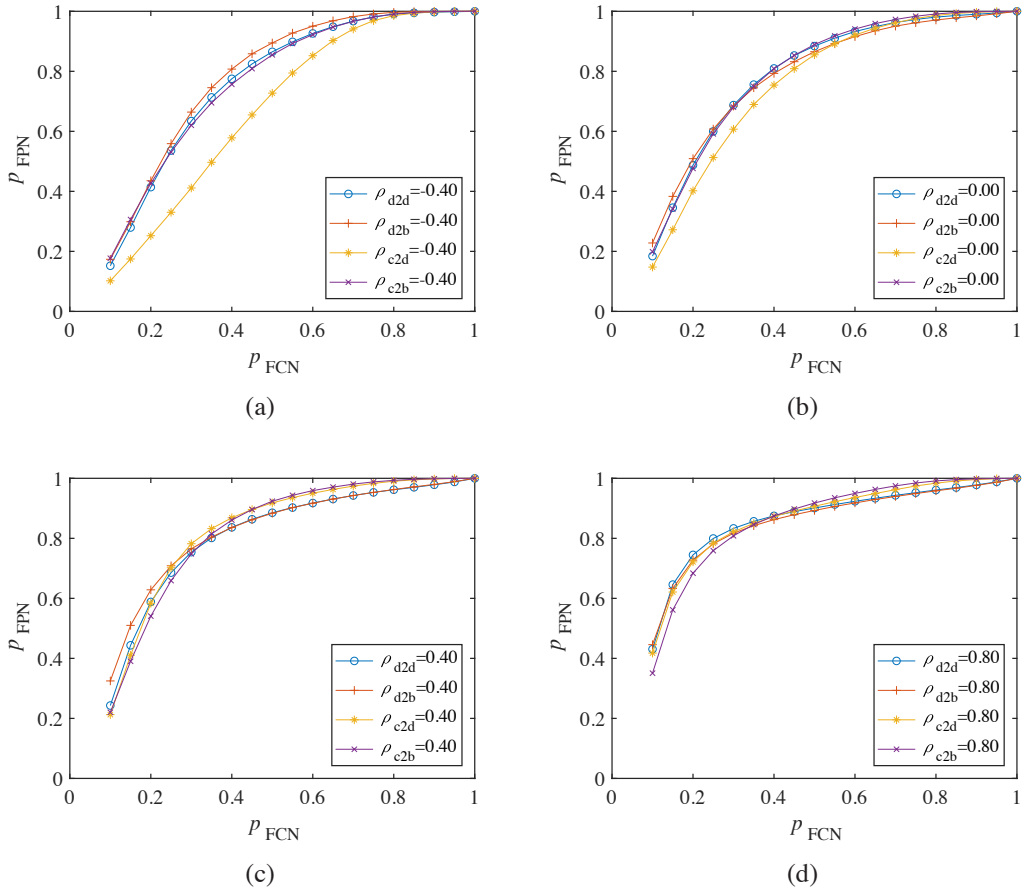


Figure 6.5: The vulnerability assessment of cyber-coupled systems where different classes of coupling patterns are implemented under four certain cases when four relative coupling correlation coefficients are given: (a) $\rho = -0.40$; (b) $\rho = 0$; (c) $\rho = 0.40$ and (d) $\rho = 0.80$.

search work [32, 152] has drawn the opposite conclusion that the higher inter-similarity (equivalent to a higher coefficient ρ) can enhance the robustness of coupled networks. On the other hand, to realize various coupling patterns for cyber-coupled power systems, in this chapter, the initial step is to select the node criticality metrics for both power and cyber networks for accessing the choice of node criticality of power and cyber nodes being coupled. The various selections of the node criticality metrics have a significant impact on examining the relationship between robustness of coupled systems and the coefficient ρ.

6.5 Summary

Smart grids, regarded as cyber-physical systems, are vital infrastructures demanding high robustness. With the integration of intelligent monitoring and controlling provided by cyber networks, a cyber-coupled power system becomes vulnerable to cyber attack and thus severe power outages might be caused. In this chapter, we introduce a model used for simulating the cascading failure in coupled systems. In particular, one coupled system is modeled as a coupled network consisting of a power network and a cyber network. More importantly, one network-based parameter called *relative coupling correlation coefficient* ρ is defined, which is used to quantify coupling patterns in coupled networks. Specifically, for a coupled network consisting of network A and B, by adopting different network-based metrics such as node degree and node capacity as node criticality metrics, a higher ρ indicates that the nodes of higher node criticality in network A tend to be connected to the nodes of higher node criticality in the network B while a lower ρ indicates that the nodes of higher node criticality in network A tend to be connected to the nodes of lower node metrics in network B. It has been remarkably found that for a given coupled system, a higher ρ, also characterized as a more assortative coupling pattern, increases the vulnerability. Notably, when identifying the optimal coupling pattern for robustness improvement, taking the node

capacity and node degree as node criticality metrics for the power and cyber networks, respectively, can achieve an improvement of the robustness of coupled networks. The main findings in this chapter cannot be obtained due the consideration of the physical power flow process in the network-based model.

Chapter 7

Conclusions and Suggestions for Future Work

In this chapter, we summarize the main contributions of the thesis and discuss the future plan for some potential research directions.

7.1 Main Contributions of the Thesis

Complex network theory has been applied for studying large real-world networked systems, especially in revealing the impact of their topological characteristics on robustness. Power systems, being critical infrastructures supporting the development of modern society, should be highly robust against cascading failure and have a low risk of a large-scale blackout. In a power network, nodes represent power substations and links represent power transmission lines. Different from the previous studies that emphasize pure topological properties and vulnerabilities of power systems, one of the main objectives in this project is to assess and enhance the robustness of power systems by using a network-based approach with the incorporation of the physical power flow process.

Moreover, power grids have evolved into smart grids by integrating with cyber

networks which provide intelligent control but at the same time pose the threat of cyber attack to power systems. A smart grid, characterized as a cyber-coupled power system can be modeled as a coupled network. The other main objective in this project is to assess the robustness of coupled systems, with employment of a model which adequately describes the failure mechanisms of cyber networks and power networks as well as the interdependence of the two networks.

The main contributions of this thesis can be summarized as follows:

1. The robustness of a power system has been assessed and enhanced from a complex network's perspective.

Enhancing the robustness of power systems has emerged as an essential topic for reducing the risk of a fast and large-scale blackout. First, a system-level method to assess the vulnerability of power systems has been developed. Specifically, one critical parameter called *onset time* is introduced to reveal the rapidity of cascading failure. Based on the *onset time* and the scale of the failed grid in a cascading failure event, we categorize each component in a power network into three types, corresponding to three levels of severity of the failed grid upon the initial failure of that component. Second, a decision tree-based learning model has been developed to extract significant network-based features. It has been found that these features can serve as effective indicators for robustness enhancement of power networks. The decision tree can provide a set of rules based on some network-based features. Through examining the effectiveness of different rules, experimental results suggest that a power network has higher robustness against cascading failure if its topology exhibits less random features and more decentralized generator distribution.

2. The profile of failure propagation in cyber-coupled power systems has been analyzed with employment of an interdependent network model.

As suggested by evidence of the cause of large-scale blackouts being initiated from a cyber attack, we have developed a model to analyze the profile of failure propagation in smart grids by considering the effect of cyber coupling. In particular, to assess the

robustness of smart grids, regarded as cyber-coupled power systems, a model is developed by considering the failure mechanisms of cyber networks and power networks as well as the interdependence of the two networks. The implementation of this model can realistically simulate the cascading failure in coupled systems. It has been found that the coupling of cyber networks accelerates and intensifies the blackout of power systems. Moreover, the profile pattern of failure propagation in a cyber-coupled power system is different from that of an individual power system.

3. The interdependence between cyber and power networks involved in modeling cascading failure in cyber-coupled power systems has been studied by considering interaction between attack and defense.

One challenge, which has been raised in the network-based model used to study the cascading failure in cyber-coupled power systems, is the interpretation of the interdependence between cyber and power networks. To comprehend the interdependence, we have developed an extended network-based model by considering the interaction between two processes, one aiming to attack (cause damage) and the other aiming to defend (protect) the components in the power network. Simulation results offer two significant findings. First, the preferred defense strategies have been identified for protecting a cyber-coupled power network, and the factors affecting the propagation profiles of the cascading failure of power networks have been highlighted. Besides, much enhanced understanding of the key parameters and their roles in controlling failure propagation have been gained through the attack-defense interaction viewpoint and the incorporation of essential physical processes in the model for analysis and possible prediction.

4. The effect of coupling patterns on the robustness of cyber-coupled power systems has been studied.

Another challenge to be addressed in modeling the cascading failure in cyber-coupled power systems is to examine how power and cyber networks are connected from a topological point of view. Specifically, the way in which the two networks are

connected is termed coupling pattern, which plays an important role in determining the robustness of the coupled network. We introduce a new parameter called *relative coupling correlation coefficient* ρ to quantify coupling patterns. In terms of node criticality metrics, various coupling patterns are constructed for robustness assessment of coupled systems. Simulation results show that the value of ρ corresponds to vulnerability of a coupled system and hence offers a perspective to designing robust coupled networks.

7.2 Suggestions for Future Work

Following the work that has been done at the current stage, some suggestions are presented on some possible research topics that could be pursued in the future.

7.2.1 Data Acquisition of Cascading Failure Events

In Chapter 4, we have proposed a decision-tree-based learning model to extract significant network-based features for robustness enhancement of power systems. Decision tree, being a popular tool in machine learning, is widely used for decision analysis. To obtain a decision tree model which can offer precise prediction in decision analysis, the availability and integrity of the data used to develop the model and to evaluate the performance of the model are crucial. Typically, the data can be obtained in two ways: collecting real-world data sets stored in power systems and generating data sets by running simulation based on analytical models.

Obtaining data from real-world power systems is challenging because of the limited availability issue. Thus, using AC/DC power models mentioned in Section 2.3 to generate data sets is an alternative solution. Then, with the data-driven analysis to enhance the robustness of power systems, effective algorithms might be gained for the identification of critical nodes or links [56] as well as the forecasting of the path of

failure propagation [155] in power systems.

7.2.2 Solutions to Mitigate Cascading Failure

One of the ultimate goals in the development of smart grids is to make power grids self-healing so that the grids would take appropriate actions to recover from a vulnerable operation status. Load shedding and islanding are two key technologies to suppress the cascading failure in power systems.

The objective of load shedding is to maintain a balance between load and generation when generation in a power system cannot adequately support all loads. During a cascading failure event, if power imbalance between generation and load demand occurs, employing load shedding, which trips a certain amount of load appropriately, can save the remaining portion of the system from a continuous process of failure propagation. Thus, a connection between identifying the appropriate power components where load shedding is performed and detecting the critical components in the power system can be built.

Islanding is used for preventing blackout by decomposing the entire power network into a number of subnetworks where no overloading occurs. In complex network theory, community detection has been used to identify the modules with high similar characteristics. Incorporating the characteristics of power grids into the existing community detection algorithms seems to be a promising direction for developing effective islanding strategies.

In Chapter 5, by considering the interaction between two processes, one aiming to attack (cause damage) and the other aiming to defend (protect) the components in the power network, it has been found that allocating defense strength in terms of capacity-based distribution can most effectively suppress cascading failure in cyber-coupled power systems. This finding provides a good starting point for discussion and further research on the identification of effective protection mechanisms for risk reduction of

severe blackout in smart grids.

7.2.3 Comprehension of Coupling Patterns

In Chapter 6, it has been demonstrated that coupling patterns have considerable impact on the robustness of cyber-coupled power systems. As coupling patterns in real smart grids have not been clearly analyzed yet, in order to optimize the coupling patterns for robustness enhancement of cyber-coupled power systems, future research should be conducted in more realistic settings, with emphasis on the way cyber and power networks are coupled from a complex network's perspective.

7.2.4 Model of Interconnected Systems

Interdependent network models serve as effective methodologies for the analysis of interconnected systems. Besides smart grids, there are many other interconnected systems which could be modeled using interdependent network-based approaches.

Power networks can be interconnected with an electric vehicle network, which forms a vehicle-to-grid [156] framework. Basically, the vehicle-to-grid infrastructure provides an operational framework for electric vehicle networks and power networks to interact. Specifically, power networks can charge electric vehicles and electric vehicles can generate power back to power networks. Interdependent network models might offer an alternative solution to study the vehicle-to-grid infrastructure and thus to address different challenges on the planning, operation and control of the vehicle-to-grid infrastructure.

One more consideration in the development of smart grids is the integration of social networks into power grids. Wide discussion has been conducted on interaction between social networks and power grids [157]. In particular, taking advantage of social network data to develop robust and consumer-centric services has emerged as an essential topic, which might be studied from an interdependent network's perspective.

Bibliography

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

[2] B. Goswami, N. Boers, A. Rheinwalt, N. Marwan, J. Heitzig, S. F. M. Breitenbach, and J. Kurths, "Abrupt transitions in time series with uncertainties," *National Communications*, vol. 9, no. 1, p. 48, Jan. 2018.

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

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

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

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

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

[8] 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.

[9] 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.

[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] A. Barrat, M. Barthélemy, R. Pastor-Satorras, and A. Vespignani, "The architecture of complex weighted networks," *Proceedings of the National Academy of Sciences*, vol. 101, no. 11, pp. 3747–3752, Mar. 2004.

[12] 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.

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

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

[15] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jimnez-Fernndez, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, Aug. 2015.

[16] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, Jan. 2010.

[17] 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.

[18] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. Design Automation Conference*, Jun. 2010, pp. 731–736.

[19] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[20] 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.

[21] 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.

[22] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Physical Review E*, vol. 70, p. 035101, Sept. 2004.

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

[24] R. K. Ahuja, K. Mehlhorn, J. Orlin, and R. E. Tarjan, "Faster algorithms for the shortest path problem," *Journal of the ACM*, vol. 37, no. 2, pp. 213–223, Apr. 1990.

[25] 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.

[26] 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/

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

[28] 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.

[29] A. Capocci, V. D. P. Servedio, F. Colaiori, L. S. Buriol, D. Donato, S. Leonardi, and G. Caldarelli, "Preferential attachment in the growth of social networks: The internet encyclopedia wikipedia," *Physical Review E*, vol. 74, p. 036116, Sept. 2006.

[30] E. Eisenberg and E. Y. Levanon, "Preferential attachment in the protein network evolution," *Physical Review Letter*, vol. 91, p. 138701, Sept. 2003.

[31] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, p. 065101, Jun. 2011.

[32] R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition," *Physical Review Letter*, vol. 105, p. 048701, Jul 2010.

[33] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, "Inter-similarity between coupled networks," *EPL (Europhysics Letters)*, vol. 92, no. 6, p. 68002, dec 2010.

[34] C.-G. Gu, S.-R. Zou, X.-L. Xu, Y.-Q. Qu, Y.-M. Jiang, D. R. He, H.-K. Liu, and T. Zhou, "Onset of cooperation between layered networks," *Physical Review E*, vol. 84, p. 026101, Aug. 2011.

[35] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, "Interdependent networks with identical degrees of mutually dependent nodes," *Physical Review E*, vol. 83, p. 016112, Jan 2011.

[36] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Physical Review E*, vol. 83, p. 036116, Mar 2011.

[37] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *Proc. 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*, Jun. 2013, pp. 1023–1028.

[38] C. D. Brummitt, R. M. D'Souza, and E. A. Leicht, "Suppressing cascades of load in interdependent networks," *Proceedings of the National Academy of Sciences*, vol. 109, no. 12, pp. 4345–4346, Mar. 2012.

[39] M. A. Di Muro, C. E. La Rocca, H. Stanley, S. Havlin, and L. A. Braunstein, "Recovery of interdependent networks," *Scientific Reports*, vol. 6, p. 22834, Apr. 2016.

[40] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, Aug. 2015.

[41] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, p. 013119, Feb. 2009.

[42] 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.

[43] 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.

[44] B. A. Carreras, D. Newman, and I. Dobson, "Does size matter?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 24, no. 2, p. 023104, Apr. 2014.

[45] Å. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk analysis*, vol. 26, no. 4, pp. 955–969, Sept. 2006.

[46] 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.

[47] 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.

[48] D. P. Chassin and C. Posse, "Evaluating north american electric grid reliability using the barabási–albert network model," *Physica A: Statistical Mechanics and its Applications*, vol. 355, no. 2-4, pp. 667–677, Feb. 2005.

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

[50] 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.

[51] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, Dec. 2014.

[52] ——, "Coordinated attacks against substations and transmission lines in power grids," in *2014 IEEE Global Communications Conference*, Dec. 2014, pp. 655–661.

[53] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 396, pp. 204 – 211, Feb. 2014.

[54] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letter*, vol. 87, p. 198701, Oct. 2001.

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

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

[57] R. Baldick, B. Chowdhury, I. Dobson, Zhaoyang Dong, Bei Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, Fangxing Li, Juan Li, Zuyi Li, Chen-Ching Liu, L. Mili, S. Miller, R. Podmore, K. Schneider, Kai Sun, D. Wang, Zhigang Wu, Pei Zhang, Wenjie Zhang, and Xiaoping Zhang, "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 *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Jul. 2008, pp. 1–8.

[58] 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.

[59] 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.

[60] P. D. H. 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.

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

[62] P. Dey, R. Mehra, F. Kazi, S. Wagh, and N. M. Singh, "Impact of topology on the propagation of cascading failure in power grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1970–1978, Jul. 2016.

[63] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 3, pp. 346–350, March 2018.

[64] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 9, pp. 627 – 633, Nov. 2006, selection of Papers from 15th Power Systems Computation Conference, 2005.

[65] S. Mei, Y. Ni, G. Wang, and S. Wu, "A study of self-organized criticality of power system under cascading failures based on ac-opf with voltage stability

margin," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with dc power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, Jan. 2015.

[71] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem, "Comparing the effects of failures in power grids under the ac and dc power flow models," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 4, pp. 301–312, Oct. 2018.

[72] 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.

[73] 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.

[74] Y. Wang, Z. Lin, X. Liang, W. Xu, Q. Yang, and G. Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers of Information Technology & Electronic Engineering*, vol. 17, no. 5, pp. 465–478, May 2016.

[75] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3847–3862, Sept. 2017.

[76] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," in *Proc. IEEE Global Communications Conference*, Atlanta, USA, 2013, pp. 2164–2169.

[77] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Transactions on Computers*, vol. 64, no. 8, pp. 2158–2168, Aug 2015.

[78] W. Kang, P. Zhu, G. Hu, Z. Hang, and X. Liu, "Cross-layer attack path exploration for smart grid based on knowledge of target network," in *Proc. International Conference on Knowledge Science, Engineering and Management*, vol. 18, no. 6. Springer, Jun. 2018, pp. 433–441.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

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

[85] 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.

[86] 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.

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

[88] 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.

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

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

[91] 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.

[92] 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.

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

[94] 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.

[95] 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.

[96] 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.

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

[98] B. Liscouski and W. Elliot, "Final report on the august 14th blackout in the united states and canada," Apr. 2004. [Online]. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[99] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, p. 045104, Apr. 2004.

[100] F. Wenli, L. Zhigang, H. Ping, and M. Shengwei, "Cascading failure model in power grids using the complex network theory," *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3940–3949, Nov. 2016.

[101] 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.

[102] V. Rampurkar, P. Pentayya, H. A. Mangalvedekar, and F. Kazi, "Cascading failure analysis for indian power grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1951–1960, Jul. 2016.

[103] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. V. Cutsem, and V. Vittal, "Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions," *IEEE Transactions on Power System*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.

[104] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with dc power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, Jan. 2015.

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

[106] E. I. Bilis, W. Krger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE System Journal*, vol. 7, no. 4, pp. 854–865, Dec. 2013.

[107] E. Bompard, L. Luo, and E. Pons, "A perspective overview of topological approaches for vulnerability analysis of power transmission grids," *International Journal of Critical Infrastructures*, vol. 11, no. 1, pp. 15–26, Jan. 2015.

[108] P. Cuffe and A. Keane, "Visualizing the electrical structure of power systems," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1810–1821, Mar. 2017.

[109] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. IEEE Conference on Decision and Control*, Dec. 2010, pp. 5792–5797.

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

[111] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE System Journal*, vol. 6, no. 3, pp. 481–487, Sept. 2012.

[112] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 81–88, Jan. 2013.

[113] Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science*, vol. 358, no. 6365, Nov. 2017.

[114] C. C. Chu and H. H. C. Iu, "Complex networks theory for modern smart grid applications: A survey," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 2, pp. 177–191, Jun. 2017.

[115] M. Rosas-Casals, S. Valverde, and R. Sol, "A simple spatiotemporal evolution model of a transmission power grid," *IEEE System Journal*, vol. 12, no. 4, pp. 3747–3754, Dec. 2018.

[116] L. Luo, B. Han, and M. Rosas-Casals, "Network hierarchy evolution and system vulnerability in power grids," *IEEE System Journal*, vol. 12, no. 3, pp. 2721–2728, Sept. 2018.

[117] H. Cetinay, F. A. Kuipers, and P. V. Mieghem, "A topological investigation of power flow," *IEEE System Journal*, vol. 12, no. 3, pp. 2524–2532, Sept. 2018.

[118] Z. Wang, M. Rahnamay-Naeini, J. M. Abreu, R. A. Shuvro, P. Das, A. A. Mammoli, N. Ghani, and M. M. Hayat, "Impacts of operators behavior on reliability of power grids during cascading failures," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6013–6024, Nov. 2018.

[119] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, Mar. 2011.

[120] N. Marwan, M. C. Romano, M. Thiel, and J. Kurths, "Recurrence plots for the analysis of complex systems," *Physical Reports*, vol. 438, no. 5-6, pp. 237–329, Jan. 2007.

[121] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic,

C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Transactions on Power System*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[122] L. Breiman, *Classification and regression trees*. New York: Routledge, 2017.

[123] W.-Y. Loh and Y.-S. Shih, "Split selection methods for classification trees," *Statistica sinica*, vol. 7, no. 4, pp. 815–840, Oct. 1997.

[124] M. Newman, *Networks: An Introduction*. London: Oxford Univ. Press, 2018.

[125] G. Latorre, R. D. Cruz, J. M. Areiza, and A. Villegas, "Classification of publications and models on transmission expansion planning," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 938–946, May 2003.

[126] Z. Yang, H. Zhong, Q. Xia, and Y. Bai, "Review and prospect of transmission topology optimization," *Proceedings of the CSEE*, vol. 36, no. 2, pp. 426–434, Jan. 2016.

[127] K. W. Hedman, S. S. Oren, and R. P. O'Neill, "A review of transmission switching and network topology optimization," in *Proc. IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–7.

[128] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A: Statistical Mechanics and its Applications*, vol. 357, no. 3-4, pp. 593–612, Nov 2005.

[129] Z. Wang, R. J. Thomas, and A. Scaglione, "Generating random topology power grids," in *Proc. Hawaii International Conference on System Sciences*, Jan. 2008, pp. 183–183.

[130] J. Lu, X. Yu, G. Chen, and D. Cheng, "Characterizing the synchronizability of small-world dynamical networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 4, pp. 787–796, Apr. 2004.

[131] S. D. Antón, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann, and H. D. Schotten, "Two decades of SCADA exploitation: A brief history," in *Proc. IEEE Conference on Applications, Information and Network Security*, Nov. 2017, pp. 98–104.

[132] Z. Wan, G. Wang, Y. Yang, and S. Shi, "Skm: Scalable key management for advanced metering infrastructure in smart grids," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 12, pp. 7055–7066, Dec. 2014.

[133] J. Liu, T. Yin, M. Shen, X. Xie, and J. Cao, "State estimation for cyberphysical systems with limited communication resources, sensor saturation and denial-of-service attacks," *ISA Transactions*, Dec. 2018.

[134] 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*, vol. 65, no. 1, pp. 115–119, Jan. 2018.

[135] 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, Jan. 2013.

[136] C. Y. Ma, D. K. Yau, X. Lou, and N. S. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1676–1686, Feb. 2013.

[137] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, Jan. 2016.

[138] Y. Wang, H. R. Karimi, and H. Yan, "An adaptive event-triggered synchronization approach for chaotic lure systems subject to aperiodic sampled data," *IEEE Transactions on Circuits Systems II: Express Briefs*, vol. 66, no. 3, pp. 442–446, Mar. 2019.

[139] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," Mar. 2016. [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[140] M. Assante, "Confirmation of a coordinated attack on the Ukrainian power grid," Jan. 2016. [Online]. Available: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[141] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, p. 55, Apr. 2014.

[142] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sciences and Information Confirmation*, Aug. 2014, pp. 626–631.

[143] B. Zhu and S. Sastry, "SCADA-specific intrusion detection/prevention systems: A survey and taxonomy," in *Proc. International Workshop on Systems Safety & Security*, Apr. 2010.

[144] "UIUC 150-bus system," Jul. 2016. [Online]. Available: http://icseg.iti.illinois.edu/synthetic-power-cases/uiuc-150-bus-system/

[145] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, Jun. 2014.

[146] G. Ho, A. Sharma, M. Javed, V. Paxson, and D. Wagner, "Detecting credential spearphishing attacks in enterprise settings," in *Proc. USENIX Security Symposium*, Aug. 2017, pp. 469–485.

[147] Microsoft, "Intelligent security: Using machine learning to help detect advanced cyber attacks," 2016. [Online]. Available: https://info.microsoft.com/rs/157-GQE-382/images/

[148] K. Kim and P. R. Kumar, "Cyberphysical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[149] Y. Liu, C. Zhao, D. Yi, and H. Eugene Stanley, "Robustness of partially interdependent networks under combined attack," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 2, p. 021101, 2019.

[150] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Physical Review Letters*, vol. 107, p. 195701, Nov. 2011.

[151] 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.

[152] F. Tan, J. Wu, Y. Xia, and C. K. Tse, "Traffic congestion in interconnected complex networks," *Physical Review E*, vol. 89, p. 062813, Jun 2014.

[153] Y. Xia, W. Zhang, and X. Zhang, "The effect of capacity redundancy disparity on the robustness of interconnected networks," *Physica A: Statistical Mechanics and its Applications*, vol. 447, pp. 561 – 568, 2016.

[154] S. Sun, Y. Wu, Y. Ma, L. Wang, Z. Gao, and C. Xia, "Impact of degree heterogeneity on attack vulnerability of interdependent networks," *Scientific Reports*, vol. 6, p. 32983, 2016.

[155] Q. Sun, L. Shi, Y. Ni, D. Si, and J. Zhu, "An enhanced cascading failure model integrating data mining technique," *Protection and Control of Modern Power Systems*, vol. 2, no. 1, p. 5, Feb. 2017.

[156] F. Mwasilu, J. J. Justo, E.-K. Kim, T. D. Do, and J.-W. Jung, "Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration," *Renewable and Sustainable Energy Reviews*, vol. 34, pp. 501 – 516, Jun. 2014.

[157] S. N. A. U. Nambi and R. V. Prasad, "Toward the development of a techno-social smart grid," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 202–209, Nov. 2016.