Application of Complex Network Theory in Power System Security Assessment

Zhuoyang Wang

Centre for Future Energy Networks, School of Electrical and Information Engineering, Faculty of Engineering and IT
The University of Sydney

This thesis is submitted in fulfilment of requirements for the degree of
Doctor of Philosophy

School of EIE November 2017

I would like to dedicate this thesis to my loving parents. Without their support, it would not have been possible for me to complete my Ph. D.. . .

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Zhuoyang Wang
November 2017

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Professor David J. Hill, who has a rigorous scientific attitude and wide perspective: he continually provided me with priceless guidance and encouragement. His generous support and knowledge enabled a much better insight and understanding for this topic and research.

I would like to thank Professor Joe Dong, who inspired me and provided me with valuable opportunities to access to numerous conferences, seminars and discussions held by world-class researchers.

In addition, I would like to thank my co-supervisor Dr. Guo Chen. Without his kind assistance and persistent help the completion of this research project would not have been possible.

Then, I want to thank all my colleagues from the Centre for Future Energy Networks for your help, especially Mr. Wang Zhang and Mr. Liyan Zhang. I really enjoy working with you my dear friends and wish you all the best.

Moreover, I would like to thank Miss. Haibo Shen, my first friend in Australia. Your support and encouragement was worth more than I can express on paper. Thank you my friend, good luck for all that you need to achieve.

Finally, I would like to thank all of those who have provided me with financial support in the form of scholarships and prizes during my Ph. D program. The benefits of those have allowed me to focus on my studies:

- *The China Scholarship Council (CSC) award from the Ministry of Education of China,*
- *Norman I price from the School of Electrical and Information Engineering (EIE) at the University of Sydney,*
- *Postgraduate Research Scholarship Scheme (PRSS) from the School of EIE.*

Abstract

The power demand increases every year around the world with the growth of population and the expansion of cities. Meanwhile, the structure of a power system becomes increasing complex. Moreover, increasing renewable energy sources (RES) has linked to the power network at different voltage levels. These new features are expected to have a negative impact on the security of the power system. In recent years, complex network (CN) theory has been studied intensively in solving practical problems of large-scale complex systems. A new direction for power system security assessment has been provided with the developments in the CN field. In this thesis, we carry out investigations on models and approaches that aim to make the security assessment from an overview system level with CN theory.

Initially, we study the impact of the renewable energy (RE) penetration level on the vulnerability in the future grid (FG). Data shows that the capacity of RE has been increasing over by 10% annually all over the world. To demonstrate the impact of unpredictable fluctuating characteristics of RES on the power system stability, a CN model given renewable energy integration for the vulnerability analysis is introduced. The numerical simulations are investigated based on the simplified 14-generator model of the South Eastern Australia power system. Based on the simulation results, the impact of different penetrations of RES and demand side management on the Australian FG is discussed.

Secondly, the distributed optimization performance of the communication network topology in the photovoltaic (PV) and energy storage (ES) combined system is studied with CN theory. A Distributed Alternating Direction Method of Multipliers (D-ADMM) is proposed to accelerate the convergence speed in a large dimensional communication system. It is shown that the dynamic performance of this approach is highly-sensitive to the communication network topology. We study the variation of convergence speed under different communication network topology. Based on this research, guidance on how to design a relatively more optimal communication network is given as well.

Then, we focus on a new model of vulnerability analysis. The existing CN models usually neglect the detailed electrical characteristics of a power grid. In order to address the issue, an innovative model which considers power flow (PF), one of the most important characteristics in a power system, is proposed for the analysis of power grid vulnerability. Moreover, based on the CN theory and the Max-Flow theorem, a new vulnerability index is presented to identify the vulnerable lines in a power system. The comparative simulations between the power flow model and existing models are investigated on the IEEE 118 bus system.

Based on the PF model, we improve a power system cascading risk assessment model. In this research the risk is defined by the consequence and probabilities of the failures in the system, which is affected by both power factors and the network structure. Furthermore, a cascading event simulation module is designed to identify the cascading chain in the system during a failure. This innovation can form a better module for the cascading risk assessment of a power system.

Finally, we argue that the current cyber-physical network model have their limitations and drawbacks. The existing "point-wise" failure model is not appropriate to present the interdependency of power grid and communication network. The interactions between those two interdependent networks are much more complicated than they were described in some the prior literatures. Therefore, we propose a new interdependency model which is based on earlier research in this thesis. The simulation results confirm the effectiveness of the new model in explaining the cascading mechanism in this kind of networks.

Table of contents

List of figures

Chapter 1

Introduction

1.1 Motivation

With smart grid projects arising all over the world, more and more distributed energy resources (DER) such as intermittent renewable energy source (RES) including wind power (WP), PV generation and electric vehicles (EV) are connecting into the system. The evidence shows that the stability of power grids is greatly impacted by the characteristics of RE unpredictable fluctuating power and reduced inertia, which means the networks may be more vulnerable, especially under attacks [1].

On the other hand, DER also affects the topology of the networks [2]. Power grids with RE sources become more complicated and changeable. They are no longer an individual network but dependent on different networks, such as communication, gas, logistics etc. The research [3] shows that a broader degree distribution increases the vulnerability of interdependent networks to random attacks, which is the opposite of how a single network behaves. Therefore, the security assessment of power grids should be highlighted to ensure robust networks in the future.

1.2 Power System Blackouts and Cascading Events

In the last decade, several major blackouts across the world were reported in many research papers [4]. The causes and the results of these blackouts are listed as follow:

A A cascaded failure was reported on 2nd July 1996 in the Western North American power system. A flashover took place in a 345 kV transmission line and created a short circuit that result in a 2 GW power interruption. Also the short circuit led voltage drop and tripped several hydro generators. Finally, power swings grow and the system collapsed after one of the 230 kV lines was tripped.[5].

B The U.S-Canadian blackout on 14th August 2003 affected about 50 million people. In this event 63 GW load was interrupted, which was 11% of the total power supply by the grid. The main reason was reported as two transmission lines loaded 44% and 88% connected to trees and tripped within two hours. The protection system didn't give the timely feedback to the operators. The insufficient supply of reactive power cause large numbers of generators tripping. Finally, a critical failure made a tie line lead to reversal of power flow in the system [6].

C The Danish-Swedish power system had a blackout on 23rd September 2003. The daily life of 4 million people was disturbed by this failure. The blackout was caused by two independent accidents. Firstly a 1200 MW nuclear power plant disconnected to the system in southern Sweden; 5 minutes later a fault occurred at a substation and tripped another 1800 MW power plant. This tripping had the consequence of very high power flow and system collapsed. The islanded system after disconnection could not maintain the dynamic balance and collapsed [7].

D Another blackout happened in Italy on 28th September 2003. This blackout started with a tie line between Italy and Switzerland flashover a tree. Because of the large phase difference across the line, the auto re-closer can not rebuild the connection. The power loss in Italy started to reduce synchronism of whole power system in Europe power grid. The interconnection line from Italy to France, Austria and Slovenia got overloaded and tripped within few minutes. Then the entire Italian power system collapsed [8].

E Attacked by strong typhoon, the power grid in Hainan Province China had a blackout on 25th September 2005. Hainan grid was an isolated islanded system, mainly composed by a 220 kV looped network. The typhoon blew over the network and a large number of 220 kV and 110 kV lines tripped. The whole grid in Hainan collapsed within few minutes [9].

F A large area blackout was caused on 16th January 2007 in Victoria, Australia. It was reported that a continuous hot weather caused a bushfire thus tripping two critical

330 kV transmission lines. Within a few seconds the Victoria system was split to three islands due the cascaded line tripping. Load shedding interrupted 2.2 GW of supply before restoration. And another 200 MW of power supply was lost because of operating errors during restoration [10].

G On 22nd February 2011, an earthquake struck the city of Christchurch, New Zealand, damaging large parts of the utility in Orion's sub-transmission and distribution networks. Over 80% of the city lost power supply. It took about 10 days to restore electricity to 90% of consumers. The direct costs were estimated at over $40 million [11].

H A thunderstorm hit the state of South Australia on 28th September 2016. The high winds, lightning strikes, hail and heavy rainfall resulted in multiple transmission system faults. The system lost the three major 275 kV transmission lines in north Adelaide in 2 minutes. This lead to 315 MW of wind generation disconnected. The uncontrolled reduction in generation increased the flow on the interconnector from VIC which then overload. The automatic-protection mechanism activated and tripped the interconnector. This resulted in the loss of power supply to all customer loads in SA (approximately 1895 MW of demand) [12].

There are several lessons we can learn from these blackout records.

The first factor relates to the topology of the grid. There is usually a big electrical distance between generators and loads in the modern power system. The inter-area transmission lines play a very important role in offering power to the load side [7]. When these major lines tripped, the remaining lines in the system will be forced to overload to participating the power transition that may cause an extensive cascade falling such as in case *E*. Also, the electrical distance is increased since the major connection between generator and load was lost. The angles deviations between generator and load increase and the line voltage depressed. This will require more reactive power to maintain the voltage and lead to loss of synchronization of the system in case *A*.

The second factor is a shortcoming of protection and monitoring systems. The protection such as relaying system is the first defence to prevent blackout, and malfunction of the protection in case *B* and *E* caused a blackout directly.

Besides those two factors, the interconnection transmission lines between different areas are also vulnerable parts in the system. The hidden risk of a cascading fault is not easy to

find out during safe operating conditions, but has a great influence under urgent situations as in cases D and H.

Overall, structural vulnerability leading to cascading failures can be considered as a major contributing factor. From the cases mentioned above we can see most of these serious blackouts are caused by a single event but end up with cascading failures across a large area. For this reason, new models and methods for power system security assessment are much necessary to prevent potential cascading events.

1.3 Security Assessment in Power Systems

The concept of a vulnerable of a system is defined as a reduced level of security that the system renders it vulnerable to the moderate disturbances during operations [13]. The term of vulnerability is defined in [14] with the context of power systems. The vulnerability is defined as the level of weakness with respect to a cascading event in this thesis. The failure in a power system is usually leads to a cascading event and therefore it is beyond the traditional concept of $N-1$ system security criteria. The vulnerability mentioned in [15] is a measure of the system's weakness with respect to a sequence of cascading events that may include line or generator outages, malfunctions or undesirable operations of protection relays, failures in communication layer, and manual operation errors. In [16], the potential sources of power grid vulnerability are discussed. It is mentioned in this research that one event may start transient state and trigger another event. The overloaded lines may be tripped by impedance relays due to the low voltage and high current operating conditions. Some typical patterns of cascading events have been introduced in [17][18] including transmission line overload, generator fault due to abnormal voltage and frequency. In this section, we want to introduce some recent works of security assessment which can be mainly classified into two types: traditional steady-state modelling and complex network based analysis.

1.3.1 Security Assessment with Steady-State Modelling

A continued power balance is required to maintain the stability of a power system. Usually a power system changes from one steady state to another. That is to say, a steady state model is adequate for assessing the security level of a power system during a cascading

event. Therefore,power system security can be performed by power flow analysis based on the steady state modelling such as $N-x$ contingency analysis, hidden failure analysis and probability risk analysis. Here we look briefly at these models.

A. $N-x$ Contingency Analysis.

"$N-1$" contingency analysis is an indispensable part of power industry to analyse the potential failures in a power system. The report [14] summarizes the $N-1$ contingency standard as a way that ensures any single contingency in the power grid will not propagate into a cascading event. In this case, the power grid operators should run all the possible cases and check for the intolerable consequences.

The analysis based on $N-1$ criterion has been a common industry practice nowadays. However, in the real power system operating, multiple unrelated events can be occurred in the same time and propagate into a cascading event[19]. Thus, $N-x$ (x equals two or even higher) contingency events need to be analysed as well. The result of $N-x$ contingency analysis heavily relies on combinatorial approaches of contingencies and extremely long computational time. The result in [20] shows that the computational resources are not fully used during the load balancing schemes due to the uneven time in different cases. Therefore, the CPU speed, network topology, time delay during the information exchange should be considered in a well-designed dynamic load balancing scheme.

B. Hidden Failure Analysis.

In [21] the power system hidden failure is denoted as the permanent defects that would cause a unexpected or false react to the disturbances in a power grid . Ref. [22][23] shows that the hidden failures in power system are usually triggered by other events and may have disastrous consequences. In the research of [21][24][25][26][27][28], the probabilistic approaches of the hidden failures are modelled as follows:

$$P_{hf} = P_0 \exp\left(\frac{-Z}{3Z_3}\right) \tag{1.1}$$

where P_{hf} is the probability of hidden failure in a relay system, Z is the impedance of the relay, and Z_3 is the zone 3 setting.

In recent years, fast simulation techniques and heuristic random search are applied to identify critical relays that may lead to some possible cascade failures. In Ref [26] a simple hidden failure model are proposed. In this model, each exposed line has a tripping probability function that is modelled as an increasing function of the power flow on the line. Those simulation shows that the maintenance of the relays is a cost-effective mitigation strategy to cascading failure.

C. Probability and Risk Analysis.

Academics have analysed power networks failure with risk theory for several years. The risk indicators can generally describe the two main factors in cascading failure, the probability of cascading and severity of event. In [25][29] several simulations are employed to demonstrate approaches. The simulation results address that one of the most effective ways to mitigate cascading events is to control the high risk sequences. Ref. [30] verified the overall cascading risk is basic to evaluating the benefits of mitigation efforts. Though the models have some gaps with real events, the research with probability risk analysis has shown the great value in detecting network security and guiding mitigation efforts.

1.3.2 Security Analysis based on Complex Network Theory

With the progress of power system security analysis, more cross-disciplinary theories have been taken into the research. However, the power flow and network topology modelling are not been considered in most of the probabilistic models. Thus, these probabilistic models only capture some generic features but neglect the details of cascading mechanisms. In recent years, CN theory is one of the most be relevant tools to analyse the vulnerability of power system. In the power grid security assessment based on CN model, several graph analysis techniques have been applied, such as based on small-world networks and scale-free networks. The basis of graph analysis applications is the mapping of the power grid topology to a CN by nodes and edges. The simplified power network is an undirected connected graph with N nodes and K links. A simple CN model is shown in Fig.1.1[19].

A. Small-world Network.

The concept of small-world network was firstly introduced to study social networks [31]. Then electrical engineers discovered that power system have the properties of a small-world

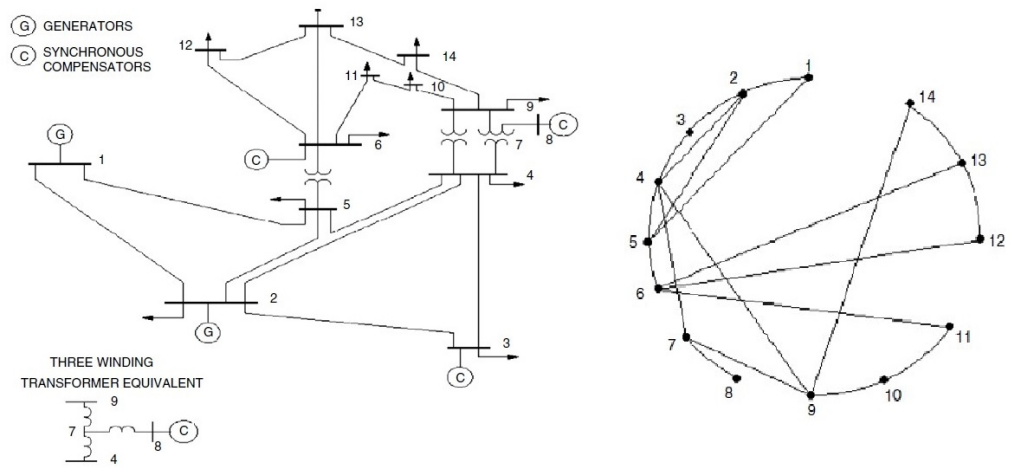

Fig. 1.1 IEEE 14 bus system and its graph model

network [32]. The grid has big clustering coefficients and relatively small distance. In this kind of network, the loss of some remote connections will increase the distance between two nodes, decrease the transfer capacity of the power grid, which can easily cause cascading events. Accordingly, these critical connections play an important role in power system stability. Therefore, the vulnerability of the power system can be identified by detecting these critical connections[32]. A small-world network based cascading failure model was proposed in [33]. This model can be used to identify the vulnerable lines in the power grid. According to the small-world network theory, those lines which removal can lead to a cascading events are the vulnerable lines in the power system.

B. Scale-free Network.

The
is described in [34]. The step of growth starts with a small number n_0 of nodes, then adds a new node with $m\,(m \leq n_0)$ links to m different nodes already existing in the network. P_i is employed to describe the probability of adding connection to an existing node i:

$$P_i = \frac{k_i}{\sum_j k_j} \tag{1.2}$$

where k_i is the degree of node i, j is the rest of the nodes in the network. Therefore, the nodes with large degree have the higher importance in a scale-free network [35]. As a result of preferential attachment, the network gains a vast number of links attached to so-called hubs.

The most important characteristics of scale-free networks is that the degree distribution follows the power-law distribution. In scale-free network a few nodes have an extremely large degree but most nodes have only a few links. Ref [36] applies the scale-free network theory to the power networks. The result shows that power networks appear to have a scale-free network structure. The paper also reveals that power networks have a number of highly-connected "hub" buses. Based on scale-free network, Liu and Gu proposed a discrete particle swarm optimization and reconfiguration strategy for power system in [37]. The scale-free network theory is highly expected to become a new direction in power system security assessment.

C. Betweenness Centrality.

It is assumed that communication between any two nodes is done via the shortest path in a network. Then betweenness centrality of a node i as $C_B(i)$ and a link l as $C_B(l)$ are defined as follows [38]:

$$C_B(i) = \sum_{(j,k)} \frac{a_{jk}(i)}{a_{jk}} \tag{1.3}$$

$$C_B(l) = \sum_{(j,k)} \frac{a_{jk}(l)}{a_{jk}} \tag{1.4}$$

where a_{jk} is the number of shortest paths between nodes j and k, $a_{jk}(i)$ is the number of shortest paths between j and k, containing node i, and $a_{jk}(l)$ is the number of shortest paths between j and k containing link l.

If the betweenness centrality exceeds a pre-specified threshold C_B max, $C_B(l) > C_B$ max or $C_B(i) > C_B$ max , then link l or node i is overloaded and removed from the initial graph. Then all betweenness centrality is updated. The propagates of cascading failure can be approached with the iteration process goes on. In this application, an underlying assumption is that the capacity for each link and each node is the same, which is normally not feasible for a real power grid. To overcome this limitation, diversified capacity is introduced in [39]. The capacity of node i is proportional to its initial load as $C_i = (1+\alpha)a_{i0}$, where α is a tolerance parameter that denotes the ability of a node to handle increasing load in order to resist disturbances. It approves that the security analysis with betweenness centrality has the potential for further improvement by refining the efficiency index in the power model.

1.4 Research Goals

As it can be seen in the above review, the prior research of security assessment of cascading failure for power system has made some significant achievement. However, the power system is extremely diverse and complicated. It is hard to find a single model which can address all aspects of cascading failure. Here are listed several problems that are important and should be solved in future research:

1. Almost all of the past studies in the security analysis of power system have been based on a traditional power grid. Little research has been done considering the impact of RE and ES. It is already evident that the stability of power grids is greatly impacted by the unpredictable fluctuating characteristics of RE, which means the networks may be more vulnerable, especially under attacks. Therefore, the impact of RE must be considered in the future research.

2. The CN theory has already shown its great advantages in vulnerability analysis on power system. However, most of the researches with CN theory have largely ignoring the electrical quantities and power flow constraints, which is one of the most important characteristics of the power grid. In the latest research of power system vulnerability based on CN [40], the power flow constraints are adopted by electrical distance and efficiency of the transmission line. It makes progress but is still not comprehensive enough to describe the power flow in the grid.

3. Most of the former research produces high risk cascading sequences and only a small number of them considering the overall risk of cascading failure. Even in these results, the overall cascading risk is approximated by extending the single cascading risk to broader part of the power network. This does not capture the actual cascading events as they happen in the grids. So what is the reasonable way to describe the overall risk of cascading failure? And what are the cascading failure sequences of highest probability?

4. Cascades between power grids and communication networks have played a prominent role in several serious cascading blackouts which happened in past decades [41]. The power grids provide the energy for the communication networks and also rely heavily on the remote controls and operations based on the latter. However, the particular research on cascading events between power grid and communication network has

been suggested [3] but so far uses overly simplistic models. Although the power grid and communication networks have been combined more and more closely, there is little research on this topic towards a feasible modelling strategy for analysis.

These problems are complicated and diverse. Each of the problems might require different modelling, approximations, assumptions and data in order to make them tractable. It is expected that these problems can be solved with the new approaches and technologies. This is the motivation for the current research on this topic: Application of Complex Network Theory in Power System Security Assessment.

1.5 Research Contributions

The main contributions of this thesis are:

1. The impacts of different levels of the RES penetration are studied based on the future grid (FG) platform under various scenarios. Then we designed a new CN efficiency model for vulnerability analyses considering these RES impacts.

2. A new direction to improve the efficiency of the communication network in a PV-ES combined system is investigated. The second-largest Laplacian eigenvalues and degree distribution are used to explain the difference of performance during two phases. The potential of an optimal communication network topology for the system is discussed.

3. A power flow based CN model for power system vulnerability analysis is proposed. Then, a new definition of vulnerability index is introduced to identify the set of vulnerable lines in a power system. The lines with a higher vulnerability index ranking are considered to have more damage to a power grid when they trip off.

4. A new CN model and approach that aims to analyse the risk of a power system to give cascading failure is investigated. The CN factors such as topology and connectivity are added to the proposed model based on the traditional risk assessment model. Six different types of electrical failures are adopted in this model. A cascading event simulation module is designed to identify the cascading chain in the system during a failure.

5. The interactions between power grid and communication network is proposed in an updated interdependency model. The dynamic simulation demonstrates that the interdependency can sometime accelerate the cascading process.

Chapter 2

Power System Vulnerability Analysis with Distributed Renewable Energy

2.1 Introduction

In conventional power systems, large thermal power plants have provided the main actions underpinning the whole operation. Centralized control, unidirectional power flow and demand driven balancing have been the main characteristics of the traditional electricity network. The transmission networks were planned and built to ensure the demands were met efficiently (and economically) and later according to the market. The load varies across different periods of a day. However the load was able to be met by the combination of dispatch and regulation processes. Among the other requirements, power flows and dynamics are required to be within bound once and stable (for both static and dynamic aspects) in order to maintain the electricity network performing. The traditional planning and control problems, which have already been difficult tasks [42], will be further challenged with all the new features of the future grid: RES, such as WP farms, PV plants, distributed generation (DG), ES and new types of loads such as electric vehicles (EV). Meanwhile, studies on new control mechanisms that will provide a more efficient way of providing energy, to reduce the peak demand and more financial beneficial for electricity consumers are proceeding. Such applications can be seen in the utilizations of the roof-top-PV and residential-size energy storage, smart meters and smart home management and so on. In all these changes, the role of modelling and analysis related to security for large numbers of scenarios remains of

central importance. In particular, the recent CSIRO funded Future Grid project [change and choice report] presents four meta-scenarios and many sensitivities for what the grid could look like for the next decades.

Some studies on the modelling and vulnerability analysis in future grids have been seen in recent years. A study on the scenario that mixed RES generation, distributed storage and also new types of load such as EV, was made for a future zero-carbon electrical grid of Australia in 2020 [43]. In this study, RES generations such as utility-sized concentrated solar power plants and large wind farms are considered for the future Australian power grid. Analysis based on the economic aspects and highest probability of wind and solar radiation geographically was conducted. However performance, stability and security assessment of the proposed network is missing from the study, which makes this study less useful. A study in [44] from UNSW proposes scenarios of the future electricity network with 100% RES generation considering a copper plate model for the National Electricity Market (NEM). It is concluded that it is technologically feasible to rely on 100% percent of the RES for the NEM provided that NEM reliability standard is applied. They also claim that the best way of reducing peak load generation capacity is by delaying large concentrated solar power plants (CSPs) dispatch and demand curtailment.

However, all these studies need to be reevaluated against a more accurate grid presentation and stability margins. The network constraints and security issues were put aside, which makes these studies require future analysis when on the operation in the real electricity network and the future grid (FG). The unpredictable fluctuating characteristics of these renewable energy sources must have introduced new security concerns for the stability of power grids. On the other hand, new network expansion also changes the topology of power networks to accommodate these new energy sources. The new network structure with renewable energy sources integration may introduce new vulnerabilities, which unfortunately have arisen as a concern for the future [45][46]. Therefore, it is necessary to carry out vulnerability assessment for FG.

The main task of this chapter is to summarize and present stability analysis using simulations based on the future grid platform under various scenarios, represented by different levels of the RES penetration as well as demand side management (DSM) uptakes. The security of the future electricity network is the main focus here; the effects of the increasing level of RES penetration and DSM uptake on the both static and dynamic stability are studied by using the simplified South-Eastern Australian power grid. Specifically speaking, the

scenarios are categorized according to: 1). Status of the load: heavy, medium and light; 2). Penetration level of the RES; 3).Uptake level of the DSM; 4).Locational, operational and economic factors. The simulation results reveal some important points in the power system stability assessment for the FG feasibility studies.

The remainder of the chapter is organized as follows: in the Section 2.2, the Australian NEM model and the demand side management model is briefly described. Detailed simulation scenarios measures and results are demonstrated in this part. The basic measures of power system CN model is described in Section 2.3. The simulation results are presented in the Section 2.4, followed by the analysis and discussions that are revealed from the simulation results.

2.2 Impact of High Renewable Penetration in Australia Future Grid

The starting point of our studies is the observation that to the best of our knowledge, no international research so far has developed a standardized comprehensive modelling framework for future grids close to what we have been accustomed to for classical systems; a suite of definitions, equations and software for power flow, stability analysis, dispatch, security and reliability. Well-known software in dynamics and market modelling such as PSS/E and Plexos respectively have included new features to cover renewables, particularly wind and PV. The newer analysis software such as DIgSILENT has been developed from the outset with future grids in mind, especially in modelling renewable energy. Thus, this study is based on Plexos for 14-Genertor for NEM market simulation and then DIgSILENT for balancing and stability simulation and analysis.

2.2.1 The Simplified 14-Generator Model of South-Eastern Australia Power System

The simplified 14-Generator, 50 Hz system model for the South-Eastern Australian grid is illustrated in Fig. 2.1 [47]. This model was originally developed for small disturbance stability studies. For convenience, it has been divided into 5 areas which stand for [47]:

- Area1: Snowy Mountains
- Area2: New South Wales (NSW)
- Area3: Victoria (VIC)
- Area4: Queensland (QLD)
- Area5: South Australia (SA)

Areas 1 and 2 are more closely coupled. Thus, there are in essence 4 main areas and hence 3 inter-area modes, as well as 10 local-area modes. AEMO has proposed this network be modelled in forms of 16 zones for the NEM as shown in the Fig. 2.1.

A. The stability analysis model with RES

In order to make a model which can serve the purpose of the study, the 14-Generator Model was rebuilt in a DIgSILENT environment with the following enhancements [48][49]:

- The capability to add solar thermal, PV or wind farm at all buses of the grid, including possible grid extensions;
- The traditional generator models have also been enhanced to allow a wider range of dynamic studies than just small-disturbance stability;
- The capability to include the demand-side representation of load, storage and demand-response at city level.

The modelling framework aims to be very flexible for considering scenarios of RES placement, randomly or from specific proposals, and optimizing which ones will provide the best overall performance. In this chapter, we illustrate this flexibility with additional RES at nodes in the four main areas. The traditional generators are replaced by RE sources with different percentages of their capacity to see the impact on performance.

According to the practical data in Australia, we can select the following nodes to accommodate the renewable energy sources.

- SA: Node 501; NPS-5; Wind Farm 1: Lake Bonney

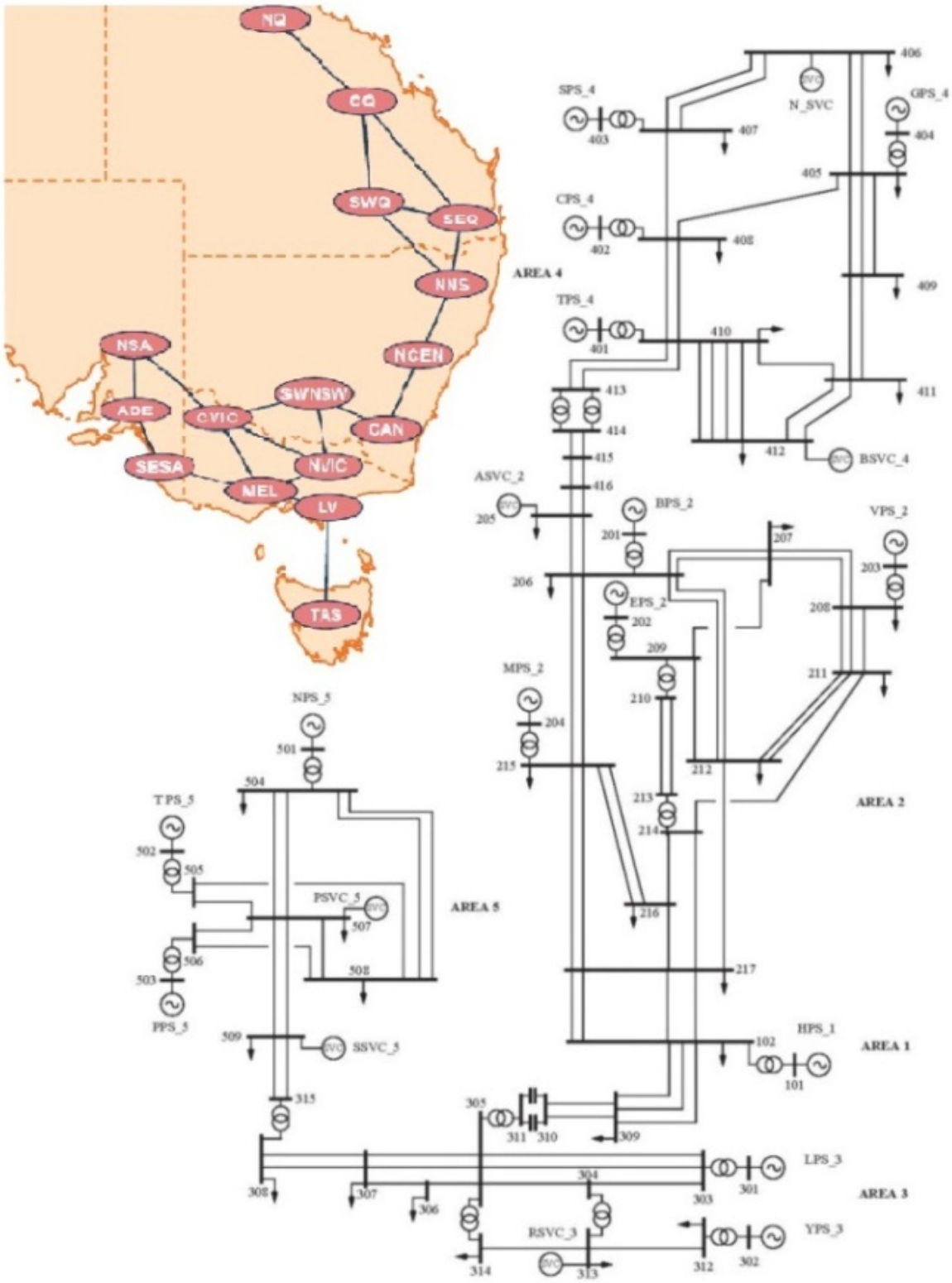

Fig. 2.1 The simplified 14-generator model of the SE Australian power system.

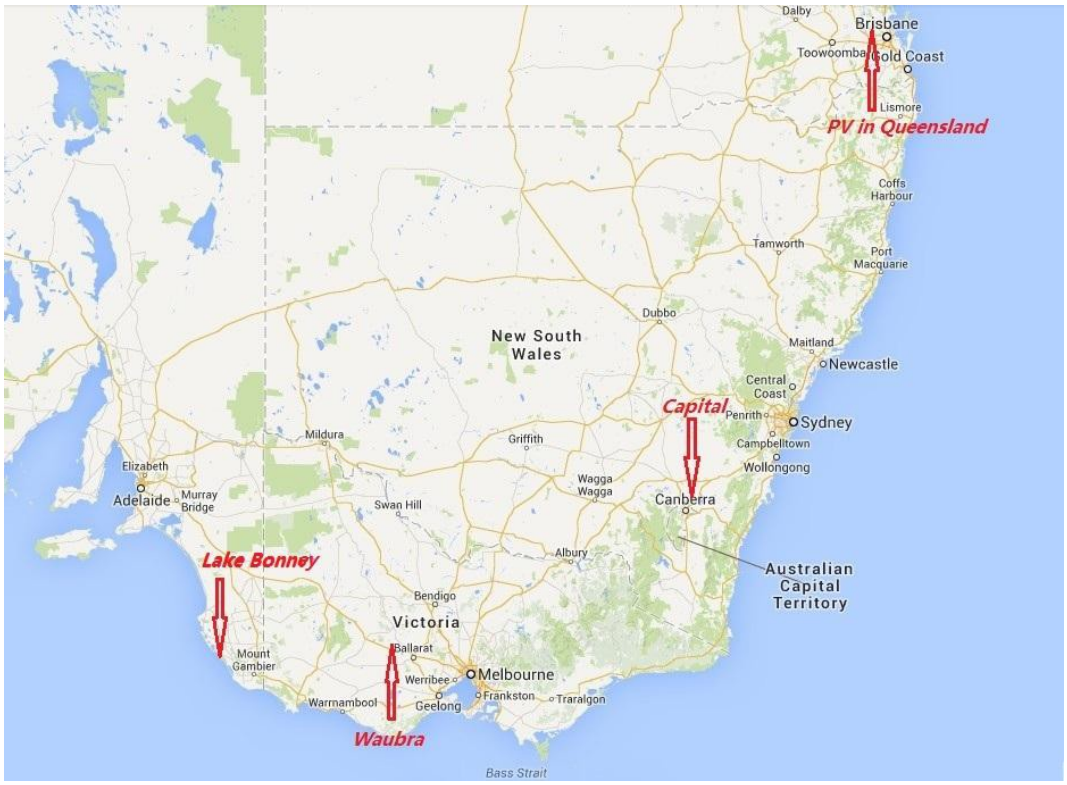

Fig. 2.2 Locations of the 4 renewable energy resources in SE Australia

- VIC: Node 301; LPS-3; Wind Farm 2: Waubra
- NSW: Node 204; MPS-2; Wind Farm 3: Capital
- QLD: Node 401; TPS-4; Photovoltaic Power Station

The geographic positions of the four power stations are shown in Fig. 2.2:

The scenarios are divided into two categories, i.e. 1) Power flow calculation under steady operation conditions and the 2) Transient analysis under short circuit conditions. Both of the two categories are performed for different penetration levels of sustainable energy sources.

To simply represent the change of actual load, we divided the daily load curve into three different levels, i.e. light load level (0 am-8 am, 22 pm-0 pm), medium load level (9 am-17 pm) and heavy load level (18 pm-21 pm) respectively. In each scenario, the wind and photovoltaic farms replace traditional generators in 10%, 20%, 30% and 40% of their capacity at each specified nodes, namely Node 501, Node 301, Node 204 and Node 401.

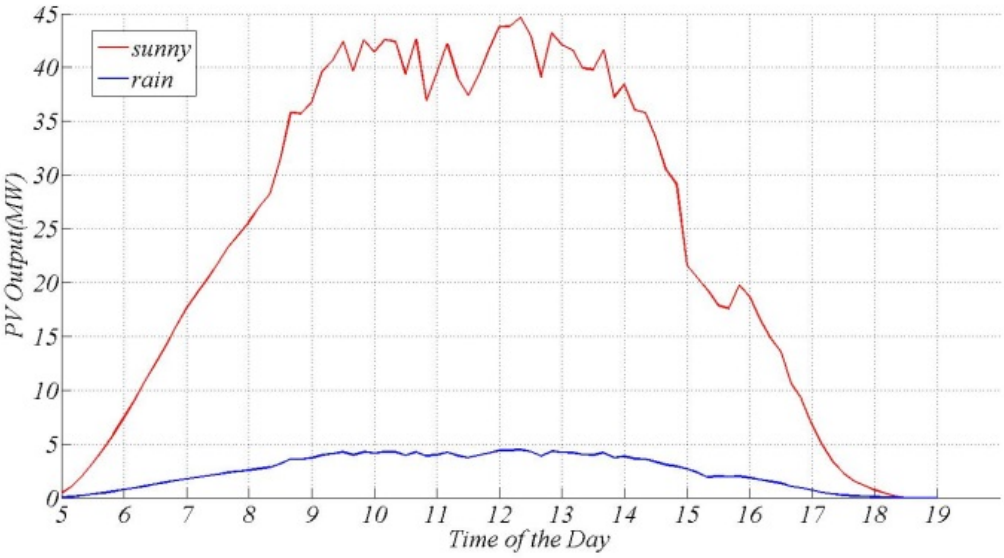

Fig. 2.3 The real-time PV power output within a day

By calculation, the penetration levels are 3.23%, 6.46%, 9.68% and 12.92% accordingly in terms of the energy generated.

In different time points of a day, the power outputs of wind/PV farms shown in Fig. 2.3 and Fig. 2.4 are drawn from the real-time data of online reports (Wind Farm Performance and UQ SOLAR Photovoltaic Data) [50][51] and scaled to different scenarios. From the practical power output data, the corresponding capacity factors of different generators have been converted throughout the day [49][52].

B. Demand side management model

The demand side management model is also analysed in this study under future grid scenarios. In order to do that, firstly, the market simulation is done by PLEXOS, which is a well-known market simulation software. The scenario is based on the dispatch process from AEMO. The model is designed based on the residential level then aggregated into different levels of the NEM future grid model according to the requirement for different study purposes. Specifically speaking, the model that we designed is a decision making optimization program where the decision can be computed at each household in order to achieve the objective of minimizing electricity bills. Mathematically, the model can be described as an optimization problem where the objective function and constraints can be described as follows:

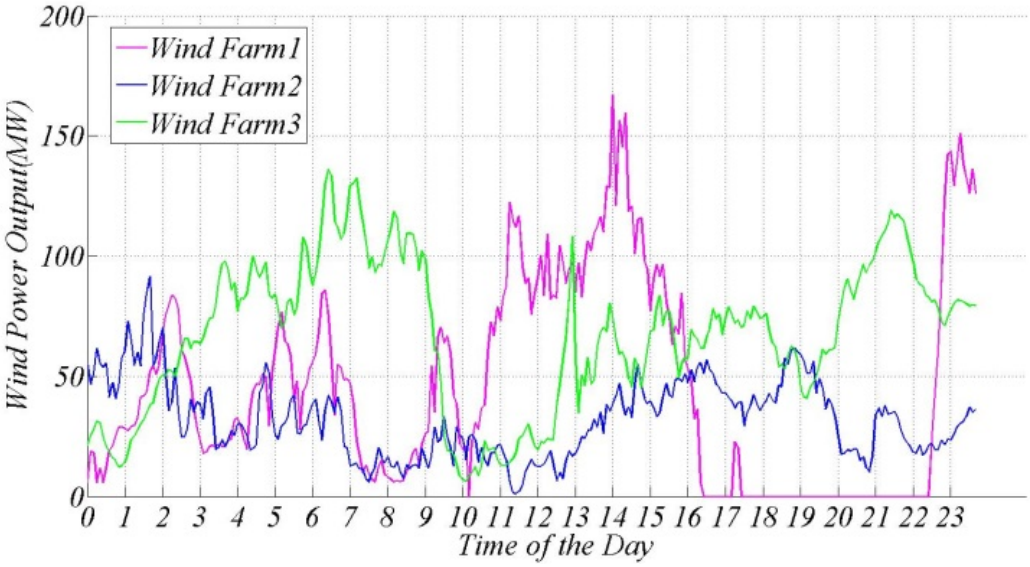

Fig. 2.4 The wind farm power output within a day

$$\min \quad C_i = \sum_{k=1}^{K} \lambda(k) * \left(A_i^k + E_i^k - P_{pv,i}^k\right) \tag{2.1}$$

$$\text{s.t.} \quad A_i^k \in \left[m_i^k, M_i^k\right] \tag{2.2}$$

$$E_i^k = \text{SOC}(k+1) - \text{SOC}(k) \tag{2.3}$$

$$Q_i^- \leq E_i^k \leq Q_i^+ \tag{2.4}$$

$$P_{pv,i}^k \geq 0 \tag{2.5}$$

where C_i denotes the electricity bill of the user i for the studies time period, normally a day and $K = 24$. Here is the list of notations:

- $\lambda(k)$: the rate of purchasing electricity from /selling electricity to the grid at time slot t;

- A_i^k: the electricity consumption of all appliances of user i within time slot k;

- $P_{pv,i}^k$: the photovoltaics system generation of user i within time slot k;

The constraint $A_i^k \in \left[m_i^k, M_i^k\right]$ shows that the total consumption of household i in time slot k should be between the minimum and maximum consumption value; (2.3) and (2.4) represent that constraints on the state of charge SOC and maximum charge/ discharge rate Q_i^- and Q_i^+ respectively. The term $A_i^k + E_i^k - P_{pv,i}^k$ actually equals to the amount of electricity that is exchanged with the grid from user i in time slot k, denoted by $P_{g,i}^k$. Therefore it indicates that the user i purchases the electricity from the grid at time slot k when $P_{g,i}^k \geq 0$; and the user i sends back the electricity to the grid when $P_{g,i}^k \leq 0$. The price is assumed to be according to Time of Use (ToU) and the consumers are only considered as the price taker at this stage.

Later this demand side model is aggregated to represent many households at the city level in order to analyse the scenarios when the demand side management is considered into the FG stability study.

2.2.2 Steady-State Calculation and Analysis

The primary analysis tool for steady-state operation is power flow analysis, where the voltages (magnitude and phase), line power flows and losses in the system are determined. This analysis is widely used for both operation and planning studies throughout the system i.e. both transmission and distribution systems. Also, some typical scenarios suggested by the recent CSIRO Future Grid Forum (FGF) [53], Zero Carbon Australia Report [54] and the AEMO 100% Renewables report [55] will be effectively analysed. The terminology for scenarios is taken from the FGF report [53].

A. Renewable thriving

It is well known that Australia has an abundance of renewable energy resources, such as wind, solar, geothermal etc. The scenarios that represent the increasing to high usage of renewable energy sources have been formed. The purpose of this study is to reveal the impact of "renewable thriving" under different penetration levels of RES considering the integration of DG and ES (residential size).

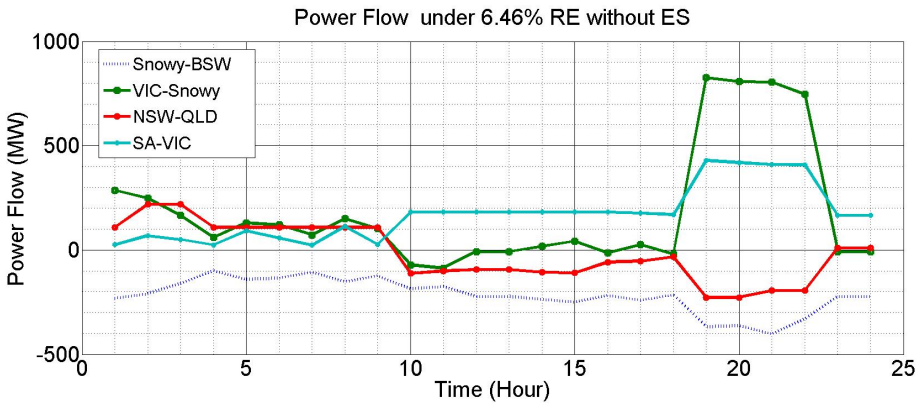

Fig. 2.5 The power flow distribution under 6.46% renewables without energy storage

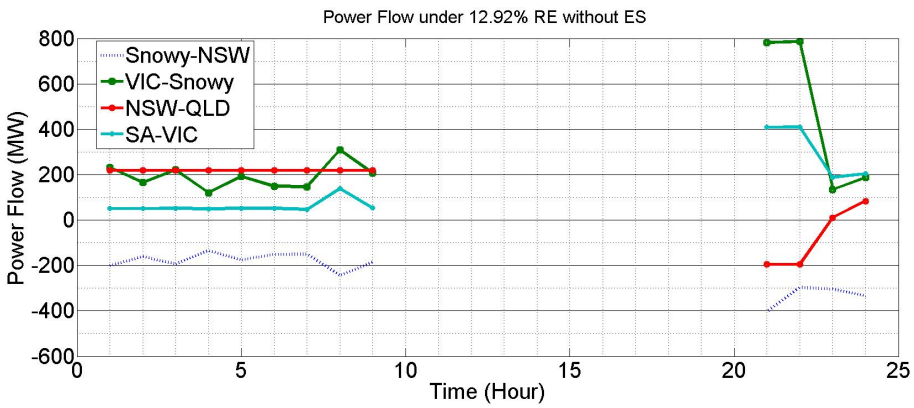

Fig. 2.6 The power flow distribution under 12.92% renewables without energy storage

Therefore the scenarios are formulated at the same location under different levels of renewable penetration and then compared to find out whether the system is stable in the name of steady-state power balance viability. The stability of the system is indicated by the non-convergence period in this study.

Fig. 2.5 and Fig. 2.6 show the power flows on an inter-connected transmission line under the RE penetration level of 6.46% and 12.92% without ES respectively. It can be seen that that under higher penetration level of renewables without energy storage integrated, the power flow cannot converge in certain periods, i.e. 11:00-21:00. It is because the intermittent characteristic of these renewables may incur imbalance between active power generation and consumption.

B. Rise of the prosumers and distributed energy storages

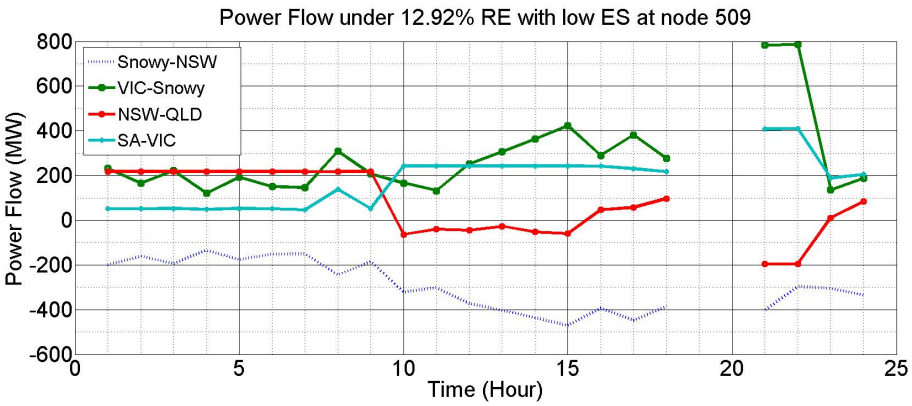

Fig. 2.7 The power flow distribution under 12.92% renewables with 40% energy storage

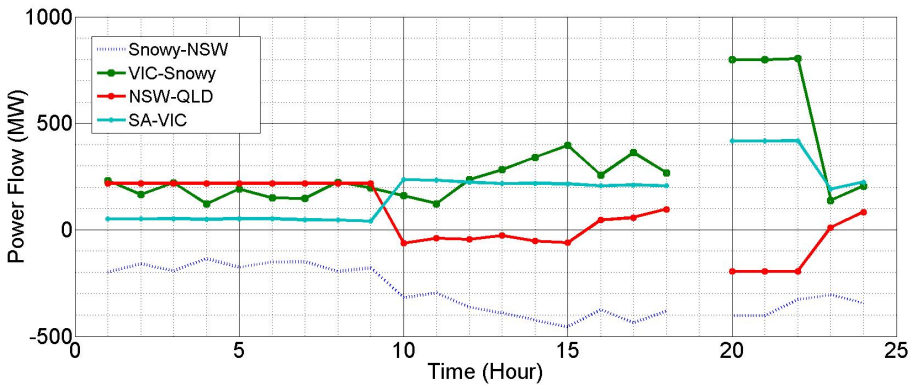

Fig. 2.8 The power flow distribution under 12.92% renewables with 80% energy storage

Prosumers are the residential customers who also supply their own electricity. The sustained high retail prices of electricity, falling costs of solar roof-top panels and increasingly innovative financing and product packaging from energy services companies are anticipated to lead to a large increase in the scale of on-site generations. In this study, the demand-side model has been aggregated into the city level. Parameters in this model can capture the percentages of uptake for the technologies involved.

The figures show when accumulated energy storage is integrated into some critical loads (such as Sydney city). Here, 40% or 80% of energy storage represent that there are 40% or 80% of the households in the selected area are installed with distributed PV-Battery system. It should be noted that this only represents the uptake by the connected nodes. Hence the figures are different from the definition of renewable penetration level. The non-convergence problem of power flow could be dramatically alleviated, which can be seen from Fig. 2.7 and Fig. 2.8 that the power flow non-convergence period time is reduced significantly. Also with

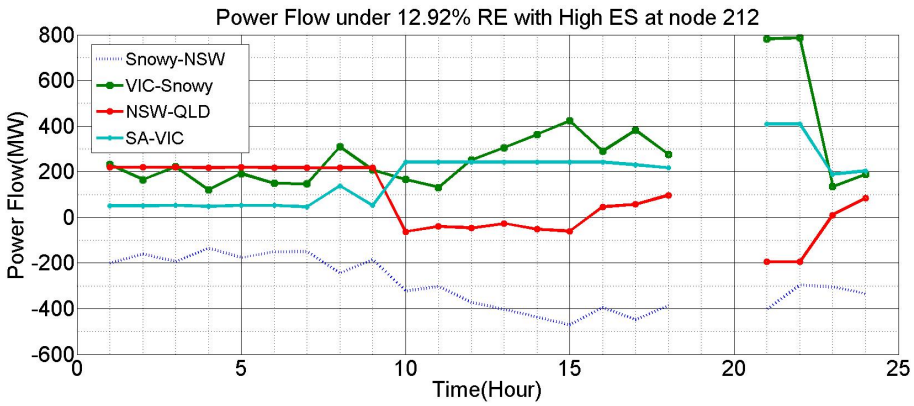

Fig. 2.9 The power flow distribution under 12.92% renewables with 80% energy storage at node 212

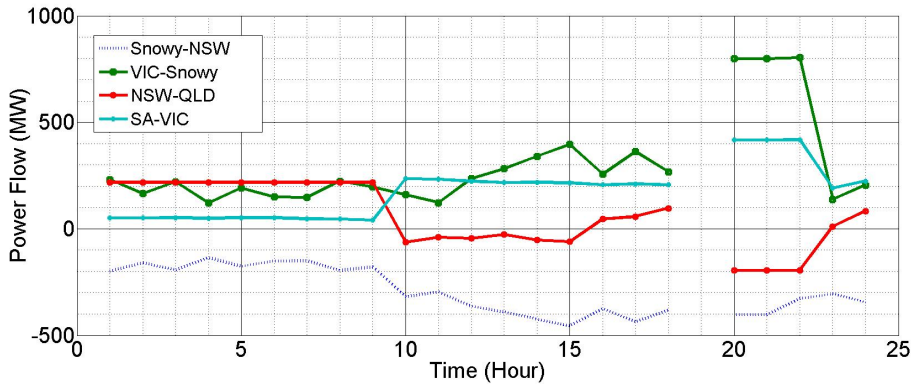

Fig. 2.10 The power flow distribution under 12.92% renewables with 80% energy storage at node 509

the increase of penetration level of energy storage, the supporting function also strengthens, making the non-convergence time shorter (from 2 hours to 1 hour). Therefore, the optimal dispatch of energy storage can indeed help the system survive from the unbalance situations in the future with high penetration level of intermittent renewable resources.

C. Impact of location of the distribution renewable energy and energy storage

The simulations also show that with the same energy storage modelling, same renewable energy generation penetration level and the same energy storage level, the impact of the energy storage to the grid could vary according to the location of the load.

It can be seen in Fig. 2.10 that when the energy storage devices are integrated in node 509 (remote load), power flows in 8 pm converge. On the other hand, as in Fig. 2.9 when

the energy storage in placed in node 212 (load centre), the power flows do not converge in 8 pm. This could indicate with same level of renewable energy penetration and ES uptake, the stability in different for different locations.

2.2.3 Dynamic Simulation and Analysis

Power system dynamic analysis aims to analyse the ability of an electric power system to regain a state of operating equilibrium after a physical disturbance for a given initial operating condition. The basic security requirement after balancing (energy, power and ramping) is maintaining adequate stability margins (angle, voltage, frequency) for specified contingencies. Power system stability for classical grids can be divided into three types [56], voltage stability, (rotor) angle stability, frequency stability.

In this section, the preliminary results on stability are presented. The dynamic analysis is done under different RES penetration levels without considering DG or ES in this stage. As mentioned above, different stabilities have been assessed in DIgSILENT, and the results are shown as follows.

A. Voltage Stability

Voltage stability analysis can be classified as large disturbance voltage stability and small disturbance voltage stability. Large disturbance voltage stability refers to the system's ability to maintain steady voltages following large disturbances such as system faults, loss of generation, or circuit contingencies. Determination of large-disturbance voltage stability requires the examination of the nonlinear response of the power system over a period of time sufficient to capture the dominant voltage dynamics. Small disturbance voltage stability refers to the system's ability to maintain steady voltages when subjected to small perturbations such as incremental changes in system load. This form of stability is influenced by the characteristics of loads, continuous controls, and discrete controls particularly voltage regulators.

Voltage stability analysis is studied with both large disturbances and small disturbances, where a short circuit is selected for the large disturbance and a reduction on the system load is used for the small disturbance analysis.

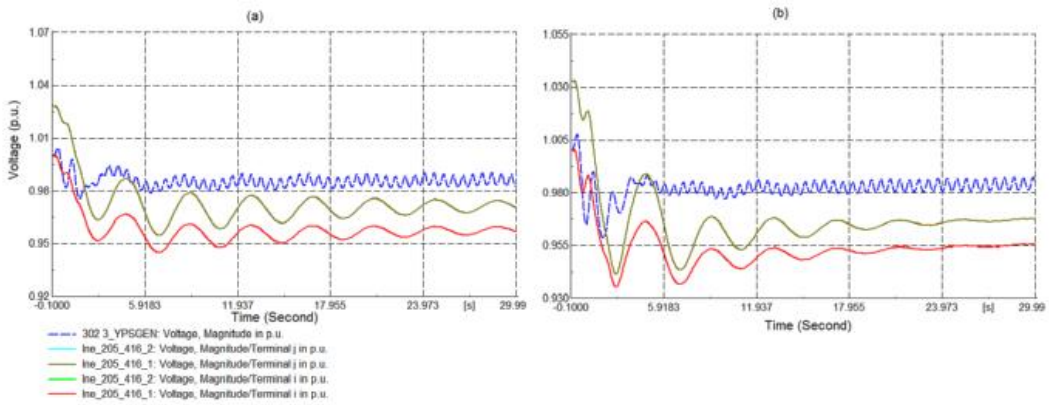

Fig. 2.11 Voltage stability with different RES penetration under small disturbance (a) 6.46% RES penetration (b)12.92% RES penetration

It can be seen from Fig. 2.11 that with the increase of penetration level of RES, the voltage stability under small disturbances gets worse. On the other hand, under large disturbance there is no significant change in voltage stability. It seems for this case the voltage stability under small disturbance is more sensitive to RES. The voltage dynamic performance deteriorates significantly due to the lack of reactive power support provided by the inverter-based RES when the penetration level increases.

B. Rotor Angle Stability

Rotor angle stability refers to the ability of the synchronous machines of an interconnected power system to remain in synchronism after being subjected to a disturbance. It depends on the ability to maintain/restore equilibrium between electromagnetic torque and mechanical torque of each synchronous machine in the system.

Compared with voltage stability, Fig. 2.12 shows that the RES does not show that much impact on rotor angle stability here. Even if there are some oscillations after the disturbance, they remain at an acceptable level and can achieve a new situation to keep system stable. We can see the dynamic behaviour is insensitive with regard to the increasing penetration level of RES. This suggests that rotor angle stability is a complex problem associated with diverse contributing factors.

C. Frequency Stability

Frequency stability refers to the ability of a power system to maintain steady frequency following a severe system upset resulting in a significant imbalance between generation and

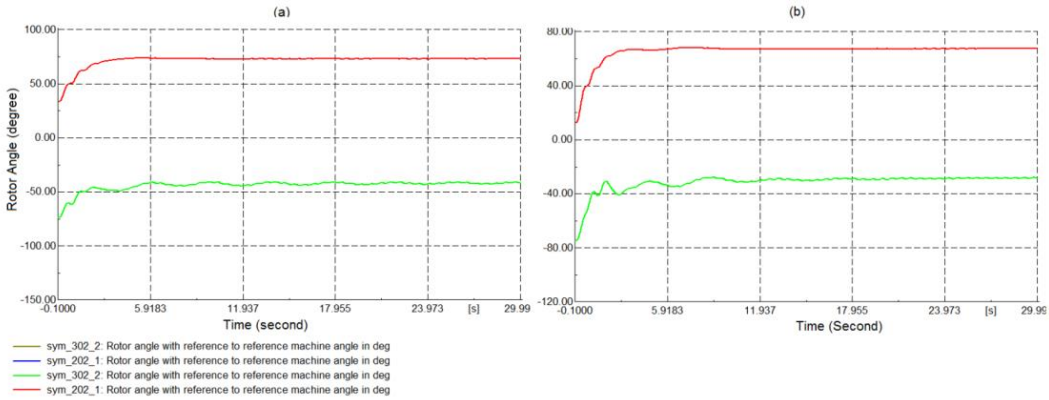

Fig. 2.12 Rotor angle Stability with different RES penetration under small disturbance (a) 6.46% RES penetration (b)12.92% RES penetration

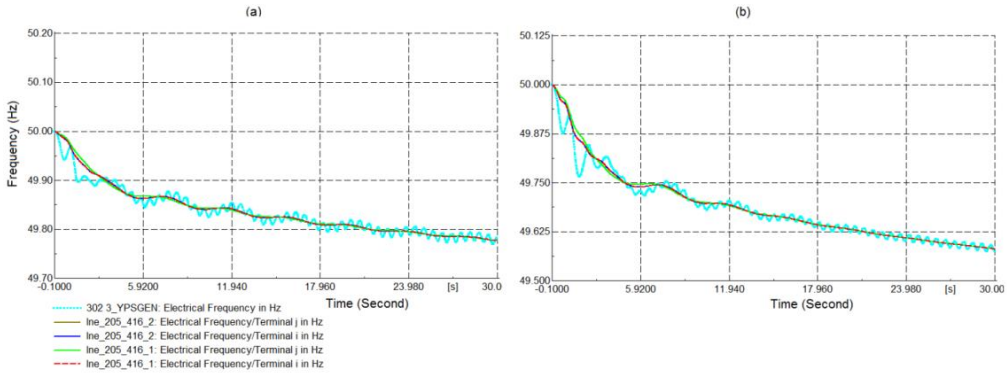

Fig. 2.13 Frequency stability with different RES penetration under small disturbance (a) 6.46% RES penetration (b)12.92% RES penetration

load. It depends on the ability to maintain/restore equilibrium between system generation and load, with minimum unintentional loss of load. Instability occurs in the form of sustained frequency swings leading to the tripping of generating units and/or loads.

Fig. 2.13 shows that the frequency stability of the system decreases gradually with the RES penetration level increase under disturbance. Also under the higher RES penetration level, the frequency change is faster compared with lower level. This may be caused by the inverter-based RE reducing the rotational inertia so that the active power balance is accelerated. This will require some new control system to maintain the frequency in future grid with high penetration level RES to balance the active power.

2.3 Power System CN Model

According to complex networks theory, a graph can be used to describe the physical connection of a power grid. Based on the topology of a power grid, a graph G with N nodes and K edges can be formed. The graph G is denoted by an $N \times N$ adjacency matrix W_{ij} describing the physical connections of the network. If there is an edge between nodes i and j , W_{ij} is set to 1, otherwise 0. The geodesic path d_{ij} between two nodes i and j is defined as the shortest path between them. The efficiency e_{ij} between nodes i and j is the reciprocal of the geodesic path. This means that the larger the d_{ij} is, the less efficiently the information can spread between the two nodes. If there is no path between nodes i and j, $e_{ij} = 0$. Once the efficiency is defined, the average efficiency of a network can then be given by:

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} e_{ij} \tag{2.6}$$

The $E(G)$ is usually applied to assess the vulnerability of a network [57]. The index can reveal how the network efficiency changes before and after disturbances. For this purpose, the load at a node i is defined as the total number of the geodesic paths passing through this node. An important feature of the model is to allocate a given capacity to each node, i.e., the maximum limit of load that a node can bear. The capacity C_i of a node i is assumed as directly proportional to the initial load carried by i,

$$C_i = \alpha L_i(0) \tag{2.7}$$

where α is a tolerance parameter. Ref. [57] shows how the damaged efficiency of a power grid changes with different α under attacks. The $L_i(0)$ is the initial load handled by node i, and it is also the initial load at iteration step $t = 0$. In most complex networks, an initial failure may cause a cascading effect and result in cascading failures. In the complex network model, the removal of a node (initial failure), will change the geodesic paths between nodes, then lead to the changes of L_i and C_i. This effect would cause some other nodes to become overloaded and then fail. These new failures would alter the geodesic paths and load of other nodes again. This progress would continue until no overloaded nodes exist. At each iteration step t, the following iterative rule is adopted [58][59]: network efficiency

$$e_{ij}(t+1) = \begin{cases} e_{ij}(0)\frac{L_i(t)}{C_i} & \text{if } L_i(t) > C \\ e_{ij}(0) & \text{if } L_i(t) \leq C \end{cases} \tag{2.8}$$

where j extends to all nodes that are connected to node i directly. At each step t, if node i is overloaded, the length of all the edges connected to it is increased. This rule can degrade the transmission capacity of node and thus decrease the efficiency of whole networks.

2.4 Vulnerability Analysis Given Renewable Energy Integration

In Fig. 2.3 and Fig. 2.4 we show the practical daily output of PV and outputs from three wind farms located in different places in Australia [60]. It is easy to find that the output of PV concentrates during the noon time, and fluctuates during its peak. As it is greatly impacted by weather conditions especially cloud cover. The wind power output mainly depends on the location of wind farm. The intermittent and unpredictable characteristics of renewable energy sources should have an impact on the vulnerability of power networks.

In order to better make vulnerability analysis allowing for RE, we modify the complex network model in Section 2.3. For distinguishing the nodes that have connected renewable resources from others, a set $\{R\}$ is defined. A node $u \in \{R\}$ means that the node is connected with a renewable energy generation source. The traditional generation in the grid is denoted as $G^{'}$.

To demonstrate the impact of RES variability on power system vulnerability, the modified model is employed here [61]. The DC power flow equation [62] is usually adopted as a rapid approximation technique to represent the relation between node power angle and real power injection in a high-voltage transmission network.

$$P = B\theta \tag{2.9}$$

where P, B and θ are the node real power injection vector, the bus susceptance matrix and the node power angle vector, respectively. In this modified model, the notion of power angle deviation is used to redefine the load at node u:

$$L_u(t) = \frac{N(\theta_u(t) - \theta_{\min}(t))}{\sum_{u \in N}(\theta_u(t) - \theta_{\min}(t))} \tag{2.10}$$

where from (2.9) we can get $\theta = [B]^{-1}P$, which will be affected by the output factor of renewable energy sources from time by time. The subscript "min" represents the minimum θ among N. Usually the reference node in the grid has the minimum θ. Similar with (2.7) in the traditional model, the capacity C_u of a node is proportional to its initial load:

$$C_u = \alpha L_u(0) \quad u = 1, 2, \cdots, N. \tag{2.11}$$

The iterative rule introduced in (2.8) is also adopted at each iteration step during the dynamic evolution here. Then the average efficiency of the network can then be given by:

$$E = \frac{1}{N_R N_{G'}} \sum_{u \in N_R} \sum_{v \notin N_R} e_{uv} \tag{2.12}$$

At the end of cascading failures, the damaged efficiency D is used to describe the normalized efficiency loss during the cascading failures[61].

$$D = \frac{E_0 - E_f}{E_0} \tag{2.13}$$

where E_0 is initial efficiency and E_f is the final efficiency after cascading failures. Therefore, we can assess the vulnerability of a network by observing the D at different iterative steps t. The modified form (2.12) compared to (2.6) is designed to focus on the node power angle changes caused by the variability characteristics of RES in assessing overall vulnerability.

In order to study the impact of renewable energy sources on network vulnerability, the Simplified 14-Generator Model of the South Eastern (SE) Australia Power System (14-Generator Model) [47] is employed for numerical simulations. The system consists of 14 generating units, 58 load buses and 180 transmission lines.

Table 2.1 Three normal steady-state operating conditions

Load Condition	Light Load	Medium Load	Heavy Load
Total Generation MW	15050	19060	23030
Total Load MW	14810	18600	22300
Area 4 to Area 2 MW	-200	300	500
Area 2 to Area 1 MW	470	740	1134
Area 1 to Area 3 MW	200	-200	1000
Area 3 to Area 5 MW	200	250	500
Time in the Day	01:00 - 09:00	09:00 - 17:00, 22:00 - 24:00	17:00 - 22:00

The power grid model with renewable energy sources integration is constructed in by DIgSILENT. The real power injection vector P represents the amount of traditional generators generation and load at each node under three load operating conditions which shown in Table.2.1, are obtained from the standard data files of the 14-Generator Model [47]. The power outputs of renewable energy generators have been taken as the average for each hour, which are obtained from practical Australia WP and PV data files [60][51]. The tolerance parameter α is set as 1.05 in this simulation.

The numerical simulations have been done for each hour during the day under different penetration levels of renewable energy, 0%, 10%, 20%, 30% and 40%. Fig. 2.14 and Fig. 2.15 show the damaged efficiency of the power grid under a targeted attack and a random attack given different penetration levels of renewable energy respectively. The random attack curves are gained by averaging 58 individual removals. The targeted attack curves are obtained by removing the highest loaded bus, i.e. the bus 212.

From the simulation outcomes, it can be seen that the curve of damaged efficiency rises with the increase of load condition under both random attack and targeted attack. Obviously, targeted attack can cause more damage to the power grid and more reduction of the efficiency. Again it verifies that power networks have the characteristics of scale-free networks. On the other hand, with the penetration level of renewable energy increasing, the damaged efficiency also increases. The actual power outputs from renewable resources are usually intermittent. Particularly PV is not able to generate any energy after sunsets which are more likely to be the

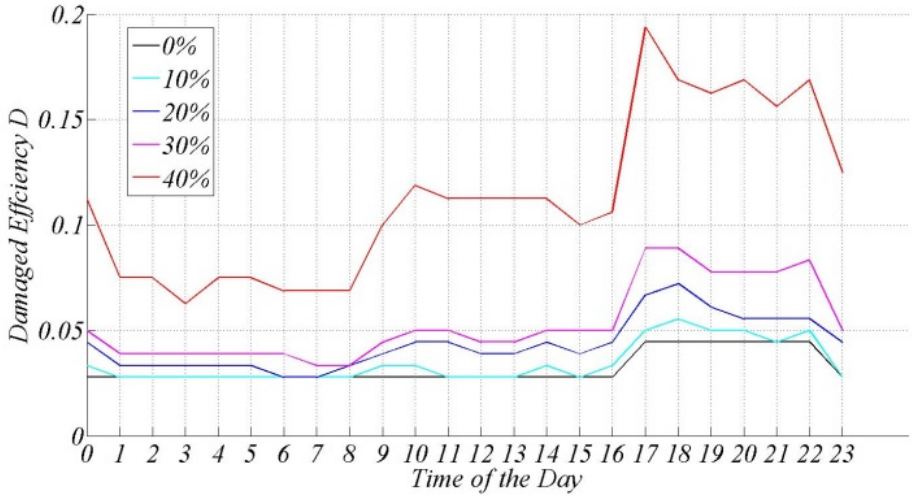

Fig. 2.14 Damaged efficiency in 14-generator model under random attack

peak load period of a day and all the gaps have to be compensated by traditional generators. Thus, the resulting oscillation of power flows in transmission lines would deteriorate with the increase of the penetration level and would be likely to spread cascade failures to larger areas in the power grid. Therefore, it can be seen from Fig. 2.14 and Fig. 2.15 that the maximum damaged efficiency appears at 18:00 in both random and targeted attack scenarios.

Besides, the renewable energy makes different influences in the damaged efficiency of power networks under random and targeted attacks. Fig. 2.16 shows the varying pattern of random and targeted attacks in the same time points (with the same load condition and output). When the renewable energy is set at a low penetration level (10% and 20%), the changes of the performance under random attack is less severe and have long tails. On the contrary, the curves change more dramatically under targeted attacks. It seems that the vulnerability of the grid is more sensitive to the penetration level of renewable energy under targeted attack. Such behaviour can also been disclosed in the 30% curve of Fig. 2.16 under targeted attacks. Meanwhile, the changes in damaged efficiency become more obvious when the penetration is over 30% under the random attacks. However, when the penetration level comes to 40%, the damaged efficiency under random attack shows significant changes. The curve rises more steeply during peak hours. Based on these results, we may come to the conclusion that the power network may have a threshold on the penetration level of the renewable energy. This threshold is associated with the topology and parameters of the network. If the value of renewable energy connected into the network is over such threshold, the network may no longer be robust to random attacks.

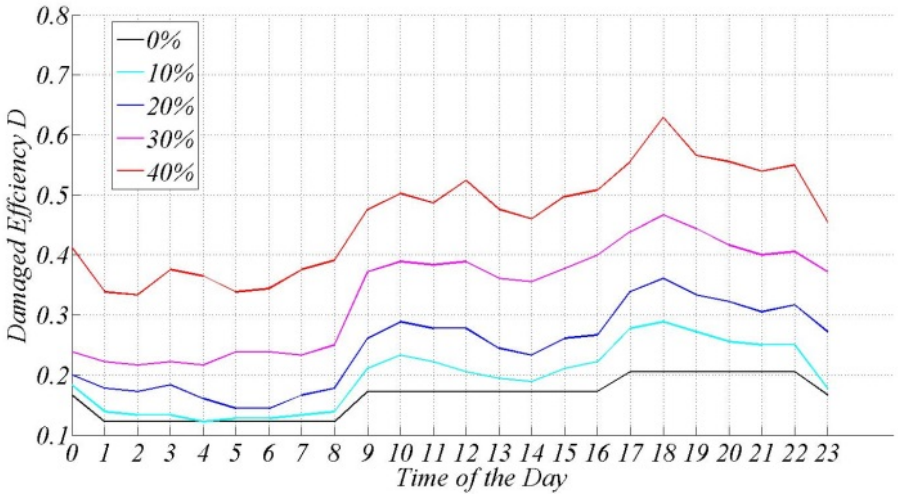

Fig. 2.15 Damaged efficiency in 14-generator model under targeted attack

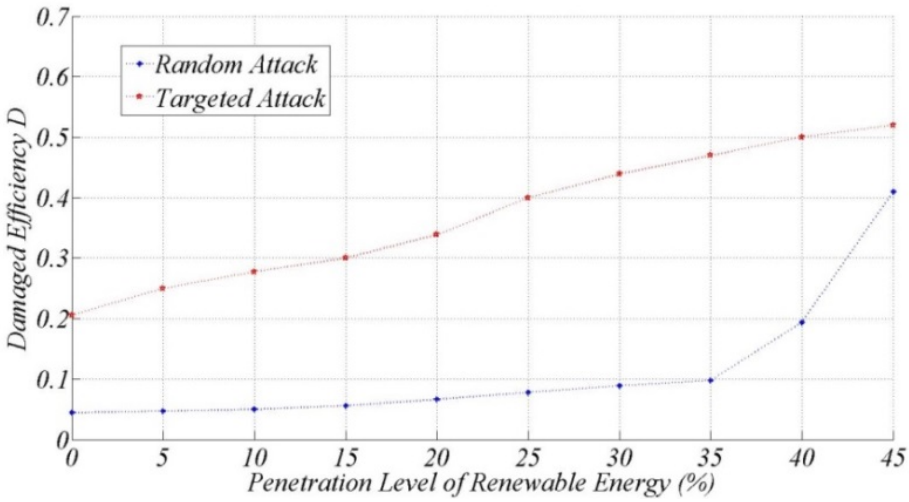

Fig. 2.16 The changes of damaged efficiency in 14-generator model with different penetration level of RES

But it is also clear that this issue needs to be studied with more refined vulnerability indices than (2.12) and (2.13). The reactance and admittance of the transmission line are not enough to describe the electrical characteristics of a power system. The DC power flow and power angle vector also has inadequacy to present the actual power transmission. Based on the new concepts, an improved model for power system security assessment is needed to overcome the those issues.

2.5 Summary

In this chapter, a simulation platform for Australian future grid with high penetration level RE scenarios is firstly presented. Then a series of simulations is designed to show the impact of high penetration level RE to the system. The simulation results show that in steady state the penetration level of RE and the locations of ES play a very important role. These two factors will impact the result of power flow calculation greatly. In the aspect of voltage stability, the performance deteriorates significantly due the lack of reactive power. The results show rotor angle stability is insensitive with regard to the RES penetration level. In terms of frequency stability, during disturbance the frequency change speed becomes faster because of the increasing inverter based RES.

In this context, we proposed a modified CN based vulnerability analysis model to demonstrate how the RES impact the vulnerability of the grid. From the simulation results, the conclusion can be drawn that the grid would suffer more serious vulnerability under attacks with the growth of renewable energy integration. In other words, the vulnerability of power network deteriorates. Compared with random attacks, the vulnerability is more sensitive to the penetration level of RE under targeted attacks. Also, we found there is a threshold on the network being robust to random attacks. We should consider those factors in the FG design and planning. However, the electrical efficiency model is obviously insufficient for power system security assessment. We will introduce our improved models and indices in the later chapters.

Chapter 3

Communication Network Topology Analysis in Power System

3.1 Introduction

As we mentioned in Chapter 2, the number of distributed PV and energy storage (ES) devices is increasing in future distribution networks. In a smart grid environment, small-scale distributed generation. Such as, the household rooftop PV in Australia [63] has demonstrated their popularity so far. Nevertheless, most of the distribution system is designed based on the assumption that the substation is the only source of energy. In the new PV-ES combined system, this distribution system has to face new challenges [64].

On the other hand, the scattered ES devices have also been receiving growing attention because of their falling price. They can be utilized as an effective "buffer" to help the system alleviate these problems if an appropriate control approach is adopted. In this context, the concept of "multi-agents" and distributed algorithms can be adopted because these distributed facilities can be regarded as small "agents". Those "agents" can exchange information with their neighbours through the communication networks among them. In this situation, the economic performance should be taken into account simultaneously.

There is already considerable existing literature discussing the different types of distributed optimization approaches to solve related problems. In Ref [65], conceptual frameworks for involving highly distributed loads in power system control actions is proposed. Besides cen-

tralized, hierarchical, and distributed control architectures are discussed along with benefits and disadvantages. Mashhour et al. [66] studies distributed energy resources by maximizing virtual power plant total profit subject to individual distributed energy resources and system operating constraints. Also a lot of research works based on distributed optimization algorithms have been studied, including the comparison between their convergence rate, accuracy, capability, etc.

However, it appears that no analyses have investigated these issues in terms of the communication network topology, especially the influence on the overall performance of the distributed algorithms. In this context, we investigate a new direction that aims at improving the efficiency of distributed optimizations in PV-ES combined system by analyzing the topology of communication network in this chapter. We use the second-largest Laplacian eigenvalues and degree distribution to explain the difference of performance during two phases. The potential of using optimal communication network topology for the system is also discussed in the latter part of this Chapter.

The remainder of this chapter is organized as follows: Section 3.2 lists the mathematical model of distributed PV-ES combined system. In Section 3.3, the approach of distributed alternating direction method of multipliers is explained. Section 3.4 demonstrates several typical topologies of communication networks. It also compares the merits of different topologies. Section 3.5 demonstrates simulation results and shows the different performance during iteration. It also gives a discussion about effect of basic graph characteristics of topology on the performance of distributed optimization. Finally, Section 3.6 gives a brief summary.

3.2 Mathematical Modelling

In our research, we take the basic optimization problem described in paper [67] as a reference model. In the future distribution network, each "agent" purchases (or sells) electric power from (or to) the distribution system and then sells the electric power to the customers. They will maximize their profit by determining the power outputs of all distributed energy resources, subject to the constraints of supply and demand balance, line flow limits, and distributed energy resources capacity limits. A simplified model is shown in Fig. 3.1.

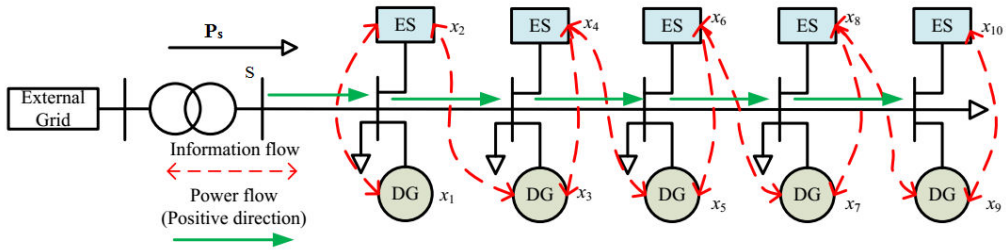

Fig. 3.1 Future distribution network with DG and ES

The mathematical model of this problem is formulated as follows:

$$f = -\rho_E P_s + \sum_{n=1}^{N} \left[\rho_d P_{dn} - C_{gn}\left(P_{gn}\right) - C_{rn}\left(P_m\right)\right] \tag{3.1}$$

where P_s is the power injection from the distribution grid to PV-ES combined system and node S is called the interface node through which the PV-ES combined system is connected to the distribution system. If P_s is negative, it represents the injection from PV-ES combined system to the distribution system and vice versa. The demand, distributed PV generation power, and ES output power at node n are denoted as P_{dn}, P_{gn}, P_{rn}, respectively. Then, the cost functions of distributed PV and ES are defined as C_{gn} and C_{rn}. The pre-assigned wholesale market price and PV-ES combined system retail price are defined as ρ_E and ρ_d, respectively. They are determined by bargaining between the PV-ES combined system and distribution system/customers. Then the optimization of the cost function (3.1) is to maximize f under following power constrains:

$$\sum_{n=1}^{N} \left(P_{dn} - P_{gn} - P_{rn}\right) - P_S = 0 \tag{3.2}$$

$$-T_m \leq \sum_{n=1}^{N} \eta_{mn}\left(P_{gn} + P_{rn} - P_{dn}\right) \leq T_m \quad (m = 1, 2, \cdots, M) \tag{3.3}$$

$$P_{gn}^{\min} \leq P_{gn} \leq P_{gn}^{\max}, \begin{cases} P_{rn} \leq P_{rn}^{dch,\max}, & P_{rn} \geq 0 \\ -P_m \leq P_{rn}^{ch,\max}, & P_{rn} \leq 0 \end{cases} \tag{3.4}$$

where:

- $P_{gn}^{\min}$,$P_{gn}^{\max}$ are the minimum and maximum distributed PV capacities.

- $P_{rn}^{dch,\max}$,$P_{rn}^{ch,\max}$ are the maximum discharging/ charging power of ES.
- N,M are the numbers of nodes and lines managed by PV-ES combined system.
- η_{mn} is the sensitivity of power injection at node to the power flow on line and T_m is the power flow limit of line m.

3.3 Distributed Alternating Direction Method of Multipliers

The distributed Alternating Direction Method of Multipliers (D-ADMM) is a distributed optimization algorithm. It was first proposed in Ref [68] and explored in Ref [69]. A communication network with N participators is formed as a graph. Each participator, also called an "agent" in the network has their private function f_p and private constraint set X_p. The goal is to minimize the sum of all functions, while constraining the solution to be in the intersection of all the sets [69], written as follows:

$$\begin{aligned} \text{minimize} \quad & f_1(x) + f_2(x) + \cdots + f_p(x) \\ s.t. \quad & x \in \bigcap_{i=1}^{p} X_i \end{aligned} \tag{3.5}$$

Since the optimization problem is solved in distributed way, there is no central or aggregation node in the network. Both f_p and X_p are private to node p. Each "agent" communicates only with its neighbors (agents that are directly connected to it) and all-to-all communications are not allowed. Each "agent" solves an optimization problem in parallel and sends the information to their neighbors. The iteration steps are as follow:

1. "Agent" p solves the optimization problem based on f_p and X_p. i.e.

$$\begin{aligned} x_p^{k+1} = \arg\min \quad & f_p(x_p) + \left(\gamma_p^k - \rho \sum_{j \in N_p} x_j^k\right)^T x_p + \frac{D_p \rho}{2} \left\|x_p\right\|^2 \\ s.t. \quad & x_p \in X_p \end{aligned} \tag{3.6}$$

2. Then, they send X_p^{k+1} to their neighbours.

3. All "agents" update their Lagrange multiplier

$$\gamma_p^{k+1} = \gamma_p^k + \rho \sum_{j \in N_p} \left(x_p^{k+1} - x_j^{k+1} \right) \tag{3.7}$$

4. Repeat step 1∼3 till the minimal sum of all functions are achieved.

In this algorithm, all "agents" can reach a solution together by exchanging solution estimates in iterations with less communications than used the centralized way. In the PV-ES combined system, each PV or ES is regarded as an "agent". Through this distributed algorithm, they collaborate to maximize the net profit gained from purchasing and selling electricity while at the same time maintain the power balance and the charging/discharging requirements.

3.4 Topology of the Communication Network

In the distribution grid, the users are connected to the feeder line in a sequence. However, the communication network can be designed to have different physical topology to the power network. The principle of D-ADMM algorithm shows the convergence speed of optimization highly relies on the structure of the communication network.

In this section, we design a series of numerical simulations to analyze the impact of the communication network topology on the calculation speed of D-ADMM. The following six different typical network connections demonstrated in Fig. 3.2 are employed:

3.5 Influence of the Different Communication Network Topology on Calculation Performance.

Numerical simulations are performed to illustrate the calculation speed among different communication networks. In each network, 5 PV and 5 ES nodes are created. Thus, there are 10 nodes in total. They are connected in different topology by using graph software NetworkX. The iteration process of the optimization is illustrated as follows, using the

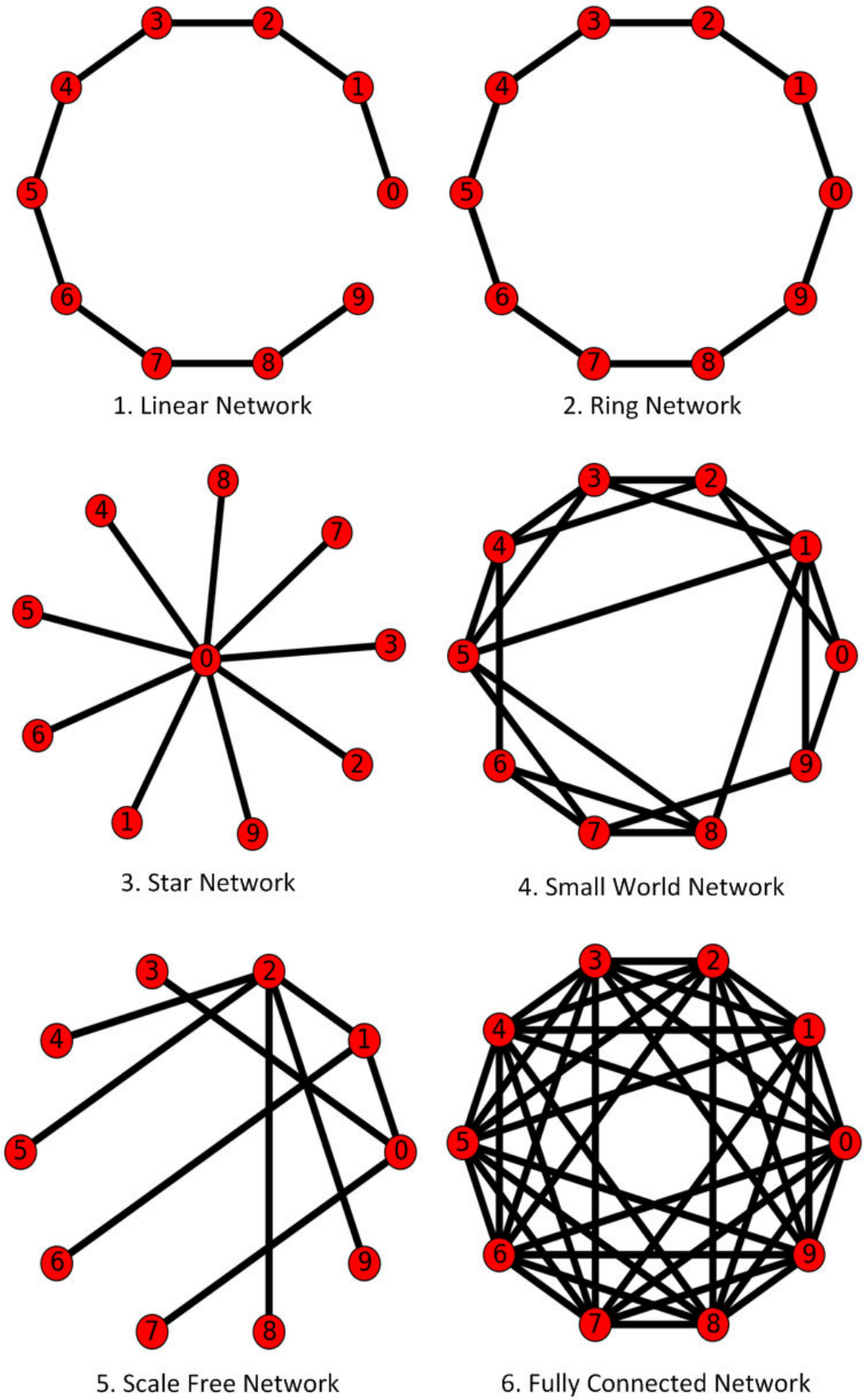

Fig. 3.2 Examples of typical topologies of communication networks

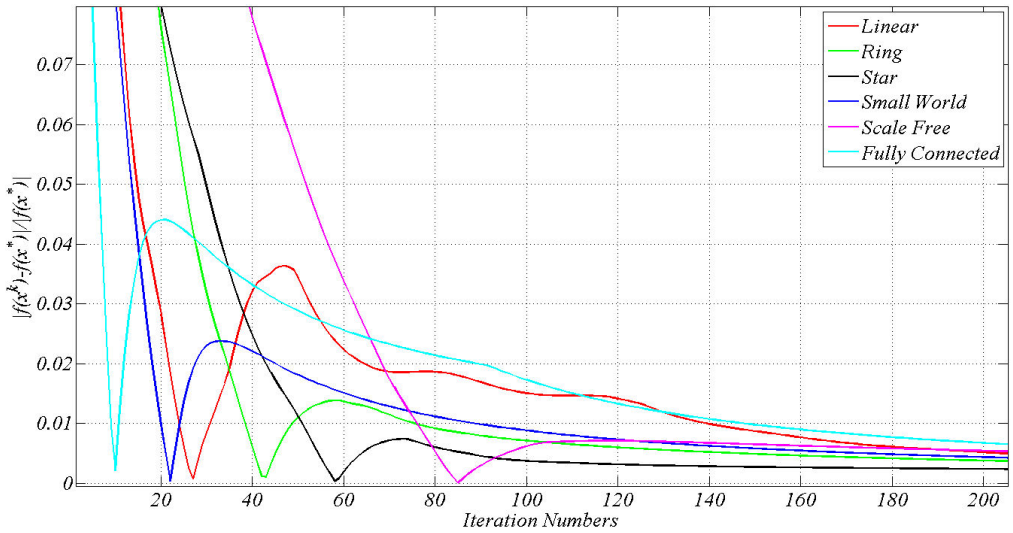

Fig. 3.3 Iteration performance of D-ADMM under different communication network topology

D-ADMM algorithm introduced in previous sections. The simulation results are elucidated in Fig. 3.3.

From the figure above, two phases can be observed during the convergence process, namely descent phase and fluctuation phase. During the descent phase, all curves experience a decrease towards the optimal solution with different velocities. Then after several fluctuations, they converge to the optimal value. However, it can be clearly seen that the iteration steps and convergence speeds are various. In some network connection, the curves decrease very fast and have large fluctuations, and others have low speed of change overall.

Several basic characteristics of network topology in graph theory and some theoretical analysis are introduced here to explain the reasons of disparity in convergence performance

A. Degree

In a graph, the degree of a node v is denoted as $deg(v)$ which is the number of edges connected to node v. The degree expresses the adjacency relationship between node v and other nodes, which shows the significance of it in the network.

B. Laplacian Eigenvalue

A Laplacian eigenvalue is the eigenvalue of a Laplacian matrix [70]. For a graph G with n nodes, its Laplacian matrix L is defined as:

$$L = D - A \tag{3.8}$$

where D is the degree matrix and A is the adjacency matrix of the graph. Then we can get

$$l_{i,j} = \begin{cases} \deg_{v_i} & i = j \\ -1 & i \neq j \text{ and } v_i \text{ is adjacent to } v_j \\ 0 & \text{otherwise} \end{cases} \tag{3.9}$$

The Laplacian eigenvalues can be used to find many other properties of the graph. There are denoted as $\lambda_n = 0 < \lambda_{n-1} \leq \cdots \leq \lambda_1$, where the strict ingenuity refers to a connected graph. One of the most important applications of spectral graph theory is to calculate the approximate sparsest cut of a graph through the second-largest Laplacian eigenvalue.

It is well-known that the second-smallest Laplacian eigenvalues, namely λ_{n-1}, can reflect connectivity of a network [70]. Connectivity is one of the basic concepts of a graph theory. It represents the minimum number of nodes or edges that need to be removed to disconnect the remaining nodes from each other. In the other words, the larger λ_{n-1} a network has, the higher it is connected. The distributions of λ_{n-1} in the typical network topologies are demonstrated in Fig. 3.4.

As we introduced in Section 3, the D-ADMM algorithm requires "agents" share the information with their neighbours during the calculation. Therefore, in a network with higher connectivity, "agents" can finish the information exchange in fewer steps. This can explain the difference of descent rates in the simulation results mentioned above. From Fig. 3.4 it can be seen that the fully connected graph has the largest λ_{n-1}. That is why it takes the least iteration numbers in the descent phase. On the contrary, the scale-free network used in this simulation has the lowest average connectivity. So the iteration curve decreases very slow and takes almost five more times than in fully connected network.

The degree distribution of a network also has great impact on the calculation speed. Based on the discussion of affiliation of Laplacian eigenvalues and degrees in [71]. Li and Pan have proved a lemma in [72]:

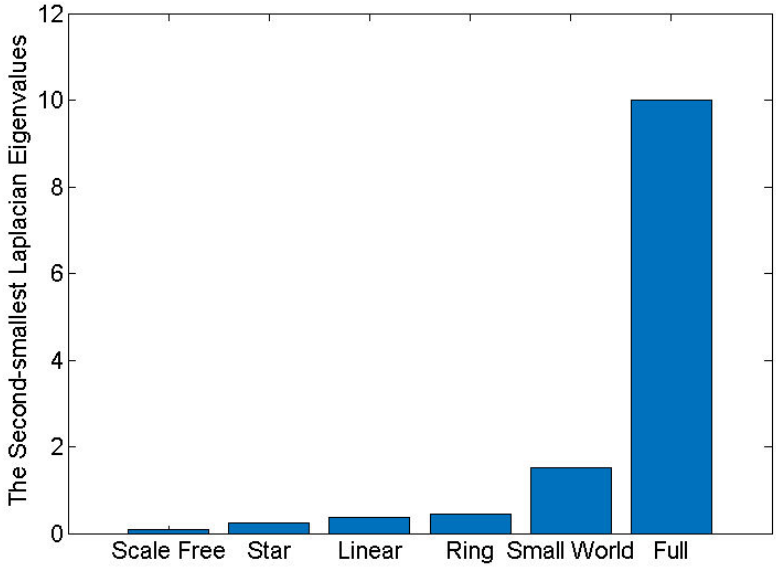

Fig. 3.4 Distribution of λ_{n-1} in typical topologies

$$\lambda_2 \geqslant D_2 \tag{3.10}$$

where λ_2 is the second-largest Laplacian eigenvalue and D_2 is the second-largest degree in the network. They also pointed out that it is difficult to find a graph with $\lambda_2 = D_2$ and in most case $\lambda_2 - D_2 > 0$. This can be classified as an extremal graph [73] problem in graph theory, which means to search for a graph with largest number of edges with certain property. A graph with $\lambda_2 = D_2$ can be called an extremal graph here. Then the smaller the difference between λ_2 and D_2 is, the closer a graph is to an extremal graph.

The fluctuation may be caused by the redundant information between "agents" communication while implementing the distributed optimization. However, the simulation shows that the difference between λ_2 and D_2 has an effect on the fluctuation level during iteration. The distribution of difference between λ_2 and D_2 in each topology is shown in Fig. 3.5.

We can clearly see that the larger difference there exists, the more intense fluctuation it has. In another word, the fluctuation during iteration step can be reduced greatly if a communication network has a closer topology to an extremal graph.

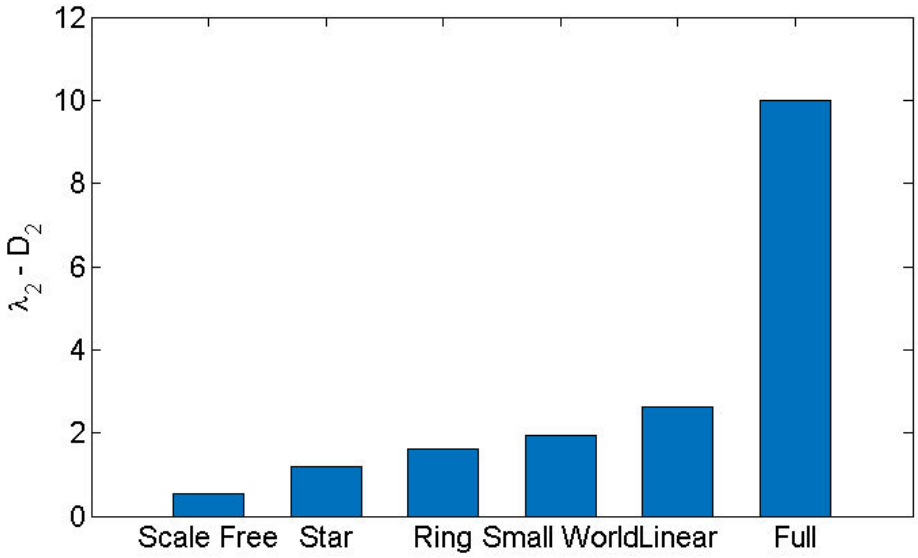

Fig. 3.5 Distribution of difference between λ_2 and D_2 in typical topologies

Here we can draw a conclusion that the connectivity of a communication network will influence the calculation speed during optimization. But it doesn't mean a network with the highest connectivity will gain the fastest convergence speed. It also has the likelihood for a long term fluctuation step. Therefore, an optimum topology for a communication network in distributed PV-ES combined system may exist. Such topology can help to improve the calculation speed of distributed algorithms theoretically. In this case, the ideal topology of the network should have maximum λ_{n-1} and minimum difference between λ_2 and D_2. With such a communication network topology, an optimum iteration curve with the highest descent rates and the lest fluctuation curve can be formed. Then the fastest optimization with the distributed algorithms can be achieved in this communication network.

3.6 Summary

In this chapter, we introduced a distributed PV-ES combined system with D-ADMM algorithm. Characteristics of six typical communication network topologies are analysed. Then, the performance of these topologies in a distributed PV-ES combined system is tested. Simulation results show that the speed of the distributed optimization algorithm in this model is highly sensitive to the communication network topology. By analysing the degrees and

Laplacian eigenvalues of these networks, we found that the descent rate during the iteration is determined by the second-smallest Laplacian eigenvalue, and the fluctuation time is related to the difference between the second-largest Laplacian eigenvalue and second-largest degree.

A hypothesis can be drawn here: there might be an optimum communication network topology. We will expand the idea in this chapter as design guidance to form a better communication network topology in Chapter 6.

Chapter 4

Power System Vulnerability Analysis based on Power Flow Model

4.1 Introduction

As we mentioned in Chapter 2, power system security has always been an important issue in the power industry and substantial research has been done to enhance the grid security and reliability. However, large scale blackouts all over the world still occur from time to time [4] during the continuous evolution of power grids. Thus, it is necessary to further develop new tools and models so as to meet the new situations and prevent potential large scale blackouts.

New developments in the complex network (CN) field have provided a new direction for power system vulnerability analysis [74]. Currently, most research is focused on network structure. The large-scale blackouts in North American and Italy were studied from the network structural vulnerability viewpoint in [75] and [59] respectively. In these studies, indexes and methodologies from graph theories, such as degree distribution, shortest path and diameter are widely used to identify the vulnerable lines in power grids. The analysis result of an American power grid based on this methodology is given by [36][76]. Based on these basic concepts, the mechanism of cascading failures has been explained in [77] and an efficiency model of cascading failure was proposed. Efficiency is defined in terms of the harmonic composition of efficiencies of edges. Ref [15] reviewed basic modelling and traditional methodologies in structural vulnerability. Furthermore, based on topology

and load distribution, two criteria to identify the critical lines are proposed in [78]. The results explain how the link nature and location impact the network's capability. Unlike these traditional physical topology models, an improved electrical topology model are proposed in [57] and [79]. A power grid is depicted as a weighted graph based on the electrical topology. Furthermore, in these models, it is assumed that the power flow is transmitted across the line of 'least resistance' in the network. Thus, the admittance is used to weight the lines in a power system. Based on this efficiency model, a lot of research has been done in recent years. Net-ability, a measure of power system performance under normal operating conditions, is considered in [62]. Also a cascade-based model is proposed in [80]. Several critical power system features are included in [40], such as Kirchhoff's Laws and power angles, and so the electrical topology model made a closer approximation to a real power grid.

However, several important issues still exist. Most of the literature analyses a power system with efficiency and the shortest path algorithm from the CN theory. In these studies, the power grid is described as an undirected graph weighted with efficiency. Nevertheless, in a real power grid, the power is driven by the generation and load distribution, voltage and rotor angle etc. Thus the power flow always has a direction. Moreover, the power neither flows along the shortest path nor all available paths. The power flows from the generation rich side to the load rich side. Also, the electrical efficiency of the transmission line gained from admittance only partly represents the actual capacity of power transmission. To the best of the author's knowledge no prior analyses are investigated in terms of the characteristics of the power system, especially the power flow and its directions.

With this background, in this chapter we investigate a new model and an approach that aims to analyse the vulnerability of power system. First, an improved power flow based model is proposed. The proposed model considers more power system features compared with the previous ones. Consequently, compared with the traditional physical model and electrical efficiency model, the proposed one is a closer approximation to real power grids. Furthermore, we adopt a new definition of vulnerability index to identify the set of vulnerable lines in a power system. The lines with a higher vulnerability index ranking are considered to deal more damage to the power grid when they trip off. It is shown in later sections that this innovation can form better approximation models for the vulnerability analysis of a power system.

This chapter organized as follows. Section 4.2 introduces the existing physical and electrical efficiency model and shows their deficiencies. Then an improved power flow

based model for power system vulnerability analysis is introduced in Section 4.3. Numerical simulations are displayed in Section 4.4 to show the performance of the proposed model. Section 4.5 is the summary for this chapter.

4.2 Existing Models and Deficiencies

4.2.1 Topological Structure Model

As we mentioned in Section 2.3 a power grid can be described as a graph G. The graph G defines an $N \times N$ adjacency matrix, A_{ij} which describes the physical connections and topology of the network. The key physical characteristics of a network can be gained from the adjacency matrix. The connectivity of a network is mainly defined by the nodal degrees and clustering coefficients. Analysing these characteristics can give an indication of the structural vulnerability of a power grid [77].

4.2.2 Electrical Efficiency Model

The topological model can only describe the physical structure and connections of a power system. However, a power grid is more than just a simple network structure. There are several electrical features such as line impedances, which can impact the performance of the whole system. Thus, based on the physical model, an updated electrical efficiency model has been proposed. In an electrical efficiency model, the power network G is denoted by an $N \times N$ admittance matrix, Y_{ij} describing the electrical efficiency of the network edges. In the admittance form, the system equations can be described as the nodal equations:

$$\overline{I_B} = \overline{Y_B V_B} \tag{4.1}$$

where $\overline{I_B}$ is the vector of injection bus currents and $\overline{V_B}$ is the vector of bus voltages measured relative to the slack bus and $\overline{Y_B}$ is the bus admittance matrix. Expanding equation (4.1):

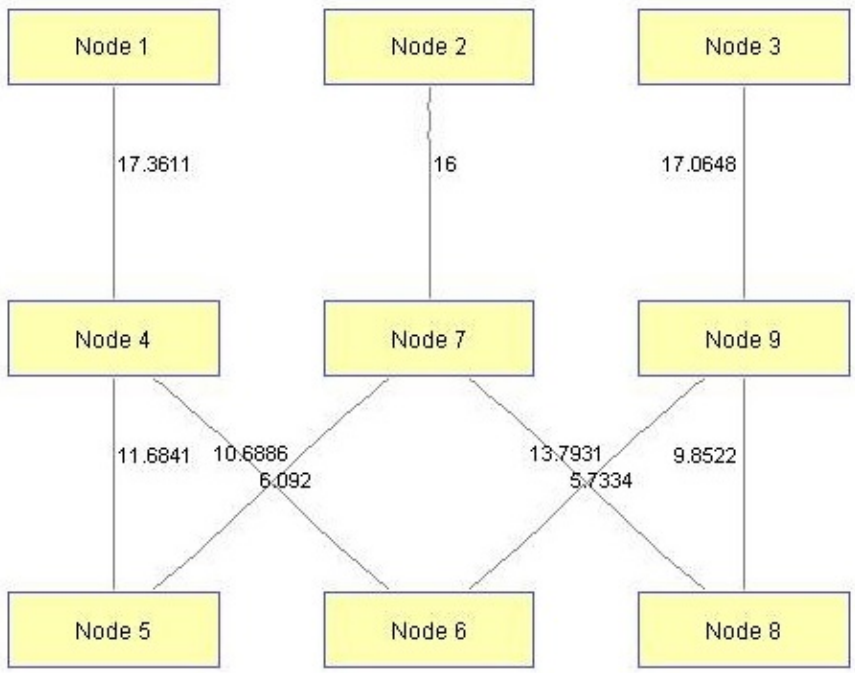

Fig. 4.1 Electrical efficiency model of IEEE 9 bus system

$$\begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n} \\ Y_{21} & Y_{22} & \cdots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \cdots & Y_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} \tag{4.2}$$

where

$$Y_{ij} = \begin{cases} -\left(G_{ij} + jB_{ij}\right), & i = j \\ \sum_{i \neq j} \left(G_{ij} + jB_{ij}\right), & i \neq j \end{cases} \tag{4.3}$$

And G_{ij} and B_{ij} is the conductance and susceptance between node i and j respectively. The bus matrix here closely captures both the real and reactive (imaginary) portions of the line admittances. For pairs of nodes i and j that do not share a direct physical connection, $Y_{ij} = 0$, otherwise Y_{ij} is the admittance of the line between node i and j. An example of the electrical efficiency model for the IEEE 9 bus test system is shown in Fig. 4.1. It can be seen that the model is an undirected graph with edges weighted by the electrical efficiency.

In this model, the electrical efficiency of the edges between nodes i and j is meant to represent the level of power transmission between the two nodes. The transmitted power is assumed to follow the path of "least resistance" in a circuit as defined in terms of Y_{ij}. That is to say, the edge with higher Y_{ij} can carry more power in the system. As a measure for performance, the average efficiency of a network E is employed.

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} Y_{ij} \tag{4.4}$$

In the process of cascading events, the average efficiency of a network E changes as the efficiency on each line changes. The network efficiency loss during failures is described as damaged efficiency D given by

$$D = \frac{E_0 - E_f}{E_0} \tag{4.5}$$

where E_0 is initial network average efficiency and E_f is the final network average efficiency after failures[17].

Therefore, the network vulnerability of a power system can be observed by calculating D for failures on different transmission lines. A failure is applied to different lines in the network causing different damage to the system. The line whose removal can cause the biggest D in the end is chosen as the most vulnerable line in the network.

Since the electrical efficiency model considers the admittance of the transmission lines in the power system, it can be used to identify not only the physical structure vulnerability but also the critical lines. A comparison of performance between the topological model and electrical efficiency model is presented in [17]. The results show that compared with the topological structure model the electrical efficiency model has a better performance in identifying the weakness of power grids.

4.2.3 The Deficiencies in the Models

From the topological structure model to the electrical efficiency model, researchers have shown the possibility of using CN theory to analyse power grid vulnerability. However, as

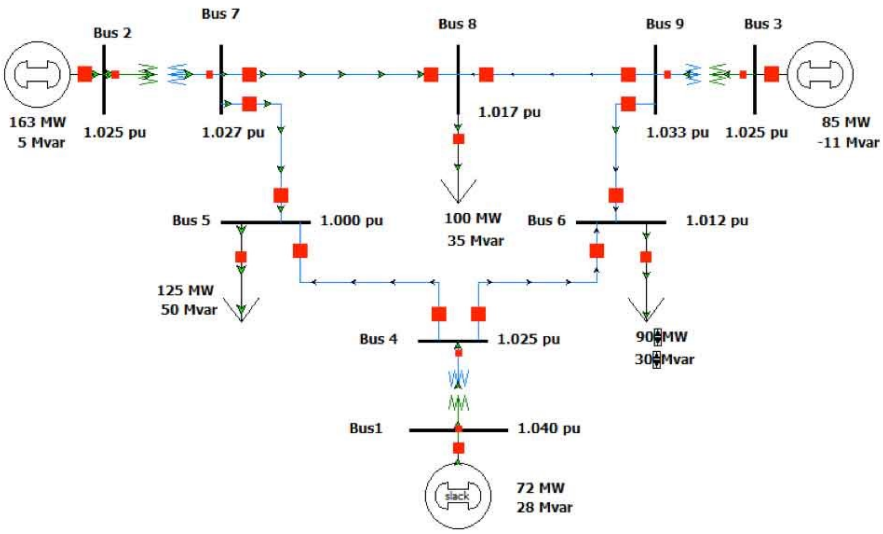

Fig. 4.2 The arrows on the edges show the power flow directions in IEEE 9 bus system

network models are used to the describe power grid, these models have some deficiencies that can't be ignored.

A. The power flow has direction and does not flow along the shortest electrical path.

Both the topological model and electrical efficiency model describe a power grid as an undirected graph. However, in an actual power system, the power flow always has a direction. Fig. 4.2 shows the power flow in the IEEE 9 bus system obtained from simulation software Power World which is convenient to show the power flow directions. The power flows in the lines are directed.

Since the power flow is driven by generation, loads and rotor angles between buses, power flow is not normally distributed according to the length of the path in the grid. Instead, it obeys electrical laws to flow from generators to loads.

B. The electrical efficiency is not a reflection of the actual power transmission level

The weight on an edge in topological model only shows the connections. In the electrical efficiency model, the weight on each edge shows the electrical connection and transmission capabilities. In other words, an edge with high efficiency is deemed to transfer more power. But in a real power system, neither of these weights shows the actual transmission level of power flow. Fig. 4.3 shows the electrical efficiency and actual power flow on each

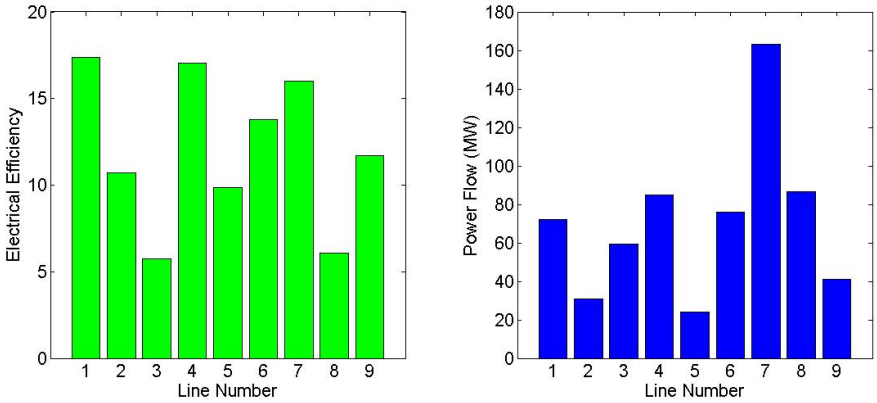

Fig. 4.3 Electrical efficiency and power flows distribution on the transmission lines in IEEE 9 bus system

transmission line in the IEEE 9 bus system. The realistic power flow distribution is gained by simulation on DIgSILENT. It can be seen that there are no real causalities between the electrical efficiency and power flow distribution in the system. From Fig. 4.3 we can see some transmission lines with low efficiency, such as line 8, transfer more power than the lines with high efficiency like line 6.

4.3 The Power Flow Based Model

4.3.1 Power Flow Model

In order to overcome the above-mentioned issues, we now propose a power flow based network model which is a weighted directed network with the following assumptions:

1. Buses and transmission lines in a power grid are classified as nodes and edges in a network model. Each node is perfectly reliable, and each edge has two states: working or failed.
2. The original network is connected and free of self-loops.
3. Each edge has its own direction, which is the same as the direction of the power flow on the transmission line. Each edge is weighted by the value of the power system's steady state power flow.

4. The degrees of all nodes are at least 2, except for the source nodes and sink nodes.

Also as a directed graph, the nodes in the model no longer have the same functions. In the power flow model, nodes can be classified to four different types. The input and output power flow of a node is denoted as F_i and F_0. The load and generation on a node is denoted as L_n and G_n respectively. The power flow that passes through each type of node obeys the following rules:

- Source nodes: $F_i = 0$, this type of node represents generator buses in the power grid, thus there is no input flow for these kinds of nodes.
- Sink nodes: $F_o = 0$, this type of node represents load buses which means only input and no output from the node.
- Transmission nodes: $F_i = F_o$, to obey the Kirchhoff's Law, for any intermediate node, the flow coming into it needs to equal the flow going out of that node.
- Transmission nodes with load and/or generator: $F_i = F_o + L_n - G_n$, in a power grid, some of the intermediate buses also have loads and/or generators on them. In this case, the total output flow should be the total input power plus the node generation then minus the node load.

Usually, there should be more than one generator and load in a real power system, so the new model should have multiple source nodes and multiple sink nodes. We will introduce the method to deal with the multi-source multi-sink problem in a later section. Fig. 4.4 shows a power flow model of the IEEE 9 bus system. This model is a directed graph and weighted by power flow. Unlike the electrical efficiency model, the edge with a higher weight transfers more power in this model.

4.3.2 Identification of Important Lines

A new vulnerability index derived from the Maximum-Flow concept is proposed in this model to identify critical lines in a power network. The Maximum-Flow Minimum-Cut Theorem, also known as Ford Fulkerson algorithm [81], is widely used in CN research to solve maximum flow problems, such as traffic flow, cash flow, information flow, power flow,

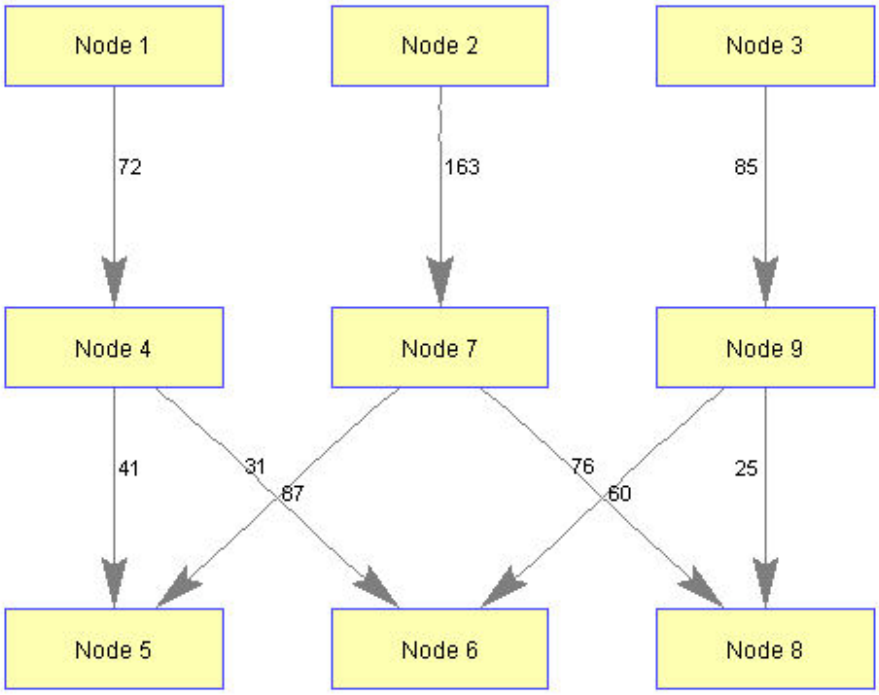

Fig. 4.4 Power flow model of the IEEE 9 bus system

etc. [82][83][84]. The purpose of the algorithm is to calculate the maximum flow a network can withstand and how to attain this limitation. The algorithm can be described as follows:

Given a network $G = (V, E)$. The capacity and flow on the edge (i, j) are defined as $c_(ij)$ and $f_(ij)$ respectively. A source node s, and a sink node t. Then define the residual network of G as $G_f(V, E_f)$. The capacity of G_f is defined as $c_{f(ij)} = c_{ij} - f_{ij}$. Then the maximum flow is calculated as follows:

1. Initially, for each edge (i, j), set the flow be $f_{if} = 0$
2. Given a path p from s to t in G_f, for all edges $(i, j) \in p$, find $c_{f(p)} = \min\left\{c_{f(ij)} \mid (i, j) \in p)\right\}$.
3. For each edge $(i, j) \in p$, set $f_{ij} = f_{ij} + c_f(p)$.

In this way, corresponding to the maximum flow in the network, we can get the flow on each edge. Then the vulnerability index of edge (i, j) can be defined as the level of flow carried by edge (i, j) compared to the value for the maximum flow of the network. To extend the idea to a multi-source multi-sink network power system, an improved index is defined

with respect to all possible max flows. For a network with m sources and n sinks, let f_{MAX}^{uv} be the maximum flow from the source node u to the sink node v and let f_{ij}^{uv} be the portion of the flow passing through the edge E_{ij} of the network. Then we define the vulnerability of the edge E_{ij} to be:

$$V_{ij} = \frac{\sum_{u=1}^{m} \sum_{v=1}^{n} f_{ij}^{uv}}{\sum_{u=1}^{m} \sum_{v=1}^{n} f_{\mathrm{MAX}}^{uv}} \tag{4.6}$$

Thus, the lines can be ranked with a vulnerability index based on the power flow they carry using (4.6). The lines with a higher value of index are given a higher ranking in this analysis.

Therefore, the procedure of the ranking process can be given as follows:

1. Build a connection network model of the power system.
2. Calculate the steady state power flow of the grid and collect data.
3. Weight the edges in the network model with the power flow gained from previous steps and determine the flow directions.
4. Calculate the maximum flow of the network for each source-sink combination.
5. Sum up the flow values and compute vulnerability index V_{ij}.
6. Rank the lines according to values of vulnerability index.

The IEEE 9 bus system is used to illustrate the difference between the electrical efficiency model and proposed model as an example here. The vulnerability index distribution in the IEEE 9 bus system is given in Fig. 4.5. The edges are ranked by efficiency and the new vulnerability index respectively. Load capacity L, the maximum amount of load a power system can carry, is employed here as a realistic measure of the network performance. The damage of the network is defined as

$$D = \frac{L_0 - L_f}{L_0} \tag{4.7}$$

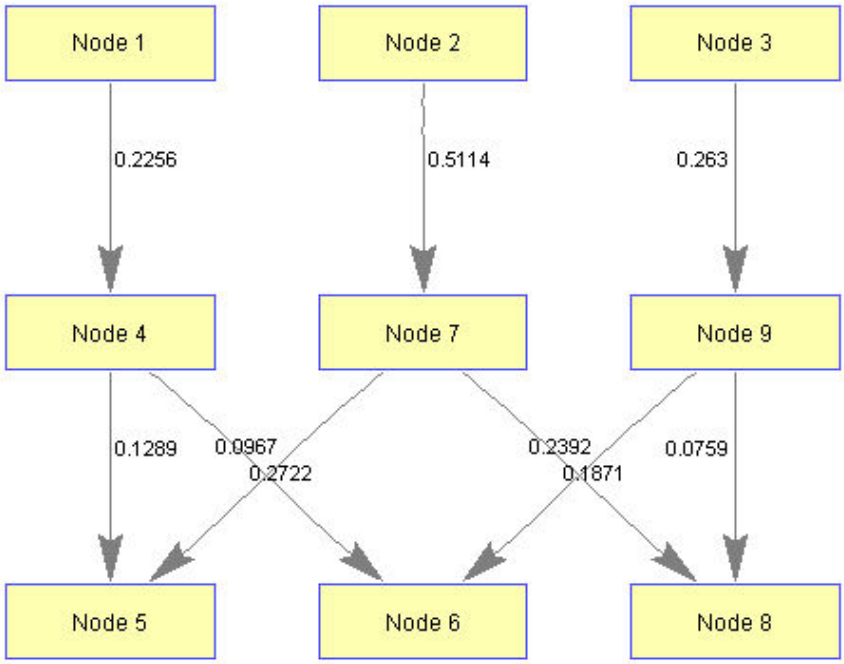

Fig. 4.5 V-index distribution of IEEE 9 bus system

Table 4.1 My caption

Ranking	**1**	**2**	**3**	**4**	**5**	**6**
Realistic Damaged Ranking (line number)	8	6	3	9	2	5
Ranking by Electrical Efficiency Model (line number)	6	9	2	5	8	3
Ranking by Power Flow Model (line number)	8	6	3	9	2	5

where L_0 is the initial load capacity, L_f is the final load capacity after removing the line from the network. The damaged efficiency also represents the load loss from the failure.

Table 4.1 shows the vulnerable line ranking identified from the power flow model, electrical efficiency model and the realistic damaged data. The electrical efficiency and vulnerability index are calculated with Matlab and the realistic damaged data is gained from the power system software DIgSILENT simulation environment. Please note line 1, 4 and 7 in this system are the lines that directly connect to the generator bus. When these lines are removed from the system, the power flow of this system will not converge. Since the removal of these lines is corresponds with shutdown of the generator from the system directly, these lines are obviously important to the system (also can be found that these lines have extremely high vulnerability index in Fig. 4.5). So we do not discuss this kind of line here.

From Table 4.1 we can see that the ranking shows the difference between two models. The ranking order by electrical efficiency is 6, 9, 2, 5, 8 and 3, does not match the realistic result. However, the ranking order by vulnerability index is 8, 6, 3, 9, 2 and 5, practically in accordance with the realistic damaged data. The results show that power flow based model has a better performance in identifying the important lines.

4.4 Case Study

A vulnerability analysis for the IEEE 118 bus test system is carried out with the methodology explained in the previous section.

The electrical efficiency and the new vulnerability index of each line in the network are calculated and normalized to their average value respectively. Fig. 4.6 shows the distributions of these normalized values on the lines. From the figure, it can be seen the results are clearly different. There are some lines which have low electrical efficiency (means less important in the traditional model) with extremely high vulnerability index (shows it is critical in this system using the power flow model). Also, the component of the vulnerability index value in this system is shown in Fig. 4.7. It can be seen that most of the lines in IEEE 118 bus system have a low value of index. Nearly 90% of the lines in the grid have an index less than 0.05. On the contrary, the remaining 10% lines have a high index, meaning that they are more critical in the system. The simulations are investigated to see the performance of proposed index in vulnerability analysis.

First, 10 targeted attacks and 10 random attacks have been applied to the simulation system according to the ranking by vulnerability index. Random attacks refer (with high probability) to the failure on any of the less important lines (lines with low vulnerability index) and targeted attacks refer to failure of the critical lines (lines with high vulnerability index). The decrease of the load capacity of the power grid is shown in Fig. 4.8.

It can be seen that after 10 targeted attacks the capacity of the network drops to almost 70%. On the other hand, the capacity drops to about 97% after random attacks. The result shows that the lines with a higher index are more vulnerable in the system. This performance also matches the characteristics of scale-free networks in CN theory. The network is very robust to random attacks and weak to targeted attacks. Meanwhile, this example illustrates

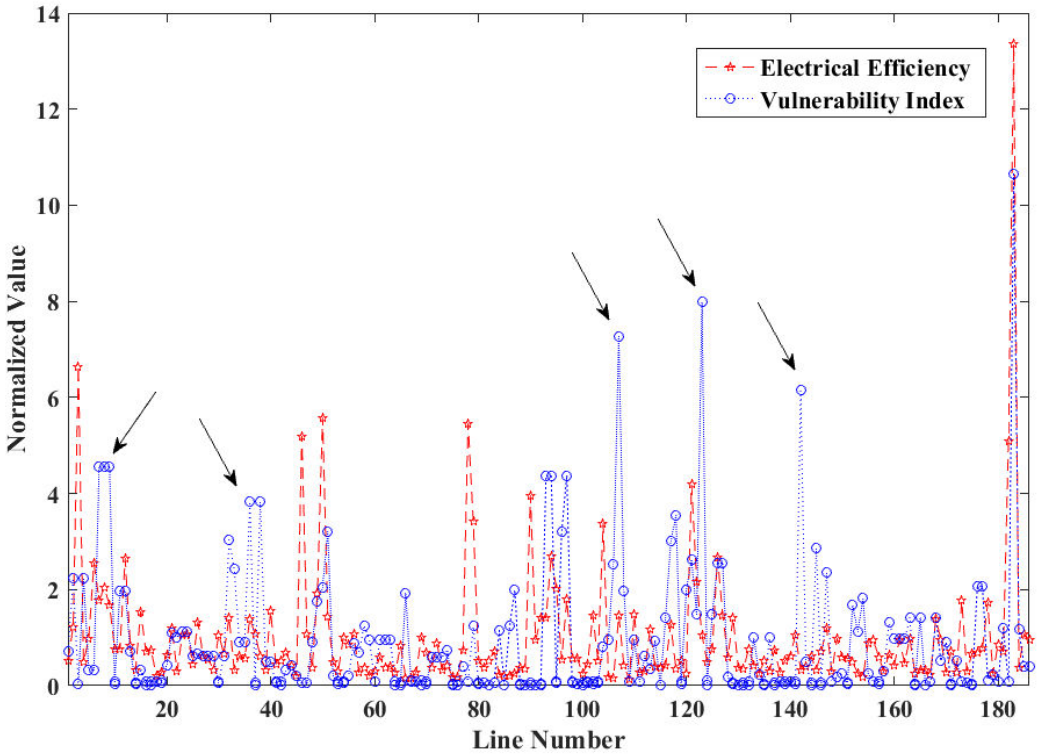

Fig. 4.6 Normalized electrical efficiency and vulnerability index distribution in IEEE 118 bus system

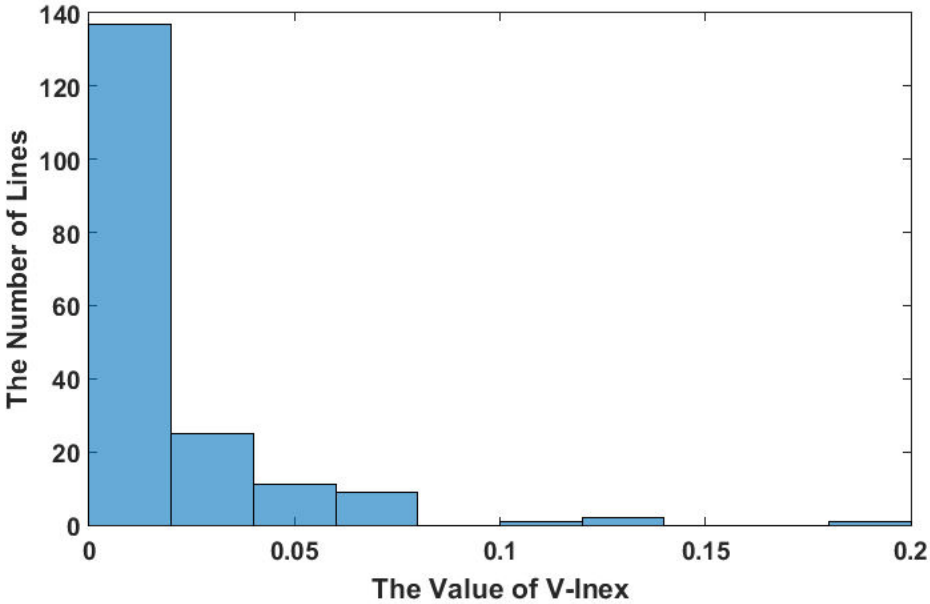

Fig. 4.7 The number of lines in IEEE 118 bus system distributed by the value of vulnerability index

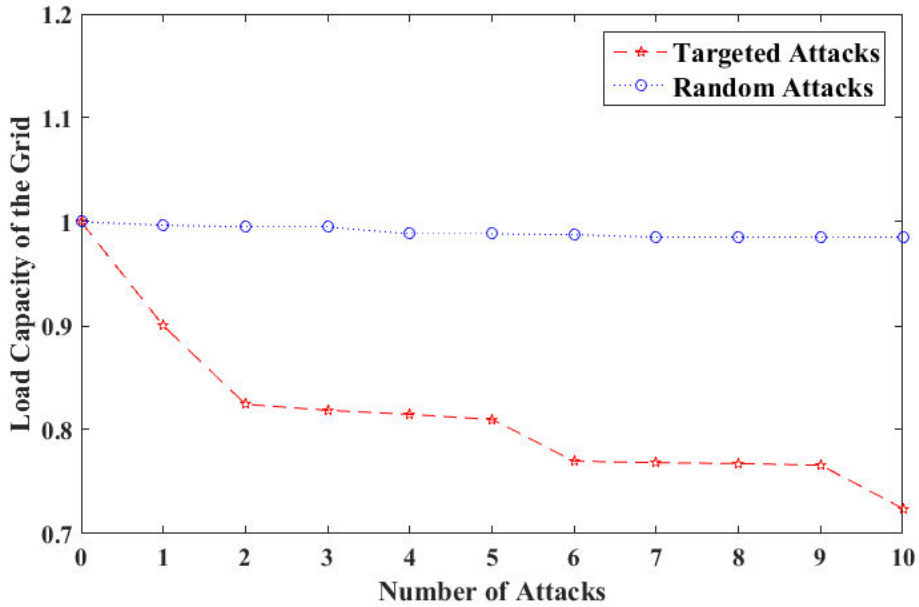

Fig. 4.8 Load capacity of IEEE 118 system after targeted and random attacks

how the vulnerability index proposed in this chapter is a reasonable way to identify the vulnerability in a power system.

Furthermore, analysis has been carried out to compare the performance between the electrical efficiency model and power flow based model. The original power flow distribution in the IEEE 118 bus system is shown in Fig. 4.9 where the power flow profile is plotted under a planar representation of the network.

It can be seen that the power flows concentrated on several critical areas. The south east part of the grid (the left edge area in the figure) is a generator heavy area. Most of the power in this grid is generated from this part and transferred to the north-western area (right side in the figure). Then we execute 10 targeted attacks which remove the top 10 ranked lines identified by the two different models to see the load shifting. The power flow distributions after the attacks are recalculated and displayed in Fig. 4.10 and Fig. 4.11.

It is shown from the figures that the difference in accuracy to identify the critical lines between two models is quite obvious. When we attack the high ranked lines in the electrical efficiency model, the power flow distribution does not change a lot. From Fig. 4.10 it can be seen that the generator heavy area still keeps the highest power flows and does not seem to be affected much by the attacks. On the contrary, when the high ranked lines gained from the

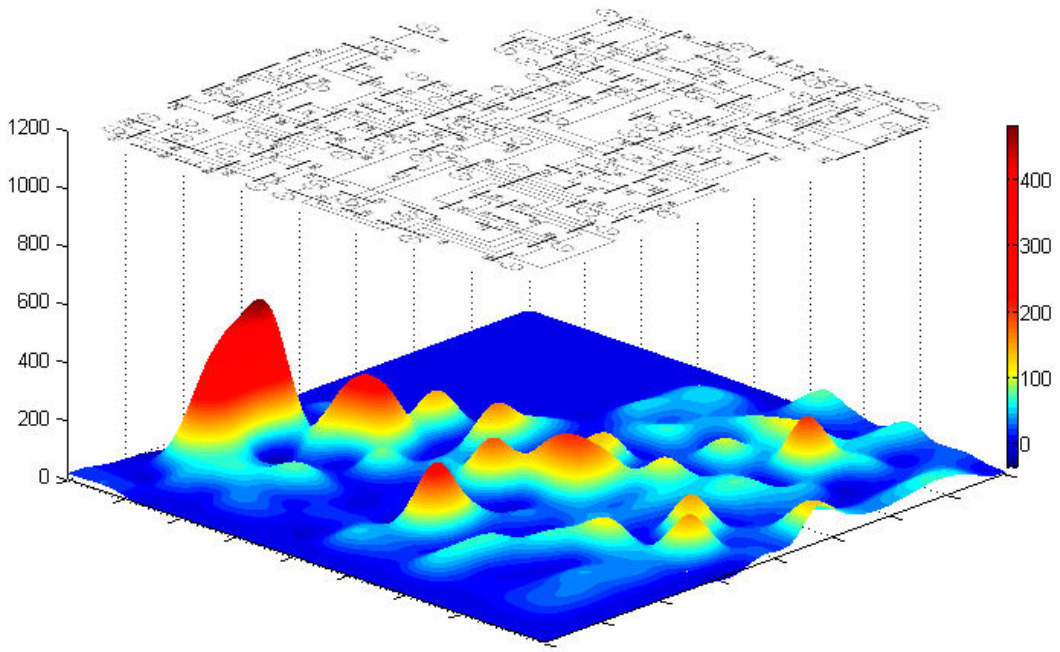

Fig. 4.9 Steady state geographical power flow distribution in IEEE 118 bus system

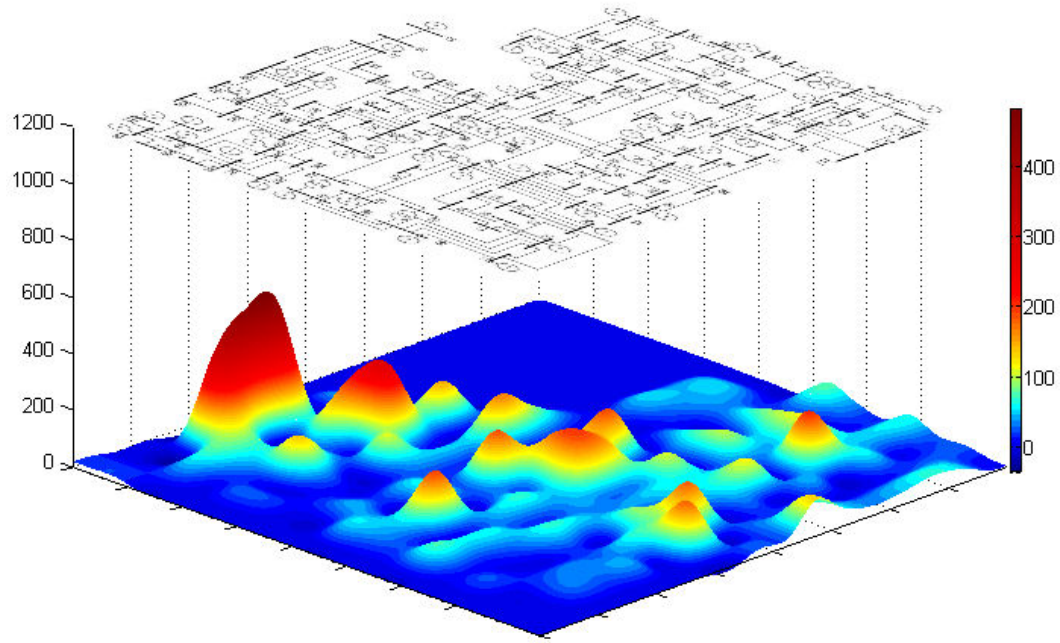

Fig. 4.10 Geographical power flow distribution in IEEE 118 bus system after ranked attacks by efficiency model

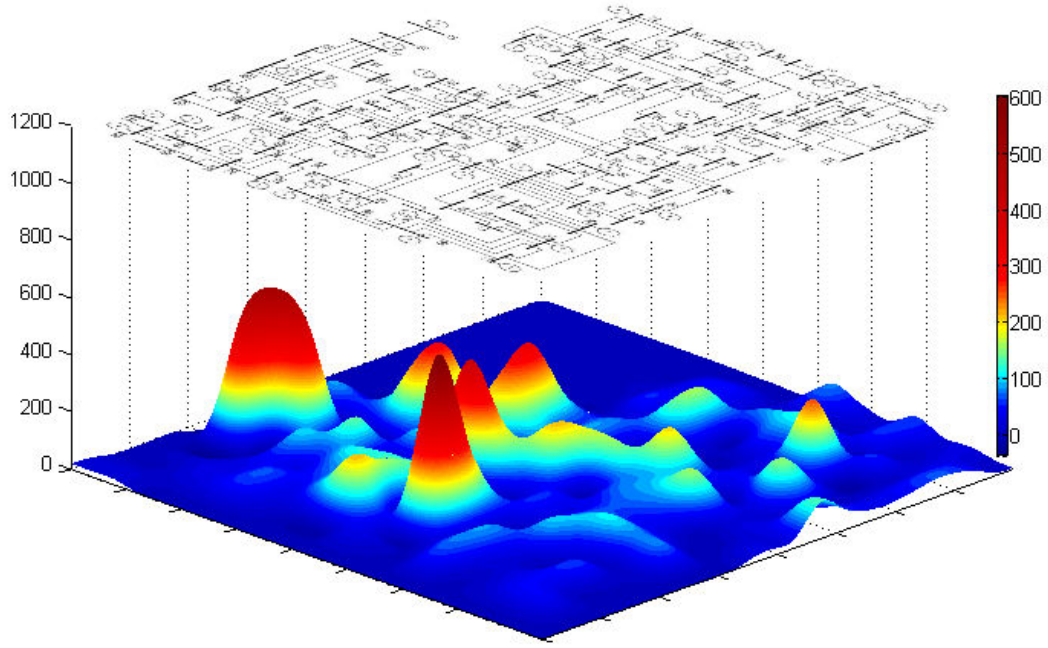

Fig. 4.11 Geographical power flow distribution in IEEE 118 bus system after ranked attacks by power flow model

power flow model are attacked, the outcome is substantial. Multiple critical lines dropped from the grid caused a great load shift in the system. To maintain the power supply to the north-western parts, the generators and transmission lines in the central area are forced to carry more power than they did in steady state. In Fig. 4.11 it can be clearly seen that more power is transferred in the middle part of the graph and this large power shift will bring an additional burden to rest of the system. It may also increase the risk of cascading events and large area blackouts in the system.

The detailed data also shows further differences between the two models. The changes of power flow on transmission lines after the attacks are demonstrated in Fig. 4.12 and Fig. 4.13 respectively. In the figures, a positive value means that the transmission line carries more power than the initial state while a negative value shows that the line loses capacity during the attacks.

From Fig. 4.12, it can be seen again that the power flow distribution before and after the attacks as ranked by electrical efficiency model changed a little. Most of the gaps are less than 100 MW. There are only 2 lines having load shift over 100 MW and the total power shift in the system is recorded as 1977.95 MW. This means there are no large power shifts

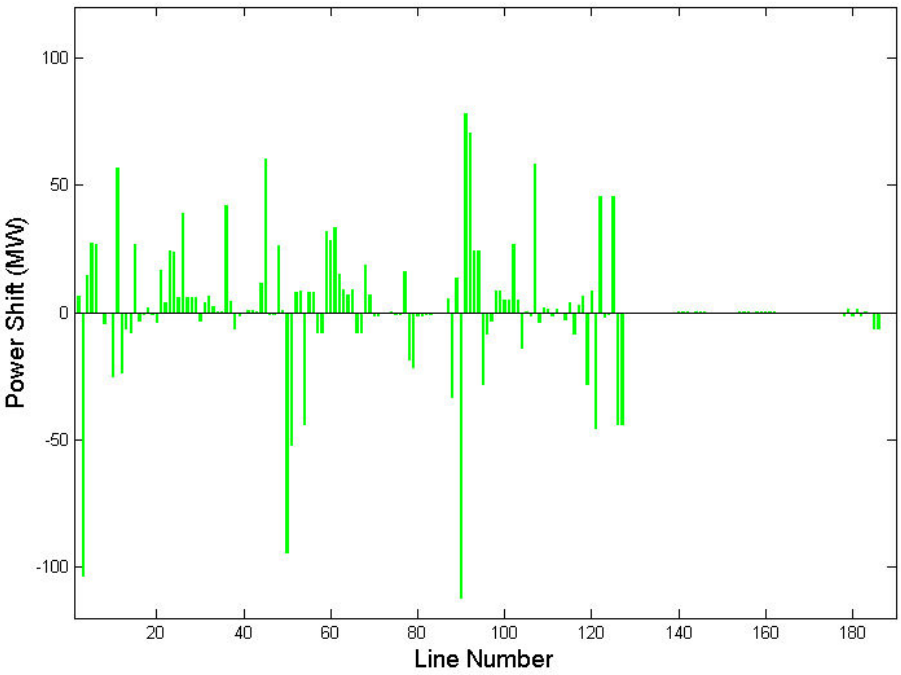

Fig. 4.12 Power flow variations on each edge in efficiency model

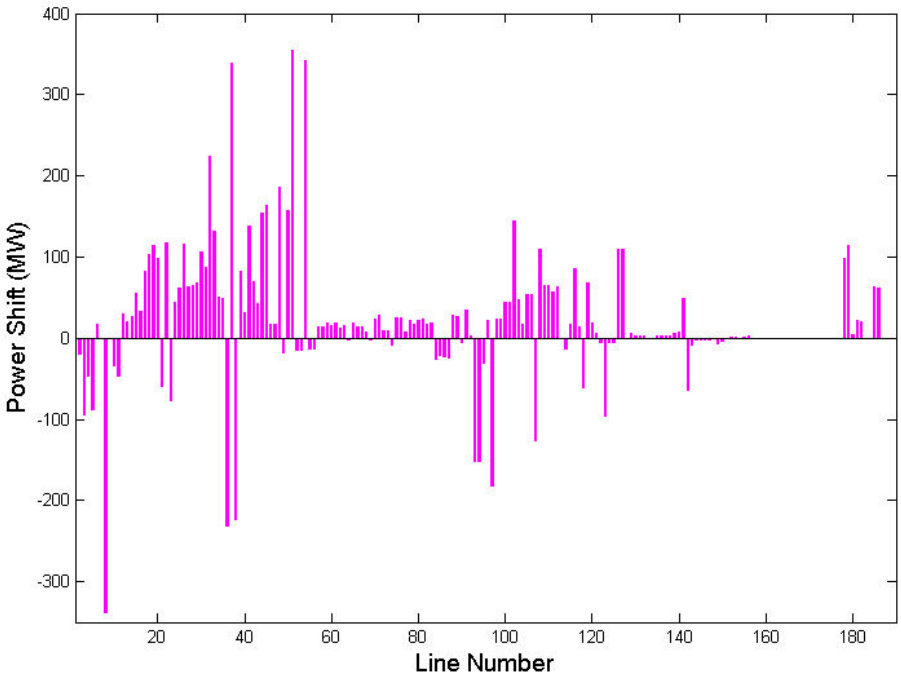

Fig. 4.13 Power flow variations on each edge in power flow model

when the lines identified by this model are attacked. On the contrary, from Fig. 4.13, it can be clearly observed that after attacks, an increased amount of power flows are observed in those lines that used to have low power flow. The total power shift is 8485.66 MW, which is over 4 times than the result from Fig. 4.12. Also 26 lines have great load shift over 100 MW. At the same time, 53 lines are forced to carry power which is 200% overload than the normal situation. For example, the line 52 carries less than 250 MW and over 600 MW before and after attacks, which is 2.4 times of the usual amount. This indicates that there has been a significant power shift between lines (or edges). The removal of several important lines from the system causes many other transmission lines to carry more power to maintain the power system operation. These lines have a high risk of overload in real power grids leading to further failures which may cause cascading blackouts.

4.5 Summary

In this chapter we proposed an improved PF based model for vulnerability analysis of power system. This model is novel in presenting a more realistic approximation of the power system. A new vulnerability index is developed to identify the vulnerable lines in a power system. Simulation results demonstrate that lines identified by this proposed model match realistic situations. The ranking via the new vulnerability index can identify critical lines in a power system more effectively and accurately. The analysis results not only provide a reference for predicting the cascading failures, but also support power system design and planning. We will expand the result gained here in Chapters 5 and 6 to analyse how the risk changes during cascading events.

Chapter 5

Power System Cascading Risk Assessment based on CN Model

5.1 Introduction

The world has witnessed several serious blackouts in power grids over the past decade. Structural vulnerability and related cascading failures were considered as a major contributing factor. Basically, most of these blackouts are caused by a single event but end up with cascading failures across a large area [4]. For this reason, new models and methods for power system security assessment are much needed to prevent potential cascading events.

Traditional power system security assessment can be classified into three types, which are deterministic assessment, probabilistic assessment and risk-based assessment [85]. Deterministic assessment aims to demonstrate the power system in tolerant to the faults that are within the "design basis", thereby defining the limits of safe operation [86]. Vulnerability analysis for a power system is usually employed to identify critical components that if failed will lead to serious damage of the system. However, this method cannot reflect the state of the grid and random probability of the failures. By considering the fault probability of all kinds of components and the random characteristics of a power system, the probabilistic methods may assess the system security more practically [84]. But some fatal failures with low probability may be neglected in the assessment process. Risk assessment on the other hand can reflect the influence of the failures by combining the consequences of the events and random probability

together. Steady-state risk assessment of a power system is largely discussed in [87] using the Monte Carlo method. Ref. [88] developed a framework combining risk with voltage problems based on the power system P-V curve. An approach that is based on assessing the line overload risk is presented in [89]. A risk index is proposed in [90] for the system planning. In addition, transient risk assessment aims to help the system operator identify the risk after an event happens. A transient stability risk assessment framework considering the load level is investigated in [91]. Based on traditional Monte Carlo simulation, [92] shows the direction of risk assessment with the fuzzy logic method. It is worth noting that previous research mainly focuses on the component-level to assess the security of a power grid. These models and methods lack a strong systems level aspect while aiming to analyse one of the most complex man-made systems in the world. Massive data acquisitions and calculations are required to reach an overview assessment.

As we saw in Chapters 1 to 4, CN theory has been studied solving practical problems of large-scale complex systems. Differently from the traditional risk assessment method which is based on the component-level, researchers want to make the security assessment based on network structure with CN methods [93]. New indices from CN theories, such as degree distribution, shortest path and diameter, are widely applied to identify the critical parts in power grids. Based on these basic concepts, the mechanism of cascading failures has been explained in [77] and an efficiency model of cascading failure is proposed. A risk graph is employed to reveal the power grid cascading failure in [94]. The model presented a new node risk-based attack strategy which is better than the load-based and degree-based attack strategies. It is shown that risk assessment with CN theory can reveal the system security from a system-level viewpoint [74], which is particularly important in study cascading failures of a power grid.

Nevertheless, several important issues still exist. In order to consider the system-level, CN based models usually neglect the detailed electrical characteristics of a power grid. In these studies, the power grid is mainly described as an undirected graph weighted with efficiency [57]. However, in a real power grid, the power flow always has a direction which is driven by the generation and load distribution, voltage and rotor angle etc. Also, the efficiency of the transmission line gained from admittance only partly represents the actual capacity of power transmission as we saw in Chapter 4.

In order to address the issue, we investigate a new model and approach that aims to analyse the risk of a power system having cascading failures. We improve the model based

on the power flow based CN model proposed in Chapter 4. The CN factors such as topology and connectivity are added to the proposed model based on the traditional risk assessment model. Also, the new model considers more practical power system features compared with the previous CN cascading model. Six different types of electrical failures are adopted in this model. Consequently, the proposed model can demonstrate improved approximation to realistic cascading failures. Furthermore, we design a cascading event simulation module to identify the cascading chain in the system during a failure. The parts with a higher risk ranking are seen as more likely to form a cascading chain when a failure occurs.

The remainder of this chapter is organized as follows. The basic concepts of improved CN model for risk assessment are introduced in Section 5.2. Then an innovated cascading event simulation module is introduced in Section 5.3. Numerical simulations are displayed in Section 5.4 to show the performance of the proposed model. Section 5.5 gives a summary for this chapter.

5.2 Improved Power System CN Model for Risk Assessment

A power grid usually has a certain number of generators, loads and buses connected by transmission lines. Thus, a power grid can be described as a graph G with N nodes and K edges. Several basic characteristics of the CN model are introduced here [95].

5.2.1 Basic Concept of Network Structure

A. Topology

The physical topology of the grid is described by an $N \times N$ adjacency matrix A_{ij}. If there is a transmission line connecting bus i and j, then A_{ij} is set to 1, otherwise 0. To simplify the model, if there are parallel lines between buses those are modified to one edge. Then we can get a simple connected graph without self-loops.

B. Degree

The degree of a node in a graph is the number of edges incident to the node. The degree of node i is denoted as $deg_{(i)}$. Then $deg_{(i)}$ expresses the adjacency relationship between node i and other nodes, which shows the significance of it in the network. The node with higher $deg_{(i)}$ carries more transmission lines.

C. Edge Weight and Direction

In the early research on power systems with CN models, the adjacency matrix A_{ij} is applied to test the vulnerability of the network [79]. Since the adjacency matrix only reflects the physical connection and ignores all the electrical characteristics, a weight that is a closer approximation to a real power grid is required. In this research, the AC power flow is used to weight the edges in the graph. That means the edge with higher weight carries more power in steady state. Physically, the power transmission lines are able to transfer power bilaterally. However in an actual steady power system, the power flow on a transmission line usually has fixed direction. In this research, the directions of the power flow are set as the positive directions of edges.

D. Edge Weight and Direction

In a CN, a node with zero input flow is called source node and a node with zero output flow is called sink node. In a power grid model, these two kinds of special nodes stand for generators and loads respectively. For other transmission bus nodes in the graph, their total output flows should equal to the total input flows. The Maximum-Flow Minimum-Cut Theorem, also known as Ford Fulkerson algorithm [96], is widely used in CN research to solve the maximum flow problems, such as traffic flow, cash flow, information flow, power flow, et.al. The purpose of the algorithm is to calculate the maximum flow that a network can withstand and how to attain this limitation. We have introduced the details of this algorithm in Chapter 4.

We saw that the Maximum Flow algorithm is effective to identify the critical lines in a power system [81]. In this chapter, the Max-Flow method is used to calculate the vulnerability index of edges, which will be explained in Section 5.2.2.

5.2.2 Risk Assessment with Improved CN Model

For the complexity of the power system, a lot of uncertain factors will impact the results of failures. The index called risk is proposed to define the possibility and seriousness of an event. The expression of risk R can be generally written as:

$$R = C \times P \tag{5.1}$$

In the equation, C describes the consequence of the failure. And P represents the probability of the event [97].

To achieve accurate risk assessment during cascading events, the risks of the nodes and lines have to be calculated separately. The risk of nodes i and edge E_{ij} can be written as follows:

$$R_i = C_i \times P_i \tag{5.2}$$

$$R_{ij} = C_{ij} \times P_{ij} \tag{5.3}$$

The consequence of a node i is defined as follow:

$$C_i = N_1 \frac{deg_{(i)}}{deg_{\mathrm{MAX}}} + N_2 \frac{p_i}{p_{\mathrm{MAX}}} \tag{5.4}$$

where

$$N_1 + N_2 = 1 \tag{5.5}$$

In the equation (5.4), $deg_{(i)}$ represents the degree of the node i, deg_{MAX} represents the maximum degree of the network. Similarly, p_i and p_{MAX} represent the power injection of node i and the maximum power injection of the system respectively. The weight N comprehensively reflects physical and electrical characteristics of the node in power system.

We can gain a node consequence which considers more topological or electrical proportion by adjusting N_1 and N_2.

The consequence of the transmission lines can be defined by a vulnerability index which the expresses the level of flow carried by the edge relative to the maximum flow of the network. For a network with m sources and n sinks, let $f_{\max}^{uv}$ be the maximum flow from the source node u to the sink node v and let f_{ij}^{uv} be the portion of the flow passing through the edge E_{ij} of the network. Then the consequence of edge E_{ij} can be written as:

$$C_{ij} = \frac{\sum_{u=1}^{m} \sum_{v=1}^{n} f_{ij}^{uv}}{\sum_{u=1}^{m} \sum_{v=1}^{n} f_{\max}^{uv}} \tag{5.6}$$

For more analysis of the power flow based model and vulnerability index, readers can refer to our previous Chapter 4 and [98]. The result from Chapter 4 shows that the lines with higher vulnerability index are more critical to the system when a failure happens.

In a real power system, generators, buses and transmission lines have their own fault probabilities. These fault possibilities of electrical devices may change during different failures. Six different types of severity failures [99], transmission line overload, bus power overload, high/low limit generator voltage violation, max/min limit generator frequency violation, are adopted in this research for comprehensive probability evaluation.

A. Transmission Line Overload

During the cascading event, a certain number of transmission lines may trip off with a certain probability. The concept of hidden failure in protection system is used to determine each line's tripping probability, which can be written as:

$$P_{ij} = \begin{cases} \overline{P_{ij}} & L_{\min} \leq L \leq L_{\max} \\ \frac{(1-\overline{P_{ij}}) \times L + \overline{P_{ij}} \times L_{\text{maxlimit}} - L_{\max}}{L_{\text{maxlimit}} - L_{\max}} & L_{\max} \leq L \leq L_{\text{maxlimit}} \\ 1 & L \geq L_{\text{maxlimit}} \end{cases} \tag{5.7}$$

where the P_{ij} denotes the overload probability of a transmission line during cascading events. The $\overline{P_{ij}}$ is the average overload probability of edge E_{ij}. The $L_{\max}$ represents the security

setting of line flow. Then maximum limit of the line capacity L_{maxlimit} is the value that the line will trip off directly.

B. Bus Power Overload

Similar to the transmission lines, a bus in power system can also overload and lose its capacity during the fault. The probability of bus overload for node i with total power injection p is defined as:

$$P_i = \begin{cases} \overline{P_i} & p_{\min} \leq p \leq p_{\max} \\ \frac{(1-\overline{P_i})\times p+\overline{P_i}\times p_{\text{maxlimit}}-p_{\max}}{p_{\text{maxlimit}}-p_{\max}} & p_{\max} \leq p \leq p_{\text{maxlimit}} \\ 1 & p \geq p_{\text{maxlimit}} \end{cases} \tag{5.8}$$

where $\overline{P_i}$ represents the average overload probability of node i. The maximal security setting and upper limit of a bus is denoted as $p_{\max}$ and p_{maxlimit} respectively.

C. Generator Failure

The failure probability of a generator is determined by the higher probability of a frequency violation and voltage violation [100]. Thus, the fault probability evaluation of generator i can be written as:

$$P_G = \text{MAX}\{P_f, P_u\} \tag{5.9}$$

where

$$P_f = \begin{cases} \overline{P_f} & F_{\min} \leq F \leq F_{\max} \\ \frac{(1-\overline{P_f})\times F+\overline{P_f}\times F_{\text{maxlimit}}-F_{\max}}{F_{\text{maxlimit}}-F_{\max}} & F_{\max} \leq F \leq F_{\text{maxlimit}} \\ \frac{(\overline{P_f}-1)\times F+F_{\min}-\overline{P_f}\times F_{\text{minlimit}}}{F_{\min}-F_{\text{minlimit}}} & F_{\text{minlimit}} \leq F \leq F_{\min} \\ 1 & F \geq F_{\text{maxlimit}} \text{ or} \\ & \quad F \leq F_{\text{minlimit}} \end{cases} \tag{5.10}$$

$$P_u = \begin{cases} \overline{P_u} & U_{\min} \leq U \leq U_{\max} \\ \frac{(1-\overline{P_u})\times U + \overline{P_u}\times U_{\text{maxlimit}} - U_{\max}}{U_{\text{maxlimit}} - U_{\max}} & U_{\max} \leq U \leq U_{\text{maxlimit}} \\ \frac{(\overline{P_u}-1)\times U + U_{\min} - \overline{P_u}\times U_{\text{minlimit}}}{U_{\min} - U_{\text{minlimit}}} & U_{\text{minlimit}} \leq U \leq U_{\min} \\ 1 & U \geq U_{\text{maxlimit}} \text{ or} \\ & \quad U \leq U_{\text{minlimit}} \end{cases} \tag{5.11}$$

where $[F_{\min}, F_{\max}]$ and $[U_{\min}, U_{\max}]$ stand for the generator frequency and voltage margin respectively. Moreover, the lower/upper limits of the frequency and voltage are denoted as $F_{\text{minlimit}}/F_{\text{maxlimit}}$ and $U_{\text{minlimit}}/U_{\text{maxlimit}}$.

From the definitions in this section we can see, the improved CN model considers more power system features compared with previous ones. Some key characteristics such as power flow, voltage and frequency are adopted in the improved CN model. This innovation can form a better approximation model for power system risk assessment compared with the existing CN model. At the same time, the improved model is not limited to component-level assessment. The consequences and probabilities of components are also considered with topological factors gained from CN theory. Thus, the proposed model can provide a system-level assessment during cascading events, which is not possible by traditional risk models.

5.3 Cascading Event Simulation Module

In a power system, a cascading failure can be triggered by either edges or nodes. An edge trigger is the tripping of a transmission line. Obviously, all power transmission on that edge is lost because of the disconnection. On the other hand, a node trigger is a failure on a bus, substation or generator. Once the node tripped from the system, lines connecting to the node are also effectively tripped since power flow cannot be transmitted through the malfunctioned node.

From the historical data, it can be asserted that the possibility of a node trigger is much lower than an edge trigger. Usually, the substations and generators are well protected. Thus, in a steady state power system, the occurrence frequency of the failure on them is quite rare. Theoretically, a node contingency is more likely caused by a cascading failure and causes

greater damage to the power system. So we only consider the cascading events initially triggered by an edge failure here. Nevertheless, node failures triggered by cascading are still considered for a better understanding of the cascading mechanism.

Typically, the generation and load keep a dynamic balance in a steady state power system. Thus, an initial risk distribution can be obtained from this steady state. A failure may break this balance and start a transient state. The balance of load and generation has to be restored via following re-dispatch process:

- Generation ramping: Power transmission disturbed by a failure causes a gap between generation and load. Thus generators need to ramp up or ramp down to maintain the system balance.
- Generation tripping/ Load shedding: However, generators have their own ramping rate limitation and output power limitation. Sometimes the system requires ramping rate and/or output over these limitations, to restore the balance. In this case, the balance cannot be restored only by generation ramping. If a surplus still exists, the generators will be tripped to decrease the total generation. On the contrary, after the generators hit their output limitation, load shedding will begin if the output is still not enough to cover the demand.
- Generation tripping/ Load shedding: However, generators have their own ramping rate limitation and output power limitation. Sometimes the system requires ramping rate and/or output over these limitations, to restore the balance. In this case, the balance cannot be restored only by generation ramping. If a surplus still exists, the generators will be tripped to decrease the total generation. On the contrary, after the generators hit their output limitation, load shedding will begin if the output is still not enough to cover the demand.

After the system achieves the new operating point, the parameters in the system have to be updated. Obviously, the topology of the system is changed due to the $N-1$ contingency. The degree of certain nodes may change as well. For power flows have been redistributed, edge weights and directions are redistributed. Therefore, the consequences and probabilities of transmission lines and buses are changed from the initial steady state. The voltage and frequency of generators are altered during ramping/tripping process. Loads may shed to keep the system operating balance.

With these updated data, a risk assessment for this stage can be obtained. The component with the highest risk ranking is considered as the next breaking point in the system. A cascading chain can be formed by combining these high risk parts from each stage. The cascading events only cease when there is no overload or the power flow of the system does not converge. In most cases, the non-convergence of power flow is caused by islanding. This means the system has collapsed and no longer a fully connected grid.

In summary, the procedure to evaluate the cascading chain in the proposed cascading event simulation module is illustrated in the following flow chart Fig. 5.1.

5.4 Case Studies

In this section, two test systems are carried out with the methodology explained in the previous sections. A small system (IEEE 14 bus system) is adopted to show the details of cascading event. Furthermore, a larger system (IEEE 39 bus system) is chosen to explain the cascading mechanism from an overall view.

5.4.1 IEEE 14 Bus System Scenario

The topology of the IEEE 14 bus system is shown in Fig. 5.2. It can be seen, there are 14 nodes and 20 edges with 5 generators and 11 loads in this system. The main power injections to the system come from generators on node1 and node 2. On the other hand, main loads in the system are located on node 3, node 4 and node 9. The consequence of nodes and edges in steady state are shown in Fig. 5.3 and Fig. 5.4 respectively. In Fig. 5.3, it can be seen that the node consequence is comprised by topological and electrical parts. Some nodes, such as node 9, are at a critical position but carry less power in the system. On the contrary, several nodes have high consequence with high importance in electrical structure. Also, it is not hard to find that this power network has the characteristics of scale-free networks. Fig. 5.4 demonstrates that most of the edges have low consequence in the system, while a few edges have an extremely high consequence at the same time. This structure shows that this power grid is robust to random attacks but can be vulnerable to the targeted attacks. The removal of lines with high risk may easily lead to a wide area cascading failure.

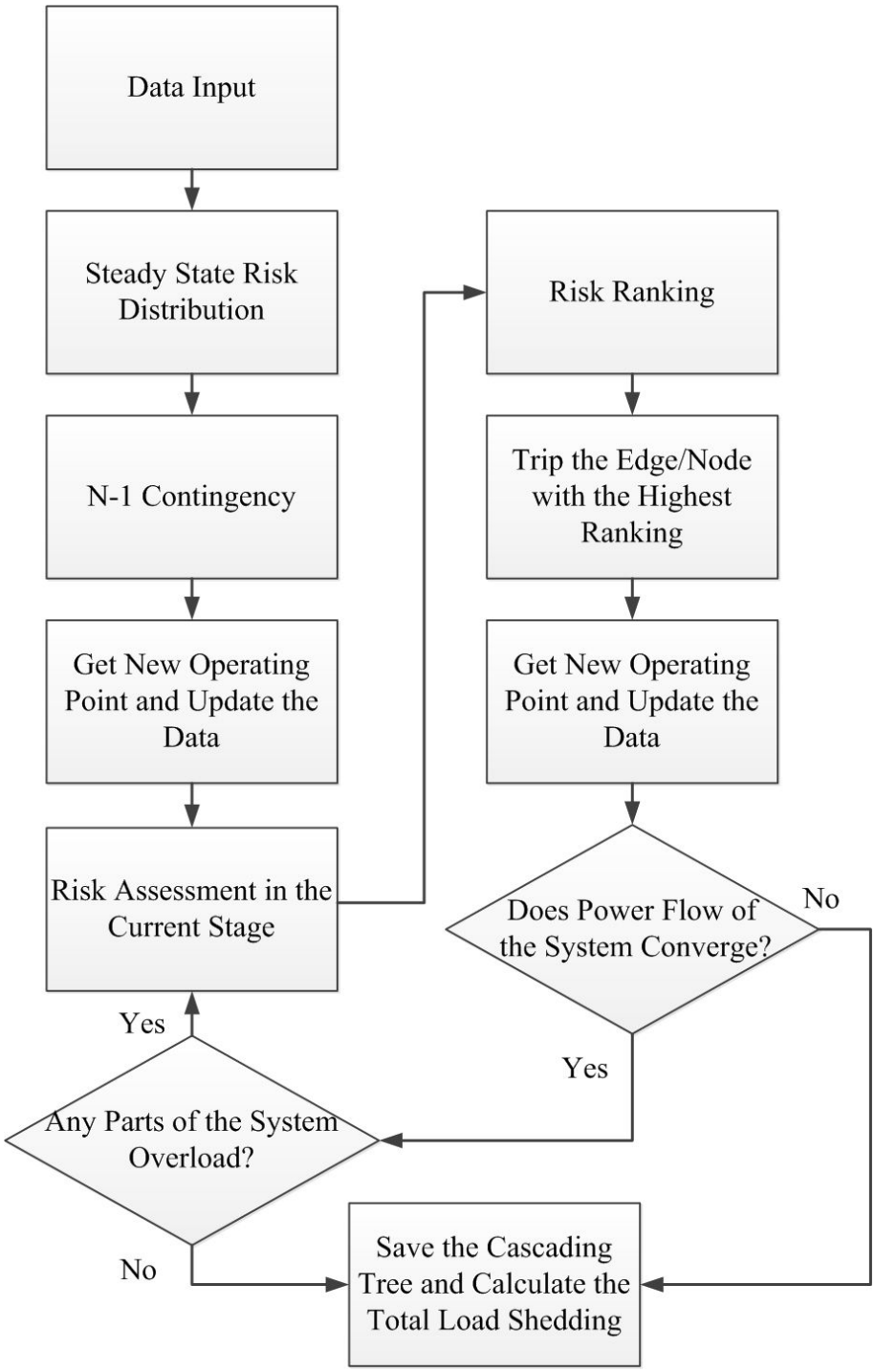

Fig. 5.1 Flow chat of cascading event simulation module

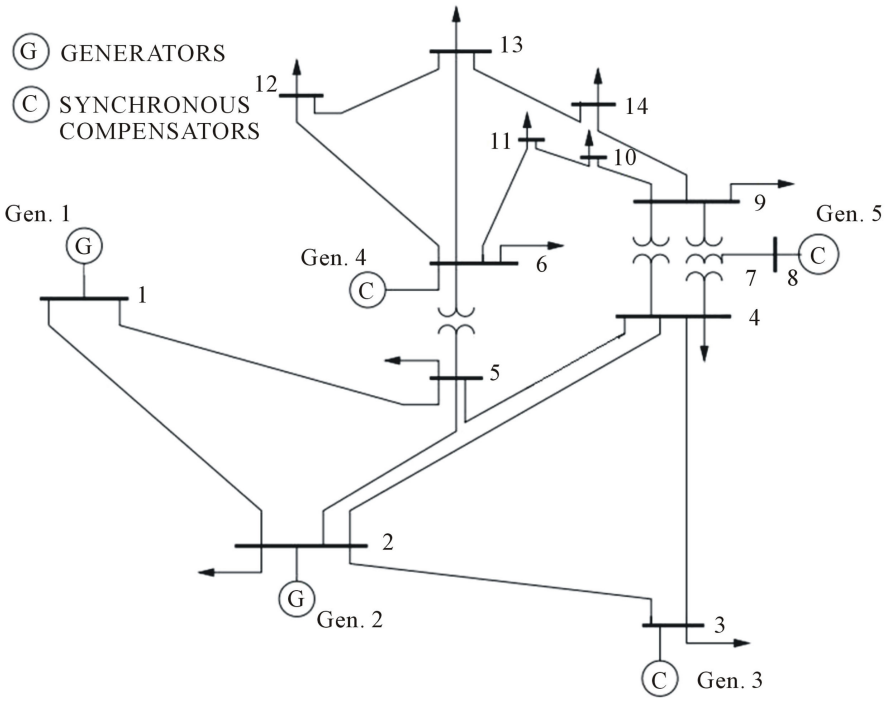

Fig. 5.2 IEEE 14 bus system

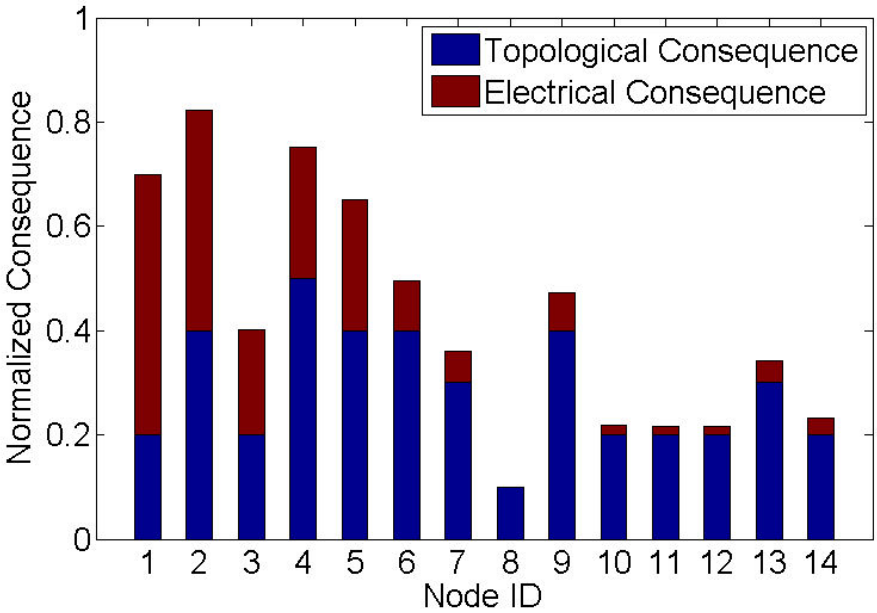

Fig. 5.3 Steady state node *C* distribution in IEEE 14 bus system

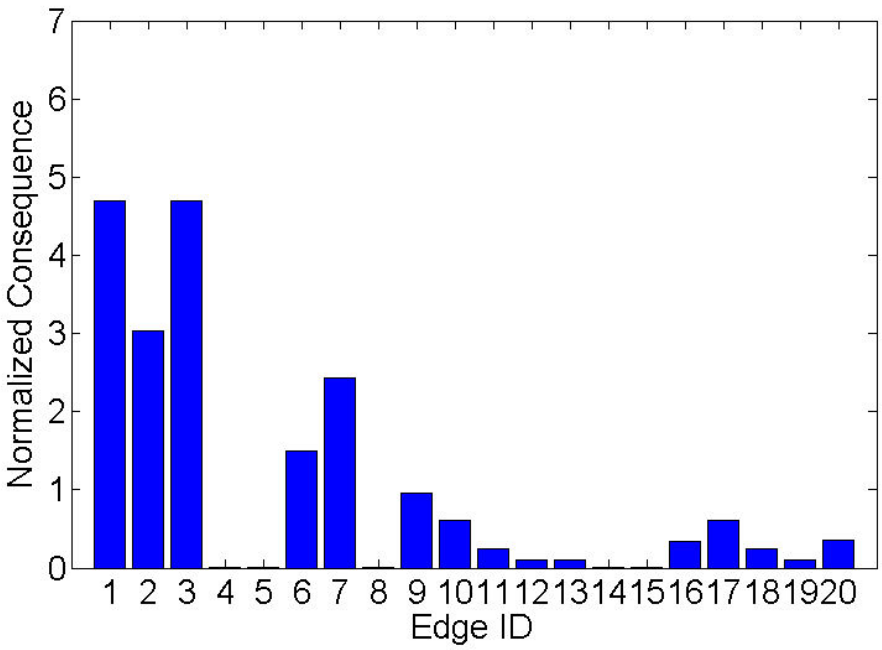

Fig. 5.4 Steady state edge C distribution in IEEE 14 bus system

A trigger event is applied on edge 3, which is the edge with the highest risk in the steady state. The cascading module follows the process described in Section 5.3. The detailed changes of risks on each node and edge are shown in Fig. 5.5 and Fig. 5.6 respectively. Stage 0 is the status from steady state, while stage 1 shows the status after first failure, and so on.

After edge 3 is removed from the system, the power supply from node 2 to node 3 has been interrupted. To maintain the power supply to the loads on node 3, node 4 has to transfer more power as it's the only node connected to node 3 now. At the same time, edges 7 and 6 are overloaded to cover the power transmission gap by losing edge 3. We can see from Fig. 5.5 and Fig. 5.6, the risk of node 4, edges 7 and 6 have increased greatly in stage 1. The failure probability of edge 7 is also increased since the power flow on the transmission line is over the security setting limit. This means that edge 7 is most likely to trip off from the system and starts a cascading in this case. When edge 7 tripped off, the burden of power supply to node 3 is completely carried by the edges 1, 2 and 6. Also, as the power injection from node 5 to node 4 is lost, the situation of node 4 gets worse. As a topological key node, node 4 is highly connected. Not only does it take on the irreplaceable position to supply the power to node 3, but it also bears the task to transfer power to nodes 7 and 9. From Fig. 5.5 we can see node 4 is likely to be the next breaking point. For the edges, it can be seen that edge 4 is also suffering an overload. As the only power input path to node 4, it carries over

300% power than it used to carry in steady state. This may result in overload and tripping off. Thus, after stage 2, node 4 or edge 4 no matter which one breaks out first, the system will collapse. Node 3 loses all power supply from outside and will shed 94 MW loads, which are over 36% of the total loads in the system.

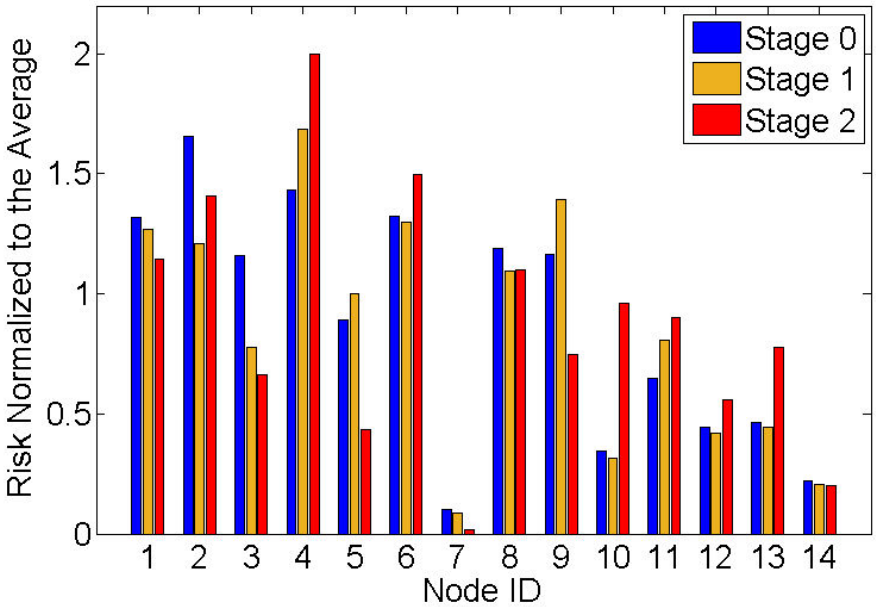

Fig. 5.5 Normalized node risk distribution in different stages during cascading event

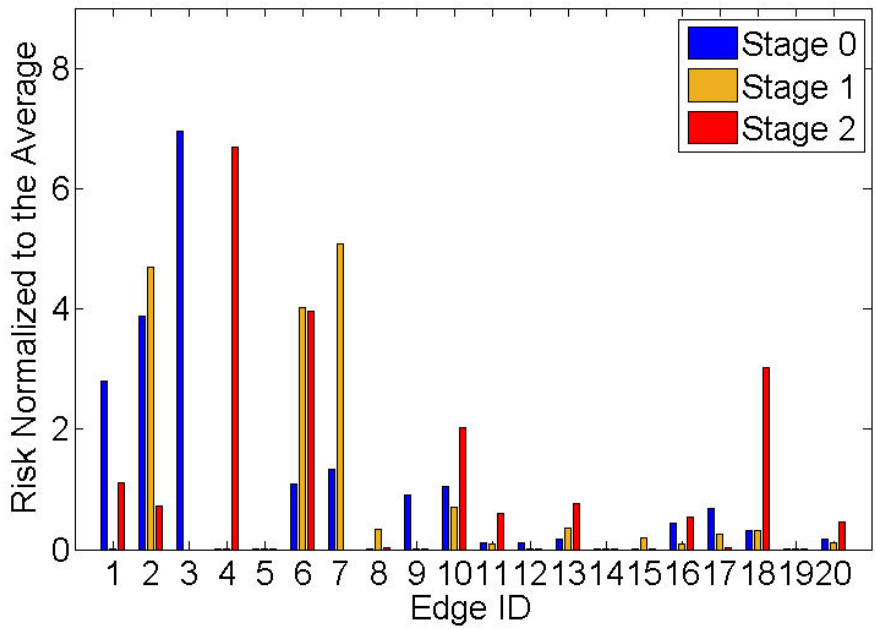

Fig. 5.6 Normalized edge risk distribution in different stages during cascading event

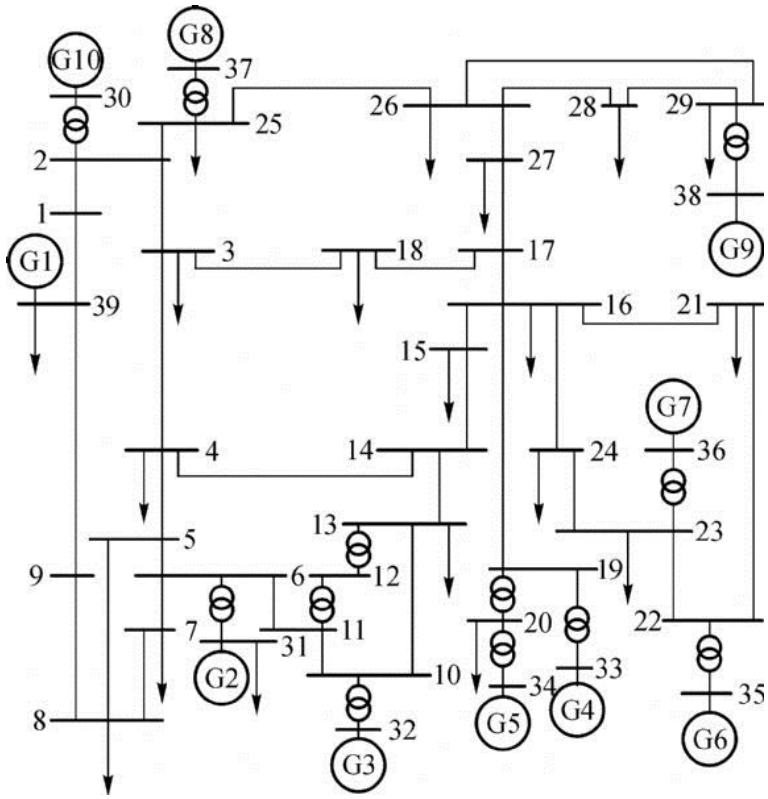

Fig. 5.7 IEEE 39 bus system

The following conclusion can be draw from the analysis above. A failure on edge 3 may lead to a cascading event in IEEE 14 bus system, and the most possible cascading chain would be edge 3- edge 7- edge4/ node4.

5.4.2 IEEE 39 Bus System Scenario

The standard IEEE 39 bus system (shown in Fig. 5.7) is chosen as a benchmark system to demonstrate the proposed method from a system-level view. The risks of each edge and nodes are calculated and normalized to their average value respectively. The steady state risk distribution in the IEEE 39 bus system is shown in Fig. 5.8. To show how the failures spread among the different areas of the grid, the risk profile is plotted under a planar representation of the power grid. It can be seen that most of the edges and nodes in the IEEE 39 bus system have low values of the risk index. On the other hand, several edges have high risk indices, meaning that they are more critical in the system.

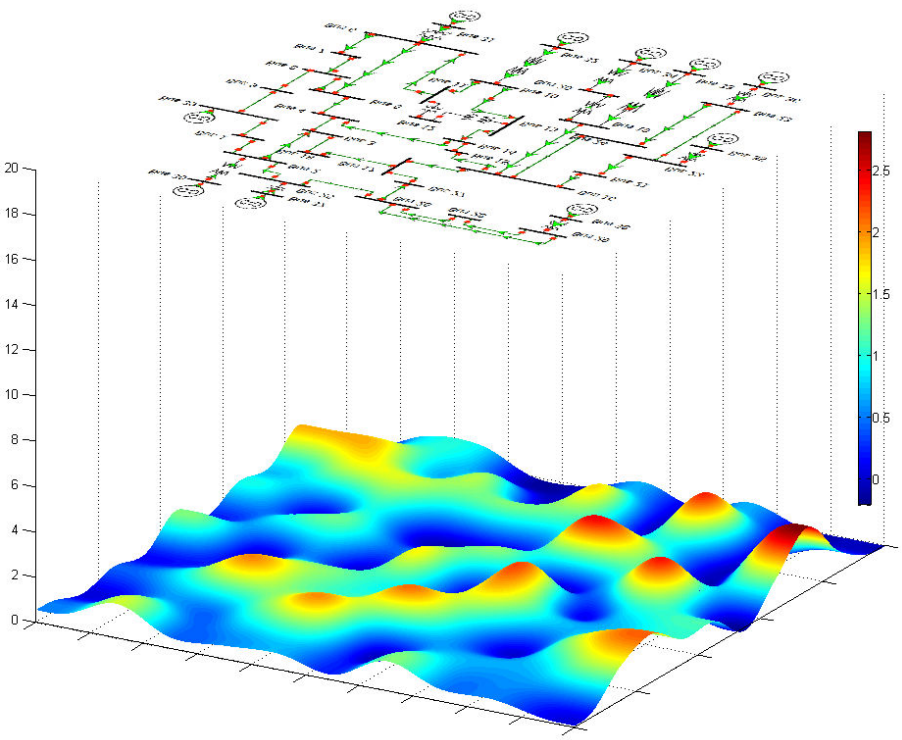

Fig. 5.8 Steady state risk geographical distribution in the IEEE 39 bus system

First, a targeted attack has been applied to edge 37, which has the highest ranking by risk index in steady state. The changes of risk distribution during cascading are displayed in Fig. 5.9 and Fig. 5.10. It can be seen that the risk distribution changed a lot from the steady state after edge 37 is tripped off. As the power supply to the loads on nodes 15, 21 and 16 from the generator on node 35 is no longer available, transmission edges in the middle part of the system are forced to carry more power to maintain the power supply. The risk of edges 23 and 10 has increased greatly compared to the others. Edge 23 has the highest risk ranking in this situation, which is most likely to trip off and start a cascading failure. It is worth noting that edge 23 is not the only the transmission edge that keeps the loads mentioned above alive but also the edge connecting the generator on node 32 with the loads on nodes 3 and 4, which are other load centres in the system. Thus, after edge 23 is removed, the power supply from the right side of the system to the load centres located on nodes 3 and 4 are interrupted. In this case, the edge 10 has to carry even more power than in the previous stage. It can be seen clearly from the figure, that edge 10 has the highest risk and is facing trip off at this stage. A large amount of load shedding is required to node 3 and 4. Otherwise, when edge 10 is tripped off by its overload, the edges connected to those nodes will be overloaded and the entire system collapses. Thus, the cascading chain here is edge 37- edge23- edge 10.

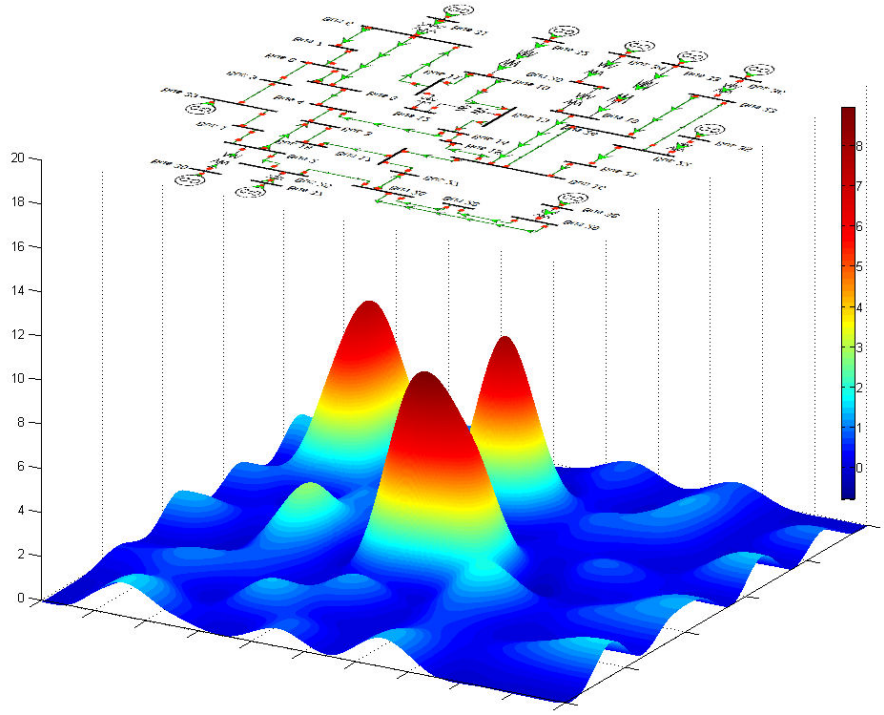

Fig. 5.9 Geographical risk distribution in IEEE 39 bus system after targeted attack stage 1

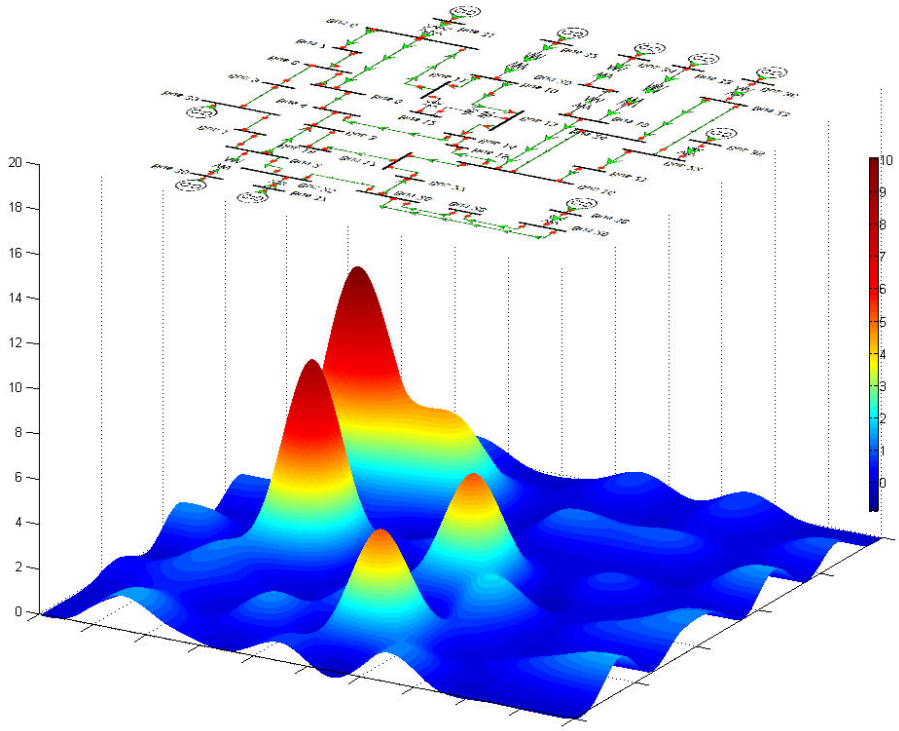

Fig. 5.10 Geographical risk distribution in IEEE 39 bus system after targeted attack stage 2

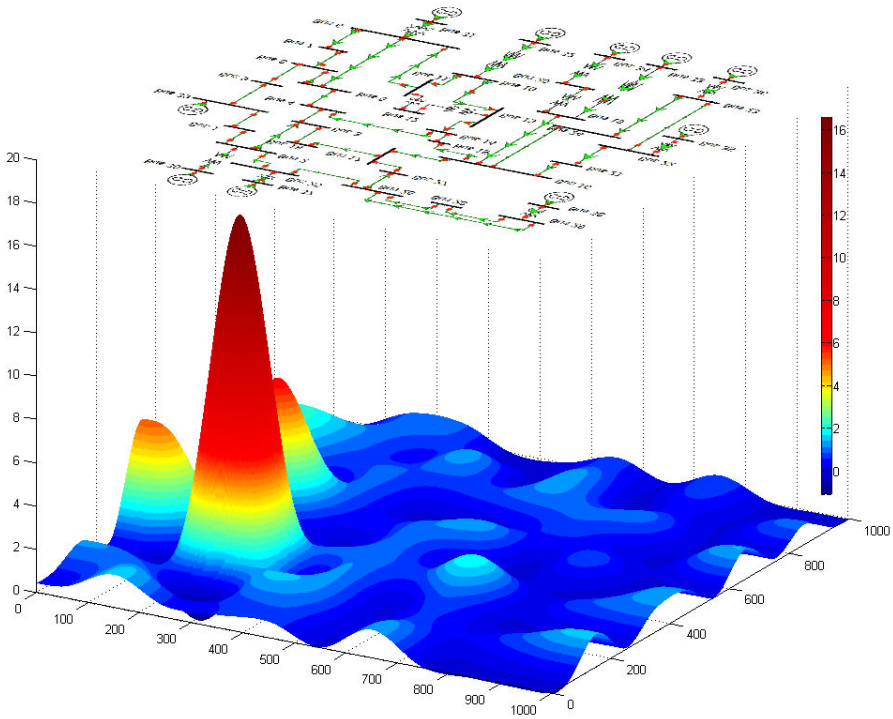

Fig. 5.11 Geographical risk distribution in IEEE 39 bus system after random attack stage 1

Furthermore, random attacks have also been applied to the simulation system. Here we take the fault on edge 1 as an example to see how the cascading failures spread in the system. The risk distributions during the cascading are shown in Fig. 5.11 to Fig. 5.13 respectively.

It can be clearly observed from Fig. 5.11 that after edge 1 is removed from the system, the risk of edge 3 has increased significantly. This edge carries over 150% more power than the normal situation. The value is over 10 times more than most of the other parts in the system. When edge 3 is disconnected, the path from node 18 to node 4 (contains edge 7, node 3 and edge 6) is going to turn into a high-risk area as shown in Fig. 5.12. This indicates that there is a great power shift between edges. In this situation, either edge 6 or edge 7 may trip off due to the excessive overload. This will speed the deterioration in the position of node 3, and bring additional burden to edge 8, which is the only power injection to this load centre after edge 3 and edge 7 are lost. Fig. 5.13 demonstrates the final stage of this cascading event, and edge 8 is holding the highest risk. Once edge 8 trips off, nodes 3 and 4 are isolated from the system. They will lose all power supply from outside and form an island. More than 500 MW loads are lost for this cascading event, which are over 13% of the loads in the entire system. The most possible cascading chain caused by this random attack

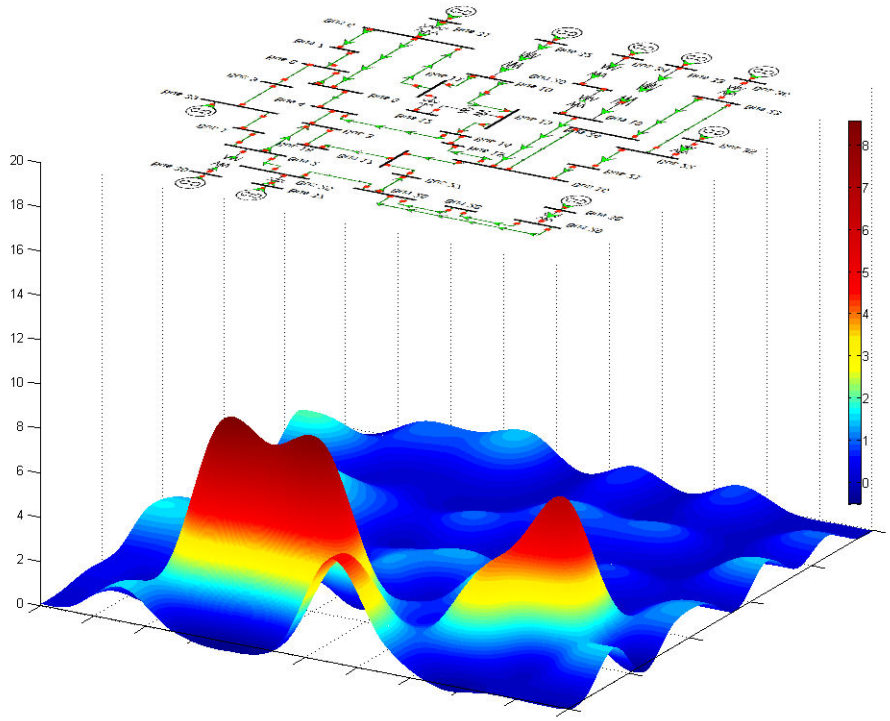

Fig. 5.12 Geographical risk distribution in IEEE 39 bus system after random attack stage 2

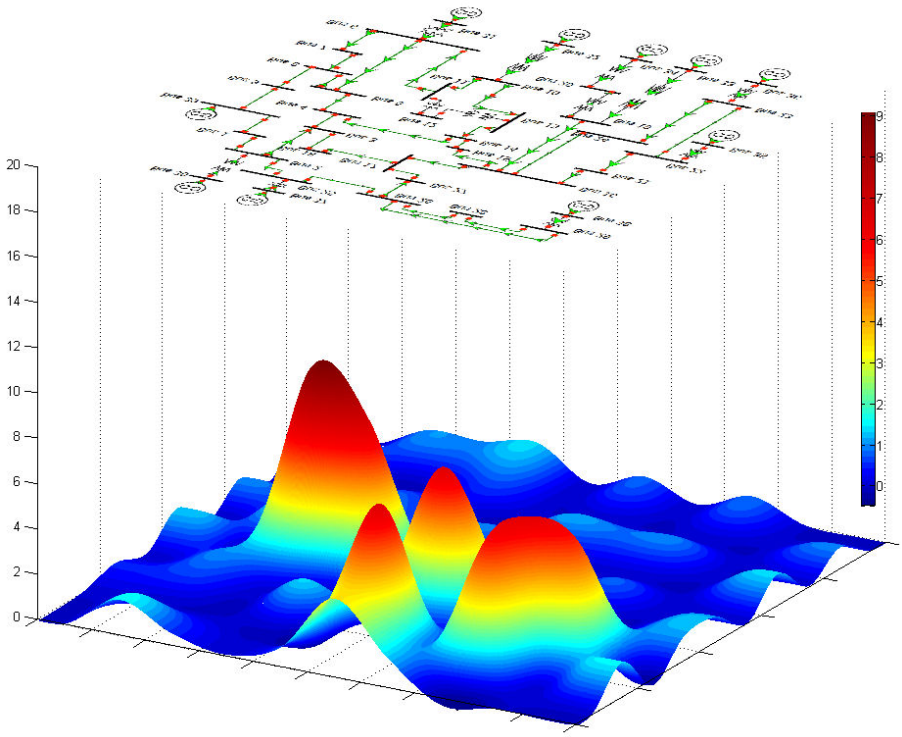

Fig. 5.13 Geographical risk distribution in IEEE 39 bus system after random attack stage 3

we can draw here is edge 1- edge 3- edge 6/edge 7- edge 8. This result can be a guidance to help the operators predict the hidden risk of cascading and make a better protection plan.

5.5 Summary

To fulfill the strengthened security standards against cascading outages, their risks should be addressed in system security assessment. Existing methods suffer from various drawbacks such as missing critical characteristics of the power system or suffering from massive simulations. In this chapter we introduce a new approach for cascading risk assessment, which considers both topological and electrical characteristics. Based on the power flow based CN model mentioned in Chapter 4, six different types of failure method on nodes and edges during cascading are considered respectively. Simulation results demonstrate the effectiveness of this approach to identify the critical part of the power system during cascading events. The possible cascading tree gained by simulation module can also help the operator to predict the next step cascading fault and minimized the damage to the system.

In this chapter, we present a new direction for risk assessment in power system. In reality, the power system is usually connected to a communication system. It is worth paying more effort on analysing the impact of cascading between those two networks. In the next chapter, the impact of these factors will be considered.

Chapter 6

Risk Assessment in Cyber-physical System

6.1 Introduction

During normal operation of a power system, primary and secondary controls are responsible for stabilizing the grid. However, during large failures such control cannot stabilize the grid. Therefore, a modern power grid should be equipped with a communication and control network. This interdependency network allows constant monitoring of the power grid with rapid response, providing optimal centralized control actions to mitigate the damage of failures. This kind of "emergency control" can not only improve the performance of the grid, it also creates a dependency between the power grid and the communication network. Specifically, when the grid is under stress, loss of communication can lead to catastrophic failures, such as failures caused by natural disaster that affect both the communication network and the power grid or the failure of communication components due to the loss of power supply from the grid. It is relevant to note that a report by Kirschen and Bouffard [41] has identified that failures in the information infrastructure were a significant factor in most recent system collapses. Therefore, studying the impact of communication network on the power system security during failures is of great importance.

The impact of a communication network on its related power grid's performance was recently studied using a simplified form of interdependency. In [3] showed that if a one-to-one

interdependency between the nodes of the power grid and the nodes of the communication network occur, the interdependent networks will be more vulnerable to failures than the isolated networks. In their "point-wise" interdependency model, a power node may fail if it loses its control connection from the communication network node, and a communication node will also fail if its power supply is lost from the power grid. Similar results can be obtained from [101][102]. Ref. [3] indicated that coupled scale-free networks are more vulnerable to failures compared to a system consisting of two random networks. Then, Buldyrev et al. extended the network model in [103], in which nodes in each network have multiple inter-links and the number of interconnections for each node is identical. Ref. [104] developed the model networks so that each node has a different number of interconnections, and the distribution of the inter-links follows a Poisson distribution. Ref. [105]proposed "regular allocation" of inter-links to show the improvement of robustness compared with random allocation techniques. Although the study of [106] modelled cascading failures in the smart grid, each communication node in the model can only have one power source.

However, in a modern power system, the structure of a communication network does not necessarily correspond to that of the power grid, which means the point-wise model is not suitable for modeling a power-communication interdependent network. Moreover, the loss of a communication network component may not directly lead to the loss of control of a corresponding power grid component. More realistically, only when the two conditions are met, that is, when the line overloads and becomes uncontrollable, does the transmission line trip off.

Based on this background, here we propose a novel approach for modeling the interactions between power systems and combined communication networks to investigate the cascading process. The PF based CN model and cascading module mentioned in Chapters 4 and 5 are adopted here for the power grid side. Based on graph theory, we built a topological model for a communication network. A data exchange rule considering the data transmission characteristics is employed. We also recommend a new approach for interdependence between a power grid and a communication network. A cascading simulation is adopted on IEEE 39 bus system. In an attempt to show how a communication network impacts the vulnerability of the power system, the results are compared with risk changes without a communication network.

The remainder of this chapter is organized as follows. In Section 6.2, communication network modeling and data exchange rules are briefly described. The method for interaction

between power systems and combined communication networks is established in Section 6.3. Case studies are carried out in Section 6.4. The conclusions and discussions are given in Section 6.5. The research in this chapter is partly based on my own publication P.3.

6.2 Cyber-Physical Network as a CN Model

The power-communication interdependent network can be divided into two general layers: the physical layer and the cyber layer. The physical layer includes electrical devices for power generation, transmission, distribution and consumption. The cyber layer is represented by the communication network, which is used to gather, transfer and process the data with consideration of the structural and transmission characteristics [107]. Data from all electrical devices is sent to the control centre via a communication network. The control centre can monitor the status of the power system and send control commands to power grids when necessary. In previous chapters, we have introduced PF based CN model for the physical layer. We focus on the CN model for the cyber layer in this chapter.

6.2.1 The CN Model of Communication Network

As it bears a resemblance to a power grid, a communication network can be described by a graph with nodes and edges. However, unlike the PF, where powers usually have a one-way direction, the data can be transferred bi-directionally in a communication network. Also the telecommunication lines usually have very high capacity compared to the data size. The transmission line "over load" situations experienced in a power system rarely occur in communication networks. The topology of a power grid is usually determined by the geographical distribution of power plants, substations, cities and industrial demands. On the other hand, the topology of communication network is more flexible and widely dispersed. The research in [102] shows that most of the communication networks have the characteristics of scale-free networks. The nodal degree is distributed as a power law; a small fraction of the communication nodes act as hubs that have a greater number edges than the average. Thus, in our research, the communication CN model is proposed as an undirected scale-free network with the following assumptions:

- The communication network is a connected network without parallel lines.

- The capacity of communication line is enough to handle all the data.
- Each bus in a power grid is coupled with a combined communication node in the cyber layer.
- For each transmission line between two buses, there are two related communication nodes. Normally, the buses have different voltages. Only the communication node coupled with the higher voltage bus is used to exchange information.
- A special communication node enacts a control centre in the cyber layer. All data collected by combined communication nodes are transferred to the control centre via other nodes. Then the control decisions made by the control centre are sent back to the physical layer via the same combined communication node.

6.2.2 The Rules for Data Exchange

As we mentioned above, the data information is transferred between a bus combined communication node and the control centre via the communication network. To demonstrate the data exchange process, data exchange rules [108] are employed as follows:

- When an unusual signal, such as transmission line overload, is observed from the power grid, the coupled combined communication node generates a message packet.
- Each message packet has a *Sender* and a *Receiver*. The packet can be sent out and received by each communication node once in every single step.
- In each step, for a communication node with a message packet, if the Receiver of the packet is in its *Neighbours* sets, the message packets are sent to the Receiver node directly.

Otherwise, the message packets will be transferred to one of the neighbour nodes based on the chosen probability P, as in (6.1) [108].

$$P_j = \frac{e^{-\beta H_j}}{\sum_{m \in N_i} e^{-\beta H_m}} \tag{6.1}$$

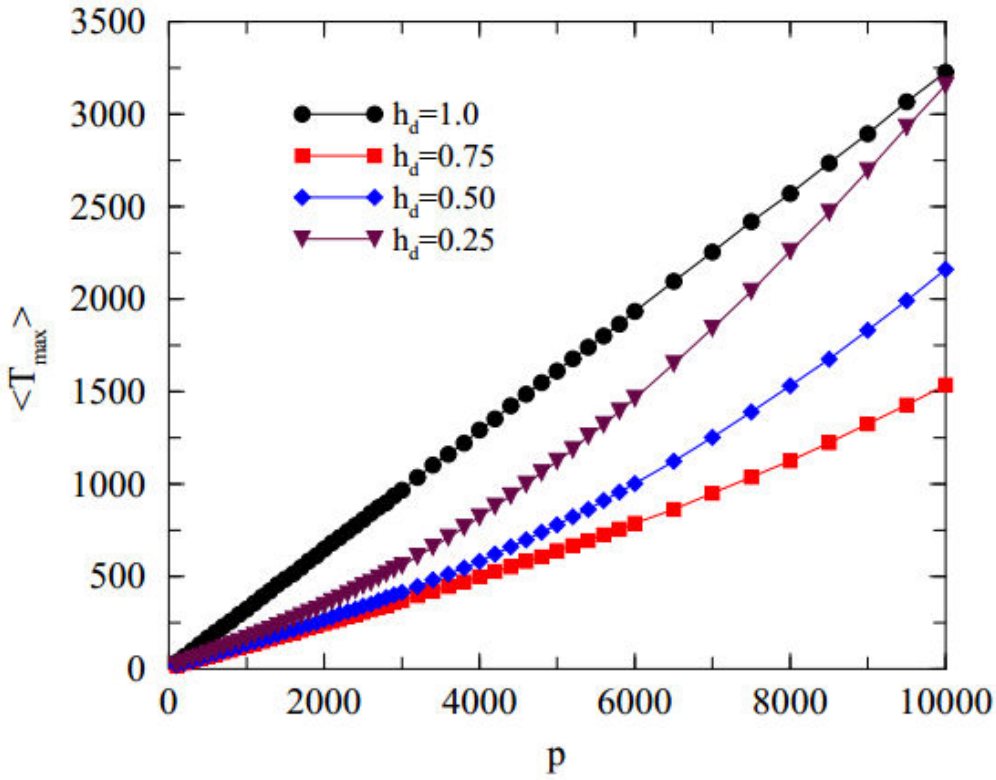

Fig. 6.1 The maximum transmission time with different h_d

$$H_i = h_d d_i + h_c c_i \tag{6.2}$$

where d_i is the shortest path between node i and j, c_i is the number of packets in the queue of node i, and $h_d + h_c = 1$. Also β is the inverse of the temperature (constant) of the communication network. In the research of this chapter, we take $\beta = 20$.

This probability clearly depends on the weight h_d, since it is straightforward to realize that if h_d is zero, the packets are diverted to the less loaded node regardless of the path length which results in an uncontrolled increase in the distance traveled by the packets from the *Sender*. Fig. 6.1 shows the maximum packet travel time T_{max} (steps) changes with different h_d in a communication network with p nodes and $\beta = 20$. It can be seen that although the tendency of the curves is to cross the straight line as p increases, there is an optimal value of h_d. So, in our research, the h_d will be set as 0.75 which approaches the optimal value.

The communication network will repeat the behaviours until the message packets are sent to the *Receiver* (in our case, mostly the control centre). Then the control commands will be sent back to the original *Sender* via the same process.

For the convenience of statistics and calculations, the time, in terms of number of steps, needed for a message packet to transfer from a combined communication node of edge ij to the control centre and receive the feedback command is defined as T_{ij}.

6.3 Interactions between Power Grid and Communication Network

The main idea for the new interdependency model between a power grid and a communication network is shown in Fig. 6.2. Initially, when a fault hits the power grid and causes an $N-1$ contingency, the power supply to the combined communication node is gone. The topology of the entire cyber layer changes as the node is removed from the communication network directly. Also the redistribution of power flow may result in other transmission lines becoming overloaded. As we introduced in previous sections, an abnormal message packet will be generated from the coupled communication nodes. The abnormal message packet is sent to the control center, obeying the data exchange rules shown in Section 6.2. The control commands are sent back to the Sender after the control centre receives this message packet. The reaction time for the overloaded transmission line to survive is limited. The inverse-time overcurrent protection is employed here as an index to identify the control command effectiveness [33]. When a line ij is overloaded, the time t_{ij} of inverse-time overcurrent protection is calculated as in (6.3) :

$$t_{ij} = \frac{K}{\left|I_{ij}/I_{\mathrm{set}ij}\right|^{\alpha} - 1} \tag{6.3}$$

$K = 7$, $\alpha = 0.3$, I_{ij} and $I_{\mathrm{set}ij}$ are the current and setting current, if $t_{ij} < T_{ij}$, the protection acts, that means the overloaded line is tripped before the control command arrive. If complete control is finished before the overloaded line is tripped, we define it as an effective control. Otherwise, it may start a new cycle of cascading failure without a timely control command.

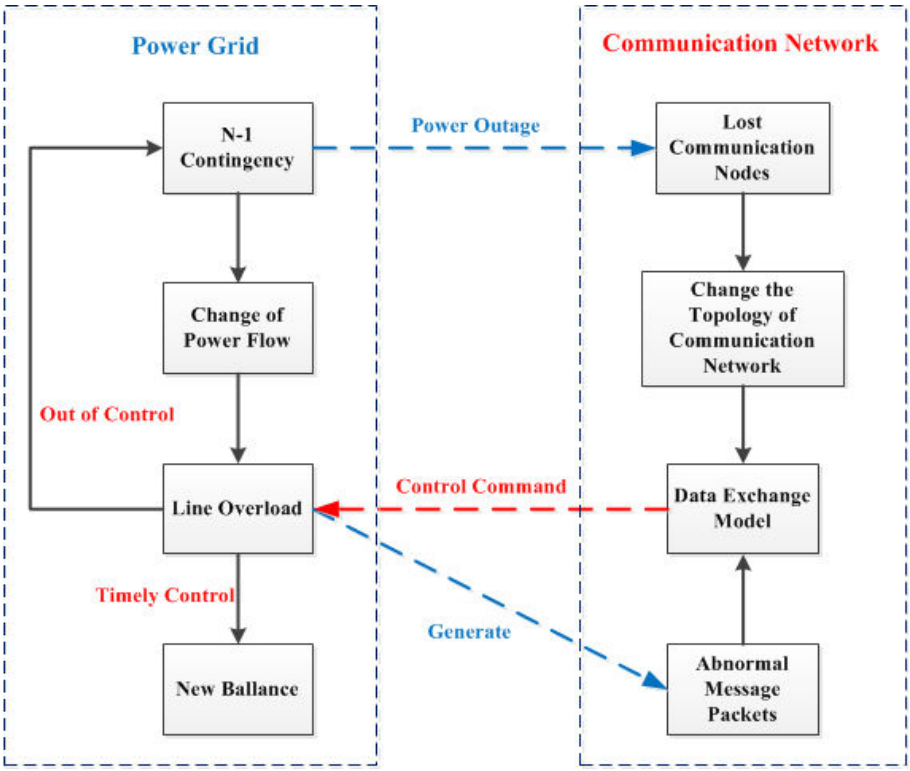

Fig. 6.2 The interdependency between power grid and communication network

It is apparent that the higher severity of overload the transmission line faces, the shorter reaction time the system has.

Here, a simple example of the cascading interdependency between a power grid and a communication network is presented. Please note the data here is purely hypothetical, and is introduced for purposes of illustrating the process described in this section.

Fig. 6.3 (a) shows the initial state of a simplified cyber-physical network. The nodes and edges on the left side, which are marked with blue, are the power grid, while the communication nodes and path are marked in green on the right side. The control centre is denoted by the yellow node. To simplify the model, we just show the power supply to the combined communication nodes here. Then, we assume the first fault occurs on edge DC.

After edge DC is removed from the power grid, edge BA, edge DB and edge EC are overloaded. From Fig. 6.3 (b) we can see the abnormal message packets are generated from combined communication nodes b, d and e. t_{BA}, t_{DB} and t_{EC} are given as 4, 2 and 5 respectively. The abnormal message packets are transferred under data exchange rules introduced in Section 6.2.

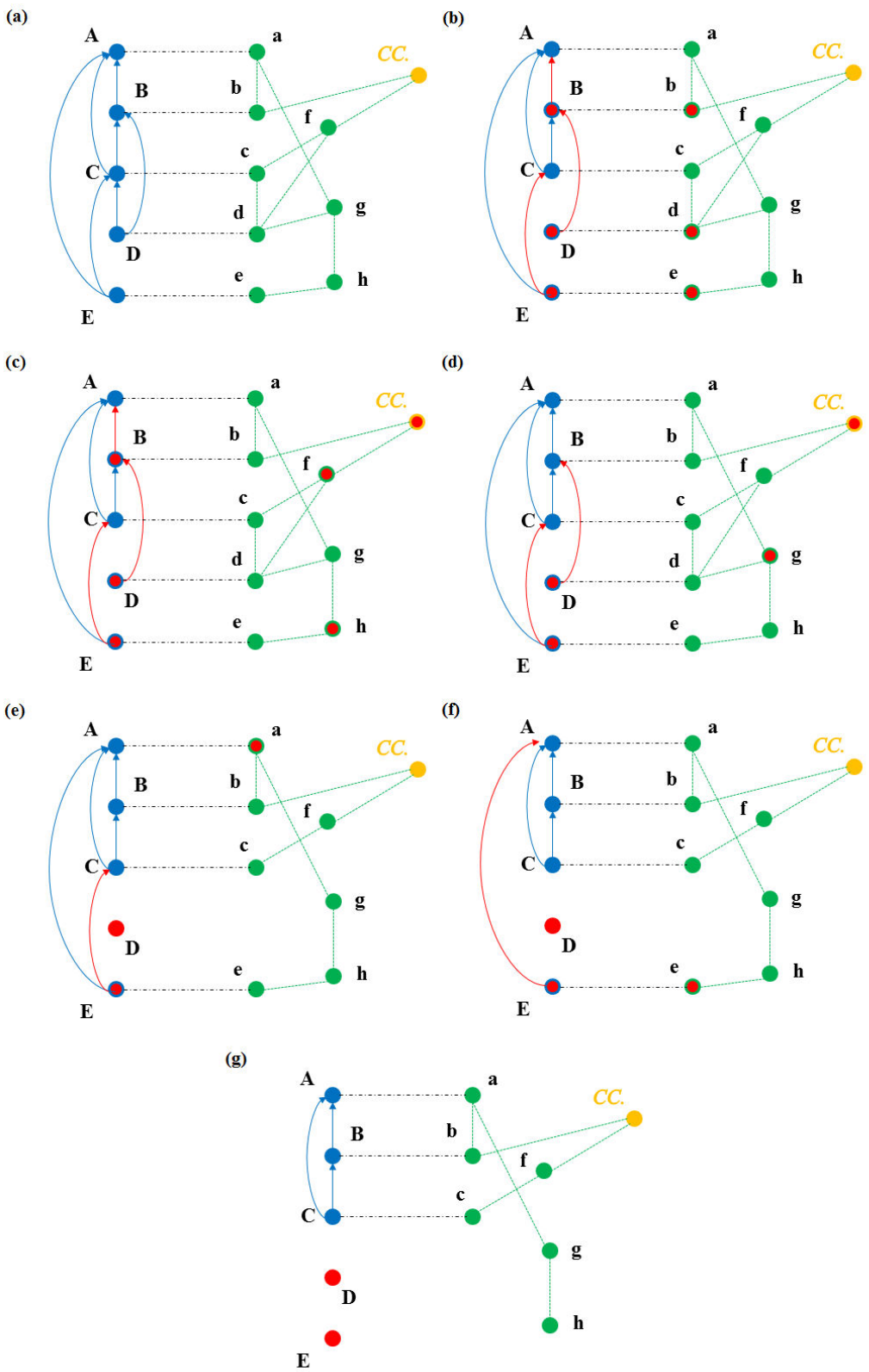

Fig. 6.3 An example of the cascading interdependency between power grid and communication network

Fig. 6.3 (c) demonstrates the data exchange progress in the system. Here we can find the abnormal message packet sent from node b has already arrived at the control centre and the control commands will be sent back to node b in the next step. From Fig. 6.3 (d), it is easy to see that the control command is received before the overload line BA trip off. Thus, in Fig. 6.3 (e), the line BA is running under permission again. In contrast, t_{DB} is larger than T_{DB} means the feedback data packet from control centre cannot be sent back to node d on time. Transmission line DB is tripped off due to the delayed control command. Meanwhile, node d is removed from the communication network as a consequence of losing power supply from the power grid. In Fig. 6.3 (f), a cascading failure is triggered. As line EA is newly overloaded, an abnormal message packet is generated in node e. Unfortunately, the control command cannot arrive in the combined communication node since $T_{EA} < t_{EA}$. Several steps later, the cyber-physical network is collapsed as it is shown in Fig. 6.3 (g).

6.4 Case Study

The IEEE 39 bus system (shown in Fig. 5.7) is chosen as a benchmark system of the physical layer to demonstrate the proposed method. The communication network with 100 communication nodes, which contains one control centre, is generated with graph software Network X. The communication nodes are connected, and its nodal degree distribution obeys a power law to form a scale-free network structure.

Firstly, random attacks are applied to the standard power system and the cyber-physical simulation system respectively. Here we pick the attack on line 2 and line 38 as a demonstration. The main load demand buses in the system are monitored to calculate the total load loss after cascading events, which are shown in Fig. 6.4. It can be seen that after the power grid is connected to the communication network, the power system performs better against random attacks. Lost capacity on each node has decreased respectively. This example illustrates the control strategy can help a power system to mitigate the damage of cascading failures.

Furthermore, the targeted attacks are applied to the cyber-physical system. Similar to the simulations we have done in Chapter 5, the power transmission line with the highest risk ranking is removed firstly. The removal of the transmission line may change the power flow distribution in the power grid and/or the topology of the communication network. A

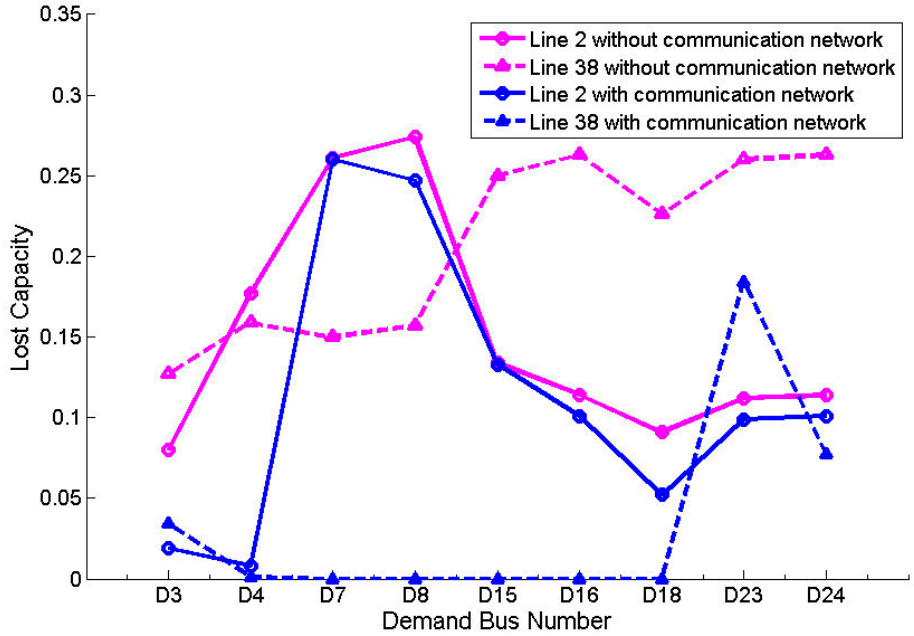

Fig. 6.4 Lost demand capacities under random attacks

cascading event will spread in the cyber-physical system until a new dynamic balance point is achieved.

To demonstrate the impact of communication network structures and connection patterns of two layers on the cyber-physical system, four different scenarios have been studied here. Besides the scale-free communication network we mentioned above, a random communication network is generated. It also has 100 communication nodes with one control centre among them. The connection of the nodes is totally random, which means the nodal degree in this communication network follows a Poisson distribution. Then these two communication networks with different structures are each connected to IEEE 39 bus system through two different ways.

In Scenario 1, the scale-free communication network is connected to the power system and obeys "degree to degree" connection rule, where we connect the power bus nodes with the highest degree to the group of highest nodal degree hubs in the communication network. The same connection rule is adopted to the random communication network in Scenario 2. Then the scale-free communication network and the random communication network are randomly connected to the power system in Scenario 3 and 4, respectively. The conditions of these four scenarios are simply summarized in Table 6.1.

Table 6.1 Four scenarios of targeted attack to cyber-physical networks

Inter-similarity	Scale-free Network	Random Network
Degree to Degree Connection	Scenario1	Scenario2
Random Connection	Scenario3	Scenario4

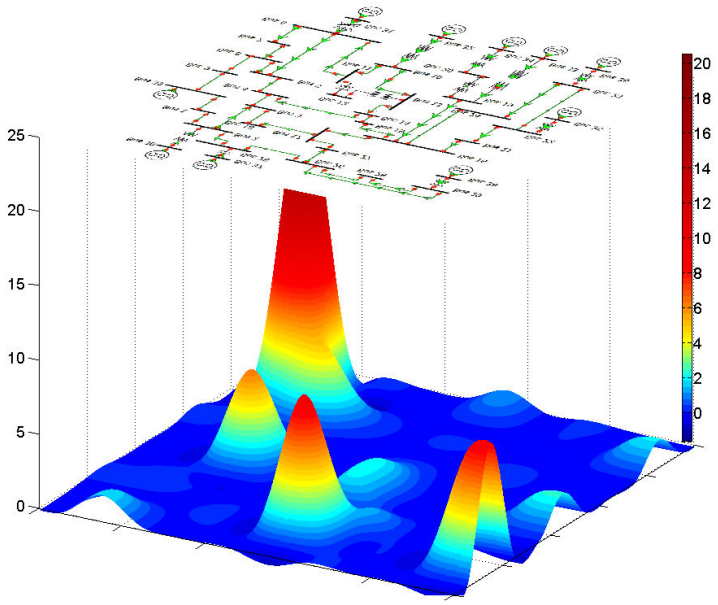

Fig. 6.5 Geographical risk distribution after attacks in Scenario 1

Since we have already introduced the detailed cascading progress in power layer in Sections 5.3 and 5.4, and the interactions between two layers in Section 6.3, here we only present the simulation results.

A complete disaster happens in Scenario 1. Once the highest risk ranking line is removed, the related transmission lines suddenly have to carry more power to neutralize the gap. Many abnormal message packets are generated in the combined communication nodes around the breaking points. However, as a communication hub coupled with node 35 lost its function, a large number (27 in this scenario) of communication nodes and telecommunication paths disconnected from the hub. This incident increases the path length the abnormal message packets need to pass through and message packets start queueing in the communication

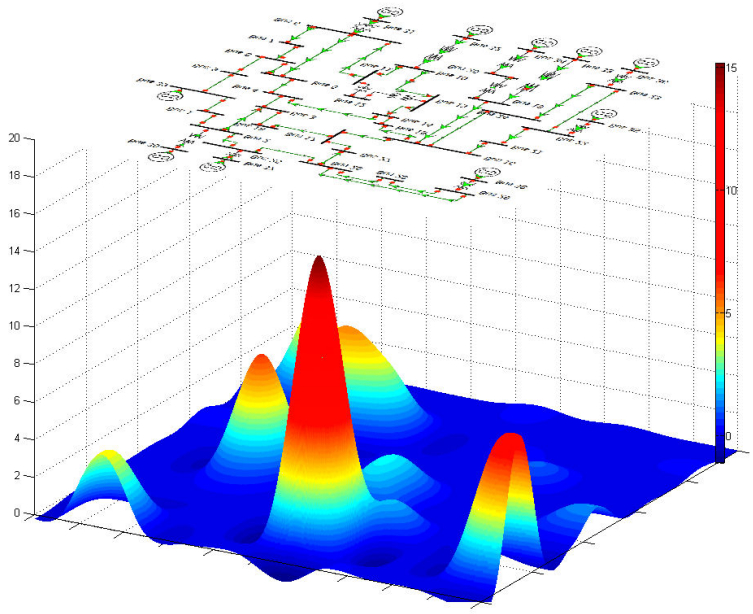

Fig. 6.6 Geographical risk distribution after attacks in Scenario 2

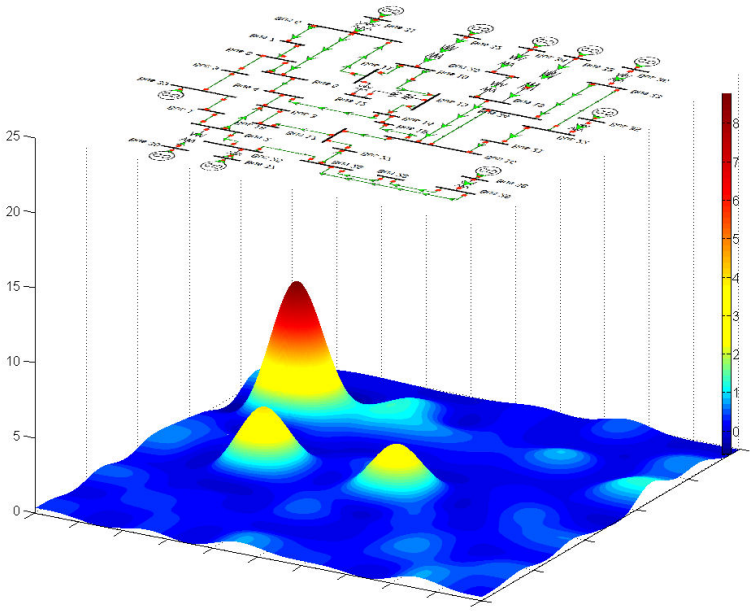

Fig. 6.7 Geographical risk distribution after attacks in Scenario 3

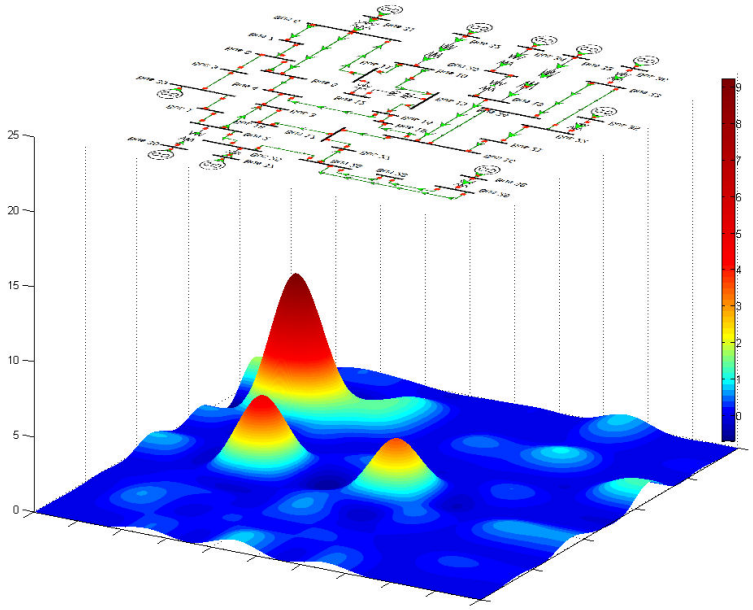

Fig. 6.8 Geographical risk distribution after attacks in Scenario 4

network. The delay to the control command leads to another line trip off and starts a cascading failure.

A similar situation is also observed in Scenario 2, although the failure was not as severe as in Scenario 1. The random network average nodes distance is larger than the one in the scale-free network. The delay still happens and leads to a larger hidden failure.

For the group of random connected networks. More communication nodes are lost in Scenarios 3 than 4. Nevertheless, the performances of these two scenarios are largely identical but with minor differences. As discussed in Chapter 3, the network structure plays an important role in communication networks. When an overload line is coupled with a scale-free network, it has higher chance to receive effective control. A communication network with hubs has diverse outcomes. When those key nodes have not been destroyed, they can provide the coupled system with a strong form of protection, but once they malfunction in the communication network, there is a great risk of collapse in both layers of the cyber-physical network.

6.5 Summary

In this chapter, we present a new approach to CN modelling in cyber-physical network security assessment. A structural communication model is coupled with a power system. A data exchange rule which improves on the existing "point-wise" interdependency model is introduced. The interactions between the two layers are described in detail. Finally, we use simulation results to explain the impact of a communication network on a power system. During random attacks, the control command can mitigate the damage to the power grid. However, sometimes the communication network can accelerate the cascading process and cause a severe blackout. Therefore, designing a robust communication structure and interdependency strategy is of great importance.

Chapter 7

Conclusions and Future Work

This thesis is motivated by the direction that the structure of power systems becomes increasing complex. For example, a single failure occurring in a vulnerable part of a power system may cause a wide area cascading collapse. Therefore, an advanced method that can assess power system security levels is needed, and complex network (CN) theory has emerged recently to be a new direction for power system security assessment. This thesis makes several extensions towards achieving more usable techniques based on CN ideas.

Firstly, we presented how power system stability is greatly impacted by the unpredictable, fluctuating characteristics of the renewable energy. The scenarios studied show that these new features are expected to have a negative impact on the stability and security of the power grid, bringing new risks of cascading failures. Thus, we introduced a new CN model for vulnerability analysis given renewable energy integration. Numerical simulations are investigated based on the 14-generator model and realistic data of solar and wind output in Australia. The results show the impact of renewable energy sources on the power network under different penetration levels and load conditions.

Secondly, we attempt to give some guidance on how to design a better communication network in a PV-ES combined system. A distributed optimization algorithm has been introduced. Units in the system exchange information through the communication network to maximize the net profit cooperatively. Then we analyse the performance of this distributed optimization algorithm on several classic network topologies in an innovative way. We investigate a series of simulations based on graph theory. The implication of Laplacian

eigenvalues and degree distribution are discussed, and we show the potential of the optimal topology for a communication network.

Then, we made a further step towards a CN model for vulnerability analysis by considering more electrical power factors. An innovative model which considers power flow (PF), one of the most important characteristics in a power system, is proposed. Moreover, based on the complex network theory and the Max-Flow theorem, we presented a new vulnerability index to identify the vulnerable lines in a power grid. In addition, comparative simulations between the power flow based model and existing models are investigated on the IEEE 118 bus system. The simulation results demonstrate that the proposed model and the index are more effective in power grid vulnerability analysis.

Based on the PF model, an improved CN model for power system cascading risk assessment is proposed. We defined risk by combining consequence and probability of the failures in this model, which are affected by both power factors and network structure. Compared with existing risk assessment models, the proposed one can evaluate the risk of the system comprehensively during a cascading event by combining the topological and electrical information. We also adopted a new cascading event simulation module to identify the power grid cascading chain from a system-level view. In addition, simulations are investigated on the IEEE 14 bus system and IEEE 39 bus system respectively to illustrate the performance of the proposed module. The simulation results demonstrate that the proposed method is effective in a power grid risk assessment during a cascade event.

Finally, we study the interaction between the power grid and the communication network. We have proposed a new interdependency model to demonstrate a cascade event between two different layers of a cyber-physical network. Unlike previous "point-wise" dependency models, in our model the loss of one node does not necessarily lead to the failure of the corresponding nodes. From the study, we can draw the conclusion that the structure of communication network has great impact on the power grid security performance.

There are more questions to be explored in this area. As can be seen in the previous chapters, the CN model has shown its great advantages in allowing an assessment procedure where the number of calculations can be related to structure. Previously, the network based modelling was largely simplified, and sometimes ignored the critical characteristics of the original systems. The power flow constraints and data exchange rules are adopted in this thesis. This is a good start, but still not comprehensive enough to describe the full

interdependency of the two network layers. It is not difficult to speculate that more peculiar characteristics and strategies of interconnected action are required in future modelling. Meanwhile, power grids are not only connected with communication networks, but also transportation networks, gas, and water supply networks. The CN model can be expanded to include three or more interdependent networks in the near future.

References

[1] Ali Pinar, Juan Meza, Vaibhav Donde, and Bernard Lesieutre. Optimization Strategies for the Vulnerability of the Electric Power Grid. 20(4):1786–1810, 2010.

[2] Stavros Lazarou, Catalin Felix Covrig, Ilhami Colak, Philip Minnebo, Heinz Wilkening, and Gianluca Fulli. Behaviour of multi-terminal grid topologies in renewable energy systems under multiple loads. *2012 Int. Conf. Renew. Energy Res. Appl. ICRERA 2012*, pages 2–5, 2012.

[3] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, 2010.

[4] Arulampalam Atputharajah and Tapan Kumar Saha. Power system blackouts - literature review. In *2009 Int. Conf. Ind. Inf. Syst.*, pages 460–465. IEEE, dec 2009.

[5] Carson W. Taylor and Dennis C. Erickson. Recording and analyzing the July 2 cascading outage. *IEEE Comput. Appl. Power*, 10(1):26–30, 1997.

[6] A White Paper, Stephen T Lee, D Ph, Nick Abi-samra, D Ph, Bill Roettger, Epri Peac, Rich Lordan, and Clark W Gellings. Factors Related to the Series of Outages on August 14 , 2003 Project Team. 2003.

[7] P. Pourbeik, P.S. Kundur, and C.W. Taylor. The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts. *IEEE Power Energy Mag.*, 4(5):22–29, 2006.

[8] 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 Europe, and recommended means to improve system dynamic performance. *IEEE Trans. Power Syst.*, 20(4):1922–1928, 2005.

[9] Xiaoxin Zhou and Changyou Yan. A blackout in Hainan Island power system: Causes and restoration procedure. *IEEE Power Energy Soc. 2008 Gen. Meet. Convers. Deliv. Electr. Energy 21st Century, PES*, 2008.

[10] Department of Primary Industries. January Supply Interruptions - Executive Summary - DELWP. Technical report, 2007.

[11] Tony Fenwick and Kristin Hoskin. Resilience Lessons : Orion ' s 2010 and 2011 Earthquake Experience Independent Report. *Earthquake*, (September), 2011.

[12] Australian Electricity Market Operator (AEMO). Preliminary Report – Black System Event in South Australia on 28 September 2016. (October), 2016.

[13] Lester H. Fink and Kjell Carlsen. Operating under stress and strain. *IEEE Spectr.*, 15(3):48–53, 1978.

[14] NERC. NERC standards, Transmission System Standards – Normal and Emergency Conditions. Technical report.

[15] Task Force on Understanding Prediction Mitigation and Restoration of Cascading Failures IEEE PES Computer and Analytical Methods Subcommittee. Vulnerability Assessment for Cascading Failures in Electric Power Systems. *IEEE Power Energy Soc. Power Syst. Conf. Expo.*, pages 1–9, 2009.

[16] Chen Ching Liu, Juhwan Jung, Gerald T. Heydt, Vijay Vittal, and Arun G. Phadke. Strategic power infrastructure defense (SPID) system a conceptual design. *IEEE Control Syst. Mag.*, 20(4):40–52, 2000.

[17] Juan Li, Koji Yamashita, Chen-ching Liu, and Michael Hofmann. Over-Excitation Tripping Events. pages 1–8, 2008.

[18] C.C Liu, J Jung, G.T. Heydt, V Vittal, and A. G. Phadke. Program on Technology Innovation: Learning to Recognize Vulnerable Patterns of Cascaded Events. Technical report, 2007.

[19] Guo Chen, Zhao Yang Dong, David J. Hill, Guo Hua Zhang, and Ke Qian Hua. Attack structural vulnerability of power grids: A hybrid approach based on complex networks. *Phys. A Stat. Mech. its Appl.*, 389(3):595–603, 2010.

[20] Zhenyu Huang and Jarek Nieplocha. Transforming power grid operations via high performance computing. *IEEE Power Energy Soc. 2008 Gen. Meet. Convers. Deliv. Electr. Energy 21st Century, PES*, pages 1–8, 2008.

[21] S. Tamronglak, S. H. Horowitz, A. G. Phadke, and J. S. Thorp. Anatomy of power system blackouts: Preventive relaying strategies. *IEEE Trans. Power Deliv.*, 11(2):708–714, 1996.

[22] A. G. Phadke and J. S. Thorp. Expose hidden failures to prevent cascading outages. *IEEE Comput. Appl. Power*, 9(3):20–23, 1996.

[23] Guo Chen, Zhao Yang Dong, David J. Hill, and Yu Sheng Xue. Exploring reliable strategies for defending power systems against targeted attacks. *IEEE Trans. Power Syst.*, 26(3):1000–1009, 2011.

[24] Koeunyi Bae and James S Thorp. A stochastic study of hidden failures in power system protection. *Decis. Support Syst.*, 24(3-4):259–268, 1999.

[25] Hongye Wang and James S. Thorp. Optimal locations for protection system enhancement: A simulation of cascading outages. *IEEE Trans. Power Deliv.*, 16(4):528–533, 2001.

[26] Jie Chen, James S Thorp, and Ian Dobson. Cascading Dynamics and Mitigation Assessment in Power System Disturbances via a Hidden Failure Model. pages 1–23, 2003.

[27] Huaqing Li, Guo Chen, Tingwen Huang, Zhaoyang Dong, Wei Zhu, and Lan Gao. Event-Triggered Distributed Average Consensus Over Directed Digital Networks With Limited Communication Bandwidth. *IEEE Trans. Cybern.*, 46(12):3098–3110, 2016.

[28] Huaqing Li, Xiaofeng Liao, Guo Chen, David J. Hill, Zhaoyang Dong, and Tingwen Huang. Event-triggered asynchronous intermittent communication strategy for synchronization in complex dynamical networks. *Neural Networks*, 66:1–10, 2015.

[29] L Mili and Q Qiu. Risk assessment of catastrophic failures in electric power systems. *Int. J. Crit. Infrastructures*, 1(1):38–63, 2004.

[30] Ian Dobson, Benjamin A. Carreras, Vickie E. Lynch, and David E. Newman. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos*, 17(2), 2007.

[31] Peter Sheridan Dodds, Roby Muhamad, and Duncan J Watts. An experimental study of search in global social networks. *Science*, 301(5634):827–9, 2003.

[32] D. J. Watts. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci.*, 99(9):5766–5771, 2002.

[33] Ye Cai, Yijia Cao, Yong Li, and Tao Huang. Interaction Between Power Grids and Communication Networks. 7(1):1–9, 2015.

[34] Xiang Li and Guanrong Chen. A local-world evolving network model. *Phys. A Stat. Mech. its Appl.*, 328(1-2):274–286, 2003.

[35] Xiao Fan Wang and Guanrong Chen. Complex networks: Small-world, scale-free and beyond. *IEEE Circuits Syst. Mag.*, 3(1):6–20, 2003.

[36] Paul Hines, Huaiwei Liao, Dong Jia, and Sarosh Talukdar. Autonomous agents and cooperation for the control of cascading failures in electric grids. *2005 IEEE Networking, Sens. Control. ICNSC2005 - Proc.*, 2005:273–278, 2005.

[37] Yan Liu and Xueping Gu. Skeleton-network reconfiguration based on topological characteristics of scale-free networks and discrete particle swarm optimization. *IEEE Trans. Power Syst.*, 22(3):1267–1274, 2007.

[38] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Phys. Rev. E. Stat. Nonlin. Soft Matter Phys.*, 65(5 Pt 2):056109, 2002.

[39] Ying-Cheng Lai, Adilson E Motter, and Takashi Nishikawa. Attacks and cascades in complex networks. *Complex networks. Pap. from Conf. 'complex networks Struct. Dyn. Funct. 23rd Annu. Conf. Cent. Nonlinear Stud. St. Fe, NM, USA, May 12–16, 2003.*, 310:299–310, 2004.

[40] Yuanyu Dai, Guo Chen, Zhaoyang Dong, Yusheng Xue, David J. Hill, and Yuan Zhao. An improved framework for power grid vulnerability analysis considering critical system features. *Phys. A Stat. Mech. its Appl.*, 395:405–415, 2014.

[41] D. Kirschen and F. Bouffard. Keeping the lights on and the information flowing. *IEEE Power Energy Mag.*, 7(1):50–60, 2009.

[42] C. R. (Colin R.) Bayliss and B. J. (Brian J.) Hardy. *Transmission and distribution electrical engineering.* Newnes, 2011.

[43] Matthew Wright and Patrick Hearps. Zero Carbon Australia Stationary Energy Plan. *Energy*, 2011:171, 2010.

[44] Ben Elliston, Mark Diesendorf, and Iain MacGill. Simulations of scenarios with 100% renewable electricity in the Australian National Electricity Market. *Energy Policy*, 45:606–613, 2012.

[45] Amir Hamed Mohsenian-Rad, Vincent W S Wong, Juri Jatskevich, Robert Schober, and Alberto Leon-Garcia. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. *IEEE Trans. Smart Grid*, 1(3):320–331, 2010.

[46] P. van Zoest, E. Veldman, Z. Lukszo, and P.M. Herder. Analysis of future electricity demand and supply in the low voltage distribution grid. *Proc. 11th IEEE Int. Conf. Networking, Sens. Control*, pages 619–624, 2014.

[47] Mike Gibbard and David Vowles. Simplified 14-Generator Model of the Se Australian Power System. (July):1–45, 2010.

[48] David Vowles and Mike Gibbard. Mudpack: A Software Package for the Small-Signal Stability Analysis of Power Systems. Technical report.

[49] PSERC. Future Grid to Enable Sustainable Energy Systems. Technical report.

[50] The University of Queensland. Sunlight - UQ Solar Photovoltaic Data.

[51] The University of Queensland. Power generated - Photovoltaic array live data feed, UQ Solar.

[52] Stewart Taggart, Geoffrey James, Zhaoyang Dong, and Christopher Russell. The future of renewables linked by a transnational Asian grid. *Proc. IEEE*, 100(2):348–359, 2012.

[53] Csiro Energy. Change and choice - The Future Grid Forum's analysis of Australia's potential electricity pathways to 2050. 2013.

[54] Beyond Zero Emissions. The Zero Carbon Australia Project.

[55] Aemo and Australian Electricity Market Operator (AEMO). 100 Per Cent Renewables Study—Modelling Outcomes. (July):111 pages, 2013.

[56] Prabha Kundur, John Paserba, Venkat Ajjarapu, Göran Andersson, Anjan Bose, Thierry Van Cutsem, Claudio Canizares, Nikos Hatziargyriou, David Hill, Vijay Vittal, Alex Stankovic, and Carson Taylor. Definition and Classification of Power System Stability IEEE/CIGRE Joint Task Force on Stability Terms and Definitions. *IEEE Trans. Power Syst.*, 19(3):1387–1401, 2004.

[57] Guo Chen, Zhao Yang Dong, David J. Hill, and Guo Hua Zhang. An improved model for structural vulnerability analysis of power networks. *Phys. A Stat. Mech. its Appl.*, 388(19):4259–4266, 2009.

[58] R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the North American power grid. *Eur. Phys. J. B*, 46(1):101–107, 2005.

[59] Paolo Crucitti, Vito Latora, and Massimo Marchiori. A topological analysis of the Italian electric power grid. *Phys. A Stat. Mech. its Appl.*, 338(1-2):92–97, jul 2004.

[60] Aneroid Energy. Wind Energy in Australia |.

[61] Réka Albert, István Albert, and Gary L. Nakarado. Structural vulnerability of the North American power grid. *Phys. Rev. E*, 69(2):025103, feb 2004.

[62] S. Arianos, E. Bompard, A. Carbone, and F. Xue. Power grid vulnerability: A complex network approach. *Chaos*, 19(1):1–6, 2009.

[63] Clean Energy Council. Clean Energy Council - Reports. Technical report.

[64] Huaqing Li, Guo Chen, and Tingwen Huang. High-Performance Consensus Control in Networked Systems With Limited Bandwidth Communication and Time-Varying Directed Topologies. *IEEE Trans. Neural Networks Learn. Syst.*, 28(5):1043–1054, 2017.

[65] Duncan S. Callaway and Ian A. Hiskens. Achieving Controllability of Electric Loads. *Proc. IEEE*, 99(1), 2010.

[66] Elaheh Mashhour and Seyed Masoud Moghaddas-Tafreshi. Bidding Strategy of Virtual Power Plant for Participating in Energy and Spinning Reserve Markets—Part II: Numerical Analysis. *IEEE Trans. Power Syst.*, 26(2):957–964, 2011.

[67] Hong Ming Yang, De Xin Yi, Jun Hua Zhao, and Zhao Yang Dong. Distributed Optimal Dispatch of Virtual Power Plant via Limited Communication. *Power Syst. IEEE Trans.*, 28(3):3511–3512, 2013.

[68] João F C Mota, João M F Xavier, Pedro M Q Aguiar, and Markus Püschel. D-ADMM: A distributed algorithm for compressed sensing and other separable optimization problems. *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pages 2869–2872, 2012.

[69] Distributed Alternating Direction and Distributed Basis Pursuit. D-ADMM : Distributed ADMM, 2013.

[70] Mihai Nica. Eigenvalues and Eigenfunctions of the Laplacian. *Waterloo Math. Rev.*, 1(2):23–34, 2011.

[71] Bojan Mohar. The Laplacian Spectrum of Graphs. *Graph Theory, Comb. Appl. Vol. 2*, 2:871–898., 1991.

[72] Jiong-Sheng Li and Yong-Liang Pan. A note on the second largest eigenvalue of a tree with perfect matchings. *Linear Algebra Appl.*, 48(May 2007):117–121, 2000.

[73] Béla Bollobas. *Extremal Graph Theory*. Dover Publications, Incorporated, 2004.

[74] Hanbo Qi, Libao Shi, Yixin Ni, and A Overall Framework. Study on Power System Vulnerability Assessment Based on Cascading Failure Model. In *IEEE PES GM*, 2014.

[75] Réka Albert, István Albert, and Gary L. Nakarado. Structural vulnerability of the North American power grid. *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, 69:1–4, 2004.

[76] Luis a. Nunes Amaral, Antonio Scala, Marc Barthelemy, and H. Eugene Stanley. Classes of behavior of small-world networks. (v), 2000.

[77] Ke Sun. Complex Networks Theory: A New Method of Research in Power Grid. *2005 IEEE/PES Transm. Distrib. Conf. Expo. Asia Pacific*, pages 1–6, 2005.

[78] Dirk Witthaut, Martin Rohden, Xiaozhu Zhang, Sarah Hallerberg, and Marc Timme. Critical links and nonlocal rerouting in complex supply networks. *Physics (College. Park. Md).*, (2):1–21, 2015.

[79] Ajendra Dwivedi, Xinghuo Yu, and Peter Sokolowski. Identifying vulnerable lines in a power network using complex network theory. *2009 IEEE Int. Symp. Ind. Electron.*, (ISlE):18–23, 2009.

[80] Adilson E. Motter and Ying Cheng Lai. Cascade-based attacks on complex networks. *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, 66(6):2–5, 2002.

[81] Ajendra Dwivedi and Xinghuo Yu. A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Trans. Ind. Informatics*, 9(1):81–88, 2013.

[82] Alexander Schrijver. On the history of the transportation and maximum flow problems. *Math. Program. Ser. B*, 91(September 1939):437–445, 2002.

[83] Nasser S. Fard and Tae H. Lee. Cutset enumeration of network systems with link and node failures. *Reliab. Eng. Syst. Saf.*, 65(June 1998):141–146, 1999.

[84] Gregory Levitin, Min Xie, and Tieling Zhang. Reliability of fault-tolerant systems with parallel task processing. *Eur. J. Oper. Res.*, 177:420–430, 2007.

[85] K. Morison, L. Wang, and P. Kundur. Power system security assessment. *IEEE Power Energy Mag.*, 2(October):30–39, 2004.

[86] Shichen Liu, Yonghua Yin, Jianfeng Yan, and Zhi-hong Yu. Review and Prospects of Research on Risk Assessment of Power System. In *IEEE China Int. Conf. Electr. Distrib.*, number Ciced, pages 23–26, 2014.

[87] Wenyuan Li. *Risk Assessment Of Power Systems:Models, Methods, and Applications*. Wiley-IEEE Press, 2005.

[88] Hua Wan, Jd McCalley, and Vijay Vittal. Risk based voltage security assessment. *IEEE Trans. Power Syst.*, 15(4):1247–1254, 2000.

[89] Youjie Dai, James D. McCalley, Nicholas Abi-Samra, and Vijay Vittal. Annual risk assessment for overload security. *IEEE Trans. Power Syst.*, 16(4):616–623, 2001.

[90] Marayati Marsadek, Azah Mohamed, and Zulkifi Mohd Norpiah. Assessment and classification of line overload risk in power systems considering different types of severity functions. *WSEAS Trans. Power Syst.*, 5(3):182–191, 2010.

[91] Shengyong Ye, Xiaoru Wang, Shu Zhou, Zhigang Liu, and Qingquan Qian. Power System Probabilistic Transient Stability Assessment Based on Markov Chain Monte Carlo Method. *Trans. China Electrotech. Soc.*, 27:168–174, 2012.

[92] Wenyuan Li, Jiaqi Zhou, Kaigui Xie, and Xiaofu Xiong. Power system risk assessment using a hybrid method of fuzzy set and Monte Carlo simulation. *IEEE Trans. Power Syst.*, 23(2):336–343, 2008.

[93] Riccardo Santini and Stefano Panzieri. A Graph-Based Evidence Theory for Assessing Risk. In *18th Int. Conf. Inf. Fusion*, pages 1467–1474, Washington, DC, 2015.

[94] Yihai Zhu and Jun Yan. Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph. *IEEE Trans. Parallel Distrib. Syst.*, 25(12):3274–3284, 2014.

[95] L.R. Foulds. *Graph Theory Applications*. Springer Science & Business Media, 2012.

[96] L.R. Ford and D.R.Fulkerson. Maximal Flow Through a Network. *Can. J. Math.*, pages 399–404, 1956.

[97] Lu Zhao, Jin Ma, and Zhi Li Lei. Power system operation risk assessment based on possibility prioritization search strategy of cascading outage. *2010 5th Int. Conf. Crit. Infrastructure, Cris 2010 - Proc.*, (2), 2010.

[98] Zhuoyang Wang, Guo Chen, David J. Hill, and Zhao Yang Dong. A power flow based model for the analysis of vulnerability in power networks. *Phys. A Stat. Mech. its Appl.*, 460:105–115, 2016.

[99] Zhaohong Bie and Xifan Wang. Evaluation of Power System Cascading Outages. *Power Syst. Technol. 2002. Proceedings. PowerCon 2002. Int. Conf.*, pages 415–419, 2002.

[100] Yuanzhang Sun, Ieee Lin Cheng, Haitao Liu, and Shan He. Power System Operational Reliability Evaluation Based On Real-time Operating State. In *2005 Int. Power Eng. Conf.*, 2005.

[101] Jianxi Gao, Sergey V. Buldyrev, H. Eugene Stanley, and Shlomo Havlin. Networks formed from interdependent networks. *Nat. Phys.*, 8(1):40–48, 2011.

[102] Marzieh Parandehgheibi and Eytan Modiano. Robustness of Interdependent Networks : The case of communication networks and the power grid. *Globecom 2013*, pages 1–6, 2013.

[103] Sergey V. Buldyrev, Nathaniel W. Shere, and Gabriel A. Cwilich. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, 83(1):1–8, 2011.

[104] Jia Shao, Sergey V. Buldyrev, Shlomo Havlin, and H. Eugene Stanley. Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, 83(3):1–9, 2011.

[105] Osman Yagan, Dajun Qian, Junshan Zhang, and Douglas Cochran. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *IEEE Trans. Parallel Distrib. Syst.*, 23(9):1708–1721, 2012.

[106] Zhen Huang, Cheng Wang, Milos Stojmenovic, and Amiya Nayak. Balancing system survivability and cost of smart grid via modeling cascading failures. *IEEE Trans. Emerg. Top. Comput.*, 1(1):45–56, 2013.

[107] First A Li Qin, Second B Hu Ting, Third C Huang Xin, and Fourth D Fang Shu-chao. Research of Test Models of Electric Power Dispatching Data Network. (Ciced):10–13, 2016.

[108] Pablo Echenique, Jesús Gómez-Gardeñes, and Yamir Moreno. Improved routing strategies for Internet traffic delivery. *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, 70(5 2):1–5, 2004.

List of Publications

Journal Papers

[1] Zhuoyang Wang, Guo Chen, David J. Hill, and Zhao Yang Dong,*"A Power Flow Based Model for the Analysis of Vulnerability in Power Networks",* Physica A, Vol. 460, pp. 105-115, 2016.

[2] Zhuoyang Wang, David J. Hill, Guo Chen, and Zhao Yang Dong, *"Power System Cascading Risk Assessment based on Complex Network Theory",* submitted to Physica A, 2016.

[3] Zhuoyang Wang, David J. Hill, Guo Chen, and Zhao Yang Dong, *"Risk Assessment in Power-Communication Interdependency Network",* in preparation for IEEE Transactions, 2016.

Conference Papers

[1] Zhuoyang Wang, Liyan Zhang, Guo Chen, and David J. Hill, *"Communication Network Topology Analysis on Distributed Optimization Performance In PV-ES Combined System",* IEEE PES General Meeting, 2015.

[2] Zhuoyang Wang, Wang Zhang, Liyan Zhang, Guo Chen, Zhao Yang Dong, and Tingwen Huang, *"Impact of Different Penetrations of Renewable Sources and Demand Side Management on Australia Future Grid",* First Workshop on Smart Grid and Renewable Energy, 2015.

[3] Zhuoyang Wang, Guo Chen, Liyan Zhang, and David J. Hill, *"Vulnerability Analysis for Power Grid Given Renewable Energy Integration",* CIGRE Conference, 2014.

[4] Liyan Zhang, Guo Chen, Zhuoyang Wang, David J. Hill, and Zhao Yang Dong, *"Robust $H\infty$ Load Frequency Control of Future Power Grid with Energy Storage Considering Uncertainty and Time Delay",* IEEE PES General Meeting, 2014.