Security Assessment for Cascading Failures of Cyber-Physical Systems Under Target Attack Strategy

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. Due to the multi-scale fusion of cyber-physical systems, attackers can attack the physical space based on cyber space intentionally. This process can cause cascading failures and then in sharp contrast with the previous physical space. Thus, how to effectively evaluate the security of cyber-physical systems becomes critical. In this paper, we model the cyber-physical systems and then analyze the cascading failure process under target attack strategy. After doing that, based on the comparative analysis of simulation experiments, we analyze the main factors affecting the security of the cyber-physical system.

Keywords: Cyber-physical systems · Target attack · Cascading failures · Security assessment

1 Introduction

With the advancement of smart grid technology, the continuous integration of technologies such as information perception, ubiquitous computing has realized the interconnection and deep integration of physical space and cyberspace, and finally formed Cyber-Physical System (CPS) [1–3]. In CPS systems, communication network needs grid network to support power energy, while power stations are controlled by communication network [4, 5]. Then the CPS systems can be regarded as interdependent systems [6–9]. 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 nodes failure in communication network. Especially, the failures may even occur recursively between the two interdependent grid network and communication network [11]. The hacker may attack the physical space based on the information space due to the integration of cyberspace and physical space. That is to say, a node in one network is attacked or invalidated [12–14], may cause cascading failure of another network node. For this reason, it is very important that carry out security risk assessment and how to ensure that the CPS system operates stably.

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 114–124, 2019.
https://doi.org/10.1007/978-3-030-21373-2_11

Many researchers have carried out research on security assessment of CPS system in recent years. The traditional reliability analysis method "fault tree analysis" [15, 16] is used in the security assessment of CPS systems such as intelligent transportation [17] and power system [18]. However, the derivative failure caused by the coupled relationship between the cyber network and the physical network in the CPS systems is not considered. Yang [19] and Chen [20] considered the cascading failure characteristics of CPS system, and simulated and verified the failure process based on interdependent network theory. But the type of attack in the actual CPS is often a highly targeted target attack [21, 22], and brings a large cascading failure risk to the CPS system. The above-mentioned security assessment methods for CPS are mainly analyzed from the perspectives of single network attributes or a single random attack. And it lacks effective analysis of the cascading failure process and security assessment of CPS under actual type of attacks.

2 System Model and Basic Concepts

In this section, we mainly introduce the model of cyber-physics systems. We analyze the actual cyber-physical system and its types of attacks, and model the types of attacks to which the actual network is subjected.

2.1 System Model

By analyzing the connection relationship between the coupled systems, we divide the connection relationships of the coupled system into two types. One is the connection inside the network, we call it the intra-network connection, and the other is the connection between the networks, which we call the inter-network connection. In order to analyze the reliability of the cyber-physical system qualitatively, we assume that the connections between the nodes of the two networks are equal ratio connection. Without loss of generality, we set $N_A : N_B = 3 : 1$, which means one node in network B is connected to three nodes in network A, and this connection is completely random. Here we use N_A and N_B respectively to show the number of nodes in the cyber network and the physical network.

2.2 Basic Concepts

In the foregoing modeling process, the model of the cyber-physical system is a coupled network composed of communication network A and physical network B. The failure of the nodes in the A network will invalidate the nodes in the B network in turn. The cascading failure will stop in the following two situations. The process of cascading failure is a very important characteristic of the cyber-physical system after being attacked. It is completely different from the failure process of single network under attack. When a network is attacked, the network will splits into a larger component and some smaller components. We stipulate that only nodes satisfy the following two conditions can maintain the function [20, 22].

(1) A node in the current network must be connected to a node in another network.
(2) The node must be within the giant connected component.

The nodes that satisfy the above two conditions are called functional nodes. The functional node is a very important node in the network. When a network is attacked, only the functional node can be retained. There is no functional node in the network illustrate that the network has completely collapsed.

3 Theoretical Analysis of Cascading Failures Process

In this section we will establish a mathematical framework to analyze the security of cyber-physical systems under target attacks.

3.1 Target Attack in Cyber Network

We use $W_\alpha(k_i)$ to represent the probability of node i with degree k attacked in initial target attack:

$$W_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=0}^{N} k_i^\alpha} \tag{1}$$

For the Eq. (1) we can see that the formula becomes meaningless when $\alpha = 0$. Therefore, we improved the above equation to get the following equation for the study of the actual coupling system:

$$W_\alpha(k_i) = \frac{(k_i+1)^\alpha}{\sum_{i=0}^{N} (k_i+1)^\alpha} \tag{2}$$

When target attack occurs, we assume that the ratio of nodes being attacked is 1-p, but we keep the edges of the remaining nodes which lead to the removed nodes. Assume $A_p(k)$ represent the number of nodes with degrees k, we can get:

$$P_p(k) = \frac{A_p(k)}{pN_A} \tag{3}$$

In the limit of $N \to \infty$, the Eq. (3) can be showed as derivative of $A_p(k)$ with respect to p. When $N \to \infty$ combining Eq. (2) with Eq. (3) we can get

$$-p\frac{dA_p(k)}{dp} = P_p(k) - N\frac{P_p(k)(k+1)^\alpha}{\sum_k P_p(k)(k+1)^\alpha} \tag{4}$$

The probability of edge deletion in the remaining node is equal to the ratio of the number of edges in the remaining node to the number of edges.

$$\tilde{p} \equiv \frac{p\mathrm{N}\langle k(p)\rangle}{N\langle k\rangle} = \frac{\sum_k P(k)kt^{(k+1)^{\alpha}}}{\sum_k P(k)k} \tag{5}$$

Where $\langle k\rangle$ is the average degree of the original network A. Then we can obtain the generating function of the remaining nodes as follows:

$$G_{Ac}(x) \equiv G_{Ab}(1-\widetilde{p}+\widetilde{p}x) \tag{6}$$

Equation (6) is the generating function of the remaining nodes after target attacked in network A. We can get $\widetilde{G}_{A0}(x)$ from the equation $\widetilde{G}_{A0}(1-p+px) = G_{Ac}(x)$ as

$$\widetilde{G}_{A0}(x) = G_{Ab}\left(1+\frac{\widetilde{p}}{p}(x-1)\right) \tag{7}$$

According to the generating function of the network, we can obtain the generating function of the underlying branching process $\widetilde{G}_{A1}(z)$ as follows:

$$\widetilde{G}_{A1}(z) = \widetilde{G}'_{A0}(z)/\widetilde{G}'_{A0}(1) \tag{8}$$

When A′ is attacked randomly to delete (1-p) proportion nodes, the degree distribution of the remaining nodes and the generating function of the corresponding degree distribution will change. The fraction of nodes that belong to the giant component is

$$g_A(p) = 1 - \widetilde{G}_{A0}[1-p(1-f_A)] \tag{9}$$

We can get the iterative equation of cascading failure by the method of generating function and percolation theory.

3.2 Equivalent Random Failure in Network A′

We assume that the fraction 1-p of nodes fails due to the attack. Then we can find the number of remaining nodes can be shown as:

$$N'_{A1} = p \cdot N_A = \mu'_1 \cdot N_A \tag{10}$$

Where μ'_1 is the fraction of the remaining nodes. According to the previous analysis, we can know that the number of nodes belonging to the giant component in N'_{A1} is

$$N_{A1} = g_A\left(\mu'_1\right) \cdot N'_{A1} = \mu'_1 \cdot g_A\left(\mu'_1\right) \cdot N_A = \mu_1 \cdot N_A \tag{11}$$

3.3 Cascading Failures in Network B Due to A-Node Failures

Owing to the coupling of the cyber-physical system, the nodes in the network B will fail due to the failure of the nodes in the network A'. The number of nodes in network B that have dependencies is

$$N'_{B2} = \left[1 - (1 - \mu_1)^3\right] \cdot N_B = \left(\mu_1^3 - 3 \cdot \mu_1^2 + 3 \cdot \mu_1\right) \cdot N_B = \mu'_2 \cdot N_B \tag{12}$$

Similar to the first step, we can obtain that the number of nodes belonging to the giant component,

$$N_{B2} = g_B\left(\mu_2^{'}\right) \cdot N_{B2}^{'} = \mu_2^{'} \cdot g_B\left(\mu_2^{'}\right) \cdot N_B = \mu_2 \cdot N_B \tag{13}$$

3.4 More Fragment in Network A′

According to the random failure of the first step, we can know that one node in network B may be connected to one, two or three nodes in network A′, or may not be connected to any node in network A′. Based on the coupled system model, the number of nodes with dependencies in the network A′ is

$$N'_{A3} = \mu_2 \cdot N_B \cdot \left[C_3^1 \cdot \mu_1 \cdot (1 - \mu_1)^2 \cdot 1 + C_3^1 \cdot (1 - \mu_1) \cdot 2 + \mu_1^3 \cdot 3\right] \Big/ \left[1 - (1 - \mu_1)^3\right] \tag{14}$$

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

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

The proportion of nodes removed from N_{A1} is equal to the same proportion of nodes removed from N'_{A1}. Then

$$N_{A1} - N'_{A3} = \left(1 - g_B\left(\mu'_2\right)\right) \cdot N_{A1} = \left(1 - g_B\left(\mu'_2\right)\right) \cdot N'_{A1} \tag{16}$$

Thus the number of nodes belonging to the giant component in N'_{A3} can be found,

$$N_{A3} = \mu'_3 \cdot g_A\left(\mu'_3\right) \cdot N_A = \mu_3 \cdot N_A \tag{17}$$

3.5 Further Cascading Failures on Network B Once Again

Similar to the second step, we can find the number of nodes with dependencies in the remaining nodes in network B

$$N'_{B4} = \left[1 - (1 - \mu_3)^3\right] \cdot N_B = \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right) \cdot N_B \tag{18}$$

As with the third step of the analysis process, we can obtain

$$N_{B2} - N'_{B4} = \left[1 - \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right)/\mu_2\right] \cdot N'_{B2} \tag{19}$$

Therefore, the fraction of the total failed nodes in network B is

$$\begin{aligned} &1 - \mu'_2 + \mu'_2 \cdot \left[1 - \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right)/\mu_2\right] \\ &= 1 - \mu'_1 \cdot \left(\mu_3^2 - 3 \cdot \mu_3 + 3\right) \cdot g_A(\mu'_3) \end{aligned} \tag{20}$$

According to the previous analysis of the cascading failure process, we can know the number of nodes in the network after each cascading failure. We can use the following equations to represent

$$\begin{cases} \mu'_{2i} = \mu'_1 \cdot \left(\mu_{2i-1}^2 - 3 \cdot \mu_{2i-1} + 3\right) \cdot g_A\left(\mu'_{2i-1}\right) \\ \mu'_{2i+1} = \mu'_1 \cdot g_B\left(\mu'_{2i}\right) \end{cases} \tag{21}$$

Where $\mu'_1 = p$. Using a similar analysis process, we can get the iterative equations under different connection ways. When the connection ratio between networks is 2:1, the iterative equation for cascading failure is

$$\begin{cases} \mu'_{2i} = \mu'_1 \cdot (2 - \mu_{2i-1}) \cdot g_A\left(\mu'_{2i-1}\right) \\ \mu'_{2i+1} = \mu'_1 \cdot g_B\left(\mu'_{2i}\right) \end{cases} \tag{22}$$

4 Numerical Simulation and Analysis

4.1 Equation Solving

For the cascading failure of the coupled system, the network will not fail again when the cascading failure stops. So we can get the following equations:

$$\begin{cases} \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} \tag{23}$$

In order to facilitate the analysis of iterative formulas for cascading failure, we define two variables x, y that satisfy the following equations

$$\begin{cases} y = \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ x = \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} (0 \le \mathrm{x}, \mathrm{y} \le 1) \tag{24}$$

Because of the complexity of the degree distribution of the network, it is difficult to solve this equation, so we use the method of drawing to find the approximate solution. First, we will write the Eq. (21) as the equations as follows:

$$\begin{cases} \mathrm{z} = \mathrm{x} \\ z = p \cdot g_B\left[p \cdot \left((x \cdot g_A(x))^3 - 3 \cdot x \cdot g_A(x) + 3\right) \cdot g_A(x)\right] \end{cases} \tag{25}$$

Then we will draw the two lines in the figure according to the two equations in Eq. (25). It is the solution of Eq. (21) when the two lines are tangent. As shown in Fig. 1.

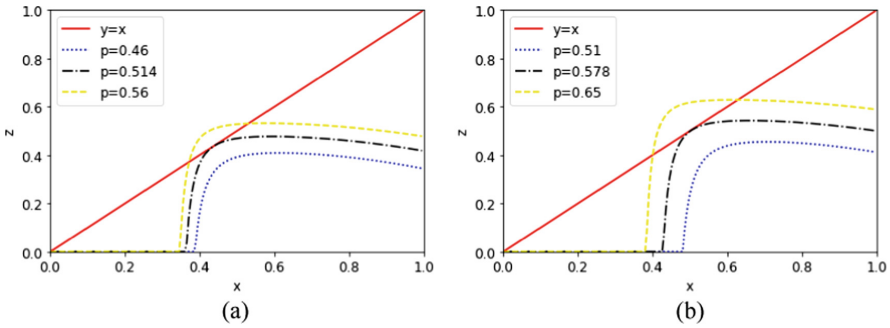

Fig. 1. Solving iterative equations

We take three values of p to represent the trend of curve change in Fig. 1. We can get more accurate theoretical solution by calculating the distance between curve and straight line. We can know that the critical threshold $p_c = 0.514$ when $\alpha = 1$ in Fig. 1(a). The curve and the straight line have no intersection point in the interval of (0, 1). When the value is equal to the critical threshold p_c, the curve is tangent to the straight line. When the value of p is greater than the critical threshold p_c, the curve has two intersection points with the straight line. In Fig. 1(b), we know that the critical threshold $p_c = 0.578$ when $\alpha = 2$. And the Figs. 1(a) and (b) have similar laws. Then we use the same method to find the critical threshold under different connection ratios. From Fig. 2 we can get $p_c = 0.557$ when $\alpha = 1$ and $p_c = 0.614$ when $\alpha = 2$ corresponding to Figs. 2(a) and (b) respectively under $N_A : N_B = 2 : 1$. We also know that $p_c = 0.49$ when $\alpha = 1$ and $p_c = 0.559$ when $\alpha = 2$ corresponding to Figs. 2(c) and (d) respectively under $N_A : N_B = 4 : 1$. So far we have obtained the theoretical solution of the coupled system. In order to ensure the correctness of the results, we will verify the correctness of the results through simulation experiments.

4.2 Simulation and Analysis

In order to verify the correctness of the results through numerical simulation, we use the probability equations presented above to represent target attacks. In the process of simulating cascading failure, the number of nodes after each cascading failure will be saved in the file to facilitate analysis of the data. When no nodes are deleted in the two networks that make up the coupled network, the cascading failure is considered to have stopped. When the cascading failure stops, we will count the number of the remaining nodes in the two networks at the end of cascading failure.

In Figs. 3(a) and (b) we take the average degree of nodes of the two networks that make up a coupled system is $\langle k \rangle = 4$. But the parameter α in the probability equation is

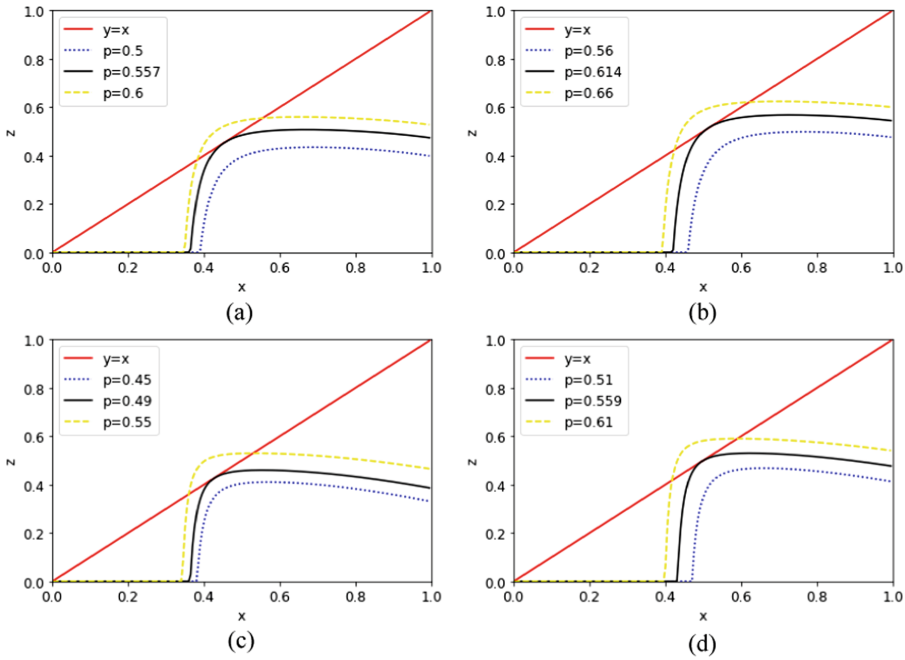

Fig. 2. Critical threshold solution

taken as 1 and 2 respectively. The proportion of nodes that were attacked was (1-p). The ordinate indicates the fraction of nodes remaining in the two networks when the cascade fails. In the process of simulating the cascading failure, in order to ensure the correctness of the experiment, we take the average value after repeat the 50 experiments for each p value. Moreover, we take two sets of p values near the critical threshold to better observe the reliability of the coupled system near the critical threshold. It shows that the reliability of the network is lower. The increase of α indicates that the probability of a node with larger degree being attacked is increasing. The reduced reliability of the network indicates that the experimental results are consistent with our expected results, and proving that our conclusions are correct. Comparing Fig. 3(a) with Fig. 3(c), we can see that as the average of the network increases, the critical threshold p_c decreases, and the decrease of the critical threshold indicates that the reliability of the coupled system is increasing. We have known that the connection between networks becomes closer when the degree of network increases, so the reliability of the coupled network will increase.

In the vicinity of the critical threshold that the position represented by the black arrow in Figs. 3(a), (b) and (c), we can see that when the value of p is greater than the critical threshold, the change trend of the two networks is close to a straight line. This phenomenon shows that the number of the remaining nodes in the network increases rapidly when the value of p increases near the critical threshold. This behavior is

characteristic of a first-order phase transition. From Fig. 3, we can see that the above curve represents the proportion of the remaining nodes in network B, and the following curve shows the proportion of the remaining nodes in network A. Since the network attack occurs in network A, we can see that the proportion of nodes in network

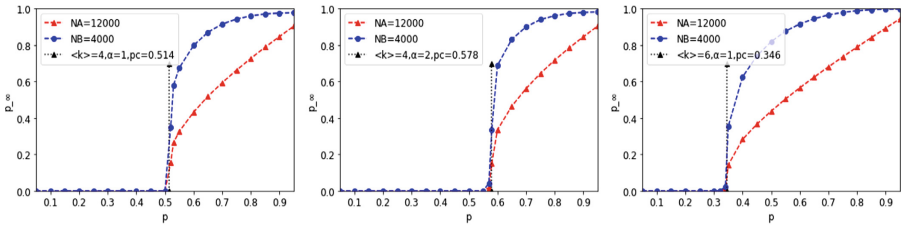

Fig. 3. The fraction of survival nodes in both networks

In Fig. 4 we select multiple values near the critical threshold. For example, when $\alpha = 1$ and $\langle k \rangle = 4$, the critical threshold is $p_c = 0.514$, we take some point for every 0.005 interval in the [0.50, 0.56] area in Fig. 4(a), and perform 50 experiments every point. And we will count the number of times the coupling system has not completely collapsed; the resulting data is represented finally by Fig. 4(a). In Fig. 4(b), we take $\alpha = 2$, and the remaining parameters are the same as in Fig. 4(a). From Figs. 4(a) and (b), we can see that the number of nodes for the coupled system increases from small to large, and as the number of nodes increases, the curve approaches the critical threshold. The critical threshold is indicated by a black arrow in the Fig. 4. We can see that the curve will produce a first-order phase transition near the critical threshold, which is completely different from the second-order phase transition in a single network when the number of nodes is large enough, which is similar to the phenomenon in Fig. 3.

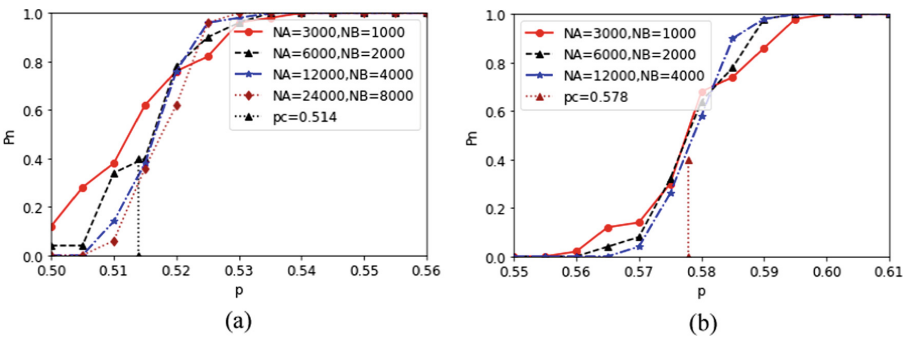

Fig. 4. The probability of having a giant component

5 Conclusion and Future Work

This paper proposes an analysis model and security assessment indicators for cyber-physical systems. Under the target attack strategy, the cascading failure process of the cyber-physical system for the attack behavior is analyzed. 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 CPS environment obeys the scale-free distribution. 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 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. Zhang, Y.: Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **11**(1), 88–95 (2017)
2. Zhang, Y.: Agent and cyber-physical system based self-organizing and self-adaptive intelligent shop floor. IEEE Trans. Ind. Inform **99**, 1 (2017)
3. Cintuglu, M.H.: A Survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv Tutorials **19**(1), 446–464 (2017)
4. Li, B.: DDOA: a Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Trans. Inf. Forensics Secur. **11**(11), 2415–2425 (2016)
5. Li, B.: Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. J. Parallel Distrib. Comput. **103**, 32–41 (2016)
6. Yağan, O.: Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures, and robustness. IEEE Trans. Parallel Distrib. Syst. **23** (9), 1708–1720 (2012)
7. Saad, W., Saad, W., Maham, B.: A colonel blotto game for interdependence-aware cyber-physical systems security in smart cities. In: International Workshop on Science of Smart City Operations and Platforms Engineering, pp. 7–12. ACM (2017)
8. Zeng, X.: E-AUA: an efficient anonymous user authentication protocol for mobile IoT. IEEE Internet Things J. **99**, 1 (2018)
9. 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)
10. Zhang, G.: Cascading failures of power grids caused by line breakdown. Int. J. Circuit Theory Appl. **43**(12), 1807–1814 (2016)
11. Liao, W.: Cascading failure attacks in the power system: a stochastic game perspective. IEEE Internet Things J. **4**(6), 2247–2259 (2017)

12. Xu, G.: An algorithm on fairness verification of mobile sink routing in wireless sensor network. Pers. Ubiquit. Comput. **17**(5), 851–864 (2013)
13. Dey, P.: Impact of topology on the propagation of cascading failure in power grid. IEEE Trans. Smart Grid. **7**(4), 1970–1978 (2017)
14. Zhang, X.: Modeling the dynamics of cascading failures in power systems. IEEE J. Emerg. Sel. Top. Circuits Syst. **7**(2), 192–204 (2017)
15. Yazdi, M.: Failure probability analysis by employing fuzzy fault tree analysis. Int. J. Syst. Assur. Eng. Manage. **8**(2), 1–17 (2017)
16. Rampurkar, V.: Cascading failure analysis for indian power grid. IEEE Trans. Smart Grid **7** (4), 1951–1960 (2016)
17. Younes, M.B.: A performance evaluation of a fault-tolerant path recommendation protocol for smart transportation system. Wirel. Netw. **11**, 1–16 (2016)
18. Sanislav, T., Zeadally, S., Mois, G.: Multi-agent architecture for reliable Cyber-Physical Systems (CPS). In: Computers and Communications, pp. 170–175. IEEE (2017)
19. Yang, G.: Synchronization control of cyber physical systems during malicious stochastic attacks. J. Tsinghua Univ. **1**, 14–19 (2018)
20. Chen, X., Zhou, Y., Zhou, H.: Analysis of production data manipulation attacks in petroleum cyber-physical systems. In: International Conference on Computer-Aided Design, p. 108. ACM (2016)
21. Sabaliauskaite, G., Mathur, A.P.: Aligning cyber-physical system safety and security. In: Cardin, M.A., Krob, D., Lui, P., Tan, Y., Wood, K. (eds) Complex Systems Design & Management Asia, pp. 41–53. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-12544-2_4
22. Fang, Y., Zio, E.: Optimizing the resilience of interdependent infrastructure systems against target attacks. In: International Conference on System Reliability and Safety, pp. 62–67. IEEE (2018)