Robustness analysis of electricity networks against failure or attack: the case of the Australian National Electricity Market (NEM)

Wensheng Wang[1], Faezeh Karimi[2], Kaveh Khalilpour[1,2*], David Green[1], Manos Varvarigos[3]

[1]Faculty of Information Technology, Monash University, Melbourne, Australia

[2]School of Information, Systems and Modelling, Faculty of Engineering and IT, University of Technology Sydney, Sydney, Australia

[3]School of Electrical & Computer Engineering, National Technical University of Athens, Greece

Abstract

This study explores network science algorithms for the robustness analysis of electricity networks. We first explore the characteristics of key network models including random graphs, small-world, and scale-free networks. Then, various measures are explored for the robustness of such networks against failure or attack, utilizing topological features and percolation theory. Both weighted and unweighted scenarios are studied, with network voltage considered as the edge weight. For a case study, we investigate the network characteristics as well as the robustness of the Australian National Electricity Market (NEM) network on the basis of these models and theories.

The NEM is the world's longest interconnected power system, with an end-to-end distance of over 5000 km between the state of Queensland in the north and the state of South Australia. Our data contains 2375 transmission lines and 1538 nodes as generators or large demand customers. Our study shows that the NEM as an unweighted network is a small-world network (with exponential degree distribution). However, as a weighted network (considering the voltage capacity of nodes), it has a scale-free topology (following a power-law degree distribution). Robustness analysis revealed that the NEM presents relatively stronger robustness when facing random errors than when facing intentional attacks to nodes with a high degree centrality. It also revealed the sensitivity of the scale-free network to deliberate attacks directed toward important "hubs" (interconnected nodes).

Keywords: Complex networks; electricity network; robustness analysis; cascading failure; percolation theory.

1. Introduction

Modern society relies increasingly on complex infrastructure networks. This complexity leads to accidents and system failures that cost billions of dollars each year. The electricity network is one such critical infrastructure, vital for many aspects of human life including finance, transportation, emergency services, and energy supply [1]. This network is often fragile when it reaches its limits and any disturbance can lead to a catastrophe [2]. For example, on 28 September 2016, a storm damaged one of the mid-north transmission lines of South Australia's electricity network. The automatic safety features of the grid isolated the generators to protect the generator equipment and consumers. This overloaded other lines and tripped them off and, less than 90 seconds after the first failure, the entire state was in darkness [3]. The cost of the blackout to businesses was estimated at A$367 million [4]. BHP Billiton alone lost U.S.$100 million because of the shutdown of its Olympic Dam mine [5].

A year before that, Tasmania's energy crisis cost A$180 million [6]. Tasmania has one of the world's most sustainable electricity systems, with hydro accounting for ~80% of the state's generation capacity. It is connected to Victoria through a high-voltage interconnector known as the Basslink. During 2015, Tasmania experienced a record dry spring. In such conditions, dam levels should not go below certain values. Nevertheless, the generous government renewable energy subsidies motivated exceeding the recovery levels, taking into account the soon-to-come rain season. Later that year, when dam levels were too low and the state depended more than ever on Basslink imports, the failure of a subsea cable disconnected Basslink [7]. It left Tasmania isolated, with insufficient backup generators. As a result, this sustainable state had to import fossil fuel generators from overseas [8], at extreme costs for its economy and its international image.

Both the above incidents began with a fault (decision or technical) that triggered a series of events, leading to catastrophe. A well-known mechanism for system breakdown is a cascade or epidemic of failures. Cascading failure is still a challenge for conventional centralised electricity grids. The issue of electricity networks and their robustness was first presented by the U.S. National Academy of Engineering as a key to civilisation progress, improving economy, security, and quality of life [9]. To understand accidents and system failures in any network including electricity, we must begin

by abstracting common features. By examining the properties of networks of events and agents that underlie real-world systems, we can identify common processes and conditions. With the increasing growth in the size and complexity of power grids, the need to understand the emergent behaviours of these systems has become more salient [10]. Over recent decades, remarkable research has been conducted to understand, characterise and model networked systems, leading to the rapid development of complex network theory [11-14][15].

Three network classes are considered suitable for the analysis and prediction of the robustness of an electricity network. Early, random graphs were proposed by Erdős and Rényi [16], which could be used to mirror large variance types of complex networks, especially applied in social networks, electricity grids, and the internet [17, 18]. Later, small-world networks were described by Watts and Strogatz [19], having high clustering coefficient levels and almost the same average length as the random graphs. This means that they could describe real-world networks better because they had more densely connected nodes. However, Albert and Barabási discovered another network class: scale-free networks, with the degree distribution following a power law. According to their study, in a Barabási–Albert model [20], some nodes (also known as hubs) have far more links than others. Nodes with more links probably attract new links, while nodes with fewer links are less likely to obtain a new link, a feature that was described as preferential attachment. Furthermore, the authors proposed that these interconnected nodes (hubs) played a more important role in the system, especially for network robustness [20].

To this end, we articulate network robustness analysis in three key steps, as shown in Figure 1. The first step includes data acquisition. It is followed by mapping the data into a network model in the second step. Once a suitable network model is chosen, then the robustness analysis can be undertaken.

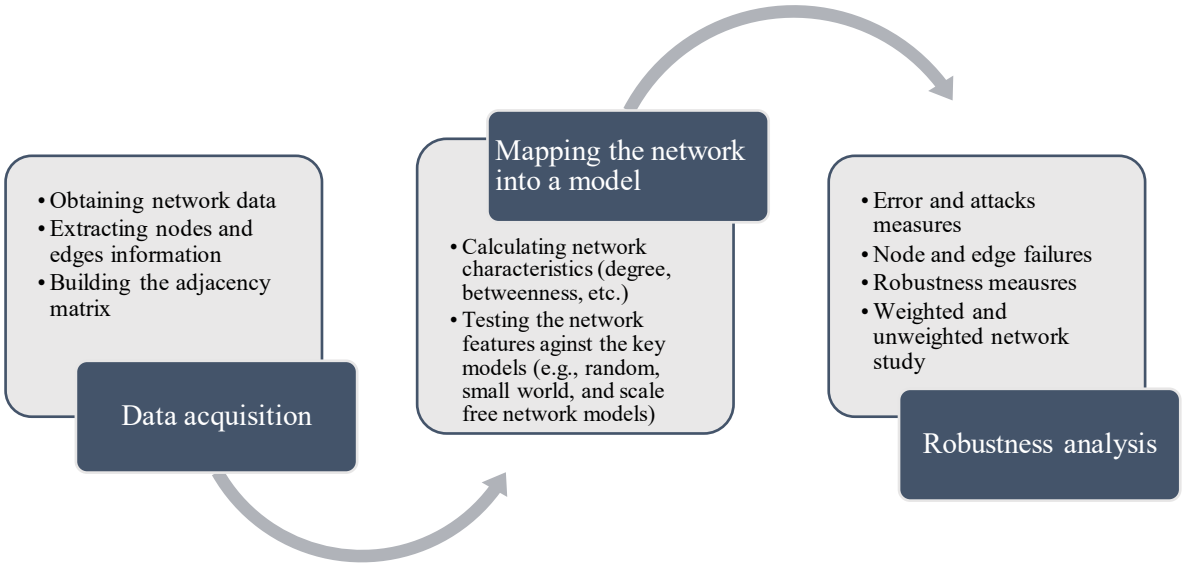


Figure 1: The network robustness analysis steps

Robustness (or resilience) analysis is a critical requirement of any network design and operation. A major failure phenomenon in a network (such as a blackout in electricity networks) is a cascading failure, which incurs huge negative effects on system robustness [21]. A cascading failure is a process in which the failure of a few parts of the system leads to the failure of other parts and this process spreads across the entire network. Research addressing this problem began using percolation theory to analogise cascading failures in complex networks [22, 23]. In the present paper, robustness to cascading failures is assessed using both topological features and component characteristics (features of connected sub-network) [24]. A general model utilised in past research is calculating the largest component (the largest connected subnetwork) of the network while removing nodes randomly or intentionally to simulate the resilience of the network to random errors or intentional attacks. The mechanism is that the network can hold a certain component until some of the elements are removed. This paper presents both edge- and nodes-removed case studies.

In 1998, Watts and Strogatz [19] reported the western U.S. electricity grid robustness using scale-free networks. In 2004, Albert et al. [10] reported the robustness of the North American power grid using the same model but with larger network size. Rosas-Casals et al. [25] studied the case of the European power grid and reported that the tolerance of scale-free networks to errors (random loss of nodes) and attacks (selective loss of interconnected nodes) was not unique, proving Albert's

proposal that interconnected nodes are more crucial. Furthermore, arguing that fragility increases with the size of the network, the authors suggested separating large power grids into isolated stable islands [25].

In this study, we examine the Australian power network from a complex network theory perspective. Australia's National Energy Market (NEM) network is one of the world's largest interconnected power systems, linking the eastern and southern states and territories (i.e., Queensland, New South Wales, Australian Capital Territory, Victoria, Tasmania, and South Australia). Western Australia and the Northern Territory are not linked to the NEM. The NEM provides about 80% of Australia's electricity consumption by approximately 9 million customers via nearly 40,000 km of transmission lines [26]. The NEM is the world's longest interconnected power system with an end-to-end distance of over 5000 km between the state of Queensland in the north and the state of South Australia [27]. Nevertheless, limited published works exist on the robustness analysis of the NEM using methodologies of network science. In recent years, NEM has witnessed a few major cascading failures, and climate change also is posing a growing risk. With the increased concern on the network resilience over fault or intentional errors, it is critical to study the topological characteristic of the network and identify possible areas of improvement. This paper attempts to build a basis for such analyses by identification of some core characteristics of this network using the real data.

The remainder of this paper is organised as follows. In the next section, we explore the characteristics and theories behind complex network models and how they have evolved and been applied in real networks. Next, we analyze the Australian NEM based on these models to identify the most accurate topology model for the NEM. We then build experiments to test the robustness of the network to errors and attacks. We conclude with a discussion of the results and their implications.

2. Network analysis theories

2.1. Random graphs

Erdős–Rényi and Gilbert–Elliott random graphs: The year 1959 is a key date in the history of network science. That year, two academic groups independently introduced models for random

graphs, known as the Erdős–Rényi model [16] and the Gilbert–Elliott model [28]. Both models can be described by probability distributions, the only difference lying in their approaches to describing the graphs [29]. The Erdős–Rényi model (ER model) describes a random graph $\Gamma_{n,N}$ with n nodes and N edges. There are $\binom{\binom{n}{2}}{N}$ possible graphs and each graph has the same probability: $1/\binom{\binom{n}{2}}{N}$. Thus, the model has the following features:

- When there are infinite nodes $(n \to \infty)$, the probability of graph $\Gamma_{n,N}$ to be completely connected is $e^{e^{-2e}}$.
- When there are infinite nodes n, the probability of the greatest connected component of the graph $\Gamma_{n,N}$ consisting of k points is $(e^{-2e})^k e^{e^{-2e}}/k!$.
- When there is an infinite number of nodes n, the probability of graph $\Gamma_{n,N}$ consisting of k+1 disjoint connected components is $(e^{-2e})^k e^{e^{-2e}}/k!$.
- Assume that randomly chosen edges from $\binom{n}{2}$ are added to the graph $\Gamma_{n,N}$, until it becomes completely connected, and V_n denotes the number of edges of the resulting completely connected random graph Γ. When there is an infinite number of nodes n, the probability $P((V_n - \frac{1}{2}nlogn)/n < x)$ is equal to $e^{e^{-2e}}$.

In conclusion, the features of ER models can be listed as:

1. No hubs and cliques: Each node is expected to have the average number of links: $D = N/(n-1) = np$.
2. Degrees follow a Poisson distribution: Each node has a binomial distribution $p^N(1-p)^{\binom{n}{2}-N}$; the total degree list follows a Poisson distribution.
3. The average path length is rather large: $APL = \ln n/\ln\langle D\rangle$ [30]

In contrast, the Gilbert–Elliott model assumes that, given n nodes, each possible edge joining a pair of these nodes has the probability p of occurring. Therefore, graphs with m edges will be created with the probability $p^m(1-p)^{N-m}$, where N denotes that there are $n(n-1)/2$ possible lines for connecting pairs of nodes.

2.2. Small-world network

The small-world network was inspired by an experiment conducted by Stanley Milgram [31] to examine the average length of the social network in the U.S. The experiments suggested that any two individuals could contact each other through at most two intermediaries. The reason behind this phenomenon is the high clustering coefficient of the social network [32], which enables strangers to be linked to one another by a very short chain.

The small-world network describes a model in which most nodes are not adjacent, but the neighbours of a node can be adjacent. As such, there is a short path between most nodes. Another typical characteristic of the small-world network is "hubs", in which some nodes have many more connections and the network's degree of distribution is fat-tailed. This is a commonality of small-world and scale-free networks (Section 2.4), as elaborated by Cohen and colleagues [33, 34]. Nevertheless, researchers still classify small-world networks as random graphs. For instance, the Newman-Watts-Strogatz model (considering site percolation) shows properties of small-world networks close to those of a random graph [35].

2.3. Scale-free networks

In the 1960s, when studying citation networks, Derek de Solla Price observed a long tail in the profile of degree distribution which seemed to follow a Pareto and Zipf distribution or power law. Later, in 1976, Price reported his findings and called the phenomenon "cumulative advantage", which is the origin of the term "preferential attachment" commonly used today [36].

In 1999, Barabási and Albert [37] published a paper studying the World Wide Web. They pointed out that the WWW, which is described as networks with complex topology, displays two general features: (i) networks growing by adding new nodes; (ii) new nodes attaching preferentially to interconnected nodes. Such networks are called scale-free because they display robust self-organisation during deployment. A year later, two groups of researchers, Dorogovtsev, Mendes and Samukhin [38] and Krapivsky, Redner, and Leyvraz [39] presented similar solutions to this phenomenon. Bollobás and colleagues presented exacting proof of the phenomenon [40]. Later in 2004, Dangalchev [41] pointed out that the feature "growth" that was first presented by Barabási and Albert [37] is not a necessary condition for creating a scale-free

network.

Because new nodes tend to attach to nodes with more links, it is common to have nodes with a much greater degree than the average. These are called "hubs" and they play an important role in the network [20]. Scale-free networks follow the small-world theory [31]. Two properties contribute to this phenomenon: (i) the clustering coefficient distribution [32], which means that low-degree nodes in dense subnetworks communicate to others via hubs and (ii) the average distance between two nodes in scale-free networks is rather small. This theory was proved by Cohen and Havlin in 2003 [34].

Barabási–Albert model: The Barabási–Albert (BA) model depicts a graph with two main features, growth and preferential attachment, coexisting in a real network [37]. As the authors explained, the network develops through two steps:

1. **Growth:** A new node is added each time with m ($\leq m_0$) links connecting m existing nodes in the network.
2. **Preferential attachment:** The probability of a link of the new node to node i depends on its degree k_i: $k_i/\sum_j k_j$.

Barabási and Albert reported that node i is added to the network at time t_i with m links: $k_i(t) = m(t/t_i)^{\beta}$, where β is the dynamic exponent and is equal to $\frac{1}{2}$. This leads to $\frac{dk_i(t)}{dt} = \frac{m}{2}\frac{1}{\sqrt{t_i t}}$, indicating that the number of nodes m decreases as the time t_i increases. Hence, older nodes are likely to acquire more links and eventually become hubs.

The BA model has the degree distribution: $p(k) \approx 2m^{\frac{1}{\beta}}k^{-\gamma}$, where $\gamma = \frac{1}{\beta} + 1 = 3$. Therefore, that model with the degree power-law distribution generates a scale-free network with the degree exponential $\gamma = 3$. The diameter of the BA model is $\ln n/(n \ln n)$, with large n. It is smaller than that of the random graphs $G(n, p)$: $\log n/\log np$ when $1 < np < c \log n$ [42].

In summary, the BA model aims to capture the process of how a real network grows into a particular status, which means it is possible to derive the origin of the network and how it comes into being. Indeed, in a random graph, a real network can be mirrored by placing links between fixed nodes and setting hidden parameters, but the graph can capture only a still status of the

network, like a picture. It seems to be real, but the process for drawing that picture does not match how the real network grows. In other words, the BA model generates a more general pattern to mirror real networks, because real networks proved to be scale-free [43].

Bianconi–Barabási model: The Bianconi–Barabási (BB) model is a variant of the BA model, named after its inventors Bianconi and Barabási [44]. Based on the concepts of the BA model, the BB model uses a new concept called *fitness*. This model assigns a fitness level to each node. The probability of forming a link between a new node to node *i* depends on its degree k_i and the fitness η_i: $\eta_i k_i / \sum_j \eta_j k_j$. Nodes with higher fitness are more likely to acquire new links [45]. The evolution of each node over time is given by $\frac{\partial k_i(t)}{\partial t} = m\left(\eta_i k_i / \sum_j \eta_j k_j\right)$. Instead of using the time t_i to value the probability of attracting new links in the BA model, the BB model uses fitness, which can exceed the limit that late-comer nodes are less likely to become hubs, a feature not occurring in the BA model.

2.4. Watts-Strogatz model (a hybrid of the random and small-world networks)

The Watts-Strogatz (WS) model, proposed by Duncan J. Watts and Steven Strogatz in 1998, is a hybrid of the random graph and small-world network, resulting in a network with concurrently small average length and high clustering coefficient [19]. The model implements clustering by combining regular rings lattice with Erdős–Rényi graphs to explain the small-world network. The key features of the WS models are:

1. No hubs but existing cliques: Based on small-world network theory, WS models have high-level clustering coefficients.
2. Degrees follow a fat-tailed distribution: lattice rings or cliques exist in the model and the nodes cluster.
3. Rather smaller average path length than the ER networks: $APL = \ln n / \ln D$

The limitation of the WS model is that it generates an unrealistic degree distribution, whereas the scale-free distribution (BA model) has often been shown to better describe real networks. On the other hand, the WS model is able to perform clustering, as seen in real networks, a feature that is absent in scale-free network models. In summary, neither the WS nor the BA model alone can

depict all the features of a real network.

In summary, networks perform different characteristics regarding their peculiar structures. Features such as degree distribution, and clustering coefficient are mostly studied for identification of different kinds of networks. As discussed above, the random graph has a sharp degree distribution, following the Poisson distribution, while the small-world and scale-free networks have a rather fat-tailed degree distribution which follow exponential and power-law distribution, respectively. Small-world networks usually have a higher level of clustering coefficient, while the other two have a rather lower value. In section 4 we will investigate the Australian electricity network topology based on these features.

3. Robustness analysis with percolation theory

3.1. Bond/site percolation

Generally, models describing a network's topological features or component features are proposed to assess the robustness of the network against (cascading) failures [46]. Features such as average path length, average clustering, largest component size, and transmission efficiency have been described as robustness indicators [47]. Percolation theory is one of the mainstream approaches widely employed in this context. It was introduced in 1957 by Broadbent and Hammersley [48] as "bond percolation". The initial problem considered a three-dimensional network of $n \times n \times n$ nodes, with the probability of p for independent connection of particular pair of two nodes, and sought to identify the probability of the existence of an open path from the top to the bottom. In graph theory, percolation is studied to assess the robustness of networks [49]. When a critical subset of nodes or links is removed from the network, it will break up the graph into rather isolated clusters. This is the percolation in graph theory [50]. The boundary of network robustness can be valued using percolation models.

There are two types of percolation in networks: (i) bond percolation, as previously mentioned, describes the probability p that an edge exists to go from one node to another; (ii) site percolation, which focuses on the nodes instead of the edge, describing each node as open with the probability p and closed otherwise. Percolation is calculated with each pair of nodes [51].

To assess the robustness of networks, the percolation threshold is used. It is the calculation by

critical p_c that describes whether there is a path of connected nodes that can traverse the network. By Kolmogorov's zero-one law, critical p_c indicates whether there exists an open path from the top to the bottom. In experiments, we can calculate the critical p_c iteratively and take the mean value as the percolation threshold as an indicator of network robustness [52].

Percolation threshold in random graphs: As previously stated, indeed, random graphs are the simplest and most widely used model for studying real networks. However, random graphs suffer an inevitable drawback in modelling the real world. The degree distribution of random networks follows a Poisson distribution due to each node having the same probability of attracting links. In the real world, however, networks (e.g., the internet) usually follow a power-law distribution or contain exponential forms that are strongly non-Poisson [53]. Indeed, WS models have been presented that can generate random graphs with non-Poisson degree distribution [17]. Thanks to the development of such models, percolation can be studied on random graphs with any degree distribution.

Percolation threshold in scale-free networks: Scale-free networks have the feature that their degree distribution is highly skewed and follows a power law, resulting in the generation of "hubs" in the networks. This characteristic correlates strongly with a network's robustness to failure. The reason is that some nodes that have many links and are quite crucial in the network can occupy only a very small part of the network, and most of the nodes in the network have very few links according to the power law. Therefore, if nodes are randomly removed, the probability that a scale-free network crashes is much lower than that of random graphs. On the other hand, if the interconnected nodes are removed intentionally, the network will be split into rather isolated subnetworks, with the result that hubs have strong robustness to errors but are very fragile to deliberate attack. These mechanisms were studied by Cohen et al. [54] and Callaway et al. [51] using percolation theory. Cohen et al. [55] also presented the proof that random removal of nodes will not destroy the network.

3.2. K-Clique percolation theory

The clique percolation method is used to identify communities in a network [56]. The term "communities" in a network describes a set of cliques that are adjacent to each other. A clique is a completely connected subnetwork of the whole network, and a k-clique is a clique that has exactly k nodes. The robustness of cliques is quite strong because the nodes are redundantly connected and none of them is critical in a clique. As such, a community comprising several overlapped

cliques has a high robustness value. This explains why the clique percolation method can also be used to study network robustness.

In summary, in a network comprised of communities, the random removal of nodes or edges (e.g., by errors) will not cause a problem, but deliberate attacks to critical nodes will put the system under threat of robustness problems. By extension, then, a network with a large number of communities will be strongly robust to errors; on the other hand, deliberate attacks may break the entire network into small isolated fractions, which can cause a catastrophe. Imagine two networks, one with many small communities, and the other with few, rather large communities. Assuming that the total numbers of nodes in the communities are the same, the network with many small communities will be more robust to deliberate attack because, when an attack occurs to a critical node connecting two communities, only a small fraction of the network is likely to fail. In contrast, a large subnetwork will be disconnected in a network with few but large communities.

In network theory, a graph with a structure made up of communities can be identified using the feature "clustering coefficient". A high-level clustering coefficient indicates the likelihood of more cliques. Thus it is generally recognised that small-world networks that have a rather higher clustering coefficient than ER networks and BA networks are always more robust.

4. Case study of the Australian national electricity network

Our analysis follows multiple steps, as depicted in Figure 1. The first step is the data acquisition and building the adjacency matrix, followed by fitting the data to a network model. Subsequently, we perform a robustness analysis.

4.1. Dataset: Australian electricity transmission lines

In this study, we examine Australia's NEM. We use the transmission lines dataset from Geoscience Australia Web Service to build a network model of this power grid. The dataset was first digitised in 2011 and last revised in December 2016, representing the Australian Energy Market Operator (AEMO) Transmission Network Diagrams [57]. The dataset includes information as to the latitude and longitude coordinates of generators and substations as well as where and how the lines traverse.

The latter is not the main target of this research. However, the outsets and destinations of the transmission lines (the start and end positions of each transmission line), the state the line belongs to, and the line's capacity are extracted from the dataset. The final graph consists of 2375 edges (transmission lines) and 1538 nodes (generators and substations).

4.2. Topological features: network model

Mapping the power grid into a topological network model is the first step in exploring a power grid from a complex network theory perspective [14]. We use the $G = (N, E)$ graph formalism to model the power grid, where $N = \{n_i\}$ indicates the set of nodes in the graph (i.e., generators and substations in the power grid), and $E = \{e_{ij}\}$ indicates the set of edges between any two nodes. As such, $e_{12} = \{n_1, n_2\}$ here means that power transfers between n_1 and n_2 through the e_{12} edge. The graph does not take direction into account. "Through the process of the mapping, the power grid has become an unvalued, undirected and sparse connected graph" [14].

In the rest of this paper, we denote the full Australian power grid as G_{AU}. The largest component, spreading across the east and south of the country, is denoted by G_{ES} and illustrated in Figure 2 with a geographical structure. The G_{ES} includes the network of six states, namely Queensland (G_{QLD}), New South Wales (G_{NSW}), Australian Capital Territory (G_{ACT}), Victoria (G_{VIC}), Tasmania (G_{TAS}) and South Australia (G_{SA}).

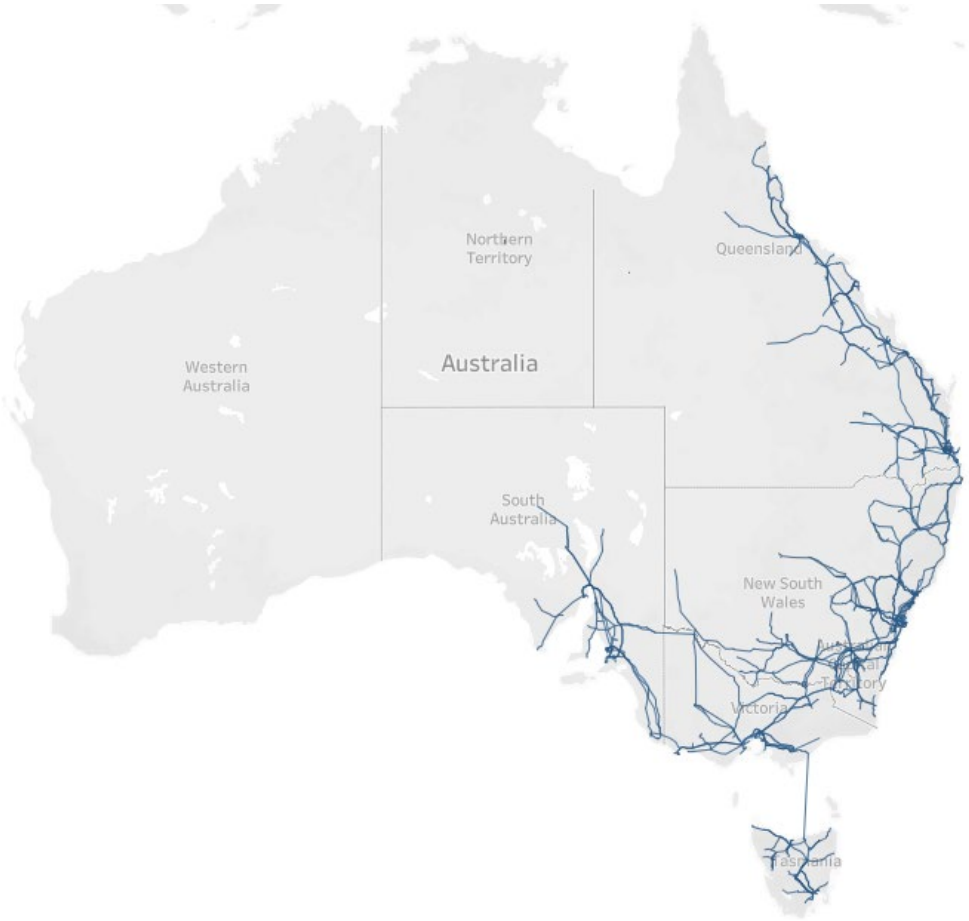


Figure 2: The East-South Australian transmission network encompassing six states: Queensland (G_{QLD}), New South Wales (G_{NSW}), Australian Capital Territory (G_{ACT}), Victoria (G_{VIC}), Tasmania (G_{TAS}) and South Australia (G_{SA}).

Past research into the topological structure of power grids has identified that they exhibit certain characteristics. For the development of complex network features, several studies have examined power grids from a complex network perspective. Although random graphs provide a basis for many comparisons, real-world networks show different patterns. Past research into power grids in Europe and the U.S. shows a pattern of small-world or scale-free network characteristics. To explore the topological features of the NEM power grid we begin with the degree distribution. Two nodes are considered neighbours if an edge connects them. The degree k_i of a node $\mathrm{n_i}$ is then defined as the number of its neighbouring nodes and the degree distribution $P(k)$ is the probability that a randomly selected node has k neighbours. The average of nodes' degrees in a network is denoted as $< k >$ [58]. In a random network, the degree distribution will follow a Poisson distribution because each node has the same probability of gaining a new link. However, if the network is a small-world network, the degree distribution will decrease more quickly

indicating nodes with a relatively high degree. In the case of a scale-free network, the degree distribution will have a power-law distribution. The cumulative degree distribution of the NEM power grid follows an exponential function with $P(k > K) = e^{-K/\gamma}$ and $\gamma = 2.04$, shown as the solid line in Figure 3 (right).

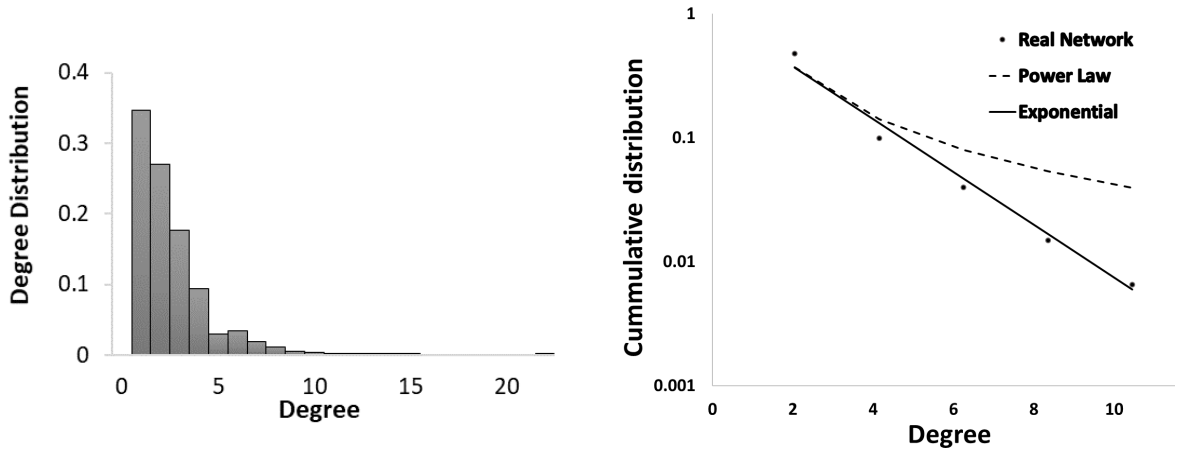


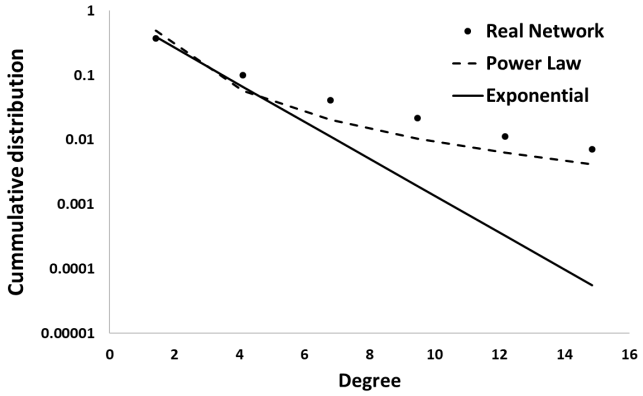
Figure 3: Unweighted degree distribution of the East-South NEM(G_{ES}); Left: Histogram of node degree distribution. Right: log cumulative degree distribution and correlation with exponential and power-law models.

In addition, nodes are connected with others that have the same degree as themselves in a small-world network, so the average nearest neighbour connectivity of a node with the degree *k* can be defined as $\langle k_{nn} \rangle = \sum_K K P_C(K|k)$, where $P_C(K|k)$ means the conditional probability that there is a link between a node with the degree *k* and another node with the degree *K*. Each node has an independent probability to have links, $P_C(K|k) = P_C(K) \approx KP(K)$. So, $\langle k_{nn} \rangle$ is approximately equal to a constant, and the correlation that $\langle k \rangle = \gamma$ is revealed. This is very useful evidence that the network follows the small-world theory.

Another property of a small-world network is the presence of hubs or nodes with high degrees. The existence of these hubs means that the path from one node to another is rather small. These characteristics of small-world networks can be explored based on two statistical properties, the clustering coefficient and the shortest path length. The clustering coefficient is defined as the fraction of the number of triangles to the total number of possible triangles for each node, meaning that the neighbours of a node are also neighbours of each other. The shortest path length is the smallest number of steps (edges) needed to reach from one node to another. On the other hand, scale-free networks have some characteristics that differ from those of small-world networks,

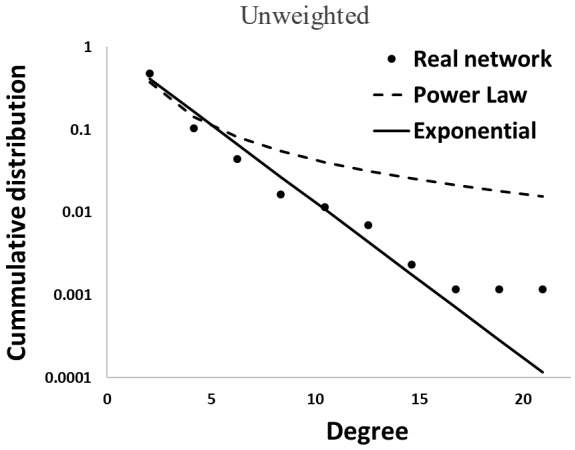
although both have a fat-tailed degree distribution. Scale-free networks have a node degree distribution following a power law and it decays more than that in small-world networks. The cumulative degree distribution can be defined as $P(k > K) = K^{-\gamma}$, shown as the dashed point line in Figure 3 (right), which does not describe the NEM well.

The weight of edges also plays an important role in studying the robustness of the network. Using the original dataset, we also examined the weighted network, where the weights of the links were derived from the voltage capacity of each transmission line. In the analysis, the voltage capacity is normalised by the average capacity: $w_{ij} = c_{ij}/\bar{c}$. As shown in Figure 4(A), the degree distribution of the weighted network follows a power-law distribution rather than the exponential distribution in the unweighted network, with $P(k > K) = K^{-\gamma}$, $\gamma = 2.03$.

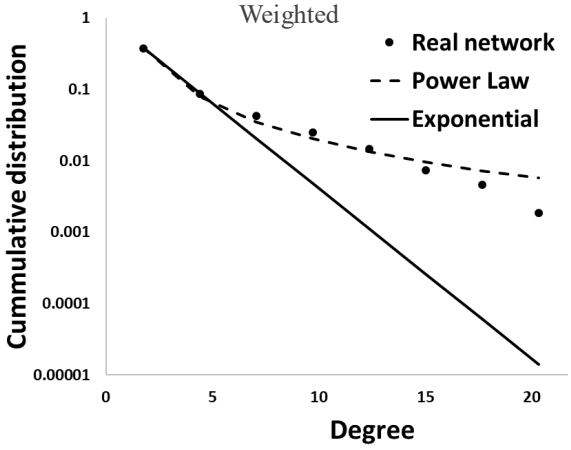


(A) Weighted East-South NEM (G_{ES})

Unweighted



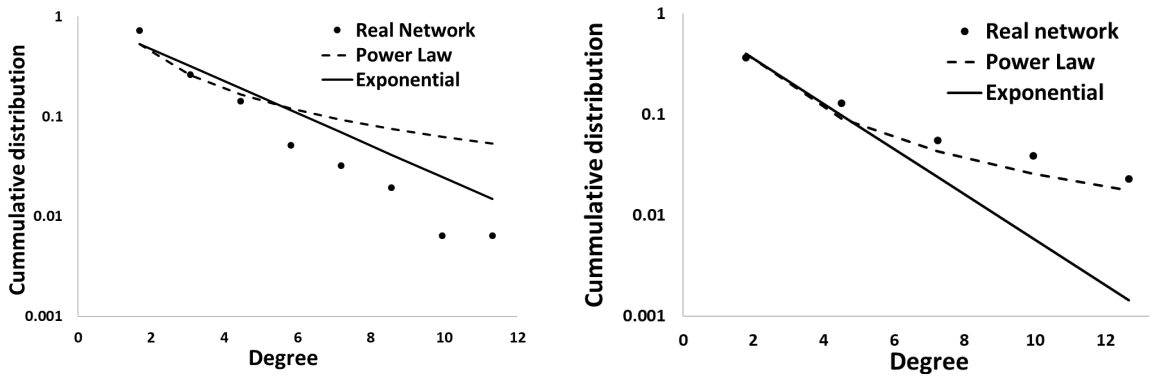
Weighted



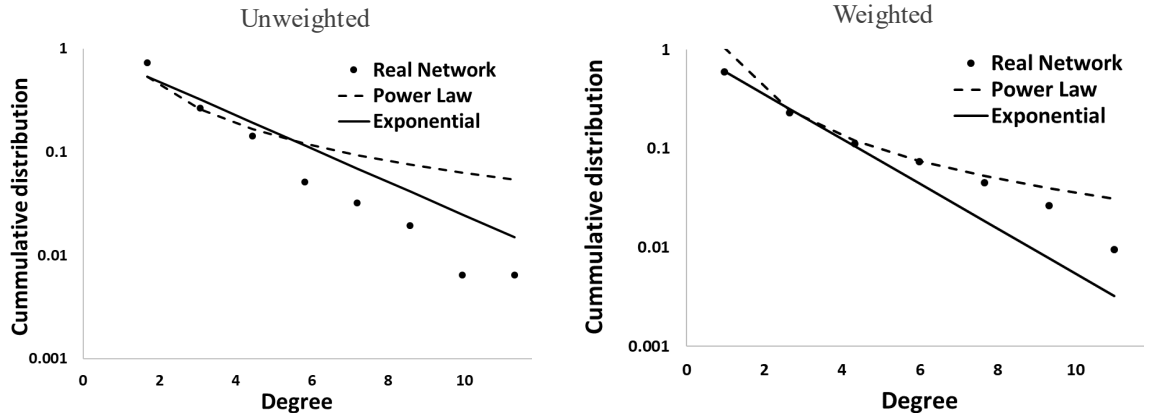
(B) New South Wales (G_{NSW})

Unweighted

Weighted



(C) Victoria (G_{VIC})



(D) Queensland (G_{QLD})

Figure 4: The cumulative degree distribution of the weighted (right) and unweighted network (left) and the fitting of exponential and power-law models. A) East-South NEM G_{ES}, B) New South Wales (G_{NSW}), C) Victoria (G_{VIC}), and D) Queensland (G_{QLD}). In all figures, the vertical axis shows the log cumulative distribution of the particular degree and the horizontal axis means the degree.

An interesting observation from Figures 3 and 4 is that the G_{ES} follows an exponential distribution as an unweighted network (Figure 3 right), whereas the degree distribution of the weighted network fits better with a power-law function (Figure 4A). The same phenomenon is observed in New South Wales, Queensland, and Victoria (Figures 4 B to D, comparing the right and left figures). In other words, the weights of edges influence the properties of nodes, although the value is not directly associated with nodes. Here, the weights of edges indicate the importance or criticality of connected nodes. In this case, edges e_{ij} with rather high weights w_{ij} (capacity c_{ij} in the original dataset) indicate that nodes n_i, n_j are more crucial than the others. In fact, transmission lines with high capacity (voltage) often occur at the outset of the generators or the main transmission line. The nodes connected by these edges are quite important because they are always generators or hubs of the network. That also explains why the weighted degree distribution

follows the power law rather than an exponential distribution. As mentioned in our literature review, clusters occur in small-world networks that cause the degree distribution to follow an exponential function. Then, the weights help to identify hubs or important nodes in the clusters. Therefore, the degree distribution will be more fat-tailed and better fitted with a power law, similar to a scale-free network.

4.3. Topological features: Network connectivity and tolerance to cascading failure

In recent studies, the robustness of networks to errors or attacks is used to describe the network tolerance of cascading failure [59]. One widely practised methodology is the analysis of network connectivity against failures. Here, we study two scenarios for performing the analysis: (1) Errors are simulated by randomly removing nodes (random errors at the generators of substations) or edges (random disconnection at transmission lines); (2) Attacks are regarded as intentional by removing specific nodes (attacks from the internet to the control centres or important hubs) or edges (intentional attacks to the transmission lines) based on statistical topology features, such as degree, betweenness and eigenvector centrality [25].

4.3.1. Robustness measure 1: largest connected component

One key characteristic used to measure a network's robustness is the largest connected component. The connected component is defined as a subgraph in an undirected network in which any two nodes are connected by at least one edge and no node is connected to an additional node outside the subgraph [60, 61]. The behaviours of the connected component are used to assess the robustness of the network.

Failure configurations also play a crucial role as parameters. Many widely studied features can be used to simulate failures, including errors or selective attacks. On the other hand, errors occurring in electricity systems are often unexpected, such that no one knows where and when they occur [25]. By randomly removing nodes in the network, we can simulate and experiment with such errors at generators or substations. On the other hand, attacks always have some strategies, and the main aim of target selection is to create the greatest loss. On the basis of that principle, critical

generators and hubs connecting many substations are most likely to be attacked, and those nodes in the network usually display unique characteristics such as a high degree centrality. Thus, features such as degree and centrality are included in the experiment [62].

Attack measures (centrality): The commonest algorithm for assessing the centrality of nodes is the betweenness centrality [63]. It is calculated by counting the number of times the node in question plays a role as a bridge along the shortest path connecting all the other node pairs: $C_B(n) = \sum_{i \neq j \neq n \in N} \frac{\sigma_{ij}(n)}{\sigma_{ij}}$, where n is a node in the node set N, $\sigma_{ij}(n)$ is the number of shortest paths that go from node n_i to node n_j and also bypass node n, and σ_{ij} is the total number of shortest paths that go from node n_i to node n_j [64]. Furthermore, a similar centrality measure is called current flow betweenness centrality, also known as percolation centrality. Instead of the shortest path, percolation centrality calculates percolated paths. Similar to calculating the shortest path between two nodes in betweenness centrality, percolation centrality calculates the shortest path between two pairs of nodes. In other words, it focuses on the shortest path between two clusters. Moreover, because the algorithm processes the shortest path based on percolation levels, weights can be involved to compute percolation level. That is an advantage over betweenness centrality. One more centrality measure in the following experiment is eigenvector centrality (also called eigencentrality), which assesses the influence of a given node on the network. The algorithm assigns a score to the node based on the scores of its neighbours. That means that nodes adjacent to other nodes with rather a high score will also have a high score, unlike degree centrality which considers a node to be influential if it is connected with many other nodes. Eigenvector centrality ranks a node as influential if it is linked to other nodes that are also important recursively. The formula can be written as: $Ax_i = \lambda x_j$, where A is the adjacent matrix, x_i, x_j is the eigencentrality score of the nodes n_i, n_j, and parameter λ is called eigenvalues [65, 66].

To analyze the impact of these centrality measures on the NEM network, we consider five scenarios, the outcomes of which are presented in Figure 5: (1) random nodes removal; (2) degree-based nodes removal; (3) current flow betweenness centrality-based (also called percolation centrality-based) nodes removal; (4) eigenvector centrality-based nodes removal; and (5) betweenness centrality-based nodes removal.

As presented in Figure 5, the average path length in the random case decreases more slowly than

those in the degree, percolation centrality, and betweenness centrality cases. The eigenvector centrality shows a rather unique trend, but its average performance appears similar to that of the random case. Therefore, it can be concluded that the robustness to random errors occurring at generators or substations, as assessed by the largest connected component, is stronger than the robustness to intentional attacks, which prefer nodes with more connections, shown by the degree-based removal in this experiment, or nodes that have more important roles as centres, as measured by current flow betweenness centrality and betweenness centrality.

Regarding the correlation between betweenness centrality and percolation centrality, it is common that both have rather similar results and shapes. It should be noted, however, that removal based on percolation centrality has a greater effect on the robustness of the network when the largest connected component drops to 0.6. A reasonable explanation is that percolation centrality focuses more on clusters, whereas betweenness centrality is based on single nodes. If we assume that several adjacent nodes have similar properties and they all have rather high betweenness centrality scores, simulation attacks based on the removal of betweenness centrality will treat them all as high priority. In fact, considering percolation centrality, only one node removal from this cluster will destroy the connectivity. The reason is similar to the reason that eigenvector-centrality-based removal does not break the network as much.

Because nodes with rather high eigencentrality scores collect in certain clusters, attacking all the nodes in a cluster one by one is not the most efficient way to break a network. Finally, it should be noted that the outcome of degree-based removal is quite similar to the outcomes of removals based on percolation centrality or betweenness centrality. The difference is that degree-based removal has an even lower largest component size than those of percolation centrality-based and betweenness centrality-based removal when the same fraction of nodes is removed. Thus, attacks based on higher degree have the greatest effect on the robustness of the network.

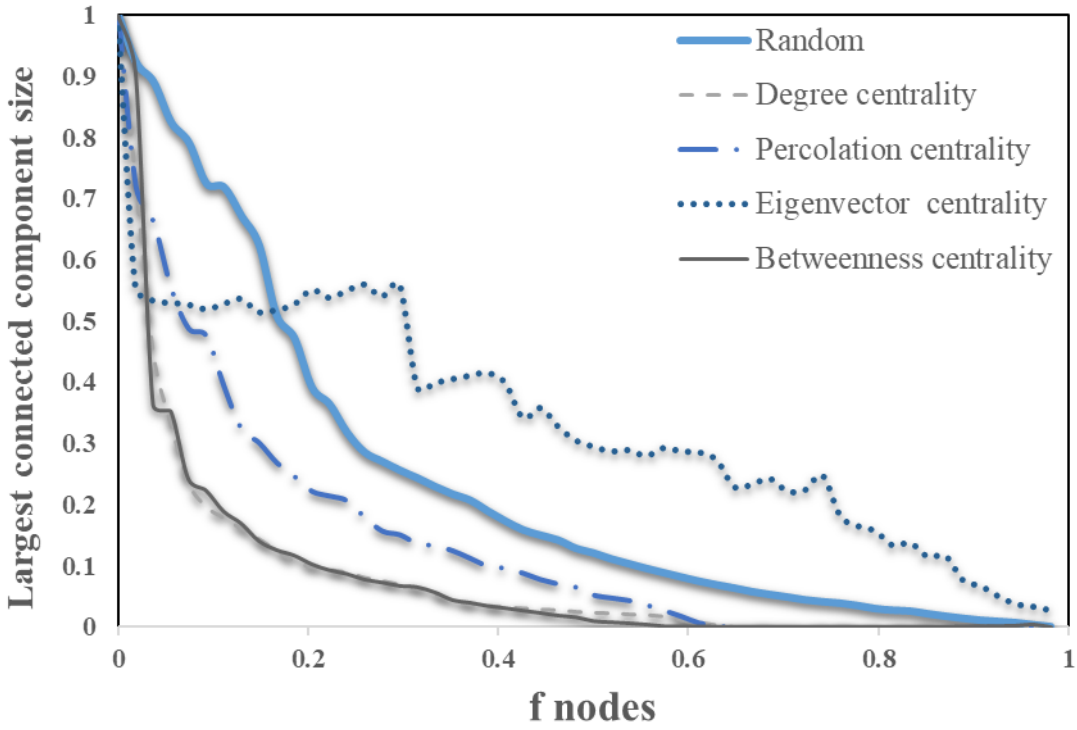
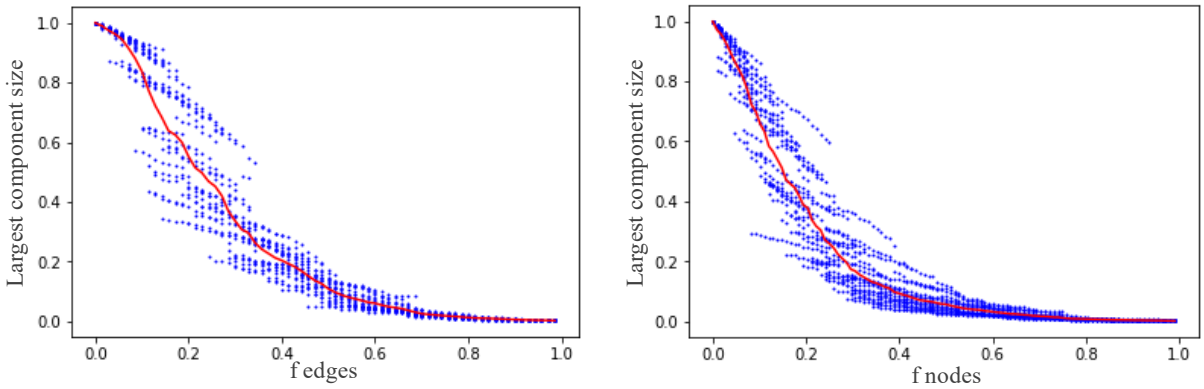


Figure 5: The effects of errors and attacks on substations or generators in the Australia East-South transmission network G_{ES}. The vertical axis represents the largest connected component size; the horizontal axis indicates the fraction f_{Comp}^{nodes} for the percentage number of removed nodes. The scatters are the average values of the experimental results after 20 random removals.

Node versus edge removal: A network is always comprised of nodes and edges. In a power transmission network, the transmission lines also face many kinds of threats and the occurrence of unexpected errors during transmission is common. Here, random edge removal is performed to simulate such errors. From Figure 6 (A and B), it appears that random removal of edges and random removal of nodes have a similar impact on the largest connected component. But there are still some differences: (1) the network seems to have stronger resilience with random node removal. If the percentage of edges or the fraction size of nodes is fixed, the largest connected component has a greater value against the removal of edges than that against the removal of nodes, (2) the trend of the largest connected component is flatter for the edge removal scenario (Figure 6 A) and it decreases more slowly when only a small fraction of edges is removed. The reason is that the removal of nodes has a greater influence on the network than the removal of edges because the loss of nodes implies that all the edges connected to those nodes will be lost as well. Therefore, attacking edges is less effective than attacking nodes directly. In other words, studying the influence of node removal is more meaningful than studying edge removal when capacity is not included as a weight in the network.



A) Random edge removal B) Random node removal

Figure 6: Tolerance of the Australian power network to (A) random edge removal, and (B) random node removal (B). The vertical axis represents the largest component size, the horizontal axis indicates the fraction f_{Comp}^{edges} for the percentage of edges/nodes removed. The scatters indicate the results of each step of removal when all nodes are removed, once the experiment finishes. To reach a general conclusion, in this study we performed the experiment 20 times and the solid line is the average value of these 20 experiments.

4.3.2. Robustness measures 2: clustering coefficient

The previous sections assessed robustness by calculating the largest connected component. Here, we use some other measures employed in the network literature. One measure is the average clustering coefficient, which describes the clustering level among adjacent nodes. Most real-world networks and complex networks have a rather high clustering coefficient, which means that nodes in these networks tend to gather together tightly into some clusters. This is also the construct of the small-world theory. The average clustering coefficient is defined as $\bar{c} = \frac{1}{n}\sum_{i=1}^{n} c_i$, where c_i is the local clustering coefficient of node n_i. The local clustering coefficient reflects how close a node's neighbours are to being a complete graph, also called a clique (see previous literature). It is written as $c_i = \frac{\lambda_G(n_i)}{\tau_G(n_i)}$, where $\lambda_G(n_i)$ is the number of subgraphs with 3 nodes and 3 edges completely connected and one of the nodes is node n_i. $\tau_G(n_i)$ is similar to $\lambda_G(n_i)$, which is the number of subgraphs with 3 nodes and 2 edges that include node $\mathrm{n_i}$. When the local clustering coefficient $c_i = 1$, a complete graph can be built with node $\mathrm{n_i}$ and any two of its neighbours [67]. The average clustering coefficient is useful for assessing a network's robustness, because clusters have strong internal relationships, which means that the removal of nodes has little effect on the cluster and the whole network. Comparing Figure 5 and Figure 7, the average clustering coefficient yields similar knowledge to the largest connected component. The order of the effects

of attack measurements on robustness remains the same: degree-based removal has the greatest influence, followed by percolation centrality-based removal, betweenness centrality-based removal, and random removal. However, the average clustering coefficient differs quite early on the eigenvector centrality-based removal compared with the trend in the largest component size (Figure 5).

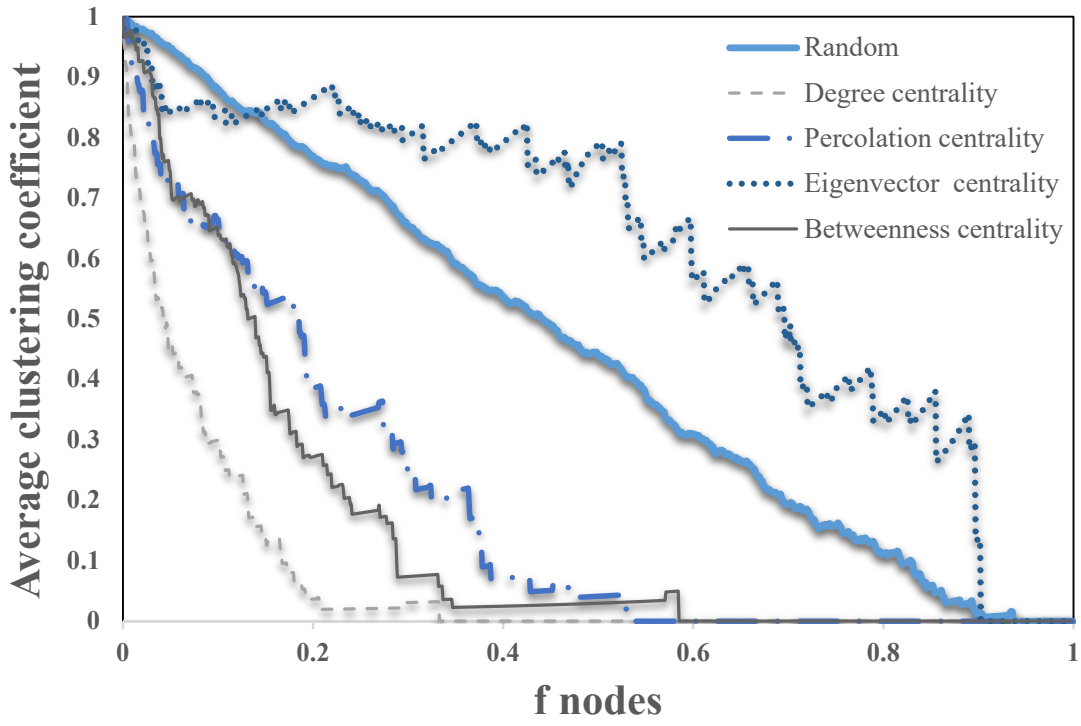
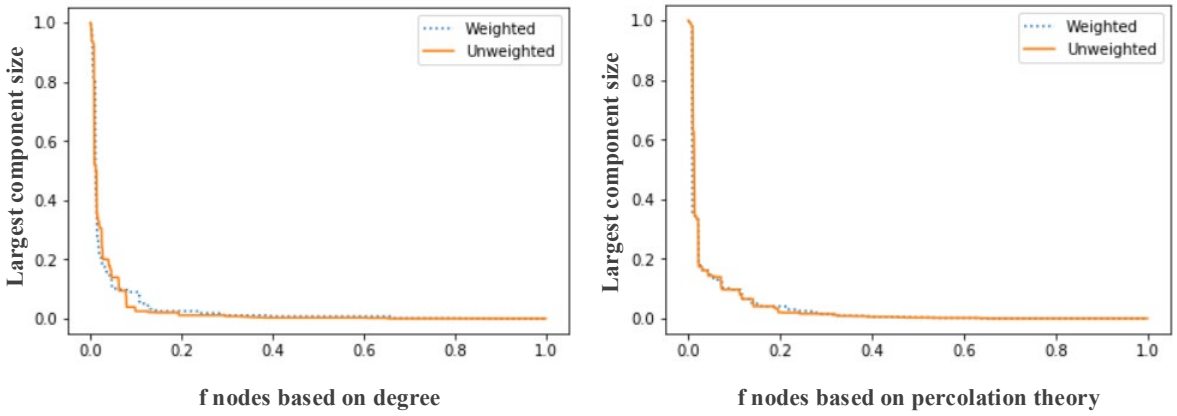


Figure 7: Effects of errors and attacks on substations or generators in the east-south Australia transmission network G_{ES}. The vertical axis represents the average clustering coefficient normalised to 1; the horizontal axis indicates the fraction f_{Comp}^{nodes} for the percentage of removed nodes. The scatters are the average values of the results of 20 random removal experiments.

4.3.3. Weighted and unweighted network study

The analyses of Figure 5 and Figure 7 are based on an unweighted NEM network. Only purely topological features are studied and no physical property of the transmission cable is included. Some important physical properties that could have a large effect on the network include: (1) the capacity (voltage) of cables; (2) the physical length of cables; (3) the transmitted frequency. Here, we investigate the weighted network with consideration of the transmission line capacity. As presented in Figure 8 (A), the largest connected component with node removal based on weighted degree tends to decrease more quickly when the fraction of node removal is rather small (around the 0.3 to 0.2 point of the largest component size). Comparing the largest connected component

size trend when removing nodes in weighted and unweighted networks shows that the attacks focused on a high degree node in a weighted network result in greater damage than those focused on a high degree node in an unweighted network. However, as presented in Figure 8 (B), there is no obvious difference between removals based on percolation centrality in weighted or unweighted networks. Percolation centrality measures how important a node is to have the shortest path. If a node with a high level of percolation centrality is removed, the shortest path is very likely to be disconnected. From Figure 8 (B), there is no large difference between unweighted and weighted experiments. Understandably, a node with a crucial role in maintaining the connectivity (shortest path) connected, is important even if it has low weight.



A) Nodes removal based on degree B) Nodes removal based on percolation theory

Figure 8: Impact of considering weighted and unweighted networks for robustness analysis of the East-South NEM G_{ES}. The vertical axis represents the largest connected component and the horizontal axis indicates the fraction for the percentage of removed nodes based on the degree (A) and removed nodes based on percolation theory(B).

5. Conclusion

Network theory is the study of the relationship between discrete objects, containing nodes as discrete objects and edges as the relationships. With this model, calculations can be applied easily to explore the characteristics behind the networks. Many topological features are widely studied in this field as measures to examine the robustness of networks.

In this review, network theories were classified into two types: (i) random graphs, including the Erdős–Rényi model, the Gilbert–Elliott model, the Geometric Random Graph that introduced Euclidean distance, the Watts-Strogatz model that has non-Poisson degree distribution; (ii) scale-free networks, including the Barabási–Albert model and the Bianconi–Barabási model, a variant

of the BA model. Then, percolation theory was discussed. Previous studies showed that the Watts-Strogatz model and scale-free networks with a non-Poisson distribution had strong robustness to errors but were sensitive to intentional attacks on critical nodes. The Watts-Strogatz networks were more robust, due to their high clustering coefficients.

In the practical section, the dataset of Australian transmission lines (NEM) was collected from Geoscience Australia. After processing and some data wrangling, the electricity network nodes and edges were extracted, and the adjacency matrix was built. Model fitting showed that the unweighted network degree distribution followed an exponential distribution: $P(k > K) = e^{-K/\gamma}$ with $\gamma = 2.04$, and the weighted networks degree distribution followed the power law: $P(k > K) = K^{-\gamma}$ with $\gamma = 2.03$. In other words, the network was a small-world network and it was more scale-free when weights were taken into consideration. Different models were then built to study the network's robustness: (1) failure measures such as random removal, degree-based removal, and centrality-based removal; (2) resilience measures such as the largest connected component, the average clustering coefficient and the average shortest path length; (3) attacking targets: generators or substations and transmission cables; (4) weighted and unweighted studies. The conclusion was drawn that attacks focusing on nodes with a rather high degree, betweenness centrality, or percolation centrality had obviously greater effects on the network largest connected component, average clustering, and average path length than system random errors. In addition, it was noted that intentional attacks on high-degree nodes in weighted networks would cause greater damage to the network. Combined with the literature, our investigation showed that, although scale-free networks are robust to random errors, they are fragile to intentional attacks. However, small-world networks, with properties such as a high clustering coefficient and a short average path length, are quite robust to both errors and attacks.

References

[1] ESCSWG. Roadmap to Achieve Energy Delivery Systems Cybersecurity. Energy Sector Control Systems Working Group; 2011.

[2] Piebalgs A. Green paper: A European strategy for sustainable, competitive and secure energy. CESifo Forum: München: ifo Institut für Wirtschaftsforschung an der Universität München; 2006. p. 8-20.

[3] AEMO. Black system South Australia 28 September 2016. Melbourne, Australia: Australian

Energy Market Operator; 2017.
[4] Eckermann D, Long N. Energy Security Target Regulations: Submission to Department of the Premier and Cabinet. South Australia: South Australian Chamber of Mines and Energy; 2017.
[5] Maclennan L. Big blackout cost us $100million: BHP Billiton. ABC new. Australia2017.
[6] Bolger R. Energy inquiry: Hydro Tasmania puts total cost of power crisis at $180m. ABC news. Australia2016.
[7] Kempton H. Fault found in Basslink cable 100km offshore. Hobart Mercury. Australia2015.
[8] Morton A. Tasmania battles to keep lights on with cloud-seeding and diesel generators. The Examiner; 2016.
[9] Willis HL. Power distribution planning reference book: CRC press; 1997.
[10] Albert R, Albert I, Nakarado GL. Structural vulnerability of the North American power grid. Physical Review E. 2004;69:025103.
[11] Albert R, Barabási A-L. Statistical mechanics of complex networks. Reviews of Modern Physics. 2002;74:47-97.
[12] Newman ME. The structure and function of complex networks. SIAM review. 2003;45:167-256.
[13] Sun K. Complex networks theory: A new method of research in power grid. 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific: IEEE; 2005. p. 1-6.
[14] Sun K, Han Z-X. Analysis and comparison on several kinds of models of cascading failure in power system. 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific: IEEE; 2005. p. 1-7.
[15] Saleh M, Esa Y, Mohamed A. Applications of complex network analysis in electric power systems. Energies. 2018;11:1381.
[16] Erdős P, Rényi A. On random graphs I. Publ Math Debrecen. 1959;6:290-7.
[17] Newman ME, Strogatz SH, Watts DJ. Random graphs with arbitrary degree distributions and their applications. Physical review E. 2001;64:026118.
[18] Newman ME, Watts DJ, Strogatz SH. Random graph models of social networks. Proceedings of the national academy of sciences. 2002;99:2566-72.
[19] Watts DJ, Strogatz SH. Collective dynamics of 'small-world'networks. nature. 1998;393:440.
[20] Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex networks. Nature. 2000;406:378.
[21] Shunkun Y, Jiaquan Z, Dan L. Prediction of cascading failures in spatial networks. PloS one. 2016;11:e0153904.
[22] Li D, Fu B, Wang Y, Lu G, Berezin Y, Stanley HE, et al. Percolation transition in dynamical traffic network with evolving critical bottlenecks. Proceedings of the National Academy of Sciences. 2015;112:669-72.
[23] Dobson I, Carreras BA, Lynch VE, Newman DE. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2007;17:026103.
[24] Mei S, Zhang X, Cao M. Power grid complexity: Springer Science & Business Media; 2011.
[25] Rosas-Casals M, Valverde S, Solé RV. Topological vulnerability of the European power grid

under errors and attacks. International Journal of Bifurcation and Chaos. 2007;17:2465-75.
[26] AEMO. National Electricity Market Fact Sheet. Australia: Australian Energy Market Operator; 2018.
[27] Brinsmead TS, Hayward J, Graham P. Australian electricity market analysis report to 2020 and 2030. 2014.
[28] Gilbert EN. Random graphs. The Annals of Mathematical Statistics. 1959;30:1141-4.
[29] Bollobás B. Random graphs. Modern graph theory: Springer; 1998. p. 215-52.
[30] Fronczak A, Fronczak P, Hołyst JA. Average path length in random networks. Physical Review E. 2004;70:056110.
[31] Travers J, Milgram S. The small world problem. Phychology Today. 1967;1:61-7.
[32] Holland PW, Leinhardt S. Transitivity in structural models of small groups. Comparative group studies. 1971;2:107-24.
[33] Cohen R, Havlin S, Ben-Avraham D. Structural properties of scale-free networks. Handbook of graphs and networks. 2002.
[34] Cohen R, Havlin S. Scale-free networks are ultrasmall. Physical review letters. 2003;90:058701.
[35] Newman ME, Watts DJ. Scaling and percolation in the small-world network model. Physical review E. 1999;60:7332.
[36] Price DdS. A general theory of bibliometric and other cumulative advantage processes. Journal of the American society for Information science. 1976;27:292-306.
[37] Barabási A-L, Albert R. Emergence of scaling in random networks. science. 1999;286:509-12.
[38] Dorogovtsev SN, Mendes JFF, Samukhin AN. Structure of growing networks with preferential linking. Physical review letters. 2000;85:4633.
[39] Krapivsky PL, Redner S, Leyvraz F. Connectivity of growing random networks. Physical review letters. 2000;85:4629.
[40] Bollobás Be, Riordan O, Spencer J, Tusnády G. The degree sequence of a scale-free random graph process. Random Structures & Algorithms. 2001;18:279-90.
[41] Dangalchev C. Generation models for scale-free networks. Physica A: Statistical Mechanics and its Applications. 2004;338:659-71.
[42] Chung F, Lu L. The diameter of sparse random graphs. Advances in Applied Mathematics. 2001;26:257-79.
[43] Barabási A-L. Network science: Cambridge university press; 2016.
[44] Bianconi G, Barabási A-L. Competition and multiscaling in evolving networks. EPL (Europhysics Letters). 2001;54:436.
[45] Pastor-Satorras R, Vespignani A. Evolution and structure of the Internet: A statistical physics approach: Cambridge University Press; 2007.
[46] Watts DJ. A simple model of global cascades on random networks. Proc Natl Acad Sci U S A. 2002;99:5766-71.
[47] Pagani GA, Aiello M. The power grid as a complex network: a survey. Physica A: Statistical Mechanics and its Applications. 2013;392:2688-700.
[48] Broadbent SR, Hammersley JM. Percolation processes: I. Crystals and mazes. Mathematical Proceedings of the Cambridge Philosophical Society: Cambridge University Press; 1957. p. 629-41.

[49] Cohen R, Havlin S. Complex networks: structure, robustness and function: Cambridge university press; 2010.
[50] Bunde A, Havlin S. Fractals and disordered systems: Springer Science & Business Media; 2012.
[51] Callaway DS, Newman ME, Strogatz SH, Watts DJ. Network robustness and fragility: Percolation on random graphs. Physical review letters. 2000;85:5468.
[52] Stauffer D, Aharony A. Introduction to percolation theory: revised second edition: CRC press; 2014.
[53] Faloutsos M, Faloutsos P, Faloutsos C. On power-law relationships of the internet topology. ACM SIGCOMM computer communication review: ACM; 1999. p. 251-62.
[54] Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the Internet under intentional attack. Physical review letters. 2001;86:3682.
[55] Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the internet to random breakdowns. Physical review letters. 2000;85:4626.
[56] Palla G, Derényi I, Farkas I, Vicsek T. Uncovering the overlapping community structure of complex networks in nature and society. Nature. 2005;435:814.
[57] Geoscience-Australia. Powerlines. In: Australia G, editor. NM Culture and Infrastructure. Australia2016.
[58] Wang XF, Chen G. Complex networks: small-world, scale-free and beyond. IEEE circuits and systems magazine. 2003;3:6-20.
[59] Wang J, Rong L, Zhang L, Zhang Z. Attack vulnerability of scale-free networks due to cascading failures. Physica A: Statistical Mechanics and its Applications. 2008;387:6671-8.
[60] Reingold O. Undirected connectivity in log-space. J ACM. 2008;55:1-24.
[61] Shiloach Y, Even S. An On-Line Edge-Deletion Problem. J ACM. 1981;28:1-4.
[62] Iyer S, Killingback T, Sundaram B, Wang Z. Attack robustness and centrality of complex networks. PLoS One. 2013;8:e59613-e.
[63] Freeman LC. A Set of Measures of Centrality Based on Betweenness. Sociometry. 1977;40:35-41.
[64] Brandes U. A faster algorithm for betweenness centrality. The Journal of Mathematical Sociology. 2001;25:163-77.
[65] Negre CFA, Morzan UN, Hendrickson HP, Pal R, Lisi GP, Loria JP, et al. Eigenvector centrality for characterization of protein allosteric pathways. Proceedings of the National Academy of Sciences. 2018;115:E12201.
[66] Newman ME. Mathematics of networks. The new Palgrave dictionary of economics. 2016:1-8.
[67] Kemper A. Valuation of network effects in software markets a complex networks approach. Heidelberg : London: Heidelberg : Physica London : Springer distributor; 2010.