Reliability Analysis of Coupled Cyber-Physical Systems Under Different Network Types

Hao Peng[1,2], Zhe Kan[1], Dandan Zhao[1(✉)], Jianmin Han[1], and Zhaolong Hu[1]

[1] College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, Zhejiang, China
ddzhao@zjnu.edu.cn
[2] Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China

Abstract. In this paper, the reliability performance analysis of coupled cyber-physical systems under different network types is investigated. To study the underlying network model, we propose a practical model for interdependent cyber-physical systems using network percolation theory. For different network models, we also study the effect of cascading failures effect and reveal mathematical analysis of failure propagation in such systems. The simulation results show that there exists a threshold for the proportion of faulty nodes and different system parameters, beyond which the cyber-physical systems collapse.

Keywords: Cyber-Physical systems · Percolation theory · Cascading failures · Interdependent network

1 Introduction

With the latest developments in communication and information technologies, the application of cyber-physical systems (CPS) [1–5] in our lives is becoming more and more extensive. Generally, the cyber-physical systems depend on two main networks: cyber layer network which provides control function or communication function and physical layer network which includes conventional power grid, smart grid. 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. However, for interdependent system architecture, the failures in one network can lead to the cascading risk in another. Actually, the breakdown of a power station network [6–10] could result in the corresponding nodes failure in communication network. Especially, the further failures may even occur recursively between the interdependent CPS and then the cascading failures are big issues in such coupled CPS.

In order to improve the reliability of CPS, it is necessary to explore the cascading failures in actual interdependent CPS systems. Recently many researchers have paid more attentions in this research field. Currents research in smart gird systems [11–14] mainly focuses on failures about load balancing and load distribution. Most of these techniques rely on methods commonly used in distributed systems. Architecture for

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 440–449, 2019.
https://doi.org/10.1007/978-3-030-21373-2_35

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 cyber-physical 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. Toft and Maasoumy et al. [19] focused on the challenges of modeling cyber-physical systems that arise from the intrinsic heterogeneity and sensitivity to timing. However, the actual interdependent CPS systems are often different network types, so this paper will study the reliability of interdependent CPS systems under different network types.

The remainder of the paper is organized as follows: Sect. 2 introduces the system model of the CPS and the related definition. Sections 3 and 4 show the cascading process analysis when attack different type of networks. Theoretical solution and simulation analysis are introduced in Sect. 5. Then Sect. 6 is the conclusion.

2 System Model

In this section, we first introduce the network model of coupled CPS. According to the study and analysis of the coupled interdependent network, we establish a model that conforms to the characteristics of the coupled CPS in reality. From the research on the existing coupled CPS system [2–4, 6], we obtain that the coupling network is usually composed of multiple networks. Without loss of generality, we assume that the coupled network consists of two interdependent networks and the type of two interdependent networks is different. Thus we specify that the two networks that form the coupled network are the SF network and the ER network respectively.

Next, we will explain some basic concepts. There are two ways that connection mode of nodes in coupled network. One is the connection between the internals of the network that the link just between nodes in a single network. The other is the connection of the nodes connecting the two networks. When one network in the coupled network is attacked, only the functional nodes that satisfies the following two conditions in the network as follows:

(1) The node must belong to the giant connected component;
(2) The node must be connected to a functional node in internal network.

When a network in coupled network is attacked, the failure of the nodes in one network affects the function of the nodes in the other network. If none of the two networks fails or the two networks completely collapse, the network reaches steady state. This iterative failure process is called cascading failures. Cascading failures are a common failure process in coupled systems. If cascading failures are not controlled, cascading failures can cause severe damage.

3 Initial Failure in SF-Network A

The two networks that compose the coupled network one is SF network, the other is ER network. The generating function of the SF network is $G_{A0}(z) = \sum_k P_A(k) \cdot z^k$. Analogously, the generating function of the ER network is $G_{B0}(z) = \sum_k P_B(k) \cdot z^k$. Then the generating function of the underlying branching processes is

$$G_{A1}(z) = G'_{A0}(z)/G'_{A0}(1) \tag{1}$$

We denote the number of nodes remaining after the node has been removed as N'_{A1}, we know that $N'_{A1} = p \cdot N_A$. The fraction of the nodes belonging to the giant connected component to the number of nodes is

$$g_A(p) = 1 - G_{A0}[1 - p(1 - f_A)] \tag{2}$$

Where f_A is function of p. f_A and p satisfy the following equation

$$f_A = G_{A1}[1 - p(1 - f_A)] \tag{3}$$

3.1 Random Failure in Network A

We assume that after being attacked, the proportion of deleted nodes is 1-p. So the number of remaining nodes in network A is

$$N'_{A1} = p \cdot N_A = \mu'_1 \cdot N_A \tag{4}$$

We denote the giant component as N_{A1}, then we can obtain

$$N_{A1} = g_A\left(\mu'_1\right) \cdot N'_{A1} = \mu'_1 \cdot g_A\left(\mu'_1\right) \cdot N_A = \mu_1 \cdot N_A \tag{5}$$

3.2 Impact of Cascading Failures on Network B

Owing to network A and network B depends on each other, nodes in network B will fail because of the failure of nodes in network A. We can calculate the number of nodes in network B that connect to nodes in network A:

$$N'_{B2} = \left[1 - (1 - \mu_1)^3\right] \cdot N_B = \left(\mu_1^3 - 3 \cdot \mu_1^2 + 3 \cdot \mu_1\right) \cdot N_B = \mu'_2 \cdot N_B \tag{6}$$

Then we will again apply the apparatus of generating functions and calculate the number of nodes in network B that belong to the giant connected component:

$$N_{B2} = g_B\left(\mu'_2\right) \cdot N'_{B2} = \mu'_2 \cdot g_B\left(\mu'_2\right) \cdot N_B = \mu_2 \cdot N_B \tag{7}$$

3.3 Further A-Nodes Cascading Failure Due to B-Node Failures

According to the random failure in Step 3.1, we can know that one node in network B may be connected to one, two or three nodes in network A, or it may not be connected to any node in network A. Here there is no relationship within or between networks, so the number of nodes with dependencies in network A is

$$N_{A3}^{'} = \mu_2 \cdot N_B \cdot \begin{matrix} [C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2 \cdot 1 + \\ C_3^1 \cdot (1-\mu_1) \cdot 2 + \mu_1^3 \cdot 3] \end{matrix} / \left[1-(1-\mu_1)^3\right] \tag{8}$$

From N_{A1} to $N_{A3}^{'}$, we obtain

$$N_{A1} - N_{A3}^{'} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1} \tag{9}$$

Since deleted nodes do not belong to N_{B2}, N_{A1}, and $N_{A3}^{'}$, the proportion of nodes removed from N_{A1} is equal to the same proportion of nodes removed from $N_{A3}^{'}$,

$$N_{A1} - N_{A3}^{'} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1}^{'} \tag{10}$$

The number of the giant component is

$$N_{A3} = \mu_3^{'} \cdot g_A\left(\mu_3^{'}\right) \cdot N_A = \mu_3 \cdot N_A \tag{11}$$

3.4 Further Fragment of Network B

The nodes in network B will fail due to the failure of the nodes in network A because of the interdependence of the coupled networks. Similar to the second step, we can get the number of nodes with dependencies in the remaining nodes in network B:

$$N_{B4}^{'} = \left[1-(1-\mu_3)^3\right] \cdot N_B = \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right) \cdot N_B \tag{12}$$

From N_{B2} to $N_{B4}^{'}$, we can obtain

$$N_{B2} - N_{B4}^{'} = \left[1 - \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right)/\mu_2\right] \cdot N_{B2} \tag{13}$$

The number of total removed nodes to the original network B is

$$\begin{aligned} 1 - \mu_2^{'} + \mu_2^{'} \cdot \left[1 - \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right)/\mu_2\right] \\ = 1 - \mu_1^{'} \cdot \left(\mu_3^2 - 3 \cdot \mu_3 + 3\right) \cdot g_A\left(\mu_3^{'}\right) \end{aligned} \tag{14}$$

The number of the giant component is

$$N_{B4} = \mu_4^{'} \cdot g_B\left(\mu_4^{'}\right) \cdot N_B \tag{15}$$

According to the previous derivation process, we can obtain the following recursion relations

$$\begin{cases} \mu_{2i}^{'} = \mu_1^{'} \cdot \left(\mu_{2i-1}^2 - 3 \cdot \mu_{2i-1} + 3\right) \cdot g_A\left(\mu_{2i-1}^{'}\right) \\ \mu_{2i+1}^{'} = \mu_1^{'} \cdot g_B\left(\mu_{2i}^{'}\right) \end{cases} \tag{16}$$

Where $\mu_1^{'} = p$. Next we will analyze the iterative process of the coupled network when attacking the ER network.

4 Initial Failure in ER-Network B

Owing to the number and the type of two networks in the coupled CPS is different; the cascading failure process is different accordingly. Next, we will analyze the cascading failure process when the ER network B is attacked.

4.1 Initial Failure in Network B

Analogously, we assume that $(1-p) \cdot N_B$ nodes in network B are removed due to attack. The number of remaining nodes is

$$N_{B1}^{'} = p \cdot N_B = \mu_1^{'} \cdot N_B \tag{17}$$

The number of the giant component is

$$N_{B1} = g_B\left(\mu_1^{'}\right) \cdot N_{B1}^{'} = \mu_1^{'} \cdot g_B\left(\mu_1^{'}\right) \cdot N_A = \mu_1 \cdot N_A \tag{18}$$

4.2 Cascading Failures on Network A Due to B-Node Failures

The failure of nodes in network B will cause the nodes in network A to fail. According to the connection relationship between network A and network B, we can calculate the number of nodes in network A with dependencies. So

$$N_{A2}^{'} = \mu_1 \cdot N_B \cdot 3 = \mu_1 \cdot N_A = \mu_2^{'} \cdot N_A \tag{19}$$

The number of the giant component is

$$N_{A2} = N_{A2}^{'} \cdot g_A\left(\mu_2^{'}\right) = \mu_2^{'} \cdot g_A\left(\mu_2^{'}\right) \cdot N_A = \mu_2 \cdot N_A \tag{20}$$

4.3 Further Fragment on Network B

Network B will continue to fragment as cascading failures proceed. To calculate the number of nodes with dependencies in network B in the third step, we define a new variable, $q_1 = g_A(\mu_2^{'})$. The number of nodes in network B with dependencies is

$$N_{B3}^{'} = \mu_2^{'} \cdot N_A \cdot \left[1 - (1 - q_1)^3\right]/3 = \mu_2^{'} \cdot \left(q_1^3 - 3 \cdot q_1^2 + 3 \cdot q_1\right) \cdot N_B \tag{21}$$

So the fraction of remaining nodes is

$$\mu_3^{'} = p \cdot \left(q_1^3 - 3 \cdot q_1^2 + 3 \cdot q_1\right) \tag{22}$$

Then the number of the giant component is

$$N_{B3} = \mu_3^{'} \cdot g_B\left(\mu_3^{'}\right) \cdot N_B = \mu_3 \cdot N_B \tag{23}$$

4.4 More Cascading Failures of Network A

Using the theory in Ref. [4], we get

$$N_{A2} - N_{A4}^{'} = \left(1 - p \cdot g_A\left(\mu_2^{'}\right) \cdot g_B\left(\mu_3^{'}\right)/\mu_2\right) \cdot N_{A2}^{'} \tag{24}$$

Then the number of the giant component is

$$N_{A4} = \mu_4^{'} \cdot g_A\left(\mu_4^{'}\right) \cdot N_A = \mu_4 \cdot N_A \tag{25}$$

The fraction can be obtained by the recursion relations,

$$\begin{cases} \mu_{2i+1}^{'} = p \cdot \left(q_i^3 - 3 \cdot q_i^2 + 3 \cdot q_i\right) \\ \mu_{2i}^{'} = p \cdot g_B\left(\mu_{2i-1}^{'}\right) \end{cases} \tag{26}$$

Where $q_i = g_A(\mu_{2i}^{'})$.

5 Theoretical Solution and Numerical Simulation

In this section, we analyze the iteration relation derived from the above model and find the corresponding theoretical solution.

5.1 Critical Threshold Solution

For the cascading failure of the coupled network, although we do not know which step the cascading failure will stopped, the network will not split again when the cascading failure stops. Thus we can get the following equations:

$$\begin{cases} \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} \tag{27}$$

In order to facilitate the analysis of iterative formulas for cascading failure, the variable x, y is defined to satisfy the following equations:

$$\begin{cases} y = \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ x = \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} (0 \le \mathrm{x}, \mathrm{y} \le 1) \tag{28}$$

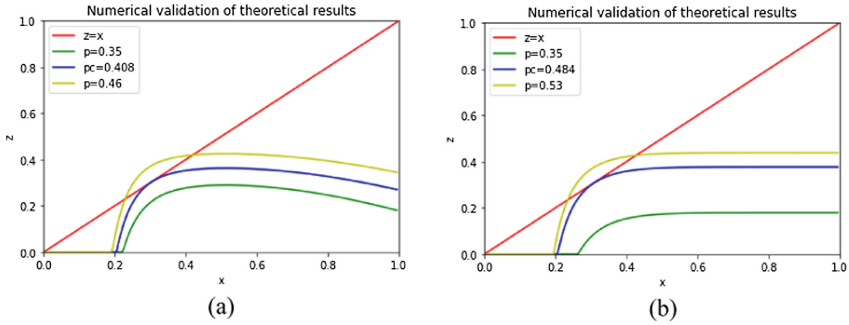

Fig. 1. Theoretical solution

Thus, Eq. (28) can be represented by the following equation set

$$\begin{cases} y = p \cdot \left((x \cdot g_A(x))^3 - 3 \cdot x \cdot g_A(x) + 3 \right) \cdot g_A(x) \\ x = p \cdot g_B(y) \end{cases} \tag{29}$$

Figure 1(a) and (b) show the cases that correspond to Eqs. (28) and (29) when attacking SF network and ER network, respectively. For the purpose of illustrate the graphical solution of Eq. (28), we plot Eqs. (28) and (29) for SF network with $\lambda = 2.8$ and ER network with $\alpha = 4$. Such as, in Fig. 1(a), the curve don't intersects with the straight line when $p < 0.408$, and the curve is tangent to the straight line when p = 0.408, the curve intersects with the straight line when p > 0.408. Thus from Fig. 1 (a), we can derive the critical threshold $p_{c-SF} = 0.408$ when attacking the SF network. Similarly, Fig. 1(b) shows that the critical threshold $p_{c-ER} = 0.484$ when attacking the ER network. We can see that the critical threshold when attacking the SF network is smaller than the critical value of the attack ER network.

5.2 Numerical Simulation

Next, we mainly verify the correctness of the theoretical results through numerical simulation. We create two networks according to the specified parameters. One is the SF network, the number of nodes is 30,000, and the other is the ER network, the number of nodes is 10000. Then according to the model described above, the two networks are connected together, that is, three nodes in the network A are randomly connected to one node in the network B, and the inter-network connection is completely random. So we have established a coupling network.

In Fig. 2, the blue curve shows the proportion of the remaining functional nodes in B and the red curve represents the proportion of the remaining nodes in network A after the cascading failure stops. We can see that the proportion of nodes in Network A is always lower than the proportion of nodes in Network B. In Fig. 2(b), although the network attack occurs in network B, the proportion of the remaining functional nodes in network B is still greater than the proportion of the functional nodes of network A. This phenomenon is caused by the connection relationship between network B and network A.

In order to further verify the correctness of the theory, we take multiple values near the critical threshold and find the probability of the existence of the giant connected component. In Fig. 3, the abscissa p represents the fraction of the nodes that were not

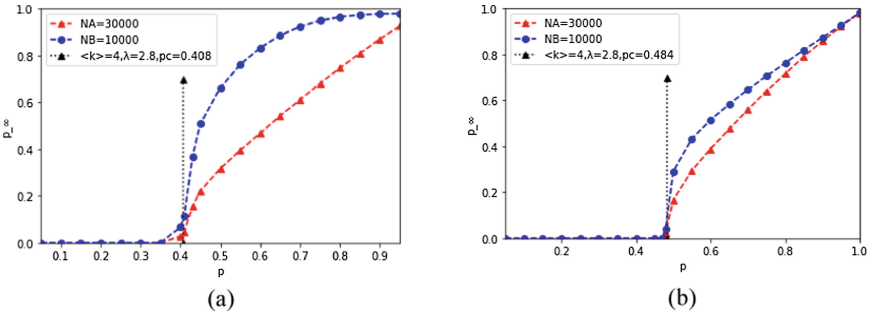

Fig. 2. The fraction of survival in both networks (Color figure online)

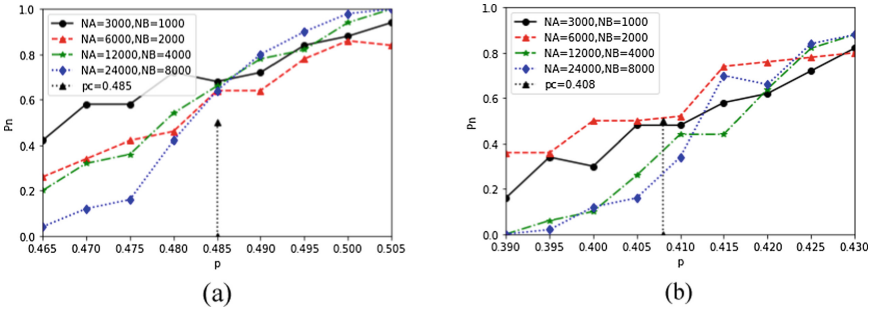

Fig. 3. Numerical validation of theoretical results

attacked to the number of nodes in the original network. The critical threshold is indicated by a black arrow. From Fig. 3(a) and (b), we can see that the number of nodes for the coupled system increases from small to large. As the number of nodes increases, the curve becomes steeper, and it is getting closer to the critical threshold. Therefore, we can infer that the curve will produce a first-order phase transition near the critical threshold, which is completely different from the second-order phase transition that characterizing percolation in a single network. Figure 3 also verifies the correctness of the conclusions from theoretical analysis.

6 Conclusion

This paper investigates the reliability performance of interdependent cyber-physical systems under different network types. Our findings demonstrate 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, 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 cyber-physical systems. We are currently investigating related work along this avenue.

Acknowledgements. This work was supported by National Natural Science Foundation of China (Grant No. 61602418, No. 61672468), Zhejiang Provincial Natural Science Foundation of China (Grant No. LQ16F020002), Social development project of Zhejiang provincial public technology research (Grant No. 2016C33168), MOE (Ministry of Education in China) Project of Humanity and Social Science (Grant No. 15YJCZH125) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK2018001).

References

1. Kurt, S.: Packet size optimization in wireless sensor networks for smart grid applications. IEEE Trans. Ind. Electron. **64**(3), 2392–2401 (2017)
2. Kamyab, F.: Demand response program in smart grid using supply function bidding mechanism. IEEE Trans. Smart Grid **7**(3), 1277–1284 (2016)
3. Zeng, X.: E-AUA: an efficient anonymous user authentication protocol for mobile IoT. IEEE Internet Things J. (99), 1 (2018)
4. Fadel, E.: Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. Comput. Commun. **101**, 106–120 (2017)
5. Aktas, A.: Experimental investigation of a new smart energy management algorithm for a hybrid energy storage system in smart grid applications. Electr. Power Syst. Res. **144**, 185–196 (2017)

6. Khan, A.A.: Requirements, design challenges, and review of routing and MAC protocols for CR-based smart grid systems. IEEE Commun. Mag. **55**(5), 206–215 (2017)
7. Khazali, A.: A stochastic–probabilistic energy and reserve market clearing scheme for smart power systems with plug-in electrical vehicles. Energy Convers. Manag. **105**, 1046–1058 (2015)
8. Ouyang, M.: Resilience assessment of interdependent infrastructure systems: with a focus on joint restoration modeling and analysis. Reliab. Eng. Syst. Saf. **141**, 74–82 (2015)
9. Garvey, P.R.: Modeling and measuring the operability of interdependent systems and systems of systems: advances in methods and applications. Int. J. Syst. Syst. Eng. **5**(1), 1–24 (2014)
10. Bayram, I.S.: Electric power allocation in a network of fast charging stations. IEEE J. Sel. Areas Commun. **31**(7), 1235–1246 (2013)
11. Xu, G.: A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks. J. Netw. Comput. Appl. **107**, 83–92 (2018)
12. Zhao, J.: Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. IEEE Trans. Smart Grid **8**(4), 1580–1590 (2017)
13. Farraj, A.: A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. IEEE Trans. Smart Grid **7**(4), 1846–1855 (2016)
14. Ozay, M.: Machine learning methods for attack detection in the smart grid. IEEE Trans. Neural Netw. Learn. Syst. **27**(8), 1773–1786 (2016)
15. Rampurkar, V.: Cascading failure analysis for Indian power grid. IEEE Trans. Smart Grid **7**(4), 1951–1960 (2016)
16. Tan, K.M.: Integration of electric vehicles in smart grid: a review on vehicle to grid technologies and optimization techniques. Renew. Sustain. Energy Rev. **53**, 720–732 (2016)
17. Li, S.: Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid **6**(6), 2725–2735 (2015)
18. Hartmann, T., Fouquet, F., Klein, J.: Generating realistic smart grid communication topologies based on real-data. In: 2014 IEEE International Conference on Smart Grid Communications, pp. 428–433. IEEE (2014)
19. Toft, M.B.: Responsible technology acceptance: model development and application to consumer acceptance of Smart Grid technology. Appl. Energy **134**, 392–400 (2014)