Balancing System Survivability and Cost of Smart Grid via Modeling Cascading Failures

Zhen Huang, Cheng Wang, Milos Stojmenovic, Amiya Nayak

Abstract—As a typical emerging application of cyber physical system, smart power grid is composed of interdependent power grid and communication/control networks. The latter one contains relay nodes for communication and *operation centers* to control power grid. Failure in one network might cause failures in the other. Moreover, these failures may occur recursively between the two networks, leading to cascading failures. We propose a k-to-n interdependency model for smart grid. Each relay node and operation center is supported by only one power station, while each power station is monitored and controlled by k operation centers. Each operation center controls n power stations. We show that the system controlling cost is proportional to k. By calculating the fraction of functioning parts (survival ratio) using *percolation theory* and *generating functions*, we reveal the nonlinear relation between controlling cost and system robustness, and use graphic solution prove that a threshold exists for the proportion of faulty nodes, beyond which the system collapses. The extensive simulations validate our analysis, determine the percentage of survivals and the critical values for different system parameters. The mathematical and experimental results show that smart grid with higher controlling cost has a sharper transition, and thus is more robust. This is the first paper focusing on improving smart power grid robustness by changing monitoring strategies, from an interdependent complex networks perspective.

Index Terms—Cyber physical system; Smart power grid; Interdependent networks; Cascading failure; Percolation theory

1 Introduction

Cyber-physical systems (CPS) transform our world with new relationships between computer-based control and communication systems, engineered systems and physical reality. The software programs, networking and computers are integrated together rather than computation alone. In a CPS, physical devices such as battery, sensors are viewed as physical components. The embedded computers and communication networks are considered as cyber components. As one of important CPS applications, smart power grid is composed of interdependent power grid and communication/control networks. Conventional electrical grids utilize centralized command and control structures, e.g., SCADA (Supervisory Control And Data Acquisition) system relying on human monitors for identifying faults and decision making. Massive blackouts have occurred in the past since the existing system lacks real-time control ability, e.g., the very recent huge blackout happened in July 2012, affected more than 600 million people in India [1].

The smart power grid concept addresses the real-time control and energy efficiency. It is an electrical grid that integrates information and communications technology and different sources of power generation e.g., fossil-fuel, solar and wind. It predicts the electricity demands in different regions, monitors the power usage of customers using smart meters, and deals with system failure rapidly.

We study the reliability of smart power grid. The communications and control infrastructures need energy to properly operate, while the power stations and electricity transmission are controlled by *operation centers*. Operation centers can also transfer and exchange information with other communication devices. The two networks are connected and mutually dependent, and smart power grid can be regarded as an *interdependent network*. The failure in either of them may lead to the failure in another. The breakdown of a power station would cause the outage of communication and control nodes, while the faults in communications and control system might lead to an improper function of power stations. Moreover, failures can occur recursively between the two networks, causing cascading failures, and potential blackout. One important parameter for discussing the smart grid robustness is the fraction of properly functioning nodes, i.e., survival ratio, after cascading failure stops [18].

Each power station can be controlled by multiple distinct operation centers, and functions as long as at least one of its operation centers is working. We believe that the more control relations (links) and devices the system has, the higher cost is required. We define the *system controlling cost* as proportionally dependent on the number of links between operation centers and power stations. Our primary interest is to find out the relation between controlling cost and system robustness. In this paper, we design a mathematical model of smart power grid to

- *Zhen Huang, Cheng Wang and Amiya Nayak are with EECS, University of Ottawa, Canada. Milos Stojmenovic is with Singidunum University, Belgrade, Serbia (E-mail: {zhuan045, cwan3, nayak}@uottawa.ca, mstojmenovic@singidunum.ac.rs)*

understand the interaction of the different components. This model enables us to study how failures propagate within the system and what are system robustness under different monitoring schemes. Our analysis offers insights for building optimal smart grid infrastructures.

Current research on robustness in smart power grid are mainly focusing on load distribution and malicious attacks. An architecture for distributed generation, which can help prevent cascading failures, is described in [5]. [13], [14] study the cascading failure in electricity grid due to the overload in a single station. To decrease the impact of cascading failure or even to prevent it, [21] analyze the tripping of overloaded lines and proposed a model to control these lines. [19] proposed three mitigation strategies and simulate them on real-world network structures to find an effective way for reducing cascading failure. Software overlays and multiple routes to deliver critical data to prevent failures were studied in [26]. Load distribution attack was deeply investigated in [25] to provide effective prevention on false data injection. However, none of previous papers considers the cascading failure between power grid and communication network, or presents more reliable architecture.

Interdependent network [2] was proposed to study the interactions between networks. The models proposed in [2], [3] are 'one-on-one' interdependency models, within which the node properly operates relying on one unique node in the other network. Such models do not correctly reflect the characteristics of smart grid since the power station normally provides energy to multiple communication devices. The 'multiple-to-multiple' interdependency models developed in [24] assumed that each node is assigned with the same number of inter links. Each node functions as long as at least one of its supporting nodes is operating. [22] points out that the interdependency in real world network is *unidirectional* rather than *bidirectional*. These articles do not follow the 'one-to-multiple' requirement of smart power grid: each communication/control node is supported by only one power station, while each power station is monitored and controlled by multiple operation centers.

1.1 Our Contribution

We propose a novel smart grid model where each power station is operated by k distinct operation centers, and each operation center could monitor and control n power stations. The defined 'system controlling cost' is simply equal to k units, and the 'monitoring capability' for each operation center is n. By calculating the fraction of functioning parts (survival ratio) after the cascading failure stops, we mathematically study the relation between system robustness, controlling cost and monitoring capability.

We follow a three-step scheme to construct 'one-to-multiple' interdependent network to model smart power grid. Both power grid and communication networks are type of scale-free networks [18], in which the degree distribution follows power law. This is the first paper to study the smart power grid robustness (the effect of cascading failures) of different monitoring strategies, using interdependent network and percolation theory. We present detailed mathematical analysis of the random failure propagation in the system. Our results show that if the proportion of initial faulty nodes exceeds a critical value, the entire system collapses. Our analysis shows that the system robustness experiences a sublinear improvement with the increase of k, while n has no impact on system robustness when the size of network is large.

The extensive simulation validates our analysis. The system robustness against random failure can be improved by increasing monitoring cost though they have nonlinear relation. Meanwhile, the critical value for a higher k is smaller, which means the system can tolerate a higher fraction of random failures. The robustness improves between $k = 1$ and $k = 2$ significantly, while the gap between $k = 10$ and $k = 15$ is small. Hence, for building a smart power grid, adding as many as possible control link is not good strategy since the massive extra cost does not improve system reliability significantly. The simulation also shows that for a small k, the system meets a second-order continues transition, while for higher k, the transition becomes sharper. Thus, the system is easier to be predicted. Our experimental results illustrate that higher n improves system robustness slightly and at the same time decreases the critical value. But the disadvantage is that the transition becomes flat so that the system is harder to be predicted. Therefore, for building smart grid infrastructures, we need carefully choose the value of k and n depending on our demands.

1.2 Organization

The paper is organized as follows. Section 2 reviews the background on cascading failure in power grid and interdependent networks. A practical model for smart power grid and its three-step construction procedure are proposed in Section 3. We introduce the math tools used in single complex networks in Section 4. The mathematical approximation for cascading failure in smart grid is given in Section 5, and we estimate the size of the remaining functioning nodes after cascading stops. Section 6 shows our extensive simulations. We draw the conclusions in Section 7.

2 Related Work

A part of existing research on CPS are focusing on designing analytical CPS model. A unique model of a generic CPS appears to be infeasible due to specifics of actuation and physical world reaction. Existing work on modelling is primarily about extracting properties from physical systems and assumed associated cyber system and matching with some network families. For example, [23] proposed an algorithm that generates random topology power grids featuring the same topology and electrical characteristics derived from the real data. [7] focused on the challenges of modeling CPSs that arise from the intrinsic heterogeneity, concurrency, and sensitivity to timing. Specific technologies applied in a particular CPS include hybrid system modeling and simulation, concurrent and heterogeneous models of computation, the use of domain-specific ontologies to enhance modularity, and the joint modeling of functionality and implementation architectures [7].

Moslehi and Kumar [16] critically reviewed the reliability impacts of major components such as energy generator, demand response, communications and electricity transportation in smart power grid. They presented a grid-wide IT architectural framework to improve the robustness of system, and discussed the technical feasibility. A power generation and distribution architecture has been discussed in [5], arguing that a distributed generation enhances the robustness of the system. Using optimization techniques and simulations, the authors showed that fault tolerance increases with the number of generators.

Blackouts during the past several decades were mostly due to the overload cascading failure. Kadloor and Santhi [13] modeled power grid as a graph and studied the system robustness. By extensive mathematical analysis, they estimated the disturbance levels the system can tolerate before a few overloaded nodes trigger a large blackout. Kinney et al. [14] used the real network structure of the North American power grid and modeled it as a weighted graph. Combining dynamical approach of the Crucitti-Latora-Marchiori model and complex networks, they studied two types of node overload progression, and showed that the disruption of 40% transmission substations leads to the cascading failure, and a single node failure can cause up to 25% loss of transmission efficiency.

The case of static overload failure was discussed in [6]. Optimization technique was used and a distance-to-failure algorithm was proposed to predict the weak points in power grid. They applied their algorithm to two real power grid examples and concluded that the failures due to overload are sufficiently sparse if the normal operational stations are healthy. Load Redistribution (LR) attack was developed and studied in [25] by analyzing their damage to power grid operation. It proposed an attack model describing the main goal of LR attack and then based on that, indicated the theory and criterion of protecting the system from LR attack.

Pfitzner et al. [21] proposed a model to focus on the analysis of tripping of already overloaded lines. By simulating on a real-world power grid structure, they showed that such controlled tripping leads to significant mitigation of cascading failure.

Infrastructures such as water supply, power grid, transportation system, fuel stations are becoming increasingly interconnected. Studying the interactions and understanding how robustness is challenging due to the interdependency among such networks.

Buldyrev et al. [2] studied the cascading failures robustness with *percolation theory* [18] which was conventionally applied in a single complex network. A 'one-to-one' correspondence model was proposed, where each node in network A functions depending on exactly one node in network B, and vice versa. The 'multiple-to-multiple' correspondence was proposed in [22], where a single node in network A operates depending on more than one node in network B, and vice versa. Each node functions as long as at least one of its supporting nodes is operating. They also assumed that not all the pairs of nodes are mutually dependent, and the interdependency is sometimes *unidirectional*. [20] described with two types of inter links. The *dependency link* makes failure in one network cause failure in the other network, while *connectivity link* enables the nodes work cooperatively. High density of dependency link makes networks more vulnerable.

The work of [2], [22] was extended in [24] by a 'regular allocation', where every node in the system is assigned same number of inter links. The regular allocation scheme is proven to be optimal when the topology of each individual network is unknown. A targeted attack was discussed in [11], where the authors pointed out that protecting the high degree nodes can improve system robustness significantly. Gao et al. [9] studied the interacting networks and presented an percolation law for a network of several interdependent networks. A survey of interdependent networks can be found in [10].

In the previous work [12], the authors proposed an 'one on one' interdependent model for smart power grid and measured the size of survivals. In the proposed model, both power grid and communication network are scale-free networks. Since no closed-form solution can be derived, simulation was used to determine the results.

3 System Model

3.1 Assumptions and Definitions

We model the smart power grid as two interconnected networks $\mathcal{N}_\mathrm{P}$ and $\mathcal{N}_\mathrm{I}$ (power grid and communication/control network, respectively). $\mathcal{N}_\mathrm{I}$ is envisioned as a part of the Internet backbone, extended with some wireless links. Both networks consist of a large number of components; some of them are considered as terminals, with limited influence to the system reliability. For instance, the breakdown of a smart meter in one house is not likely to cause the failure of other components. We only consider the components that have some dependencies or are providing connectivity. Nodes in $\mathcal{N}_{\mathrm{P}}$ represent the power plants, substations, transformers and new energy generators. Nodes in $\mathcal{N}_{\mathrm{I}}$ are *Autonomous Systems (AS)*. There are two types of ASs: *Operation Centers*, which monitor and control power stations and exchange information with other communication devices, and *Relaying ASs*, for relaying messages in smart grid system, with no direct impact on power stations. S_{P} and S_{I} are sizes of $\mathcal{N}_{\mathrm{P}}$ and $\mathcal{N}_{\mathrm{I}}$, respectively.

The distribution of power stations and edges in power grid was studied and modeled in [4], [17], which considered power grid as a scale-free network. A scale-free network is a network whose degree distribution follows a power law, $\mathbf{P}(z) \propto z^{-\gamma}$, where $\mathbf{P}(z)$ is the probability that the degree of a node is z, γ is power law exponent. Extensive data show that Internet is also a scale-free network [8], [18].

3.2 Interdependent Model

We refer to edges that connect the nodes from different networks as *Inter Links*. We assume that each power station in $\mathcal{N}_{\mathrm{P}}$ is operated by k operation centers, and functions properly as long as at least one of them works. The *monitoring capability* of each operation center is defined as the number n of power stations it can control. Thus, each node $\mathcal{N}_{\mathrm{P}}$ has k CD (Control-Dependency) inter links and each operation center has n CD links. Meanwhile, each power station has multiple ED (Energy-Dependency) links to ASs in $\mathcal{N}_{\mathrm{I}}$, while each node in $\mathcal{N}_{\mathrm{I}}$ has only one ED link.

We define the cost including hardware, software and labour as *Controlling Cost*, measured based on two parameters: k and the number of operation centers m. k determines $k \cdot S_{\mathrm{P}}$, the total number of CD inter links required. To minimize the cost with a fixed k, we minimize m by fully utilizing the control capability of each operation center. In other words, the minimum controlling cost is achieved for $m = \frac{k \cdot S_{\mathrm{P}}}{n}$. Thus the minimum controlling cost is proportional to k. In the rest of paper, we simply consider the controlling cost to be k. For each k, we automatically calculate the minimum m in the cost formula. Figure 1 gives a sketch of our model, with $k = 1, m = 3, n = 2$.

We construct interlinks by applying a three step procedure:

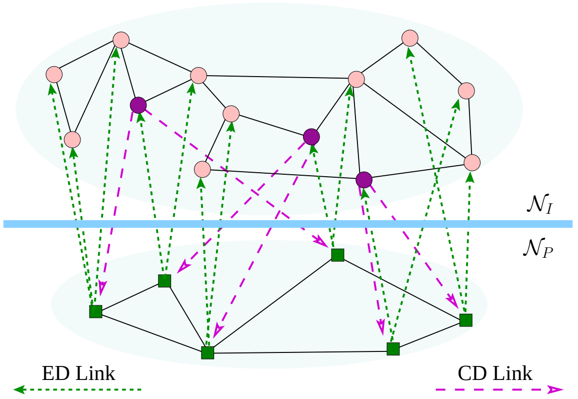


Fig. 1. Each node in $\mathcal{N}_{\mathrm{I}}$ has one energy inter link from $\mathcal{N}_{\mathrm{P}}$, and each node in $\mathcal{N}_{\mathrm{P}}$ is controlled by $k = 1$ operation centers. Three dark nodes ($m = 3$) are operation centers and each controls $n = 2$ nodes from $\mathcal{N}_{\mathrm{P}}$.

3.2.1 Allocating ED Link

We consider each node in $\mathcal{N}_{\mathrm{P}}$ as a bin and nodes in $\mathcal{N}_{\mathrm{I}}$ are balls. The allocation follows the well-known *Balls and Bins* problem, where S_{I} balls have to be independently and uniformly put into S_{P} bins, the probability that one ball is assigned into i-th bin is $\frac{1}{S_{\mathrm{P}}}$. For each bin, the probability it has t balls is given by:

$$\mathbf{P}(t) = \binom{S_{\mathrm{I}}}{t} \cdot (\frac{1}{S_{\mathrm{P}}})^{t} \cdot (1 - \frac{1}{S_{\mathrm{P}}})^{S_{\mathrm{I}}-t}. \qquad (1)$$

Hence, the number of *AS* t that is supported by each power station follows a binomial distribution with $\mathbf{B}(S_{\mathrm{I}}, \frac{1}{S_{\mathrm{P}}})$.

3.2.2 Choosing Minimum Number of Operation Center

We choose uniformly m nodes at random as operation centers from $\mathcal{N}_{\mathrm{I}}$. The relation between m, n and k is given by

$$m = \frac{k \cdot S_{\mathrm{P}}}{n}, \qquad (2)$$

where each node in $\mathcal{N}_{\mathrm{P}}$ is monitored by k operation centers, thus totally $k \cdot S_{\mathrm{P}}$ links are required, and each operation center can control n power stations.

3.2.3 Allocating CD Link

Subsequently, we match m operation centers and S_{P} power stations so that each operation center is allocated n power stations, and each power station is controlled by k operating centers. This can be done in a sequence, by operating centers selecting power stations at random but only among stations not selected k times already.

4 Mathematical Analysis

In this section, we show how cascading failure propagates in smart grid. Then we introduce the math tools that be used in a single complex network. Before starting, we list the definitions and notations in Table 1. We introduce a notation $F_{\mathcal{N}}(\phi)$ from [10], [24] to represent the expected fraction of giant component in the subnetwork which occupies the fraction ϕ of the nodes in the entire network $\mathcal{N}$. In our work, we focus on a subclass of scale-free networks whose node degree strictly follows the power law degree distribution. Then, besides the fraction ϕ, $F_{\mathcal{N}}(\phi)$ only depends on the node degree distribution of $\mathcal{N}$, [2], [10]. Furthermore, since we only consider the networks (including the sequence of subnetworks and giant components) with infinite size, the power law distribution is completely determined by the power law exponent. Thus, in this paper, we let $F(\phi, \lambda)$ represent the expected fraction of giant component in the subnetwork which occupies the fraction ϕ of the nodes in the entire scale-free network with a power law degree distribution, where λ is the power law exponent. Accordingly, $F(\phi, \lambda_{\mathrm{P}})$ and $F(\phi, \lambda_{\mathrm{I}})$ represent the fractions of giant components for network $\mathcal{N}_{\mathrm{P}}$ and $\mathcal{N}_{\mathrm{I}}$ whose power law exponents are λ_{P} and λ_{I}, respectively.

4.1 Failure Cascading Process

We define system robustness in our model as the fraction of survivals after the cascading failure stops, i.e., the nodes that still can operate. We focus on how this failure cascading propagates and then estimate the survivals. Considering smart grid as two complex networks, we assume two conditions should be satisfied if a node is in work:

1) The node belongs to the *giant component*.
2) At least one inter link is connected to this node, where this link comes from a functioning node in the other network.

We begin with a random removal of $(1-\phi)\cdot S_{\mathrm{I}}$ nodes in $\mathcal{N}_{\mathrm{I}}$ as the simulation of initial failures or attacks. After this removal, the related intra links and inter links of deleted nodes are removed. As a result, $\mathcal{N}_{\mathrm{I}}$ begins to fragment into disconnected components. Due to our Condition 1, only the nodes belong to giant component can operate properly. Therefore, the nodes in small components are considered as failure. Now owning to the interdependency, a part of nodes in $\mathcal{N}_{\mathrm{P}}$ lost inter links so they are unsatisfied with Condition 2. Then these nodes and related links are removed. The fragmentation in $\mathcal{N}_{\mathrm{P}}$ might lead to further failures in $\mathcal{N}_{\mathrm{I}}$, because now some nodes in $\mathcal{N}_{\mathrm{I}}$ have no inter links. This cascading failure continues recursively between two networks, and reaches one of the following two final status: *1)* all nodes are faulty and the giant component disappears; *2)* the two giant components in $\mathcal{N}_{\mathrm{P}}$ and $\mathcal{N}_{\mathrm{I}}$ are mutually connected. One complete cascading failure example is given by Fig. 2. Initially, ten nodes and six nodes are in $\mathcal{N}_{\mathrm{I}}$ and $\mathcal{N}_{\mathrm{P}}$ respectively. After one node is attacked in $\mathcal{N}_{\mathrm{I}}$, the entire system collapses.

TABLE 1
Notations for the analysis

k	number of operation centers that control a power station, it represents the system controlling cost
n	monitoring capability of operation center
m	number of operation centers
$\mathbf{P}_{\mathrm{P}}(z), \mathbf{P}_{\mathrm{I}}(z)$	intra degree distribution for network $\mathcal{N}_{\mathrm{P}}, \mathcal{N}_{\mathrm{I}}$
$\lambda_{\mathrm{P}}, \lambda_{\mathrm{I}}$	power law exponent of $\mathbf{P}_{\mathrm{P}}(z), \mathbf{P}_{\mathrm{I}}(z)$.
$F(\phi, \lambda_{\mathrm{P}}), F(\phi, \lambda_{\mathrm{I}})$	the fraction of giant component in the subnetwork which occupies the fraction ϕ of the nodes in the entire network $\mathcal{N}_{\mathrm{P}}$ and $\mathcal{N}_{\mathrm{I}}$

4.2 Generating Function for An Individual Network

Generating function and percolation theory are widely used to solve the problems in complex network. We describe the generating function for a single network that will also be used in studying interdependent networks. We introduce generating function into our model. Let us assume the nodes in $\mathcal{N}_{\mathrm{P}}$ are assigned a degree z with the same probability $\mathbf{P}_{\mathrm{P}}(z)$, which follows power law in scale-free network. Thus $\mathbf{P}_{\mathrm{P}}(z) \propto z^{-\lambda_{\mathrm{P}}}$. The generating function is defined as

$$G_{\mathrm{P}}(u) = \sum_{z=0}^{\infty} \mathbf{P}_{\mathrm{P}}(z) \cdot u^{z}, \tag{3}$$

where u is an arbitrary variable. The *excess degree distribution* [18] is the number of edges attached to a vertex other than the edge we arrived along, and given by

$$H_{\mathrm{P}}(u) = \sum_{z=0}^{\infty} Q_{\mathrm{P}}(z) \cdot u^{z} \tag{4}$$

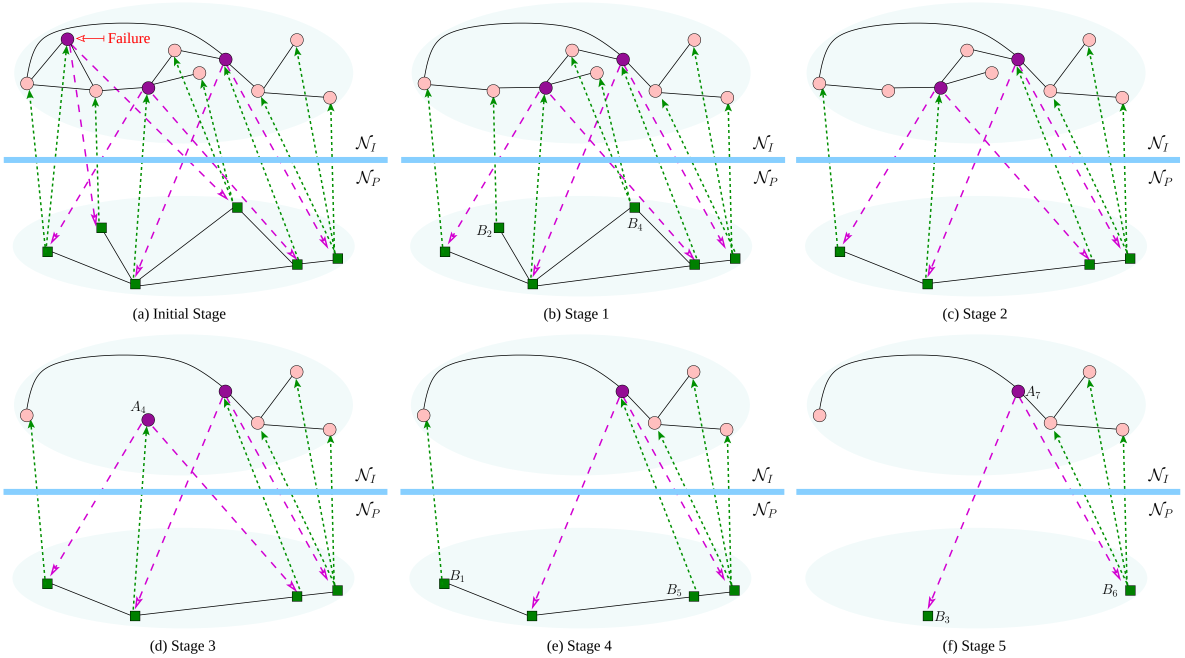
$$Q_{\mathrm{P}}(z) = \frac{(z+1)\cdot \mathbf{P}_{\mathrm{P}}(z+1)}{\bar{z}}, \tag{5}$$

where $\bar{z}$ is the average degree of network $\mathcal{N}_{\mathrm{P}}$. Using Eq. (3), $\bar{z}$ is calculated

$$\bar{z} = \sum_{z=0}^{\infty} z \cdot \mathbf{P}_{\mathrm{P}}(z) = \frac{\partial G_{\mathrm{P}}}{\partial u}|_{u \to 1} = G'_{\mathrm{P}}(1) \tag{6}$$

Then $H_{\mathrm{P}}(u)$ can be written as

$$\begin{aligned} H_{\mathrm{P}}(u) &= \bar{z} \cdot \sum_{z=0}^{\infty} (z+1)\cdot \mathbf{P}_{\mathrm{P}}(z+1) u^{z} \\ &= \bar{z} \cdot \sum_{z=0}^{\infty} z \mathbf{P}_{\mathrm{P}}(z) u^{z-1} \\ &= \bar{z} \frac{\partial G_{\mathrm{P}}}{\partial u} = \frac{G'_{\mathrm{P}}(u)}{G'_{\mathrm{P}}(1)} \end{aligned} \tag{7}$$



(a) Initial Stage

(b) Stage 1

(c) Stage 2

(d) Stage 3

(e) Stage 4

(f) Stage 5

Fig. 2. A sketch of cascading failure in smart grid. Initially, power grid $\mathcal{N}_\text{P}$ has 6 nodes while Internet has 10 nodes. Each node in $\mathcal{N}_\text{P}$ is operated by one operation center, which implies $k = 1$. Each operation center in $\mathcal{N}_\text{I}$ can operate 2 power stations, $n = 2$. Three dark nodes are randomly chosen and assigned as operation centers. The random attack causes the failure of one operation center, thus all its related links are removed. In stage 1, the remaining nodes in $\mathcal{N}_\text{I}$ are mutually reachable, therefore consist of a giant component. B_2 and B_4 lose control, thus in Stage 2 they are out of work. In Stage 3, due to the loss of energy inter links, some nodes in $\mathcal{N}_\text{I}$ are removed. As a result, nodes A_4 is disconnected from the giant component, thus fails. Consequently, B_1, B_5 are faulty since they lose the control inter links from A_4. In Stage 5, the remaining nodes in $\mathcal{N}_\text{P}$ are disconnected, therefore no giant component exists. Due to our Condition 1, the entire $\mathcal{N}_\text{P}$ collapses. As a result, the nodes in $\mathcal{N}_\text{I}$ lost energy support, thus fail.

Once removing a fraction $1 - \phi$ of nodes from network $\mathcal{N}_\text{P}$, the remaining fraction ϕ of the network will have different degree distribution [22], with a new argument $1 - \phi + \phi u$ [10]. According to the results of a single network, the proportion of giant component $F(\phi, \lambda_\text{P})$ of subnetwork ϕ is given by

$$\begin{cases} F(\phi, \lambda_\text{P}) = 1 - G_\text{P}[1 - \phi + \phi \cdot u] \\ u = H_\text{P}[1 - \phi + \phi \cdot u] \end{cases} \tag{8}$$

The functional forms of $G_\text{P}(u)$ and $H_\text{P}(u)$ are complicated, deriving the closed form of Eq. (8) is still a challenge [2], [3], [18]. However, an approximation expression for $F(\phi, \lambda_\text{P})$ was introduced:

Lemma 1 ([8]): For a single scale-free network $\mathcal{N}_\text{P}$, for $2 < \lambda < 3$, with some approximation and simplification, it holds that $F(\phi, \lambda_\text{P}) \propto \epsilon \cdot \phi^{1/(3-\lambda_\text{P})}$, where ϵ is a predefined constant.

We can analogously define $G_\text{I}(u), H_\text{I}(u), F(\phi, \lambda_\text{I})$ for network $\mathcal{N}_\text{I}$ as counterparts to $G_\text{P}(u), H_\text{P}(u), F(\phi, \lambda_\text{P})$ for $\mathcal{N}_\text{P}$.

TABLE 2
Notations for math approximation

P'_i, C'_i	the remaining subnetwork in $\mathcal{N}_\text{P}$ and $\mathcal{N}_\text{I}$ with at least one support inter links in stage i
P_i, C_i	the functioning giant component in P'_i, C'_i
$\widetilde{P'_i}, \widetilde{C'_i}, \widetilde{P_i}, \widetilde{C_i}$	the number of nodes in P'_i, C'_i, P_i, C_i
$\mu'_{p_i}, \mu'_{c_i}, \mu_{p_i}, \mu_{c_i}$	the fractions to P'_i, C'_i, P_i, C_i. i.e., $\widetilde{P'_i} = \mu'_{p_i} \cdot S_\text{P}$

5 Math Approximation for Failure Cascading

We analyze the dynamics of cascading failure using percolation theory in this section. The objective of this study is to quantify the system robustness with different k and n, by means of estimating the functioning giant component size in both $\mathcal{N}_\text{P}$ and $\mathcal{N}_\text{I}$. The notations needed in this section are listed in Table 2.

5.1 Stage 1: Random Removal in $\mathcal{N}_\mathrm{I}$

We begin our estimation with random removal of a fraction $1-\phi$ of nodes in $\mathcal{N}_\mathrm{I}$. The size of remaining network C_1' is $S_\mathrm{I}\cdot\phi$, therefore $\mu'_{c_1}=\phi$. We assume this value is a positive integer if S_I is sufficiently large. According to our Condition 1, only the nodes belonging to the giant component can operate properly, next step is to calculate the size of giant component. The size of giant component C_1 is

$$\widetilde{C_1} = \widetilde{C_1'}\cdot F(\mu'_{c_1},\lambda_\mathrm{I}) = \mu'_{c_1}\cdot S_\mathrm{I}\cdot F(\mu'_{c_1},\lambda_\mathrm{I}) = \mu_{c_1}\cdot S_\mathrm{I}$$
$$\mu_{c_1} = \mu'_{c_1}\cdot F(\mu'_{c_1},\lambda_\mathrm{I}), \qquad (9)$$

where μ_{c_1} implies the fraction of C_1 to $\mathcal{N}_\mathrm{I}$. We notice only the nodes in C_1 are still in work at the end of this stage.

5.2 Stage 2: Fragmentation on $\mathcal{N}_\mathrm{P}$

As the network fragmentation from $\mathcal{N}_\mathrm{I}$ to C_1, a part of inter links are removed. Thus, some nodes in $\mathcal{N}_\mathrm{P}$ would be faulty, because they lost the control inter links. As a result of Stage 1, the fraction $1-\mu_{c_1}$ of nodes are gone. If the network size is large enough, then the fraction $1-\mu_{c_1}$ of operation centers are removed since the initial failures are random. Because each operation center has the same control capability n, the probability for each control link to be removed can be approximated by $1-\mu_{c_1}$. With this respective, a node in $\mathcal{N}_\mathrm{P}$ loses all its k control links (totally out of control) with the probability of $(1-\mu_{c_1})^k$. Denoting P_2' is the subnetwork belong which the nodes retain at least one control link, we have

$$\widetilde{P_2'} = (1-(1-\mu_{c_1})^k)\cdot S_\mathrm{P}$$
$$\mu_{p_2'} = 1-(1-\mu_{c_1})^k \qquad (10)$$

Within P_2', the probability for a node loses $k-i$ of its control links follows the binomial distribution $\mathbf{B}(k,\mu_{c_1})$. The size of giant component in P_2' is

$$\widetilde{P_2} = \widetilde{P_2'}\cdot F(\mu'_{p_2},\lambda_\mathrm{P}) = \mu'_{p_2}\cdot S_\mathrm{P}\cdot F(\mu'_{p_2},\lambda_\mathrm{P}), \qquad (11)$$
$$\mu_{p_2} = \mu'_{p_2}\cdot F(\mu'_{p_2},\lambda_\mathrm{P}). \qquad (12)$$

Each node in P_2 can survive from P_2' with a probability $\widetilde{P_2}/\widetilde{P_2'} = F(\mu'_{p_2},\lambda_\mathrm{P})$. As a result, the expected number of nodes with i control inter links in P_2 is given by

$$\widetilde{P_2}|_i = \binom{k}{i}\mu_{c_1}^i(1-\mu_{c_1})^{k-i}\cdot F(\mu'_{p_2},\lambda_\mathrm{P})\cdot S_\mathrm{P}, i <= k. \qquad (13)$$

As a consequence of this fragmentation, the control inter links which operate the nodes belong to P_2' but not to P_2 become *ineffectiveness* even they are still alive. They will have no impact on the cascading failure in the following stages. Thus, we consider these links as faulty and remove them from the system. From P_2' to P_2, the probability for the control link to be removed is approximate to $1-F(\mu'_{p_2},\lambda_\mathrm{P})$, then an operation center in C_1 has i control links with the probability of

$$\mathbf{P}_\mathrm{o}(i) = \binom{n}{i}F(\mu'_{p_2},\lambda_\mathrm{P})^i\cdot(1-F(\mu'_{p_2},\lambda_\mathrm{P}))^{n-i}, i <= n. \qquad (14)$$

5.3 Stage 3: Recursive Failure to $\mathcal{N}_\mathrm{I}$

The removal of nodes and inter links in Stage 2 affects $\mathcal{N}_\mathrm{I}$. The nodes in network $\mathcal{N}_\mathrm{I}$ may lose energy inter link thus stops operating. We observe the number of energy inter links subnetwork P_2 provides is approximately $\widetilde{P_2}\cdot\sum_{t=0}^{S_\mathrm{I}} P_t\cdot t$, when $\widetilde{P_2}$ is large enough (law of large numbers is satisfied). Initially the total number of energy inter links is S_I since each node in S_I depends on only one power stations. With this respective, the probability for one energy inter link removal is

$$1-\frac{\widetilde{P_2}\cdot\sum_{t=0}^{S_\mathrm{I}} P_t\cdot t}{S_\mathrm{I}} = 1-\mu_{p_2}.$$

The number of nodes in C_1 that has an energy inter link from P_2 is given by

$$\widetilde{C_3'} = \widetilde{C_1}-\widetilde{C_1}\cdot(1-\mu_{p_2}) = \mu_{p_2}\cdot\mu_{c_1}\cdot S_\mathrm{I}.$$

That is, passing from C_1 to C_3', a fraction $1-\mu_{p_2}$ of nodes are broken. As we did in the previous stages, the next step is to calculate the size of giant component of C_3'. As mentioned in [2], it is indeed not an easy task. Instead, we consider the joint effect of the node removal in Stage 1 and Stage 3 are equivalent, i.e., the effect of removing the fraction of $1-\mu_{p_2}$ of nodes in C_1 has the same effect as taking out the same fraction size from C_1' in terms of calculating the giant component size of C_3'. We find that the fragmentation from $\mathcal{N}_\mathrm{I}$ to C_3' can be modeled by removing node of a fraction of

$$1-\phi+\phi\cdot(1-\mu_{p_2}) = 1-\phi\cdot\mu_{p_2}$$

in Stage 1. Thus, the equivalent $\mu'_{c_3}=\phi\cdot\mu_{p_2}$, by which the size of giant component C_3 in subnetwork C_3' is

$$\widetilde{C_3} = \mu'_{c_3}\cdot S_\mathrm{I}\cdot F(\mu'_{c_3},\lambda_\mathrm{I}) = \mu_{c_3}\cdot S_\mathrm{I}. \qquad (15)$$

5.4 Stage 4: Further Fragmentation in $\mathcal{N}_\mathrm{P}$

As network $\mathcal{N}_\mathrm{I}$ splits to C_3 in previous stage, more control inter links are removed and so forth more nodes in $\mathcal{N}_\mathrm{P}$ is going to be faulty. Notice the probability each operation center survives from C_1 to C_3 is $\frac{\mu_{c_3}}{\mu_{c_1}}$. The number of control inter links the network C_1 has is approximated to $\sum_{i=1}^{n} i\cdot\mathbf{P}_\mathrm{o}(i)\cdot\mu_{c_1}\cdot m$. Since each operation center survives with same probability, the number of existing control links in C_3 can be given by $\sum_{i=1}^{n} i\cdot\mathbf{P}_\mathrm{o}(i)\cdot\mu_{c_3}\cdot m$. Thus, the probability of a control inter link to be removed is $1-\frac{\mu_{c_3}}{\mu_{c_1}}$.

Consequently, the probability for a node in P_2 with i control inter links stopping function is $(1 - \frac{\mu_{c_3}}{\mu_{c_1}})^i$. Combining with Eq. (13), the number of nodes that will be removed in P_2 is

$$\begin{aligned} R &= \widetilde{P_2}|_i \cdot (1 - \frac{\mu_{c_3}}{\mu_{c_1}})^i \\ &= \binom{k}{i} \mu_{c_1}^i (1-\mu_{c_1})^{k-i} \cdot F(\mu'_{p_2}, \lambda_\mathrm{P}) \cdot S_\mathrm{P} \cdot (1 - \frac{\mu_{c_3}}{\mu_{c_1}})^i \\ &= S_\mathrm{P} \cdot F(\mu'_{p_2}, \lambda_\mathrm{P}) \cdot \binom{k}{i} \cdot (1-\mu_{c_1})^{k-i} \cdot (\mu_{c_1} - \mu_{c_3})^i \\ &= S_\mathrm{P} \cdot F(\mu'_{p_2}, \lambda_\mathrm{P}) \cdot ((1-\mu_{c_3})^k - (1-\mu_{c_1})^k) \end{aligned} \tag{16}$$

So, the size of P'_4 is

$$\begin{aligned} \widetilde{P'_4} &= \widetilde{P_2} - R \\ &= S_\mathrm{P} \cdot F(\mu'_{p_2}, \lambda_\mathrm{P}) \cdot (1 - (1-\mu_{c_3})^k) \end{aligned} \tag{17}$$

Passing from P_2 to P'_4, the fraction $1 - \widetilde{P'_4}/\widetilde{P_2} = 1 - (1 - (1-\mu_{c_3})^k/\mu'_{p_2}$ of nodes are removed. As we do in Stage 3, in terms of the size of giant component in P'_4, that is equivalent to remove the same fraction of nodes from P'_2. The proportion of nodes that has to be removed from S_P to P'_4 is

$$1 - \mu'_{p_2} + \mu'_{p_2} \cdot (1 - \frac{1-(1-\mu_{c_3})^k}{\mu'_{p_2}}) = (1-\mu_{c_3})^k$$

Thus, the equivalent $\mu'_{p_4} = 1 - (1-\mu_{c_3})^k$. The corresponding fraction of giant component $\mu_{p_4} = \mu'_{p_4} \cdot F(\mu'_{p_4}, \lambda_\mathrm{P})$.

5.5 Transcendental Equations for Failure Cascading

Following the previous steps, we can obtain the size of giant component $\widetilde{C_1}, \widetilde{P_2}, \widetilde{C_3} \cdots$ in a certain stage, but no one knows in which stage the cascading failure stops. Our main aim is to estimate the size of functioning parts in the final stage. When repeating the above calculations, we can observe the pattern of equations:

$$\begin{gathered} \mu'_{c_1} = \phi, \;\; \mu_{c_1} = \mu'_{c_1} \cdot F(\mu'_{c_1}, \lambda_\mathrm{I}) \\ \mu'_{c_3} = \phi \cdot \mu_{p_2}, \;\; \mu_{c_3} = \mu'_{c_3} \cdot F(\mu'_{c_3}, \lambda_\mathrm{I}) \\ \cdots, \;\; \cdots \\ \mu'_{c_{2j+1}} = \phi \cdot \mu_{p_{2j}}, \;\; \mu_{c_{2j+1}} = \mu'_{c_{2j+1}} \cdot F(\mu'_{c_{2j+1}}, \lambda_\mathrm{I}) \end{gathered}$$

and

$$\begin{gathered} \mu'_{p_2} = 1 - (1-\mu_{c_1})^k, \;\; \mu_{p_2} = \mu'_{p_2} \cdot F(\mu'_{p_2}, \lambda_\mathrm{P}) \\ \mu'_{p_4} = 1 - (1-\mu_{c_3})^k, \;\; \mu_{p_4} = \mu'_{p_4} \cdot F(\mu'_{p_4}, \lambda_\mathrm{P}) \\ \cdots, \;\; \cdots \\ \mu'_{p_{2j}} = 1 - (1-\mu_{c_{2j-1}})^k, \;\; \mu_{p_{2j}} = \mu'_{p_{2j}} \cdot F(\mu'_{p_{2j}}, \lambda_\mathrm{P}) \end{gathered}$$

To determine the state of the system in the end of cascading failure, we look at $j \to \infty$. The networks stop fragmenting and the functioning giant components are fixed. Thus, the following equations hold

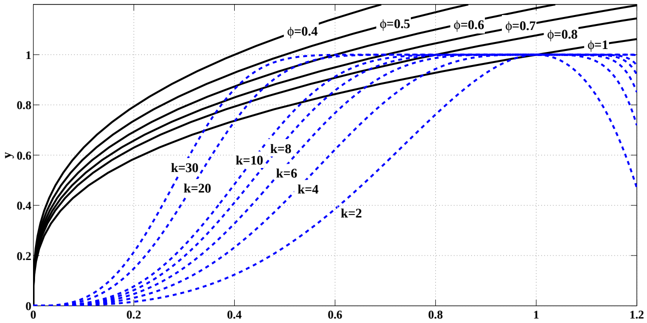


Fig. 3. Solutions for Eq. (20) for $\lambda_\mathrm{P} = \lambda_\mathrm{I} = 2.5$, $\epsilon_1 = \epsilon_2 = 1$. The solutions are the corner points of two lines. It is clearly shown for some cases there is no intersection ($\phi = 0.8, k = 4$). For some cases one intersection exists ($\phi = 0.6, k = 20$). For the others, two non-trivial solution exist.

$$\begin{gathered} \mu'_{c_{2j+1}} = \mu'_{c_{2j+3}} = \mu'_{c_{2j-1}} \\ \mu'_{p_{2j}} = \mu'_{p_{2j+2}} = \mu'_{p_{2j-2}} \end{gathered}$$

Let $x = \mu'_{c_{2j+1}} = \mu'_{c_{2j+3}} = \mu'_{c_{2j-1}}$ and $y = \mu'_{p_{2j}} = \mu'_{p_{2j+2}} = \mu'_{p_{2j-2}}$, then we obtain a set of transcendental equations

$$\begin{cases} x = \phi \cdot y \cdot F(y, \lambda_\mathrm{P}) \\ y = 1 - (1 - x \cdot F(x, \lambda_\mathrm{I}))^k \end{cases} \tag{18}$$

where $F(\cdot, \lambda_\mathrm{P}), F(\cdot, \lambda_\mathrm{I})$ are according to Eq. (8).

The fraction of nodes that still function in the final steady state in both networks can be calculated by

$$\begin{cases} \lim_{j\to\infty} \mu_{p_j} = \mu_{p_\infty} = y \cdot F(y, \lambda_\mathrm{P}) \\ \lim_{j\to\infty} \mu_{c_j} = \mu_{c_\infty} = x \cdot F(x, \lambda_\mathrm{I}) \end{cases} \tag{19}$$

This analysis can be applied to any type of networks. This gives us a complete solution for the fraction of survivals in $\mathcal{N}_\mathrm{P}$ and $\mathcal{N}_\mathrm{I}$. If we can find a non-trivial solution for x and y, then we can compute the remaining number of survivals.

5.6 Graphic Solution

According to Lemma (1), let $F(y, \lambda_\mathrm{P}) = \epsilon_1 \cdot y^{1/(3-\lambda_\mathrm{P})}$ and $F(x, \lambda_\mathrm{I}) = \epsilon_2 \cdot x^{1/(3-\lambda_\mathrm{I})}$, where ϵ_1 and ϵ_2 are predefined constants. Eq. (18) comes to

$$\begin{cases} x = \phi \cdot y \cdot \epsilon_1 \cdot y^{1/(3-\lambda_\mathrm{P})} \\ y = 1 - (1 - x \cdot \epsilon_2 \cdot x^{1/(3-\lambda_\mathrm{I})})^k \end{cases} \tag{20}$$

In general, it is difficult to derive an expression for x, y depending on k, ϕ. Instead, we can solve Eq. (20) with graphic method [2] for a given set of $\lambda_\mathrm{P}, \lambda_\mathrm{I}, \epsilon_1, \epsilon_2$.

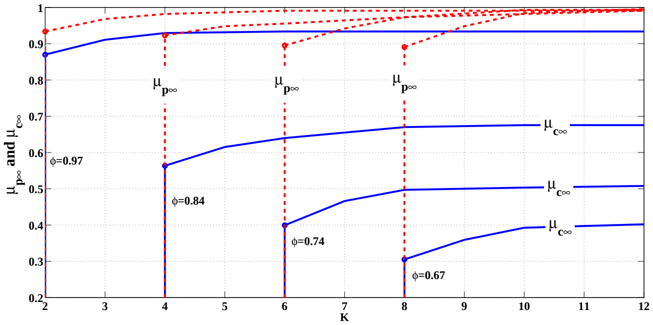


Fig. 4. A solution for μ_{p_∞} and μ_{c_∞}, given $\lambda_{\rm P} = \lambda_{\rm I} = 2.2$, $\epsilon_1 = \epsilon_2 = 1$. For $k = 2, 4, 6, 8$, the threshold $\phi_c = 0.97, 0.84, 0.74, 0.67$ respectively. The first-order discontinues transition occurs at each ϕ_c.

We draw two function curves of Eq. (20) and the intersections are the solutions of x, y. Fig. 3 and Fig. 4 give complete graphic solutions, based on which we obtain some insightful findings as following:

- A critical threshold ϕ_c exists, beyond which the system collapses. For the case of $k = 20$, we find there is no intersection if $\phi < 0.6$, i.e., no solution exists. While for $\phi > 0.6$, the two curves have two intersection points. So ϕ_c is approximate to 0.6 for the case of $k = 20$. For $\phi < \phi_c$, both networks go into complete fragmentation in the end. If $\phi > \phi_c$, the two non-trivial intersections are corresponding to two sets of giant component sizes. In this case, the solution is the point that is closer to the initial status, because the system fragmentation stops at this point and never goes to the small one.
- The ϕ_c varies for different values of k. For instance, it is about 0.73 for $k = 10$ and 0.83 for $k = 6$ ($\lambda_{\rm P} = \lambda_{\rm I} = 2.5$). We find ϕ_c becomes lower for a higher k, which matches with the intuition that the smart power grid is more reliable if each power station has more control inter links.
- The survival ratios of both networks experience *first-order transition* at ϕ_c. Fig. (4) gives an example solution for μ_{p_∞} and μ_{c_∞}. For the case of $k = 4$, ϕ_c equals 0.84, there is no giant component existing for $k < 4$. While for $k = 4$, both μ_{p_∞} and μ_{c_∞} have a step function.
- The improvements of μ_{p_∞} and μ_{c_∞} are sublinear with the increasing of k, and reach upper bounds. Note that for all the cases in Fig. (4), μ_{p_∞} approaches to 1. This gives us a meaningful guide that adding control inter links improves system robustness significantly when k is small. While when k is sufficiently large, increasing k does not affect the robustness except ϕ_c.

However, finding the non-trivial solution for scale-free network is challenging since the exactly value of ϵ is still unknown, [2], [8], [9], [18]. To the best of our knowledge, deriving the closed-form solution of Eq. (8) is still open. Therefore, in this work, we resort to the standard graphical method for simulations.

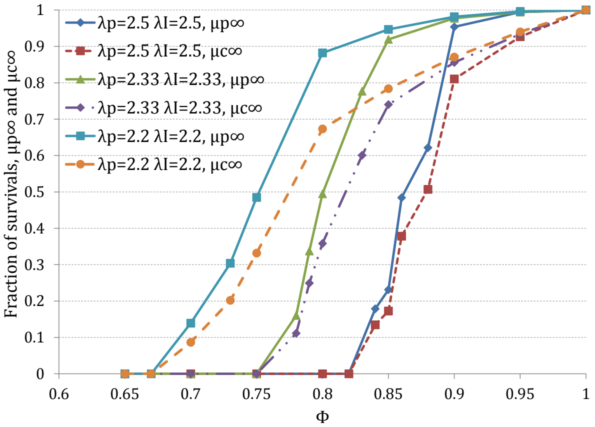


Fig. 5. The fraction of survivals in both networks with different $\lambda_{\rm P}$ and $\lambda_{\rm I}$. The initial networks size $S_{\rm P} = 1000, S_{\rm I} = 10000$, k=2, n=5. The generalized Barabási-Albert model is used to construct the two scale-free networks. The initial random failure $1 - \phi$ is occurs in network $\mathcal{N}_{\rm I}$.

6 Experimental Validation

In this section, we generate an interdependent network and simulate cascading failure to obtain the fractions of functioning parts (survival ratio) μ_{p_∞} and μ_{c_∞}. To generate the scale-free network with different power-law distributions, we adopt the *generalized Barabási-Albert model* [18], whose power law exponent can vary in the range $(2, +\infty)$. In all the experiments the same approach is employed: first, we construct two scale-free networks representing $\mathcal{N}_{\rm P}$ and $\mathcal{N}_{\rm I}$; then we remove the fraction of $1 - \phi$ nodes in $\mathcal{N}_{\rm I}$ as random failure.

6.1 ϕ_c and System Robustness

We firstly discuss the values of μ_{p_∞} and μ_{c_∞} with different exponents of $\lambda_{\rm P}$ and $\lambda_{\rm I}$.

Fig. 5 clearly shows with the decreasing of $\lambda_{\rm P}$ and $\lambda_{\rm I}$, which means that the more nodes with high degree, the better robustness of entire system. Only 50% of nodes survives for $\lambda_{\rm P} = \lambda_{\rm I} = 2.33$ when $\phi = 0.5$, but it is approximate 0.9 for $\lambda_{\rm P} = \lambda_{\rm I} = 2.2$. ϕ_c is also highly influenced by λ. It is 0.67 for $\lambda_{\rm P} = \lambda_{\rm I} = 2.2$, while this increases to 0.82 for $\lambda_{\rm P} = \lambda_{\rm I} = 2.5$.

We notice when the initial failure or attack upon Internet is small, i.e., less than 5%, the entire power grid is extremely reliable for all three systems. The curves of μ_{p_∞} remain stable on the right of corner points (0.8 for $\lambda_{\rm P} = \lambda_{\rm I} = 2.2$), and drop rapidly on the left. One more observation is that μ_{p_∞} and μ_{c_∞} are either zero or nonzero simultaneously which indicates that the power grid and Internet are either totally broken or not.

6.2 Cost and Robustness

Our main aim is to find the relation between system cost and system robustness. Fig. 6(a) and 6(b) give detailed curves on various values of k.

It is shown that as the increasing of k, μ_{p_∞} and μ_{c_∞} increase. This implies a practical meaning that if we let more operation centers control each power station, the system would has a much higher robustness. In the case of $k = 1$, the system could not bear even 2% failure, the threshold $\phi_c = 0.98$. If we add one more control link to each node, i.e., $k = 2$, the system robustness experiences a huge improvement. Not only the ϕ_c dramatically decreases to 0.67, but also the system can tolerate small scale of failure: there is no impact to power grid even 10% of communication nodes are initially faulty.

In the case of $k = 15$, the power grid remains totally function, even if 60% of communication network is destroyed. The ϕ_c equals 0.2, approximate five times promotion compared to 0.98 for the case $k = 1$. Noticing in Fig. 6(b), the decrease of μ_{c_∞} is quite flat for $k = 15$. The loss of Internet is almost all due to the initial failure.

The important finding according to Fig. 6(a) and 6(b) is that the relation between robustness and cost is sublinear. The improvement between $k = 2$ and $k = 1$ is significant, while the gap between $k = 15$ and $k = 10$ is tiny. Hence, for building a smart power grid, adding as many as possible control link is not our choice since the massive extra cost does not improve system reliability remarkably.

The proposed *first-order discontinuous transition* [2] in interdependent networks says the size of giant component meets a sharp transition when ϕ is approaching to ϕ_c. To be specific, if the network size is infinite, the transition becomes a *step function*. Since the real networks are all non-infinite, this transition could never be first-order. Normally, there is a small transition interval including the value of ϕ_c. Fig. 7 shows how our model transits around ϕ_c for different k.

In case of $k = 5$, the giant components always exist in both μ_{p_∞} and μ_{c_∞} for $\phi > 0.42$, while the system collapses when $\phi < 0.36$. Thus, the transition interval is [0.36, 0.42], during which the system might either collapses or not. Note that for larger k, the transition interval is smaller, i.e., the transition is more sharp. Our finding validates the conclusion proposed by [15], that is, when the coupling between the networks is reduced, at a critical coupling strength the transition becomes a second-order continuous phase transition.

A sharp transition is preferred for the realistic smart grid, since the smaller transition interval makes the system easy to be predicted and controlled.

6.3 Various Allocation Strategies with System Robustness

We now discuss the impact of different operation center capability n. In this simulation series, the value of k is set to 2. We change the value of n to explore the different system robustness. Fig. 8(a) and Fig. 8(b) reveal the relations between robustness and n.

Generally, the system performance improves with increasing n. As shown in Fig. 8(a), in the case of $n = 2$, μ_{p_∞} is equal to 0.95 when the initial failure is $1-\phi = 0.15$. While it almost equals 1 for the case of $n = 200$ under the same situation. We observe promoting n decreases the threshold value ϕ_c in all cases.

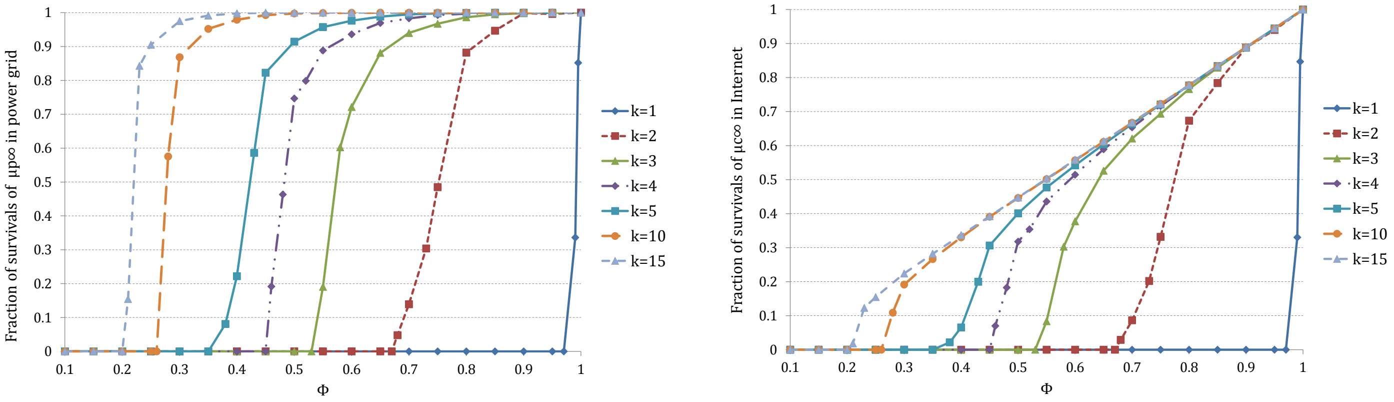
We notice for all the cases of n, on the right side of the corner point $\phi = 0.8$, both μ_{p_∞} and μ_{c_∞} approach to 1 steadily. While on the left side, the curves drop to zero more rapidly. Note that for higher n, the slope is smaller. Comparing Fig. 6(a) and Fig 8(a), it is clearly shown that the corner point position is determined by k rather than n. A distinct k completely has a different corner point, while there is only a sightly change for different n with a specific k.

Now we consider the transition intervals. Fig. 9 gives the detailed curves for different values of n. When n is equal to 2, the interval is [0.71, 0.77]. It extends dramatically for the case of $n = 200$, with the approximate value between [0.37, 0.77]. Hence, increasing n extends the transition internal, i.e., the transition is much more flat.

6.4 Validation of Theoretical Analysis

Our extensive simulations validate the mathematical analysis in Section 5.6. Some conclusions are listed as follows:

- The system robustness against random failure can be improved by increasing controlling cost, i.e., adding more control links for each target (power station). The robustness improvement is nonlinear with cost promotion, which has been demonstrated by our figures. Both mathematical and experimental results show the power grid is intact against random failure when k is large enough.
- The critical threshold ϕ_c is inverse proportional to the value of k. The transition at ϕ_c is first-order in mathematical analysis, while it is second-order in simulation. The reason is that the real world network is non-infinite. Meanwhile, increasing controlling cost k shortens the transition interval in real smart grid, and makes system easier to be predicted and controlled.
- The monitoring capability n of each operation center has no impact on system robustness according to the transcendental Eq. (18). While our simulations give a little



(a) μ_{p_∞} varies with different value of k

(b) μ_{c_∞} varies with different value of k

Fig. 6. System Robustness vs. k. The initial networks size $S_{\mathrm{P}} = 1000, S_{\mathrm{I}} = 10000$, $\lambda_{\mathrm{P}} = \lambda_{\mathrm{I}} = 2.2$, $n = 5$.

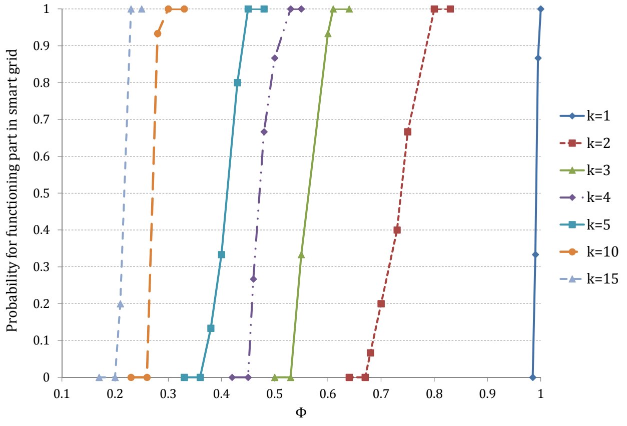


Fig. 7. The different probabilities varies with k for the entire system to have a functioning part after cascading failure stops. $\lambda_{\mathrm{P}} = \lambda_{\mathrm{I}} = 2.2$, $n = 5$. For the case of $k = 3$, the entire smart grid system collapses if $\phi < 0.53$; for $\phi > 0.6$, giant components always exist in both μ_{p_∞} and μ_{c_∞}. During the interval, there is a probability for giant component existing.

bit different story. The reason is that the network size for simulation is finite, while our math calculation is based on the assumption that the number of nodes is large enough so that *Law of Large Numbers* is satisfied. The experimental results are meaningful because the real world network size is always non-infinite.

• Based on our analysis, we would conclude that it is important to find a trade-off between expenditure and performance for building smart grid infrastructures. While if the controlling cost is fixed and we still want to promote the system robustness. Then one possible way is: increasing monitoring capability n. Consequently, the total number of operation center required decreases. By this way, the reliability experiences a slight improvement. But the disadvantage of this method is obvious: the transition interval is extended so that the entire system becomes unpredictable.

7 Conclusions

We study the system robustness of smart grid against cascading failure between its power grid and communication network. Using percolation theory, we calculate the size of functioning giant component after the cascading failure stops. Our work indicates that in smart grid, a threshold exists for the proportion of faulty nodes, beyond which the system collapses. Meanwhile, our mathematical analysis gives a relation between system robustness and controlling cost. By extensive simulations, we validate our mathematical analysis and obtain the accurate results. It is suggested that increasing monitoring cost indeed improves robustness, but trade-offs between expenditure and performance should be discussed. This work is helpful to build a reliable smart grid infrastructure, with considering the cost. In the future work, we will investigate the issues on decreasing the impact of cascading failure.

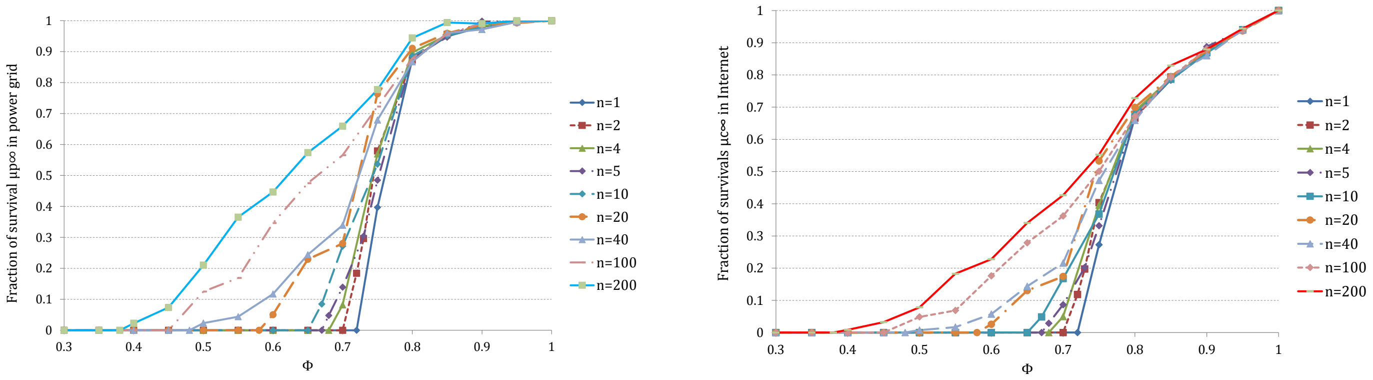
References

[1] Avaliable at : http://spectrum.ieee.org/energywise/energy/the-smarter-grid/disappointing-monsoon-season-wreaks-havoc-with-indias-grid/?utm_source=energywise&utm_medium=email&utm_campaign=080112.

[2] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464:1025–1028, 2010.

[3] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E*, 83:016112, Jan 2011.

[4] D. P. Chassin and C. Posse. Evaluating north american electric grid reliability using the barabási–albert network model. *Physica A: Statistical Mechanics and its Applications*, 355(2-4):667–677, September 2005.



(a) μ_{p_∞} varies with different value of n

(b) μ_{c_∞} varies with different value of n

Fig. 8. System Robustness vs. n. The initial networks size $S_{\mathrm{P}} = 1000$, $S_{\mathrm{I}} = 10000$, $\lambda_{\mathrm{P}} = \lambda_{\mathrm{I}} = 2.2$, $k = 2$.

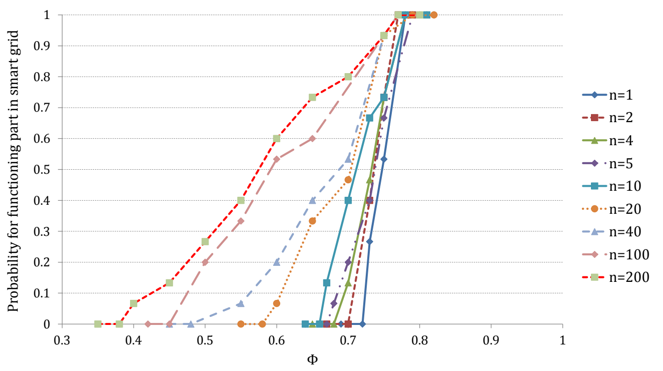


Fig. 9. Transition intervals for various allocation strategies. $S_{\mathrm{P}} = 1000$, $S_{\mathrm{I}} = 10000$, $\lambda_{\mathrm{P}} = \lambda_{\mathrm{I}} = 2.2$, $k = 2$.

[5] X. Chen, H. Dinh, and B. Wang. Cascading failures in smart grid - benefits of distributed generation. In *IEEE SmartGridComm 2010*.

[6] M. Chertkov, F. Pan, and M. G. Stepanov. Predicting failures in power grids: The case of static overloads. *IEEE Trans. Smart Grid*, 2(1):162–172, 2011.

[7] P. Derler, E.A. Lee, and A.Sangiovanni-Vincentelli. Modeling cyber-physical systems. *Proceedings of the IEEE (special issue on CPS)*, 100(1):13–28, 2012.

[8] S. N. Dorogovtsev and J. F. F. Mendes. *Evolution of Networks: From Biological Nets to the Internet and WWW*. Oxford University Press, 2003.

[9] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. Robustness of a network of networks. *Phys. Rev. Lett.*, 107, 2011.

[10] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin. Networks formed from interdependent networks. *Nature Physics*, 8:40–48, 2012.

[11] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. Robustness of interdependent networks under targeted attack. *Physical Review E - Statistical, Nonlinear and Soft Matter Physics*, 83, 2011.

[12] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak. Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In *The 8th IEEE Conference on Industrial Electronics and Applications*, 2013.

[13] S. Kadloor and N. Santhi. Understanding cascading failures in power grids. *CoRR*, abs/1011.4098, 2010.

[14] R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the north american power grid. *Eur. Phys. J. B*, 46:101–107, 2005.

[15] E. A. Leicht and R. M. D'Souza. Percolation on interacting networks. arxiv.org/abs/0907.0894, 2009.

[16] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. *IEEE Transactions on Smart Grid*, 1:57–64, June 2010.

[17] Y. Nan, L. Wenying, and G. Wei. Study on scale-free characteristic on propagation of cascading failures in power grid. *IEEE Energytech*, pages 1–5, 2011.

[18] M. E. J. Newman. *Networks: An Introduction*. Oxford University Press, 2010.

[19] S. Pahwa, A. Hodges, C. M. Scoglio, and S. Wood. Topological analysis of the power grid and mitigation strategies against cascading failures. *4th IEEE Systems Conference*, 2010.

[20] R. Parshani, V. Buldyrev, and S. Havlin. The critical effect of dependency groups on the function of networks. *Proc. National Academy of Sciences*, 108, 2011.

[21] R. Pfitzner, K. S. Turitsyn, and M. Chertkov. Controlled tripping of overheated lines mitigates power outages. *CoRR*, abs/1104.4558, 2011.

[22] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. Cascade of failures in coupled network systems with multiple support-dependent relations. *Phys. Rev. E*, Mar 2011.

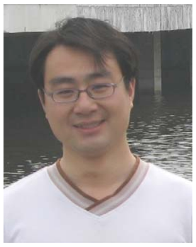
[23] Z. Wang, A. Scaglione, and R.J. Thomas. Generating statistically correct random topologies for testing smart grid communication and control networks. *IEEE Trans. Smart Grid*, 1(1):28–39, 2010.

[24] O. Yagan, D. Qian, J. Zhang, and D. Cochran. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures and robustness. *IEEE Trans. Parallel Distrib. Syst.*, 23(9):1708–1720, 2012.

[25] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid*, 2(2):382–390, 2011.

[26] C. Zimmer and F. Mueller. Fault tolerant network routing through software overlays for intelligent power grids. In *ICPADS*, pages 542–549. IEEE, 2010.

Zhen Huang is currently a Ph.D candidate in Electrical and Computer Engineering at University of Ottawa. He received his Master's degree in Electrical and Computer Engineering from University of Ottawa in 2011, and B.E. degree in Communications Engineering from Southwest University of Science and Technology in 2010, China. His research interests include complex networks, wireless sensor network, cyber-physical system and vehicular ad hoc networks.



Cheng Wang received his PhD degree in Department of Computer Science at Tongji University in 2011. Currently, he is a post doctoral fellow in School of Electrical Engineering and Computer Science at University of Ottawa. His research interests include smart grid, wireless networking, mobile social networks, and mobile cloud computing.

Milos Stojmenovic received the Bachelor of Computer Science degree at the School of Information Technology and Engineering, University of Ottawa, in 2003. He obtained his Masters degree in computer science at Carleton University in Ottawa, Canada in 2005, and completed his PhD in the same field at the University of Ottawa, Canada in 2008. Currently he is an Assistant Professor at the Singidunum University, Serbia. He was a visiting researcher at Japans National Institute of Advanced Industrial Science and Technology in 2009. He published over thirty articles in the fields of computer vision, image processing, and wireless networks. His work implements machine learning techniques such as AdaBoost and SVM classification which in turn use Higher order Autocorrelation features (HLAC) to perform Image segmentation and classification.

Amiya Nayak received his B.Math. degree in Computer Science and Combinatorics and Optimization from University of Waterloo in 1981, and Ph.D. in Systems and Computer Engineering from Carleton University in 1991. He has over 17 years of industrial experience in software engineering, avionics and navigation systems, simulation and system level performance analysis. He is in the Editorial Board of several journals, including IEEE Transactions on Parallel and Distributed Systems, International Journal of Parallel, Emergent and Distributed Systems, International Journal of Computers and Applications, and EURASIP Journal of Wireless Communications and Networking. Currently, he is a Full Professor at the School of Electrical Engineering and Computer Science at the University of Ottawa. His research interests are in the area of fault tolerance, distributed systems/algorithms, and mobile ad hoc networks.