Reliability analysis in interdependent smart grid systems

Hao Peng, Zhe Kan, Dandan Zhao, Jianmin Han, Jianfeng Lu, Zhaolong Hu

PII: S0378-4371(18)30104-3
DOI: https://doi.org/10.1016/j.physa.2018.02.028
Reference: PHYSA 19148

To appear in: *Physica A*

Received date : 16 November 2017
Revised date : 22 January 2018

*Highlights (for review)

Highlights:

1. Based on complex network theory, we study the reliability in interdependent smart grid systems.
2. We focus on understanding the structure of smart grid systems and studying the underlying network model, their interactions, and relationships.
3. We show that how cascading failures occur in the interdependent smart grid systems.
4. Based on percolation theory, we also study the effect of cascading failures effect and reveal detailed mathematical analysis of failure propagation in such systems.
5. We analyze the reliability of our proposed model caused by random attacks or failures by calculating the size of giant functioning components in both networks.

Reliability Analysis in Interdependent Smart Grid Systems

Hao Peng[a], Zhe Kan[a], Dandan Zhao[a,1], Jianmin Han[a], Jianfeng Lu[a], Zhaolong Hu[a]

[a] *Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, China*

Abstract: Complex network theory is a useful way to study many real complex systems. In this paper, a reliability analysis model based on complex network theory is introduced in interdependent smart grid systems. In this paper, we focus on understanding the structure of smart grid systems and studying the underlying network model, their interactions, and relationships and how cascading failures occur in the interdependent smart grid systems. We propose a practical model for interdependent smart grid systems using complex theory. Besides, based on percolation theory, we also study the effect of cascading failures effect and reveal detailed mathematical analysis of failure propagation in such systems. We analyze the reliability of our proposed model caused by random attacks or failures by calculating the size of giant functioning components in interdependent smart grid systems. Our simulation results also show that there exists a threshold for the proportion of faulty nodes, beyond which the smart gird systems collapse. Also we determine the critical values for different system parameters. In this way, the reliability analysis model based on complex network theory can be effectively utilized for anti-attack and protection purposes in interdependent smart grid systems.

***Keywords*:** Complex network; Smart gird systems; Percolation theory; Cascading failures;

1. Introduction

In recent years, the application of smart grid system [1] ~ [5] in our lives is becoming more and more extensive. To a certain extent, the smart grid system has changed our way of life. Generally, the smart grid systems depend on two main networks: grid network (conventional power grid) and communication network (providing control function and communication function). In the work-in-progress, smart grid systems need power generation[6] using different kinds of energy sources e.g., fossil-fuels, solar, wind, geothermal, transmission of energy from source to destination, intelligent distribution by monitoring the demand of power in different regions, monitoring the power usage by customers using smart meters, and integrating other facilities e.g., plugged-in-electrical vehicles[7]. In this way, the smart grid systems change significantly and improve the energy usage efficiency in the last few years.

In smart grid systems [3] ~ [5], communication network needs grid network to support power energy, while power stations are controlled by communication network. Thus, the two networks are connected and mutually interdependent. Then smart grid systems can be regarded as interdependent systems [8]~[9]. However, for interdependent system architecture, the failures in one network can lead to the cascading risk in another. For example, the breakdown of a power station network [10] could lead the corresponding cascading failure of some nodes in communication network, while in reverse faults in communication network might cause failures of the power station

[1] Corresponding author. E-mail address: ddzhao@zjnu.edu.cn (D.D. Zhao).

network. Especially, the cascading failures may even occur recursively between the two interdependent grid network and communication network. We call it cascade of failures. Cascading failures are big issues in such coupled networks. Understanding the underlying cascading failures patterns to protect interdependent smart grid systems is quite necessary.

In order to improve the reliability of the smart grid systems, it is necessary to explore the cascading failures in interdependent smart gird systems. Recently many researchers have paid more attentions in this research field. Currents research [11]~[14] in smart gird systems mainly focuses on failures about load balancing and load distribution. Most of these techniques rely on methods commonly used in distributed systems. An architecture for distributed generation way, which can help prevent cascading failures, is described in Ref.[15]. However, fault analysis and the impact of communication network on power grid were not mentioned. Optimization mechanisms have been used to balance demand and supply in Ref.[16]. Besides, the researcher has deeply investigated load distribution attack to provide effective prevention on false data injection [17]. Fault location method in smart grid has been investigated in Ref.[18]. Obviously, existing work on modelling smart gird systems is mainly about extracting properties from physical systems and assumed associated cyber system and matching with some physical network families. For example, Hartmann et al. [18] proposed an mechanism that generates random topology power grids featuring the same topology and electrical characteristics generated from the real world. Toft and Maasoumy et al. [19]~[20] focused on the challenges of modeling smart grid systems that arise from the intrinsic heterogeneity and sensitivity to timing. Specific technologies applied in some smart grid systems include hybrid system modeling and heterogeneous models of computation, the use of domain-specific ontologies to strengthen modularity, and the joint modeling of functionality and implementation architectures [21]. From discussed above, we can see that most of the previous research works don’t clearly present a mathematical analytical framework to not only analyze propagation process of cascading failures, but also present better model which is more fault tolerant.

In this paper, the aims are to reveal the reliability influence of the smart grid systems under random attack strategy. The results can provide guidance for safety design and protection of smart grid systems. It is difficult to establish a theoretical analysis model for the above research. Therefore, a numerical analysis based interdependent networks model is used to dynamically simulate the cascading failure process, where reasonable explanation of results is also presented. The outline of the paper is as follows: we discuss how we construct a theory model of interdependent smart grid systems in Section 2. In Section 3, we analyze the cascading failures process and define the problems we try to study. Section 4 indicates the extensive simulation results and more analysis points. Conclusions are summarized in Section 5.

2. Model descriptions

In this section, we mainly focus on modeling the interdependent smart grid systems. And we will describe more details about the types of the two interdependent networks and the relationship between them. Meanwhile, we will introduce the process of cascading failures by analyzing a simple network model.

2.1 Notations

For simplicity, we use network A, B stands for the power grid network and communication network respectively. The number of power grid network and communication network are assumed to haveN_A and N_B respectively. In **Table 1** we list some key notations in theoretical analysis.

Table 1: Key Notations in Theoretical Analysis

N_A, N_B	The number of nodes in communication and power grid network
N'_{Ai}, N'_{Bj}	The number of nodes in communication and power grid network which have supporting interlink at stage ***i*** and ***j***.
μ'_i, μ'_j	The fraction of nodes that have supporting interlink at stage ***i*** and ***j***.
N_{Ai}, N_{Bj}	The number of nodes in communication and power grid network which belong to the giant component at stage ***i*** and ***j***.
μ_i, μ_j	The fraction of nodes that belong to the giant components
$\langle k \rangle_A$, $\langle k \rangle_B$	The average degree of network A and network B.

2.2 Model Construction

We consider the smart grid system consisting of two interdependent networks [22]~[24], i.e., the power grid and communication networks. In the actual scene, we can see that the number of nodes in the communication network is much larger than the number of nodes in the power network. So the number of nodes in the communication network is different with the number of nodes in the power network. Simply put, we assume that the number of nodes in the two networks is proportional in our model. In this paper, we stipulate that N_A/N_B are equal to 1:3. It means that one node in the power grid network supports three nodes in the communication network. And the degree distribution of the nodes in these two networks follows the passion distribution.

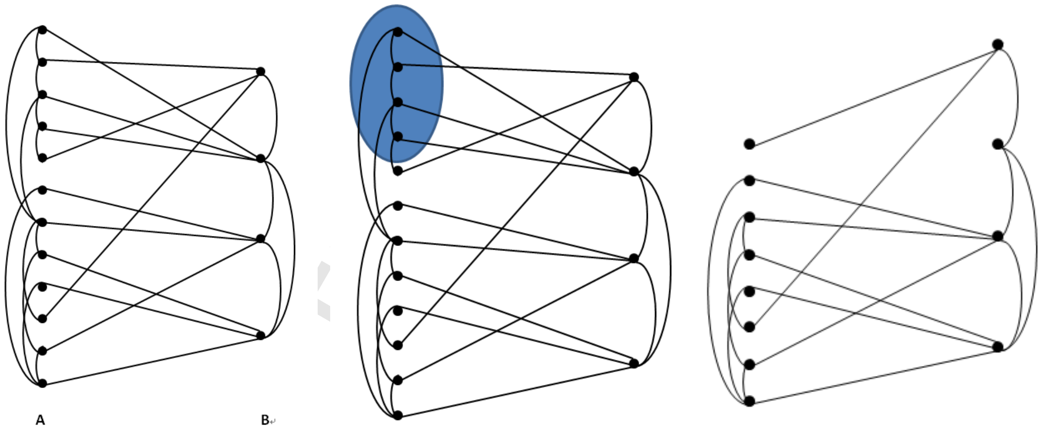
We refer to the connection of nodes in a single network as intra links. Without loss of generality, we consider the two interdependent networks as ER networks. Besides, we refer to the connection of nodes in two networks as inter links. The intra links and inter links are undirected. In the smart grid systems, the attack never directly happens on the power grid network; these attacks are generally attack the communications network. So we assume that attacks occur in the communication network initially. When the communication network is attacked, we assume that a node can maintain the function only if the following two conditions are satisfied [3], [4]:

1) The node has at least one inter link with a node that functions.

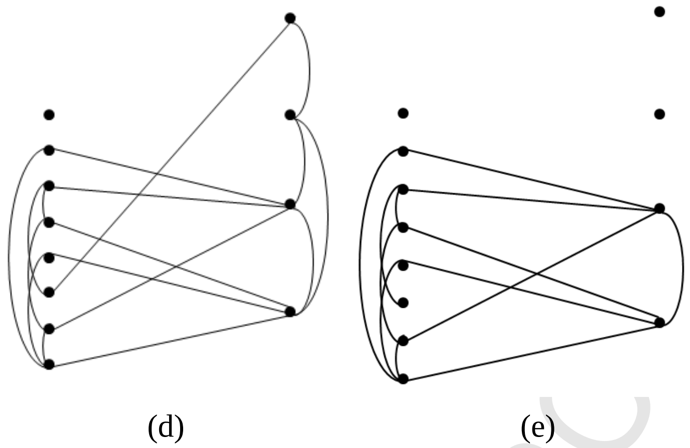
2) The node belongs to the giant component of its own network.

At the beginning we remove $(1-\mathrm{p})\,N_A$ of nodes in N_A. Due to the failure of these nodes, the intra links and inter links of these nodes are also removed. Owing to the dependence of the two networks, in the next step, some nodes fails in N_B because of lose their inter links. As the cascading failure, the power grid network also becomes fragment, according to the condition 2). In the remaining nodes there will be some nodes fail again. The failure of these nodes will lead to the further failure of nodes in the communication network. In the case, this failure will continue recursively between the two interdependent networks. Finally, this process will reach two stable states that one is that nodes in both networks are completely failure, other one is that the giant component is mutually inter connected without further cascading failures.

In order to understand the cascading failure process, we establish a simple model to simulate the failure process, as shown in Figure 1.



(a) (b) (c)



(d) (e)

Figure 1: A simple case of cascading failure process. (**a)** Each node in network A depends on one node in network B. But each node in network B depends on three nodes in network A. The intra links are shown by arcs. The inter links are shown by straight lines. (**b)** The nodes in the shadow are attacked. (**c)** The nodes that are attacked and the edges connected to these nodes are all removed. (**d)** The nodes that are not in the giant component are removed, and meanwhile remove the edges connected to these nodes. (**e)** The second node in network B is removed because the nodes that have not dependent nodes in network A. then repeat the process of (**c)** and (**d)**. Finally the system reaches a steady state that no further links and nodes are removed.

3. Theoretical analysis

Next, we give a mathematical analysis of the cascading failure process in the model of interdependent smart grid system. In order to analyze this process, we will make use of generating function and percolation theory [5]~[7]. Here, we define the generating function of the degree distributions in network A as,

$$G_{A0}(z) = \sum_k P_A(k) z^k \quad (1)$$

Where $P_A(k)$ is the degree distribution of network A. As described above, the network A satisfy ER network model whose degrees are Poisson-distributed. The generating functions of the underlying branching processes is

$$\mathrm{G}_{\mathrm{A1}}(z) = G'_{A0}(z) / G'_{A0}(1) \quad (2)$$

When random removed of fraction 1-p of nodes, the degree distribution of the remaining nodes will change, then the generating function of the new distribution also change [1]. We know that it is equal to the generating function of the original distribution with argument $1 - p \cdot (1 - z)$ [24]. After removed in the beginning, the number of remaining nodes is $N'_{A1} = p \cdot N_{\mathrm{A}}$, the fraction of nodes that belong to the giant component of network N'_{A1} is

$$g_A(p) = 1 - G_{A0}\left[1 - p(1 - f_A)\right] \quad (3)$$

Where f_A is a function of *p*. The relationship between f_A and *p* can be represented by the following transcendental equation [6], [7]:

$$f_A = G_{A1}\left[1 - p(1 - f_A)\right] \quad (4)$$

In the network B we can also get the same result. Based on this theory, we can get the following derivation process.

3.1 Random Failure in Network A

We assume random attack or random break happen in systems, then we begin our analysis with random removal of a fraction 1-p of nodes in A. After the initial remove in the this stage, the failure is caused by the fragmentation of the N'_{A1} which

$$N'_{A1} = p \cdot N_A = \mu'_1 \cdot N_A \quad (5)$$

Where μ'_1 is the proportion of N'_{A1} to the entire network A, $\mu'_1 = p$. The number of the giant component N_{A1} of N'_{A1} is

$$N_{A1} = g_A(\mu'_1) \cdot N'_{A1} = \mu'_1 \cdot g_A(\mu'_1) \cdot N_A = \mu_1 \cdot N_A \quad (6)$$

The fraction of functioning nodes after the first stage failures is

$$\mu_1 = \mu'_1 \cdot g_A(\mu'_1) \quad (7)$$

3.2 Cascading Effects in Network B

Since the nodes in network B depend on the nodes in network A, the removed nodes in network A will lead to the failure of nodes in network B. In the first stage, we can obtain the fraction of the remaining nodes in network A. Owing to one node in network B connect with three nodes in network A, corresponding fraction of nodes remains functional in network B. The expected number of nodes that still remain functional is

$$N'_{B2} = \left[1 - (1 - \mu_1)^3\right] \cdot N_B = (\mu_1{}^3 - 3 \cdot \mu_1{}^2 + 3 \cdot \mu_1) \cdot N_B = \mu'_2 \cdot N_B \quad (8)$$

$$\mu'_2 = \mu_1{}^3 - 3 \cdot \mu_1{}^2 + 3 \cdot \mu_1 = (\mu_1{}^2 - 3 \cdot \mu_1 + 3) \cdot \mu'_1 \cdot g_A(\mu'_1) \quad (9)$$

The number of the giant component N_{B2} of N'_{B2} is

$$N_{B2} = g_B(\mu'_2) \cdot N'_{B2} = \mu'_2 \cdot g_B(\mu'_2) \cdot N_B = \mu_2 \cdot N_B \quad (10)$$

$$\mu_2 = \mu'_2 \cdot g_B(\mu'_2) \quad (11)$$

3.3 Further Failures in Network A

We will analyze what happens during cascading process. After the first stage, we know that one node in network B can be connected to one node, two nodes, or three nodes in network A, and other nodes don't connected. **Table 2** shows the proportion of the number of nodes in the network A to which the nodes in the network B are connected.

Table 2: The proportion of the number of nodes in the network A to which the nodes in the network B are connected.

0	1	2	3
$(1-\mu_1)^3$	$C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2$	$C_3^2 \cdot \mu_1{}^2 \cdot (1-\mu_1)$	$\mu_1{}^3$

There is no relationship between the intra links and inter links, then after failures in the second stage, the proportion of nodes in network B that are connected to the number of nodes has changed, as **Table 3** shows.

Table 3: The proportion of the number of nodes in the network A after the nodes in the network B being removed in the second stage.

1	2	3
$C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2 / \left[1-(1-\mu_1)^3\right]$	$C_3^2 \cdot \mu_1{}^2 \cdot (1-\mu_1) / \left[1-(1-\mu_1)^3\right]$	$\mu_1{}^3 / \left[1-(1-\mu_1)^3\right]$

Now we can compute the number of functional nodes due to the fragmentation of functional nodes in network B.

$$N'_{A3} = \mu_2 \cdot N_B \cdot \left[C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2 \cdot 1 + C_3^2 \cdot \mu_1{}^2 \cdot (1-\mu_1) \cdot 2 + \mu_1{}^3 \cdot 3\right] / \left[1-(1-\mu_1)^3\right] \tag{12}$$

$$N'_{A3} = \mu_1 \cdot g_B(\mu'_2) \cdot N_A \tag{13}$$

From N_{A1} to N'_{A3}, we know that

$$N_{A1} - N'_{A3} = (1-g_B(\mu'_2)) \cdot N_{A1} \tag{14}$$

Now we borrow an idea from [1], owing to all the nodes that were removed in the stage of the beginning attack do not belong to N_{B2}, N_{A1} and N'_{A1}, the removal of these nodes from N_{A1} is equivalent to the removal of the same fraction of nodes from N'_{A1}. Thus

$$N_{A1} - N'_{A3} = (1-g_B(\mu'_2)) \cdot N_{A1} = (1-g_B(\mu'_2)) \cdot N'_{A1} \tag{15}$$

The fraction of nodes that removed from network A in third stage is

$$1-\mu'_1 + (1-g_B(\mu'_2)) \cdot \mu'_1 = 1-\mu'_1 \cdot g_B(\mu'_2) \tag{16}$$

Thus, we can obtain that

$$\mu'_3 = \mu'_1 \cdot g_B(\mu'_2) \tag{17}$$

The number of the giant component N_{A3} of N'_{A3} is

$$N_{A3} = \mu'_3 \cdot g_A(\mu'_3) \cdot N_A = \mu_3 \cdot N_A \tag{18}$$

$$\mu_3 = \mu'_3 \cdot g_A(\mu'_3) \tag{19}$$

3.4 More Fragments in Network B Again

Due to the failures in the third stage, some nodes in network B will be removed. Here we can compute the number of remaining nodes,

$$N'_{B4} = \left[1-(1-\mu_3)^3\right] \cdot N_B = (\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3)\cdot N_B \tag{20}$$

From N_{B2} to N'_{B4}, we know that

$$N_{B2} - N'_{B4} = \left[1-(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3)/\mu_2\right]\cdot N_{B2} \tag{21}$$

As we show in the third stage

$$N_{B2} - N'_{B4} = \left[1-(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3)/\mu_2\right]\cdot N'_{B2} \tag{22}$$

Then, the fraction of nodes that removed from network B in fourth stage is

$$1-\mu'_2 + \mu'_2 \cdot (1-(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3)/\mu_2) = 1-\mu'_1\cdot(\mu_3^2 - 3\cdot\mu_3 + 3)\cdot g_A(\mu'_3) \tag{23}$$

So

$$\mu'_4 = \mu'_1 \cdot (\mu_3^2 - 3\cdot\mu_3 + 3)\cdot g_A(\mu'_3) \tag{24}$$

The number of the giant component N_{B4} of N'_{B4} is

$$N_{B4} = \mu'_4 \cdot g_B(\mu'_4)\cdot N_B = \mu_4 \cdot N_B \tag{25}$$

And we can obtain the fraction of functional nodes as

$$\mu_4 = \mu'_4 \cdot g_B(\mu'_4) \tag{26}$$

3.5 Transcendental Equations for Cascading Failures

According to the previous analysis process, we can get the recursion relations of the fraction of nodes that removed from network in each stage

$$\begin{cases} \mu'_{2i} = \mu'_1 \cdot (\mu_{2i-1}^2 - 3\cdot\mu_{2i-1} + 3)\cdot g_A(\mu'_{2i-1}) \\ \mu'_{2i+1} = \mu'_1 \cdot g_B(\mu'_{2i}) \end{cases} \tag{27}$$

Where $\mu'_1 = p$. So the Eq. (27) can be written as

$$\begin{cases} \mu'_{2i} = p \cdot (\mu^2_{2i-1} - 3 \cdot \mu_{2i-1} + 3) \cdot g_A(\mu'_{2i-1}) \\ \mu'_{2i+1} = p \cdot g_B(\mu'_{2i}) \end{cases} \tag{28}$$

In next section we will give a detailed analysis of Eq. (28).

4. Numerical simulations

Although we have obtained the recursion relations between the two networks in the cascading failure process, no one knows in which stage the cascading failures will stop. Our main goal is to get the final size of the giant connected component. We denote the fraction of nodes that remain functional in network A and in network B as μ_{A_∞} and μ_{B_∞} respectively. When the cascading process stops, the giant components in the two networks have no further fragments. In this way, we can get the following equivalence relationship,

$$\begin{cases} \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} \tag{29}$$

For simplicity, we denote $\mathrm{y} = \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2}$ and $x = \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3}$ ($0 \le x, y \le 1$). Where $\mu_{A_\infty} = x \cdot g_A(x)$ and $\mu_{B_\infty} = y \cdot g_B(y)$

On the basis of the equation (28) and the simplicity of μ'_{2i} and μ'_{2i+1},we can get

$$\begin{cases} x = p \cdot g_B(y) \\ y = p \cdot \left[(x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right] \cdot g_A(x) \end{cases} \tag{30}$$

This equation group have one trivial solution, x=0 and y=0 for any *p*. Excluding y we can obtain a single equation

$$x = p \cdot g_B \left[p \cdot \left[(x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right] \cdot g_A(x) \right] \tag{31}$$

This equation be solved graphically (Fig 1). Firstly we draw the straight line $z = x$, and then we draw the curve $z = p \cdot g_B \left[p \cdot \left[(x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right] \cdot g_A(x) \right]$ in the different p value. From Fig.2, when the value of p is very small, the curve doesn't intersect the straight line in $0 < x \le 1$. As the value of P increases, the straight line intersects the curve for the first time in p=0.42, which the curve touches the straight line at a single point. When P continues to grow, two intersections will appear. So we can estimate that the critical threshold is $p_c = 0.42$.

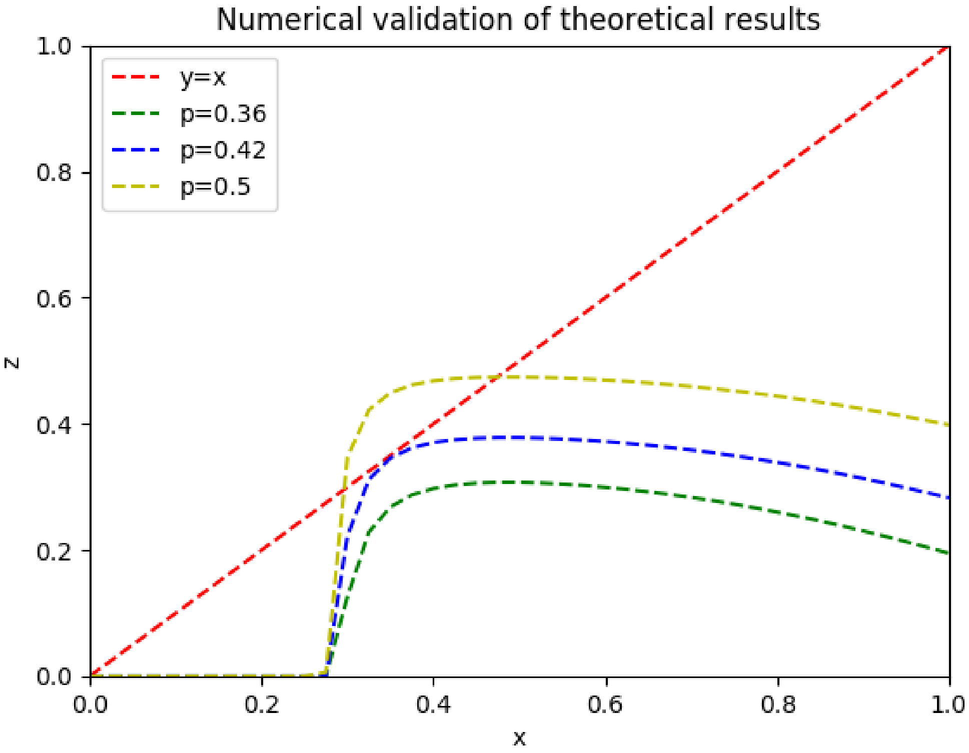


Figure 2: Solution of the equation (30). Both networks are ER networks, and the average degree of the two networks is 4.

Next, we will use simulation experiments to verify the correctness of our mathematical analysis. In the experiment, we use random remove to represent the random attacks on the network.

4.1 Simulation Setup

In the simulation setting, we generate two interdependent networks using ER model. In our design, each node in network B is randomly connected to three nodes in network A. Then we randomly remove the fraction (1-p) of nodes from network A. After that, the initial attack will cause the cascading failures. Our experiment will simulate the cascading failure process at each step. When nodes have no more failures, the process will stop.

4.2 Results and Analysis

First we compare the fraction of remaining nodes μ_{2i} and μ_{2i+1} in the case of different p, with the same average degree. As shown in Fig 3, we compared three group experiments in which only the average degree of the two networks is different. For the value of p is from 0.2 to 1.0. From Fig. 3, we can see that as the average degree increases, the remaining number of nodes in the network grows synchronously until the cascading process stops. This phenomenon indicates that as the average degree of the network increases, the connection between the networks is more closely, which means the smart grid is more reliable. Besides, in Fig. 3, we can also observe that $\mu_{2i+1} = 0$ when $\mu_{2i} = 0$ and it indicates that the network will disintegrate when the other network disintegrate in the coupled interdependent network.

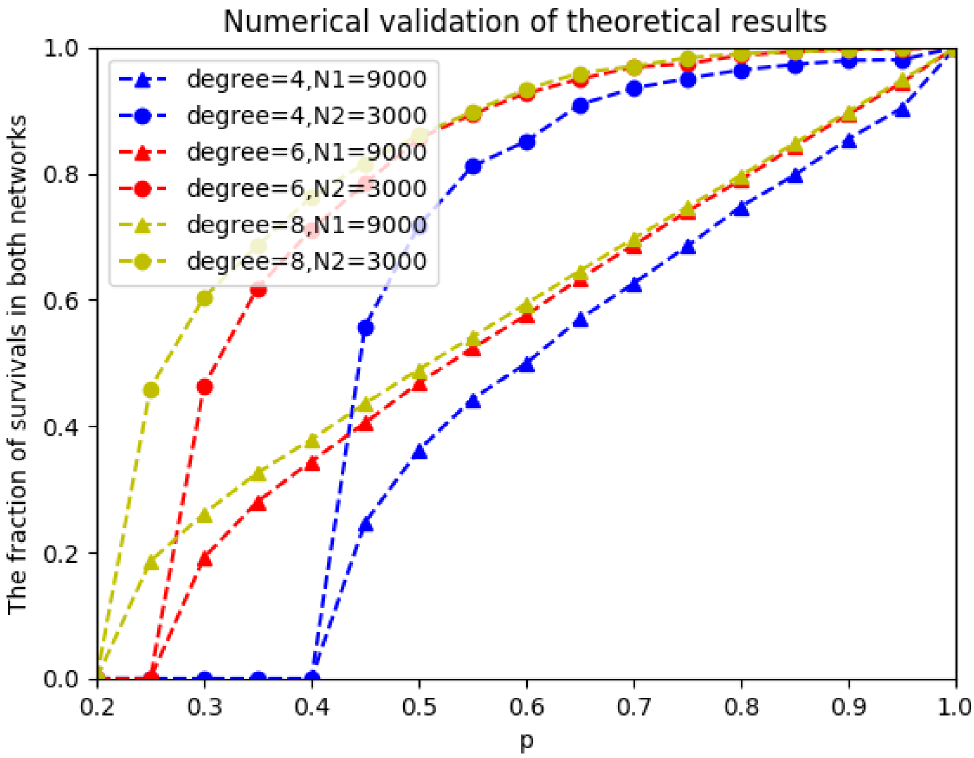
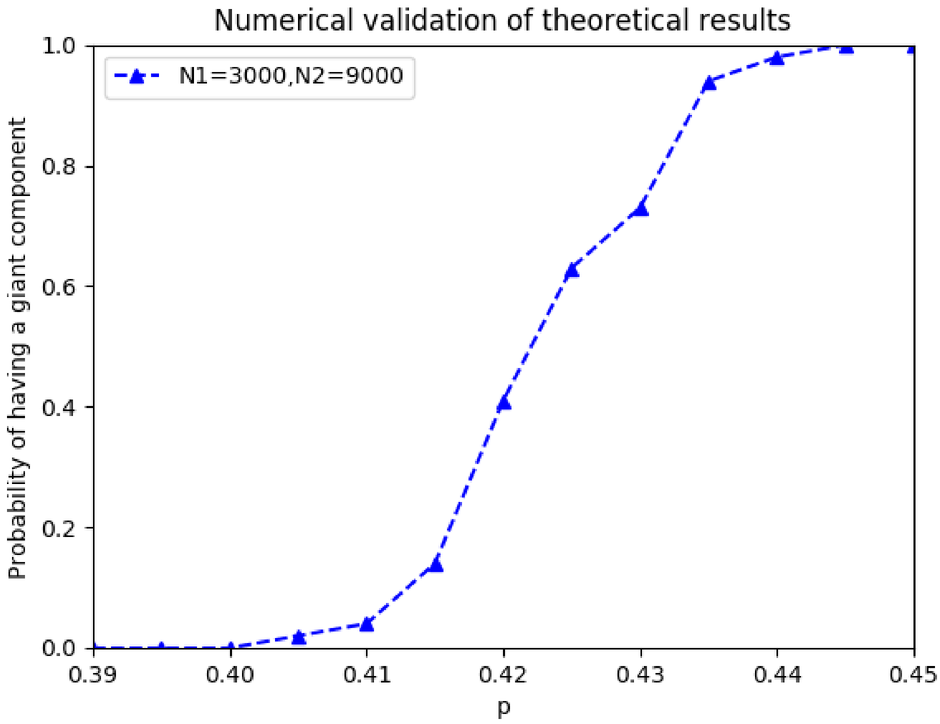
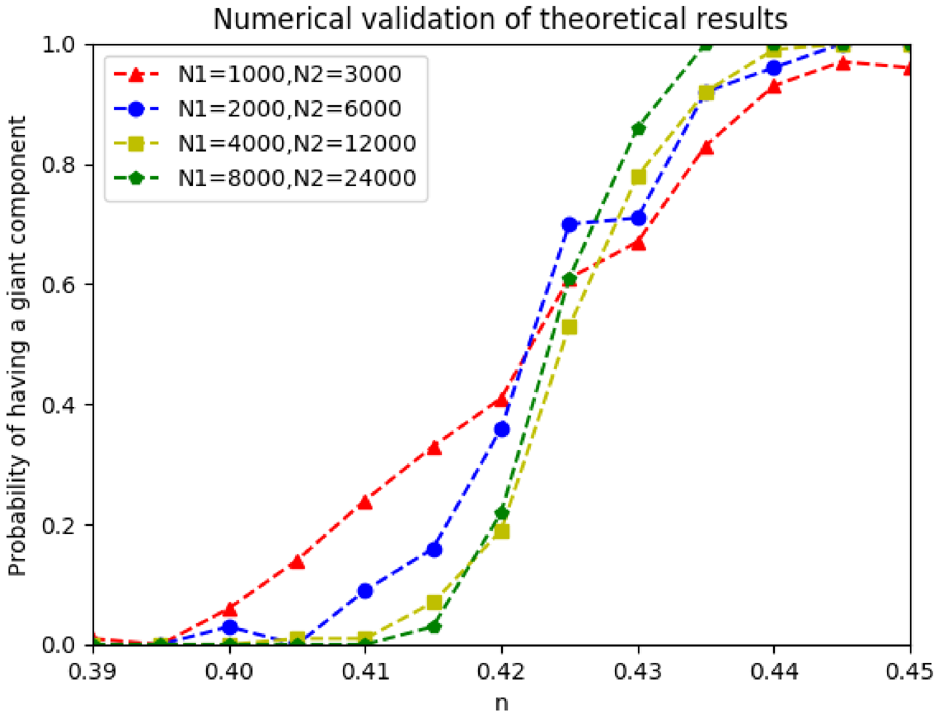


Figure 3: The fraction of survivals in both networks. In our simulation both networks are ER networks with the same average degree $\langle k \rangle_A = \langle k \rangle_B = 4$. The number of communication network and power grid are 9000, 3000 respectively.

In order to verify the correctness of our theoretical analysis, we take several values near the critical threshold p_c. For each value, we can get the probability of having a giant component using the experiment. Fig. 4a shows that the system will disintegrate when $p < 0.40$, but has a giant component when $p > 0.45$. In the scope of [0.40, 0.45], the system may have a giant component or not. From Fig. 4b, we know that the curve tends to rise linearly near 0.42. Thus the transition at p_c is continuous which indicate it is second-order transition. But when the number of nodes in the network is large enough, it will only have the first-order transition.



(a)

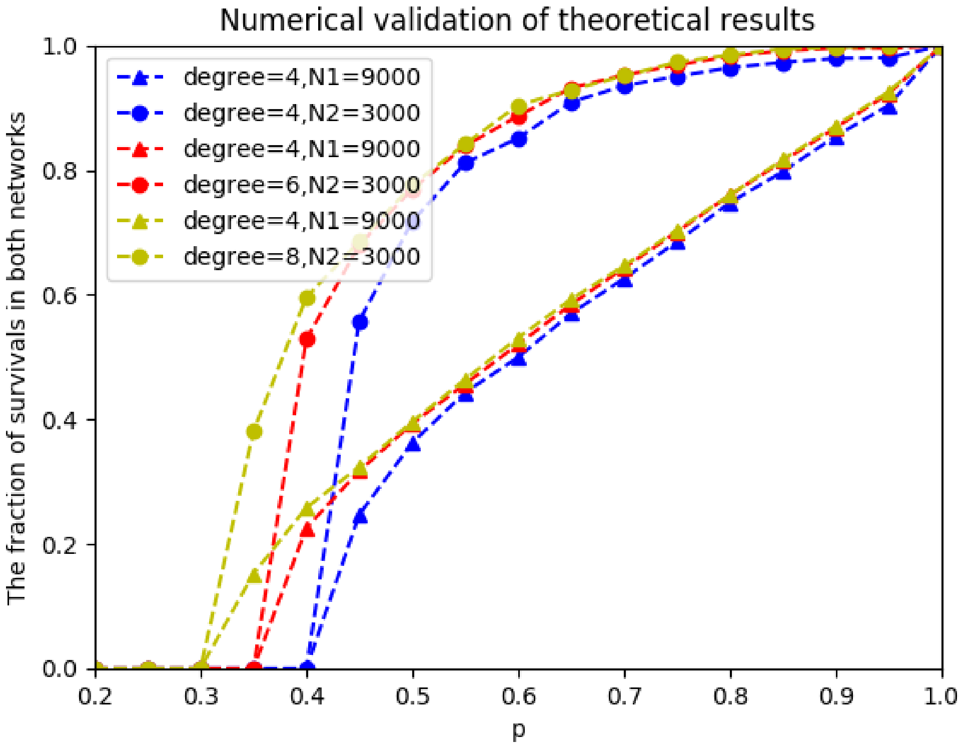


(b)

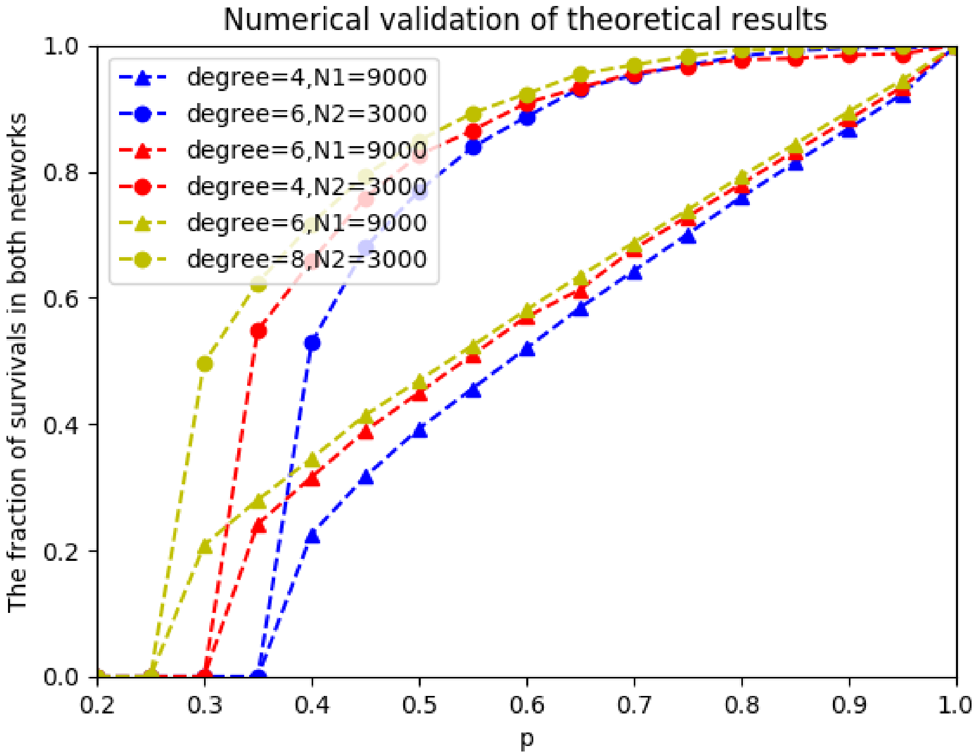
Figure 4: The probability of having a giant component. **(a)** both networks are ER networks with the same average degree $\langle k\rangle_A = \langle k\rangle_B = 4$, The number of communication network and power grid are 9000, 3000 respectively. **(b)** both networks are ER networks with the same average degree

$\langle k \rangle_A = \langle k \rangle_B = 4$, too. But we do four group experiments with different nodes number. The simulation results are in agreement with our analytical results.

We now show how the system reliability depends on the different values of average degree. In Fig 5(a), the blue line is the case where the two networks have the same average degree of the nodes. The red line and the yellow line are the case where the two networks have the different average degree of the nodes. In Fig 5(b), the average degree of nodes in each group of experiments is different. From the Fig 5(a) and Fig 5(b), we can get the same conclusion as Figure 3.



(a)



(b)

Fig 5: The fraction of survivals μ_{2i} and μ_{2i+1}. The number of communication network and power grid are 9000, 3000 respectively. Both networks are ER networks. The initial attack (1-p) occurs in network A.

From Fig.3~Fig.5, we show that the fraction of survivals μ_{2i} and μ_{2i+1} have no connection with the number N_A and N_B. In other words, it is determined by the distribution of degrees of nodes in the network and the fraction of removed (1-*p*) in the beginning. And then, we can draw the conclusion that the reliability of smart grid system becomes robustness with the increase of average degree. In this way, when we design robustness smart grid systems, we need to increase the inner average degree and then we can make the interdependent smart grid systems invulnerability to resist random attacks or random breakdown. So for real interdependent smart grid systems, our analysis shows that if we keep the average degree in a high level, the system reliability in terms of random failure or random breakdown remains in a reliable level.

5 Conclusions

We study the reliability and cascading risk of a smart gird system in which a cyber network overlays a grid network. To check the network reliability against random nodes failures, we estimate the fraction of nodes that still remain functional after the cascading failures process stops, and then we can obtain the correct results by simulation experiment. Our findings show that there is always a critical threshold value. If the percentage of failing nodes is greater than the critical value, the interdependent smart gird systems will collapse. Our theory analysis and simulation experiment also show that, if both networks satisfy the same degree distribution, the system reliability does not have the direct connection with the system size.

However, our proposed analysis model still has some limitations which could be our future work. For instance, we consider both networks are ER networks while the realistic settings are scale-free. Meanwhile, the giant components could not always work in reality. It is also of interest to study models that are more realistic than the existing ones in this paper. Clearly, there are still many open questions about interdependent smart grid systems. We are currently investigating related work along this avenue.

Acknowledgements

This work was partly supported by National Natural Science Foundation of China (Grant No.61602418, No.61672468 and No.61402418), Zhejiang Provincial Natural Science Foundation of China (Grant No.LQ16F020002 and No. LY15F020013), Social development project of Zhejiang provincial public technology research (Grant No.2016C33168 and No.2017C33054), MOE (Ministry of Education in China) Project of Humanity and Social Science (Grant No.15YJCZH125), Key Lab of Information Network Security, Ministry of Public Security (Grant No.C15610).

References

[1] Kurt S, Yildiz H U, Yigit M, et al. Packet size optimization in wireless sensor networks for smart grid applications[J]. IEEE Transactions on Industrial Electronics, 2017, 64(3): 2392-2401.

[2] Kamyab F, Amini M, Sheykhha S, et al. Demand response program in smart grid using supply function bidding mechanism[J]. IEEE Transactions on Smart Grid, 2016, 7(3): 1277-1284.

[3] Tuballa M L, Abundo M L. A review of the development of Smart Grid technologies [J]. Renewable and Sustainable Energy Reviews, 2016, 59: 710-725.

[4] Fadel E, Faheem M, Gungor V C, et al. Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications [J]. Computer Communications, 2017, 101: 106-120.

[5] Aktas A, Erhan K, Ozdemir S, et al. Experimental investigation of a new smart energy management algorithm for a hybrid energy storage system in smart grid applications[J]. Electric Power Systems Research, 2017, 144: 185-196.

[6] Khan A A, Rehmani M H, Reisslein M. Requirements, Design Challenges, and Review of Routing and MAC Protocols for CR-Based Smart Grid Systems[J]. IEEE Communications Magazine, 2017, 55(5): 206-215.

[7] Khazali A, Kalantar M. A stochastic–probabilistic energy and reserve market clearing scheme for smart power systems with plug-in electrical vehicles[J]. Energy Conversion and Management, 2015, 105: 1046-1058.

[8] Ouyang M, Wang Z. Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis[J]. Reliability Engineering & System Safety, 2015, 141: 74-82.

[9] Garvey P R, Pinto C A, Santos J R. Modelling and measuring the operability of interdependent systems and

systems of systems: advances in methods and applications[J]. International Journal of System of Systems Engineering, 2014, 5(1): 1-24.

[10] Bayram I S, Michailidis G, Devetsikiotis M, et al. Electric power allocation in a network of fast charging stations[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(7): 1235-1246.

[11] McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid[J]. IEEE Security & Privacy, 2009, 7(3).

[12] Zhao J, Zhang G, La Scala M, et al. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1580-1590.

[13] Farraj A, Hammad E, Al Daoud A, et al. A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 1846-1855.

[14] Ozay M, Esnaola I, Vural F T Y, et al. Machine learning methods for attack detection in the smart grid[J]. IEEE transactions on neural networks and learning systems, 2016, 27(8): 1773-1786.

[15] Rampurkar V, Pentayya P, Mangalvedekar H A, et al. Cascading failure analysis for Indian power grid[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 1951-1960.

[16] Tan K M, Ramachandaramurthy V K, Yong J Y. Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques[J]. Renewable and Sustainable Energy Reviews, 2016, 53: 720-732.

[17] Li S, Yılmaz Y, Wang X. Quickest detection of false data injection attack in wide-area smart grids[J]. IEEE Transactions on Smart Grid, 2015, 6(6): 2725-2735.

[18] Hartmann T, Fouquet F, Klein J, et al. Generating realistic smart grid communication topologies based on real-data[C]//Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on. IEEE, 2014: 428-433.

[19] Toft M B, Schuitema G, Thøgersen J. Responsible technology acceptance: Model development and application to consumer acceptance of Smart Grid technology[J]. Applied Energy, 2014, 134: 392-400.

[20] Maasoumy M, Sanandaji B M, Sangiovanni-Vincentelli A, et al. Model predictive control of regulation services from commercial buildings to the smart grid[C]//American Control Conference (ACC), 2014. IEEE, 2014: 2226-2233.

[21] Zhu Y, Yan J, Tang Y, et al. Joint substation-transmission line vulnerability assessment against the smart grid[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(5): 1010-1024.

[22] Gao J, Buldyrev S V, Stanley H E, et al. Networks formed from interdependent networks[J]. Nature physics, 2012, 8(1): 40-48.

[23] Gao J, Buldyrev S V, Havlin S, et al. Reliability of a network of networks[J]. Physical Review Letters, 2011, 107(19): 195701.

[24] Gao J, Buldyrev S V, Stanley H E, et al. Percolation of a general network of networks[J]. Physical Review E, 2013, 88(6): 062816.