Hindawi
Security and Communication Networks
Volume 2022, Article ID 1800434, 10 pages
https://doi.org/10.1155/2022/1800434

Research Article

Security Situation Awareness Assessment of Heterogeneous Cyber-Physical Systems in Multiple Load Mode

Xing Yang,[1] Ziyi Xie,[2] Zhen Qian,[2] Xuhong Zhang,[3] Dandan Zhao,[2] Songyang Wu,[4] Hao Peng,[2] Dongtao Zhu,[1] and Zhenyu Liang[1]

[1]*State Key Laboratory of Pulsed Power Laser Technology, Advanced Laser Technology Laboratory of Anhui Province, Electronic Countermeasure Institute, National University of Defense Technology, Hefei 230037, China*
[2]*Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, China*
[3]*Zhejiang University and Binjiang Institute of Zhejiang University, Hangzhou, Zhejiang, China*
[4]*The Third Research Institute of Ministry of Public Security, Shanghai 201204, China*

Correspondence should be addressed to Songyang Wu; wusongyang@stars.org.cn

Received 5 September 2022; Revised 27 September 2022; Accepted 28 September 2022; Published 13 October 2022

Academic Editor: Shudong li

As the Internet of Things technology develops rapidly, cyber-physical systems (CPSs) have provided critical technologies in the industrial field. A smart grid is a typical application of the CPS, which is formed by the coupling of the power network and communication network. In general, the two networks are heterogeneous. Considering the characteristics of the power network, the ordinary percolation network model is not suitable for the network carrying physical flow. Therefore, we propose an interdependent network model with a load. That is, nodes in the physical network have loaded. Then, we research the security of CPS under the multi-load mode. The rule for node failure is different from the percolation model. When a node's load exceeds its capacity, the node fails. Through the theoretical analysis, we obtained the iterative equation of the percolation threshold and analyzed it through simulation experiments. We adopt both linear and nonlinear capacity models. It is found that appropriately increasing the average degree of ER network can improve its ability to resist attacks. In contrast, the power exponent of the SF network has less influence on the critical value of network percolation. In addition, we found that increasing the capacity parameter in the linear capacity model can improve the robustness of the network, where the variation of the ER-ER network is more evident than that of the SF-SF network. Increasing the capacity parameter in the nonlinear capacity model can significantly increase the network's ability to resist attacks. However, due to the increase in economical cost, we can improve the network's reliability by increasing the node capacity while controlling the cost.

1. Introduction

With the rapid development of the Internet and communication technology, the Internet of Things has attracted widespread attention[1–12]. The Industrial Internet of Things is the deep integration of the Internet of Things technology in industrialization and informatization. In the industrial field, through computing, communication, and control, cyber-physical system [13] provides information services for industrial control systems, such as intelligent perception and dynamic control. Today, the modern industrial development is more and more intelligent and informationized, and CPS provides new opportunities in technology and has been widely used in monitoring and control fields [14], intelligent transportation systems [15, 16], and intelligent aerospace [17].

CPS provides data services through computing resource network and physical resource network. Data transmission becomes increasingly coupled with the increasing integration of physical devices and communication networks. We usually model the CPS as two interdependent networks: the physical network and the communication network [18–20]. Due to the interdependence and complexity of the network [21, 22], the failure of a node in one network will not only

affect the network's connectivity but also affect the nodes interacting with it in another network. The node failure chain reaction occurs between the two networks, resulting in cascading failures [23]. Therefore, it is necessary to study CPS's safety and robustness.

Chen et al. [24] employed random network and IEEE Standard Bus test case to model CPSs and studied the robustness of cyber-physical power systems under various attack scenarios. They found that considerable clusters, respectively, in physical power grid and communication network are mutually interdependent to survive in cascading failure. Also, targeted attack disintegrates systems into more clusters than random attack, but with less nodes remaining than random attack. Liu et al. [25] studied a converged railway network composed of railways, regional railways, and urban rail transit. They found that with targeted attacks on the highest connected nodes of the coupled network, the robustness decreased as the number of network layers increased. Peng et al. [26] studied the robustness of cyber-physical systems under deliberate attacks, where nodes between networks are connected in a one-to-many ratio. Under the same parameters, they found that the threshold of preferentially attacking SF network is always smaller than that of preferentially attacking ER network, and the security of network is higher. Yang et al. [27] optimized the modelling method of the cyber-physical system, and the connection ratio of nodes between networks was many-to-many. Under the same attack parameters, they found that the threshold of the ER-ER network is larger than that of the SF-SF network, and the power exponent has little effect on the robustness of the network.

We found that the percolation network model [28–30] is unsuitable for physical flow networks. For example, cascading failures arise from the reorganization of flows in electric power grids [31]. Here, the network links have some fixed capacity, and percolation theory provides an abstracted model of vulnerability and cascades in the power grid but neglects the dynamics of flows and the capacities on links. Therefore, this paper proposes an interdependent CPS model with load [32–34]. We assign initial load and capacity to nodes in the physical network and specify load redistribution rule when nodes fail. In this model, the communication and physical networks have different cascading rules. A node in the communication network survives when it belongs to the giant connected component. In the physical network, the survival of a node considers whether the node's current load exceeds its capacity. When the node's load does not exceed its capacity, the node survives. Otherwise, the node fails. On the interdependent physical network and communication network, we analyze the cascading failures of CPS, where the physical network has load characteristics and the communication network has percolation characteristics.

2. Proposed Model

In the network, the load-capacity model [21, 22] allocates a certain initial load and capacity to nodes or edges and redistributes load of faulty nodes according to the load redistribution rule. A general load-capacity model consists of three essential elements: initial load, capacity, and load redistribution. A CPS usually consists of a communication network and a coupled physical network. Nodes inside the network are randomly connected, and the two networks have no degree correlation. We optimize the physical network according to the load-capacity model and assign initial load and capacity to nodes. Then, we build an interdependent CPS model with load, as shown in Figure 1.

We set the network A to be a physical network composed of nodes $\{a_1, a_2, \ldots, a_N\}$, and the number of nodes is N. Based on the load-capacity model, we assign an initial load and capacity to each node a_i and define the load redistribution rule:

(i) Initial load: we define $L_i(z) = \alpha \cdot z^{-\eta}$ as the initial load of node a_i, where α and η are constants and z is the degree of node a_i.

(ii) Capacity: load-capacity models include linear and nonlinear load-capacity models. The linear capacity of node a_i is defined as $C_i = (1+\beta) \cdot L_i^0$, where $\beta \rangle 0$ is the capacity parameter and L_i^0 is the initial load of node a_i. The nonlinear capacity is defined as $C_i = L_i^0 + \beta \cdot (L_i^0)^\gamma$, where $\beta \rangle 0$ and $\gamma \rangle 0$ are the capacity parameters.

(iii) Load redistribution rule: after a node is attacked and fails, its own load will be redistributed to other nodes. There are several redistribution rules: load average redistribution rule for the remaining nodes; load average redistribution rule for neighbour nodes; difference load redistribution rule; initial load redistribution rule [35]. In the network, when a node fails, its neighbor nodes are often the most easily affected, so it is reasonable and practical to redistribute the failed node's load to its neighbor nodes. In a random network, the degree distribution of nodes is relatively uniform, and evenly distributing the load of the failed node to its neighbor is not easy to cause the failure of the neighbor nodes. So in this paper, we adopt the second allocation rule. Assuming that the load carried by the node a_i before the failure is L_i, it has m neighbor nodes, and then when a_i fails, each neighbor node a_j received additional payload $\Delta L_{ji} = L_i/m$. If the node a_j receives an additional load and the load exceeds its capacity, it will cause the node to fail, and the load of the faulty node will be further redistributed to the neighbor nodes.

In the physical network, the node is functional when its load does not exceed capacity. We set the network B to be a communication network composed of nodes $\{b_1, b_2, \ldots, b_M\}$, and the number of nodes is M. In the communication network, the node is functional when it belongs to the giant connected component [36, 37].

Assuming that the initial failure occurs on the network A, the load of the failed node is transferred to other nodes according to the load redistribution rule. If a node receives additional load beyond its capacity, that node will also fail,

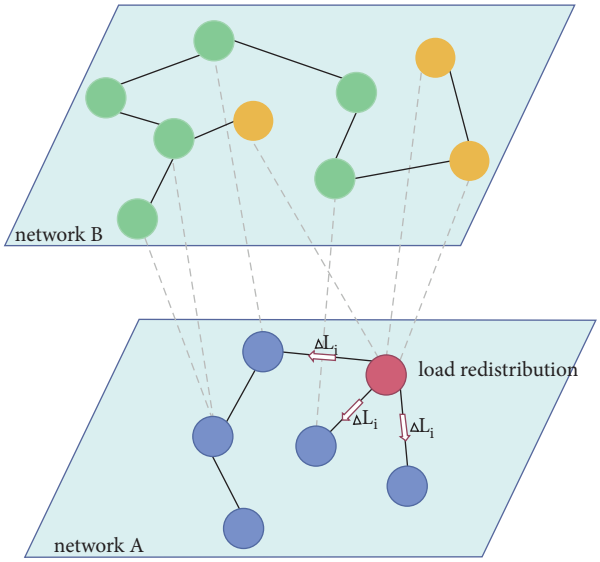

Figure 1: Model of an interdependent CPS with a load. When the red node in network A fails, its load is evenly distributed to the neighbor nodes, and the red node and its connected edges are deleted. The yellow node in network B fails by losing a dependent edge.

and its load will be further redistributed to other nodes. In the network B, those nodes connected to the failed nodes in the network A will fail due to the loss of dependent edges. After deleting the faulty node, those nodes not part of the giant connected component will also be deleted. Failed nodes of B, in turn, affect nodes in A, causing cascading failures in the interdependent networks A and B. An illustration of fault propagation is shown in Figure 2.

3. Proposed Method

The conditions for node survival are different in the physical and communication networks, so our methods for calculating the proportion of functional nodes in the giant connected components are also different. In the network A, we define several random variables and events. (1) Z_i is a random variable and represents the number of neighbor nodes of node i. (2) X_i is a random variable and represents the number of neighbor nodes that make i fail by transferring its load. (3) $\mathbf{O}_i$ is an event and indicates that i fails due to transferring the extra load of neighbor nodes.

Under the condition of $X = x$, when the load transferred from x neighbor nodes plus a load of node i itself exceeds its capacity, the probability of event $\mathbf{O}$ occurring is 1. Otherwise, it is 0, which is

$$P(\mathbf{O}|X = x) = \begin{cases} 1, & x > \dfrac{(T-1)\cdot\alpha\cdot z^{\eta}}{\sum_0 \alpha\cdot z^{\eta}/z}, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Under the condition of $Z = z$, the probability of taking out x neighbor nodes is

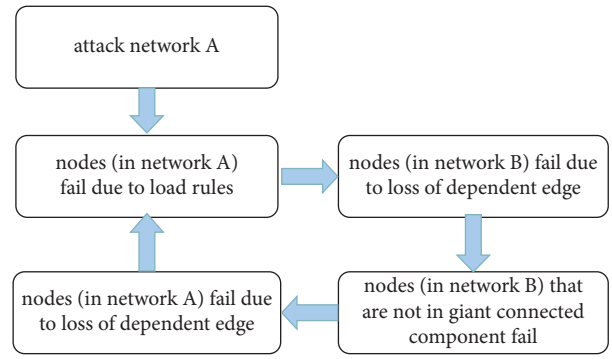

Figure 2: Process illustration of fault propagation in the model of interdependent CPS.

$$P(X = x \mid Z = z) = \frac{1}{2^z}\binom{z}{x}. \tag{2}$$

Further, under the condition of $Z = z$, we get the probability of event O:

$$P(\mathbf{O} \mid Z = z) = \sum_{x=0}^{z} P(\mathbf{O} \mid X = x)\cdot P(X = x \mid Z = z). \tag{3}$$

We define u to represent the probability that node i cannot reach the functional component through its neighbors. In the network, when we delete $(1-\varphi)$ proportion of nodes, there are two cases where the node does not belong to the functional component. (1) The node is deleted, and the probability is $(1-\varphi)$. (2) The node is overloaded and fails due to receiving additional loads from neighbor nodes, with the probability of $\varphi\cdot u^z\cdot P(\mathbf{O}|Z=z)$. We define the event $\mathbf{E}(\varphi)$ as a node that is not the functional node in the network, and its probability is

$$P(\mathbf{E}(\varphi)) = 1 - \varphi + \varphi\cdot u^z\cdot \mathrm{P}(\mathbf{O} \mid Z = z). \tag{4}$$

After removing the nodes of $(1-\varphi)$, the probability that nodes in the remaining network belong to functional nodes is $\sum_0 P_d(z)\cdot(1 - P(\mathbf{E}(\varphi)))$. $P_d(z)$ is the probability function of the network degree distribution. In the initial network A, the proportion of functional nodes among remaining nodes is

$$\begin{aligned} J(\varphi, A) &= \frac{\sum_0 P_d(z)\cdot(1 - P(\mathbf{E}(\varphi)))}{\varphi}, \\ &= \sum_0 P_d(z)\cdot\left(1 - u^z\cdot P(\mathbf{O} \mid Z = z)\right). \end{aligned} \tag{5}$$

The expression of u can be obtained by calculation:

$$u = \sum_{z=0} Q(z)\cdot\left(1 - \varphi + \varphi\cdot u^z\cdot P(\mathbf{O} \mid Z = z)\right), \tag{6}$$

where $Q(z) = (z+1)\cdot P_d(z+1)/z$, and then we can obtain the functional node ratio $J(\varphi, A)$ of the nodes in the network A after the load is propagated.

According to the theoretical process derived by Buldyrev et al. [38], we consider two interdependent networks A and

Table 1: Proportion of remaining functional nodes at each stage in the cascading failure.

	Network A	Network B
The first stage	$\varphi_1' = p$ $\varphi_1 = \varphi_1' \cdot g_A(\varphi_1')$	
The second stage		$\varphi_2' = \varphi_1' \cdot (\varphi_1^2 - 3 \cdot \varphi_1 + 3) \cdot g_A(\varphi_1')$ $\varphi_2 = \varphi_2' \cdot g_B(\varphi_2')$
The third stage	$\varphi_3' = \varphi_1' \cdot g_B(\varphi_2')$ $\varphi_3 = \varphi_3' \cdot g_A(\varphi_3')$	
The fourth stage		$\varphi_4' = \varphi_1' \cdot (\varphi_3^2 - 3 \cdot \varphi_3 + 3) \cdot g_A(\varphi_3')$ $\varphi_4 = \varphi_4' \cdot g_B(\varphi_4')$
...	...	...
The 2i stage		$\varphi_{2i}' = \varphi_1' \cdot (\varphi_{2i-1}^2 - 3 \cdot \varphi_{2i-1} + 3) \cdot g_A(\varphi_{2i-1}')$ $\varphi_{2i} = \varphi_{2i}' \cdot g_B(\varphi_{2i}')$
The 2i+1 stage	$\varphi_{2i+1}' = \varphi_1' \cdot g_B(\varphi_{2i}')$ $\varphi_{2i+1} = \varphi_{2i+1}' \cdot g_A(\varphi_{2i+1}')$	

B. Under random failure, the probability function of a node in the network A belonging to a giant connected component is

$$g_A(p) = 1 - G_{A0}[1 - p \cdot (1 - f_A)], \tag{7}$$

where p is the proportion of surviving nodes in the network A and $f_A = G_{A1}(1 - p \cdot (1 - f_A))$. $G_{A0}(x) = \sum_k P_A(k) \cdot x^k$ is the generating function of A degree distribution of the network, and $G_{A1}(x) = G_{A0}'(x)/G_{A0}'(1)$ is the generating function of the residual network degree distribution. Similarly, the probability function of a node in the network B belonging to a giant connected component is

$$g_B(p) = 1 - G_{B0}[1 - p \cdot (1 - f_B)]. \tag{8}$$

Table 1 shows the proportion of remaining functional nodes at each stage in the cascading failure process of networks A and B.

φ is the proportion of remaining functional nodes. Cascading failure process reaches a steady state when the following equations are satisfied:

$$\begin{cases} \varphi_{2i}' = \varphi_{2i-2}' = \varphi_{2i+2}', \\ \varphi_{2i+1}' = \varphi_{2i-1}' = \varphi_{2i+3}'. \end{cases} \tag{9}$$

We define the variables $0 \le x, y \le 1$ to satisfy the above equations, namely, $x = \varphi_{2i}' = \varphi_{2i-2}' = \varphi_{2i+2}'$ and $y = \varphi_{2i+1}' = \varphi_{2i-1}' = \varphi_{2i+3}'$. According to the derivation in the table, we further get the following equations:

$$\begin{cases} y = p \cdot \left((x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right) \cdot g_A(x), \\ x = p \cdot g_B(y). \end{cases} \tag{10}$$

Substitute y into x to get

$$x = p \cdot g_B\left(p \cdot \left((x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right) \cdot g_A(x)\right). \tag{11}$$

This equation cannot be directly solved analytically. We define the following equation system, the intersection of the two curves is the numerical solution, and then the size of the giant connected component in the network B is obtained:

$$\begin{cases} s = x, \\ s = p \cdot g_B\left(p \cdot \left((x \cdot g_A(x))^2 - 3 \cdot x \cdot g_A(x) + 3 \right) \cdot g_A(x)\right). \end{cases} \tag{12}$$

In network A, we replace $g_A(x)$ with $J(\varphi, A)$, and (12) changes to the following equations:

$$\begin{cases} s = x, \\ s = p \cdot g_B\left(p \cdot \left((x \cdot J(\varphi, A))^2 - 3 \cdot x \cdot J(\varphi, A) + 3 \right) \cdot J(\varphi, A)\right). \end{cases} \tag{13}$$

Theoretically, the theoretical value can be solved in the equation, but the equation is transcendental and cannot be solved exactly.

4. Experiments

In this paper, we adopt two capacity models: linear capacity and nonlinear capacity. Two basic network types, ER-ER and SF-SF [39–41], are used to construct the interdependent CPS. Experiments simulate the changes of nodes in the CPS after being attacked. We output the survival of nodes in physical network A and communication network B while maintaining a steady state. In addition, we also analyze the power exponent and average degree of the network, as well as the influence of the capacity parameters β and γ on the network cascading failures. The networks A and B are constructed according to the node ratio of 1: 3, the number of nodes $N = 3000$, and $M = 9000$. Each node in network A depends on three nodes in network B, and each node in network B is uniquely dependent on one node in network A. We set the number of simulations for each experiment as twenty under different parameters.

4.1. Linear Capacity Model. Under the linear capacity model, we study the effect of average degree k of ER network, power exponent λ of SF network, and capacity parameter β on the robustness of the interdependent CPS.

First, we use the ER-ER and SF-SF network models to construct an interdependent CPS network with load

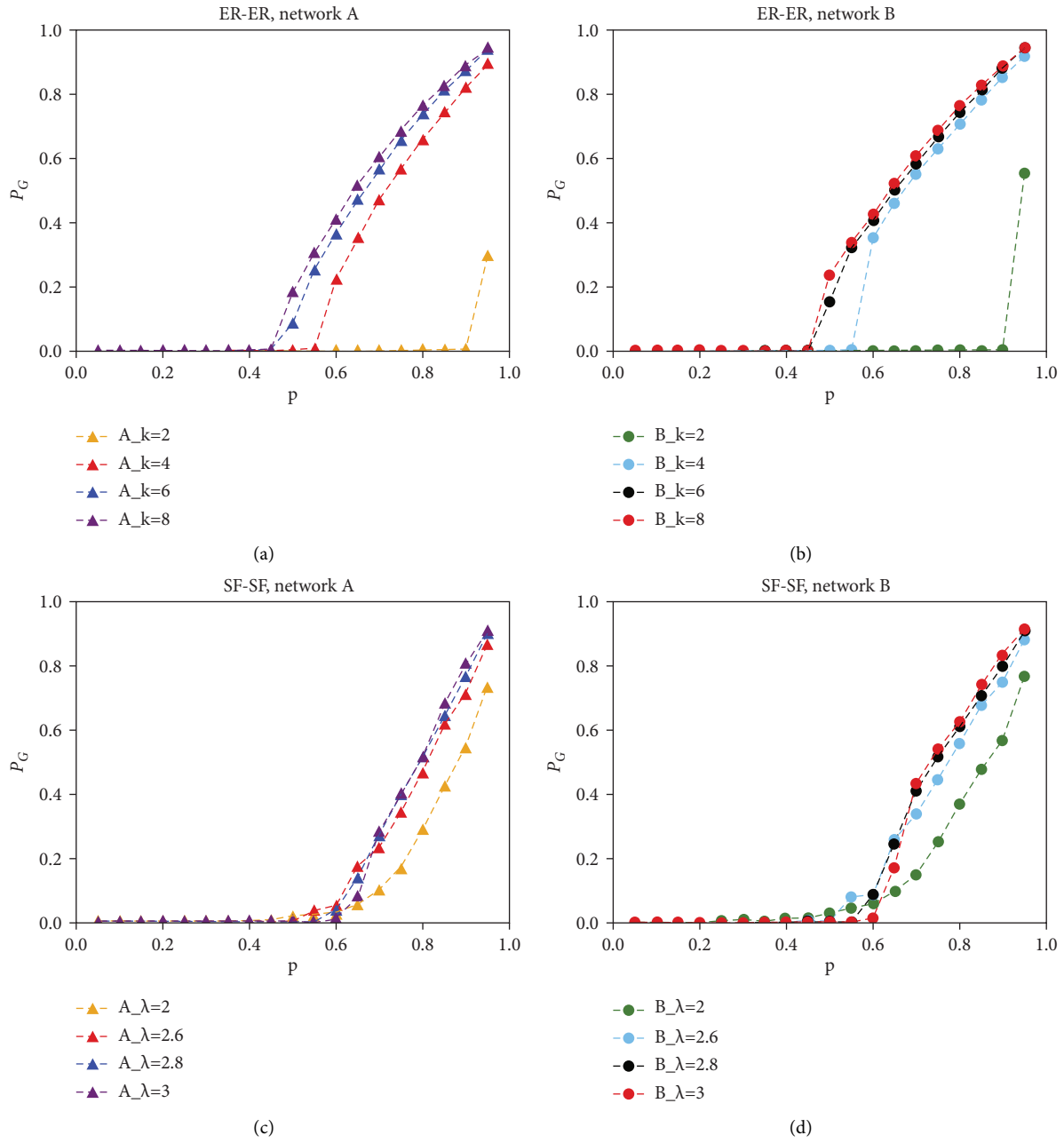

FIGURE 3: Based on the linear capacity model. (a) Change of the PG in network A when network type is ER-ER. (b) Change of the PG in network B when network type is ER-ER. (c) Change of the PG in network A when network type is SF-SF. (d) Change of the PG in network B when network type is SF-SF. Where $k = 2, 4, 6, 8$, $\lambda = 2, 2.6, 2.8, 3$, PG is the giant connected component size, p is the proportion of remained nodes.

characteristics, and set the constant $\alpha = 1.5$, $\eta = 2$, and the capacity parameter $\beta = 2$.

When the average degree of ER network $k = 2, 4, 6, 8$, as the node attack ratio $(1 - p)$ decreases, in the steady state, the change of the giant connected component size P_G of the networks A and B is shown in Figures (a)3 and 3(b). We find that when $k = 2$, the network collapses at a meagre attack ratio. With the increase of the average degree k, the network's threshold p_c has been greatly improved. In particular, when $k \geq 4$, the effect of network defence against attacks increases significantly, but as k continues to increase, the change of network robustness becomes insignificant. Comparing Figures 3(a) and (b)3 at the same value of k, we find that the performance of networks A and B is slightly different. When $k = 4, 6, 8$, under different p values, the size of P_G in network B is very close. But in network A, we can clearly see that when k increases, the size of P_G also increases. In network A, when k increases, the number of neighbors of the node also increases, and the failed node distributes less load to each neighbor, so that the neighbor node is not easy to overload and fail.

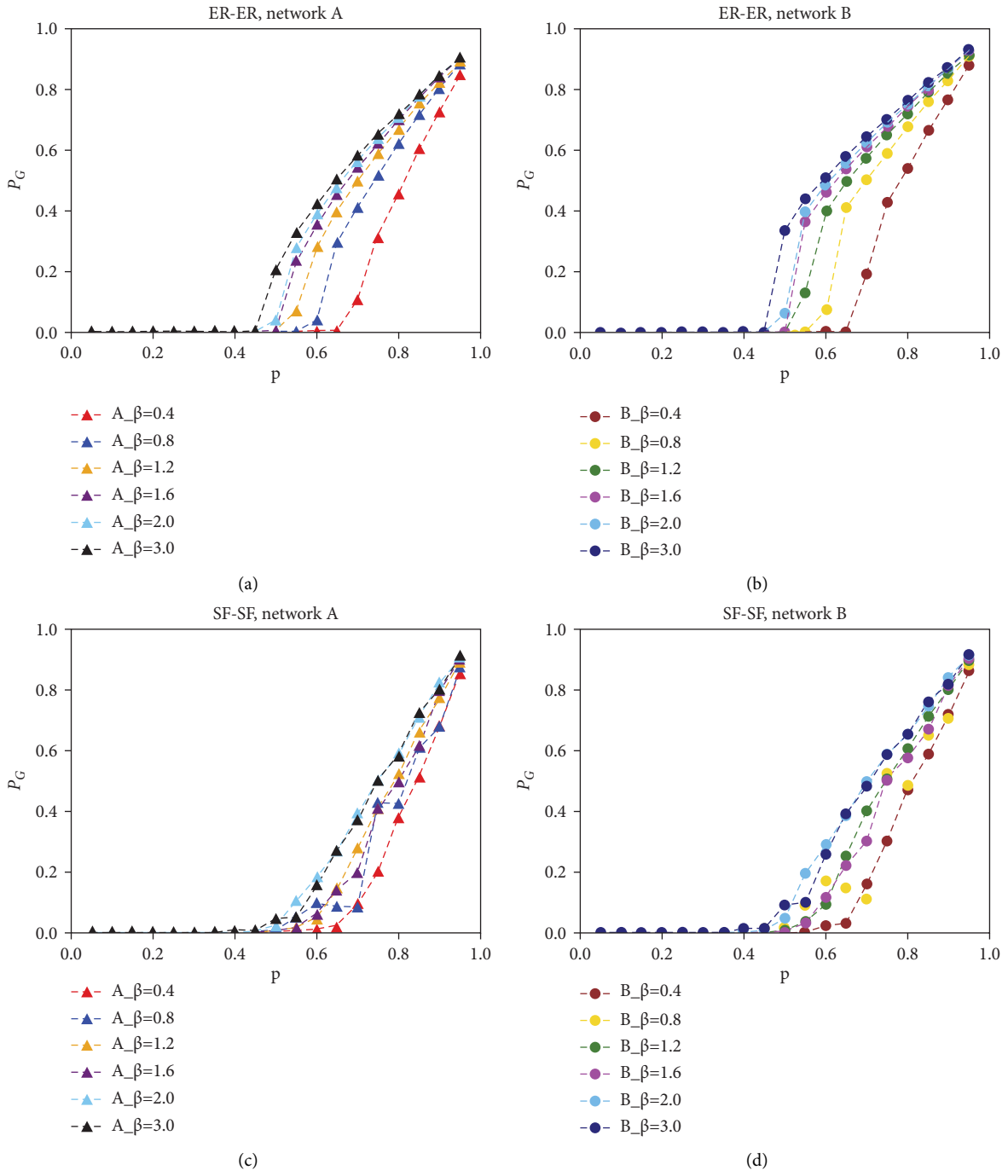

Figure 4: Based on the linear capacity model. (a) Change of the PG in network A when network type is ER-ER. (b) Change of the PG in network B when network type is ER-ER. (c) Change of the PG in network A when network type is SF-SF. (d) Change of the PG in network B when network type is SF-SF. Where k = 6, λ= 2.6, β= 0.4, 0.8, 1.2, 1.6, 2.0, 3.0, β is the capacity parameter.

When the power exponent of SF network $\lambda = 2, 2.6, 2.8, 3$, as the node attack ratio $(1 - p)$ decreases, P_G changes in networks A and B are shown in Figures 3(c) and 3(d). We found that with the increase of λ, the survival ratio of network nodes increased, but it was not obvious, and λ had less impact on the network robustness. Comparing the ER-ER and SF-SF networks, under certain conditions, we found that the percolation threshold of ER network is smaller than that of the SF network, which indicates that the ER-ER network is more resistant to random failures than the SF-SF network.

Next, we further investigate the effect of capacity parameter β on the robustness of the network. We set the average degree $k = 6$ and the power exponent $\lambda = 2.6$. We compared the changes in the survival ratio of network nodes under different capacity parameters β, as shown in Figure 4.

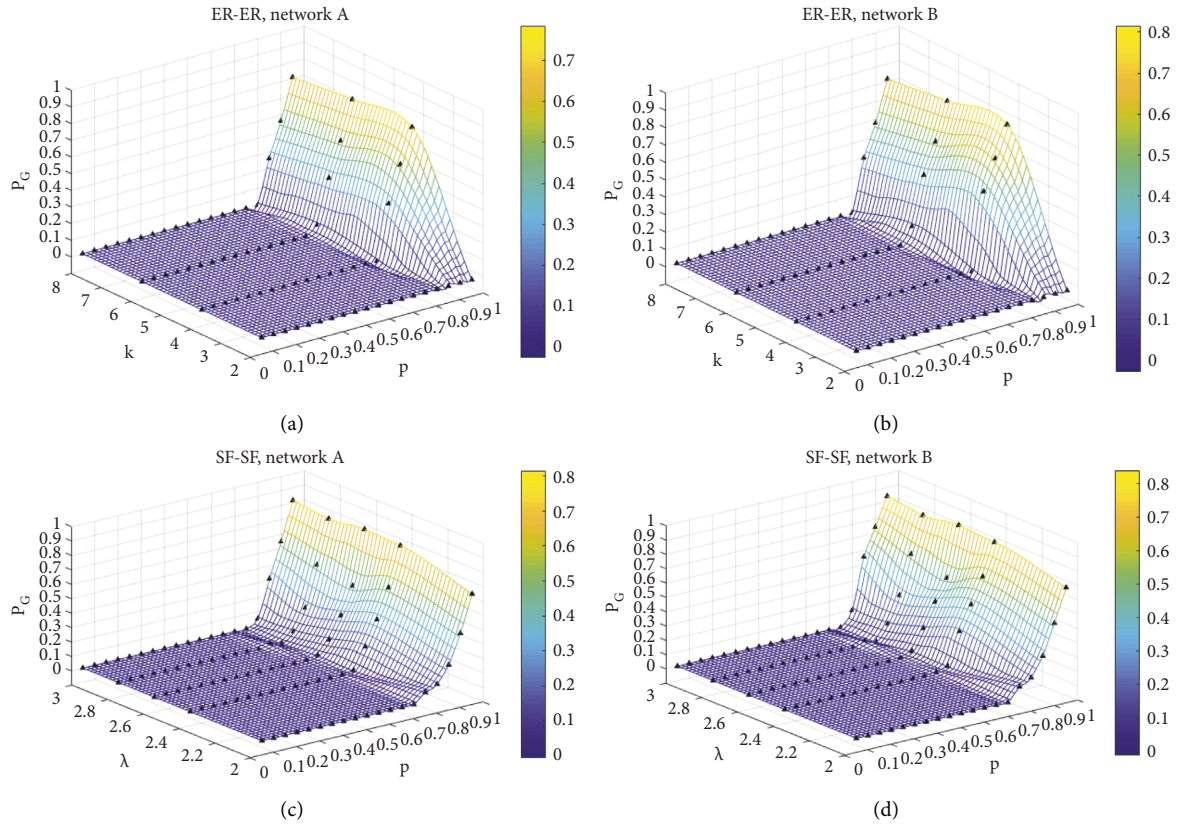

FIGURE 5: Based on the nonlinear capacity model. (a) Change of the PG in network A when network type is ER-ER. (b) Change of the PG in network B when network type is ER-ER. (c) Change of the PG in network A when network type is SF-SF. (d) Change of the PG in networ*k* B when network type is SF-SF. Where $k = 2, 4, 6, 8$, $\lambda = 2, 2.4, 2.6, 2.8, 3$.

In the ER-ER network, with the increase of β, the threshold p_c of the network also increases, indicating that increasing the capacity of nodes can improve the ability of the network to resist attacks to a certain extent. However, in the SF-SF network, the increase of β does not significantly improve the network robustness, which means that blindly increasing the capacity of network nodes cannot resist attacks well.

Comparing the two network models, we find that when β increases to a larger value, the critical value of network percolation will no longer increase. We speculate that there is a threshold for node capacity. When this threshold is exceeded, no matter how much the node's capacity is increased, it cannot effectively affect the robustness of the network.

4.2. Nonlinear Capacity Model. In this section, we study the security of the CPS network constructed based on the nonlinear capacity model through the same simulation experiments. First, we explore the effects of the average degree k of ER network and the power exponent λ of the SF network on network percolation. Set the initial load of node as $L_i(z) = \alpha \cdot z^{-\eta}$, where $\alpha = 1.5$, $\eta = 2$. The capacity of the node is $C_i = L_i^0 + \beta \cdot (L_i^0)^{\gamma}$, where $\beta = 0.4$, $\gamma = 0.7$.

When the network type is ER-ER, under different average degrees and node attack ratios, the node survival ratios corresponding to the network A and B are shown in Figures 5(a) and 5(b), respectively. The black triangles correspond to the size of the giant connected component P_G in each case. We find that when $k < 4$, the survival rate of nodes decreases rapidly, and the ability of the network to resist random failures is poor. When $k \geq 4$, the percolation threshold p_c is around 0.8, and the change is not apparent. Therefore, we speculate that appropriately increasing the average degree of ER network can improve the robustness of the network. When $k \geq 4$, continuing to increase the average degree will not have a good effect.

When the network type is SF-SF, under different power exponents and node attack ratios, the node survival ratios corresponding to the network A and B are shown in Figures 5(c) and 5(d), respectively. We found that the influence of the power exponent on network percolation is relatively weak. When λ increases from 2 to 3, the threshold changes between 0.8 and 0.9, and the ability of the network to resist attack is relatively poor.

Next, we explore the effect of capacity parameter γ on the network percolation. When the network model is ER-ER, we fix other parameters to remain unchanged, where $\alpha = 1.5, \eta = 2, \beta = 0.4$, and $k = 4$. When the capacity parameter γ takes different values, the relationship between the node survival ratio P_G (in the network A and B) and the different nodes' attack ratio $(1 - p)$ is shown in Figures 6(a) and 6(b).

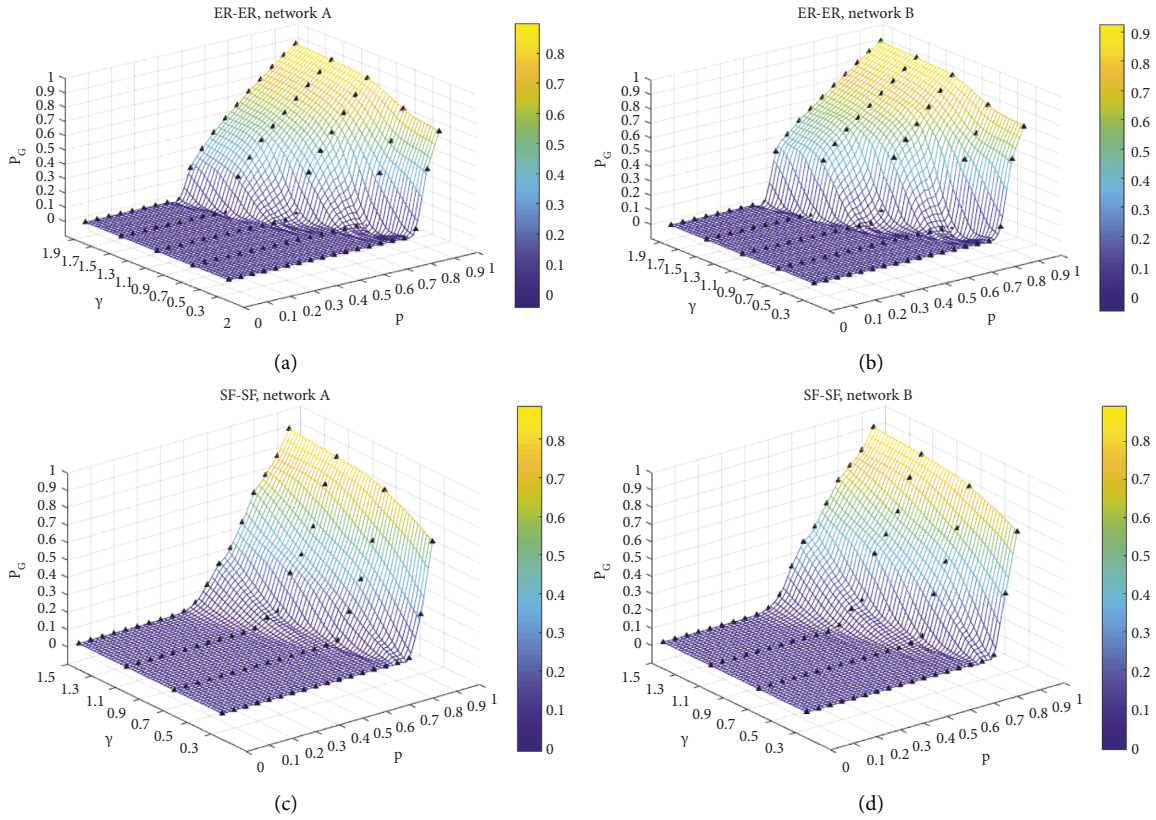

Figure 6: Based on the nonlinear capacity model. (a) Change of the PG in network A when network type is ER-ER. (b) Change of the PG in network B when network type is ER-ER. (c) Change of the PG in network A when network type is SF-SF. (d) Change of the PG in networ*k* B when network type is SF-SF. Where $k = 4$, $\lambda = 2.6$, $\gamma = 0.5, 0.9, 1.3, 1.7, 2.0$, γ is the capacity parameter.

We found that when $\gamma = 0.3$, the attack ratio that the network can withstand is around 0.2; when $\gamma = 1.5$, the attack ratio that the network can withstand is around 0.6. With the increase of γ, the percolation threshold p_c increases, and the ability of the network to withstand random attacks is significantly enhanced.

When the network model is SF-SF, set the power exponent $\lambda = 2.6$, and other parameters are the same as above. Under different capacity parameters γ, the relationship between P_G (in the network A and B) and the different attack ratio $(1 - p)$ is shown in Figures 6(c) and 6(d). We found that when $\gamma = 0.3$, the attack ratio that the network can withstand is around 0.1; when $\gamma = 1.5$, the attack ratio that the network can withstand is around 0.45. The increase of γ has a greater impact on network percolation, which can enhance the ability of the network to resist attacks. However, the increase of γ means that the node capacity must be increased, and there is a certain pressure on the economic cost. Therefore, appropriately increasing the node capacity can make the network better resist random attacks in the case to control the cost.

Compared with the ER-ER and SF-SF networks, the ER-ER type network can withstand more attacks under the same capacity parameter γ. This is because of the characteristics of scale-free networks. The degree value of a small number of nodes is substantial. Once these critical nodes fail, the network often faces more significant risks. Further, we focus on the performance of networks A and B under different capacity parameters. Whether in the ER-ER network or SF-SF network, the size of P_G in network A is similar to that in network B under different p. We guess that the nature of the nonlinear capacity model makes the failure effect of nodes in network A similar to those in network B.

5. Conclusions

In this paper, we model a cyber-physical system to study network percolation under different conditions. We obtained the iterative equation of the theoretical network threshold through theoretical analysis and conducted simulation experiments.

We propose a new CPS network model: the physical network has a load characteristic in two interdependent networks. Nodes are assigned loads and capacities, and we determine the load redistribution rule. The node failure rule in the physical network differs from the percolation model. When a node's load exceeds its capacity, it will fail due to overloading. In addition, we also consider linear and nonlinear capacity models, in which the network behaves slightly differently. We found that the average degree of the ER network can affect the critical value of percolation in the network to a certain extent. In contrast, the power exponent of the SF

network has a weak effect on the critical value. However, blindly increasing the average degree will not be very effective in improving the network's ability to resist attacks. In the linear capacity model, we found that increasing the capacity parameter β can reduce the percolation threshold and improve the robustness of the network. Among them, the change in the ER-ER network is more evident than in the SF-SF network. In the nonlinear capacity model, we found that increasing the capacity parameter γ can reduce the percolation threshold and improve the network's ability to resist attacks.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was partly supported by the National Key Research and Development Program of China under grant no. 2019YFC0118800, the National Natural Science Foundation of China under grant nos. 62072412, 61902359, 61702148, and 61672468, the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security under grant no. AGK2018001, and the Key Lab of Information Network Security, Ministry of Public Security, under grant no. C20607.

References

[1] Y. W. Wang, C. Chen, Z. W. Chen, and J. J. He, "Attribute-based user revocable data integrity audit for internet-of-things devices in cloud storage," *Security and Communication Networks*, vol. 2020, Article ID 8837456, 10 pages, 2020.

[2] J. T. Ning, G. S. Poh, X. Y. Huang, R. Deng, S. W. Cao, and E. C. Chang, "Update recovery attacks on encrypted database within two updates using range queries leakage," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1–1180, 2020.

[3] S. Shan, "Cryptanalysis of a certificateless hybrid signcryption scheme and a certificateless encryption scheme for Internet of Things," *Security and Communication Networks*, vol. 2022, Article ID 6174031, 6 pages, 2022.

[4] J. T. Ning, J. Xu, K. T. Liang, F. Zhang, and E. C. Chang, "Passive attacks against searchable encryption," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 789–802, 2019.

[5] W. C. Ding, W. B. Zhai, L. Liu, Y. Gu, and H. Gao, "Detection of packet dropping attack based on evidence fusion in IoT networks," *Security and Communication Networks*, vol. 2022, pp. 1–14, Article ID 1028251, 2022.

[6] M. O. Rahman, M. A. Kashem, A. A. Nayan et al., "Internet of Things (IoT) based ECG system for rural health care," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, pp. 470–477, 2021.

[7] H. Wu, H. Tian, S. S. Fan, and J. Z. Ren, "Data age aware scheduling for wireless powered mobile-edge computing in industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 398–408, 2021.

[8] G. Q. Xu, H. P. Bai, J. Xing et al., "SG-PBFT: a secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 1–11, 2022.

[9] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the SOA-based Internet of Things: discovery, query, selection, and on-demand provisioning of web services," *IEEE Transactions on Services Computing*, vol. 3, no. 3, pp. 223–235, 2010.

[10] Z. Bi, L. D. Xu, and C. Wang, "Internet of Things for enterprise systems of modern manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1537–1546, 2014.

[11] G. Q. Xu, W. Y. Dong, J. Xing et al., "Delay-CJ: a novel cryptojacking covert attack method based on delayed strategy and its detection," *Digital Communications and Networks*, 2022.

[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[13] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in Industry 4.0: a review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 697–701, Malaysia, December 2014.

[14] E. Bartocci and Y. Falcone, *Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory*, pp. 135–175, Springer, Berlin, 2018.

[15] G. Xiong, F. H. Zhu, X. W. Liu et al., "Cyber-physical-social system in intelligent transportation," *IEEE/CAA Journal of Automatica Sinica*, vol. 2, no. 3, pp. 320–333, 2015.

[16] D. B. Rawat, C. Bajracharya, and G. Yan, "Towards intelligent transportation Cyber-Physical Systems: real-time computing and communications perspectives,"pp. 1–6, IEEE, Fort Lauderdale, FL, USA, June 2015.

[17] Y. Lu, "Cyber physical system (CPS)-Based industry 4.0: a survey," *Journal of Industrial Integration and Management*, vol. 02, no. 03, Article ID 1750014, 2017.

[18] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A colonel blotto game for interdependence-aware cyber-physical systems security in smart cities," *The 2nd International Workshop*, 2017.

[19] X. J. Zeng, G. Q. Xu, X. Zheng, Y. Xiang, W. L. Zhou, and E-Aua, "E-AUA: an efficient anonymous user authentication protocol for mobile IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1506–1519, 2019.

[20] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks," *Journal of Network and Computer Applications*, vol. 107, no. apr, pp. 83–92, 2018.

[21] D. H. Shin, D. Qian, and J. Zhang, "Cascading effects in interdependent networks," *IEEE Network*, vol. 28, no. 4, pp. 82–87, 2014.

[22] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, Article ID 065102, 2002.

[23] L. Ding and M. Tan, "Robustness of random scale-free networks against cascading failure under edge attacks," *Journal of Communications*, vol. 11, no. 12, pp. 1088–1094, 2016.

[24] L. Chen, D. Yue, C. Dou, Z. Cheng, and J. Chen, "Robustness of cyber-physical power systems in cascading failure: survival of interdependent clusters," *International Journal of Electrical Power & Energy Systems*, vol. 114, Article ID 105374, 2020.

[25] S. Liu, C. S. Yin, D. J. Chen, H. X. Lv, and Q. P. Zhang, "Cascading failure in multiple critical infrastructure interdependent networks of syncretic railway system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 6, pp. 5740–5753, 2022.

[26] H. Peng, Z. Qian, Z. Kan, H. Ye, Z. Fang, and D. D. Zhao, "Security assessment for cascading failures of cyber-physical systems under target attack strategy," in *Proceedings of the International Conference on Frontiers in Cyber Security*, pp. 315–327, Springer, Tianjin, China, November 2020.

[27] X. Yang, Z. Qian, X. H. Zhang et al., "Cascading failure dynamics against intentional attack for interdependent industrial Internet of Things," *Security and Communication Networks*, vol. 2022, Article ID 6848156, 2022.

[28] D. Zhou, A. Bashan, R. Cohen, Y. Berezin, N. Shnerb, and S. Havlin, "Simultaneous first-and second-order percolation transitions in interdependent networks," *Physical Review E*, vol. 90, no. 1, Article ID 012803, 2014.

[29] S. W. Son, G. Bizhani, C. Christensen, P. Grassberger, and M. Paczuski, "Percolation theory on interdependent networks based on epidemic spreading," *EPL*, vol. 97, no. 1, Article ID 16006, 2012.

[30] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: percolation on random graphs," *Physical Review Letters*, vol. 85, no. 25, pp. 5468–5471, 2000.

[31] R. M. D'Souza, "Curtailing cascading failures," *Science*, vol. 358, no. 6365, pp. 860-861, 2017.

[32] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: a topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

[33] P. Hines, K. Balasubramaniam, and E. C. Sanchez, "Cascading failures in power grids," *IEEE Potentials*, vol. 28, no. 5, pp. 24–30, 2009.

[34] E. Zio and G. Sansavini, "Component criticality in failure cascade processes of network systems," *Risk Analysis*, vol. 31, no. 8, pp. 1196–1210, 2011.

[35] S. Wang, Y. Yang, L. Sun, X. Li, Y. Li, and K. Guo, "Controllability robustness against cascading failure for complex logistic network based on dynamic cascading failure model," *IEEE Access*, vol. 8, Article ID 127450, 2020.

[36] Y. Y. Liu, J. J. Slotine, and A. L. Barabási, "Controllability of complex networks," *Nature*, vol. 473, no. 7346, pp. 167–173, 2011.

[37] S. N. Dorogovtsev, J. F. F. Mendes, and A. N. Samukhin, "Giant strongly connected component of directed networks," *Physical Review E*, vol. 64, no. 2, Article ID 025101, 2001.

[38] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[39] E. Renyi, "On random graph," *Publicationes Mathematicate*, vol. 6, pp. 290–297, 1959.

[40] B. Bollobás, "The evolution of random graphs," *Transactions of the American Mathematical Society*, vol. 286, pp. 257–274, 1984.

[41] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.