Hindawi
Complexity
Volume 2023, Article ID 9790451, 1 page
https://doi.org/10.1155/2023/9790451

Retraction

Retracted: Cascading Failure Dynamics against Intentional Attack for Interdependent Industrial Internet of Things

Complexity

Received 19 December 2023; Accepted 19 December 2023; Published 20 December 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Peng, Z. Qian, Z. Kan, D. Zhao, J. Yu, and J. Han, "Cascading Failure Dynamics against Intentional Attack for Interdependent Industrial Internet of Things," *Complexity*, vol. 2021, Article ID 7181431, 15 pages, 2021.

Hindawi
Complexity
Volume 2021, Article ID 7181431, 15 pages
https://doi.org/10.1155/2021/7181431

Research Article

Cascading Failure Dynamics against Intentional Attack for Interdependent Industrial Internet of Things

Hao Peng,[1] Zhen Qian,[1] Zhe Kan,[2] Dandan Zhao,[1] Juan Yu,[1] and Jianmin Han[1]

[1]*Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, China*
[2]*School of Cyber Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China*

Correspondence should be addressed to Dandan Zhao; ddzhao@zjnu.edu.cn

Received 18 May 2021; Accepted 29 July 2021; Published 10 August 2021

Academic Editor: Chenquan Gan

The emerging Industrial Internet of Things (IIoT) provides industries with an opportunity to collect, aggregate, and analyze data from sensors, including motion control, machine-to-machine communication, predictive maintenance, smart energy grid, big data analysis, and other smart connected medical systems. The physical systems and the cyber systems are organically integrated, forming an interdependent IIoT. This system provides us with enormous advantages, but at the same time, it also introduces the main safety challenges in the design and operation phase. To exploit the security threats of IIoT systems, in this paper, we propose a novel security-by-design approach for interdependent IIoT environments across two different levels, namely, theory modeling and runtime simulation. Our method theoretically analyzes the cascading failure dynamics of the intentional attack network. Simultaneously, we verified the theoretical results through simulations and gave the risk factors that affect the system's security to mitigate potential security attack threats. Besides, we prove its applicability through comparative simulation experiments to study application environments that rely on IIoT, which shows that our method helps identify risk factors and mitigate IIoT attacks' mechanism.

1. Introduction

In recent years, with human society's progress and the widespread use of the Internet, many emerging technologies and industries are booming. Emerging industries such as artificial intelligence, Internet of things, virtual reality, blockchain, big data, and cloud computing have accelerated the development and application of modern high-tech technologies.

With the rapid development of communication and sensor technology [1, 2], the Internet of things technology has attracted extensive attention in the emerging digital world. The goal of the Internet of things is to create a world of the Internet of things. The emergence of Internet of things technology has dramatically changed people's way of life, work, and entertainment. It has been everywhere in transportation, home furnishing, medical treatment, learning, and logistics. We found that the Internet of things technology has been embedded in people's daily life, intelligently connecting things or objects around us. The industrial Internet of things is the deep integration of the Internet of things in industrialization and informatization. In 2011, Germany first proposed the concept of Industry 4.0 [3, 4] and took CPS (cyber-physical system) as the primary goal of Industry 4.0 development [5]. Industrial Internet of Things (IIoT) is a subset of the Internet of Things (IoT) [6], which requires a higher level of security, security, and reliable communication [7]. In the industrial field, future information application scenarios and CPS technology have high adaptability. CPS provides critical technology for the ubiquitous industrial Internet of things technology.

According to the US National Science Foundation (NSF), CPS seamlessly integrates computing and physical components. As the core architecture of IIoT, the goal of CPS is to realize the deep integration of information systems and physical systems [8]. CPS has been applied in many areas, such as intelligent transportation systems [9, 10], monitoring, and control [11, 12], national defense weapon

systems, intelligent aerospace, smart home, and other fields [13, 14]. CPS's impact is enormous, and its emergence will change the way people interact with the physical world [15]. In the modern industrial system [16], we pay special attention to the security of information technology [17]. CPS provides new opportunities in technology and brings more and more attention and challenges [18]. If these risks are not analyzed and handled appropriately, the consequences will be severe.

Part of the existing research focuses on the design and evaluation of CPS modeling. Because CPS is widely used in various industries, and the physical resource network and computing resource network of each industry are different, it is almost impossible to model CPS as a general model. Aiming at the information physical production system (CPPS), Ref. [19] proposes a system architecture that can adapt to the independent processing line. For the hierarchical control system, network physical modeling and network emergency assessment are carried out in Ref. [20]. In the context of targeted destructive impact, Pavlenko and Zegzhda [21] proposed a new network physical system security evaluation method. Ribeiro and Björkman [22] critically compare today's automation solutions with their potential network physical solutions. Wireless sensor actuator network is applied in industrial automation. Lu et al. [23] review the existing technology of industrial wireless control systems. Ref. [24] models and evaluates the energy management system of networked and automated electric vehicles and develops a network attack analysis method. The emergence of CPS attracts more people's attention to the physical network world, which is the opportunity.

However, we know that a general modeling method is not popular in the network physical world. The scale, topology, and connection heterogeneity of networks bring great challenges. We know that CPS is composed of two networks, and the two networks are interdependent. In network physical systems, physical devices such as batteries and sensors are regarded as physical components. Embedded computer and communication networks are considered network components. Generally, it is the interdependent computational-resource network and physical-resource network that the CPS model as Ref. [25]. In the interconnected system, the destruction of a node usually affects the whole system and brings essential influence. The interdependence between nodes leads to a node failure chain reaction called cascading failure [26]. Cascading failures will have a significant impact on CPS. Therefore, CPS needs to evaluate the risk of the coupled network.

This paper makes a significant contribution to the security of the IIoT system composed of CPS. Traditional fault analysis methods, such as fault tree analysis [27], are widely used in the CPS system [28]. However, this method does not consider the cascading failure of two networks in CPS due to the coupling relationship. Other scholars [29] have considered this cascading failure problem, but only under the deliberate attack strategy. In real life, the attack is often targeted and deliberate [30, 31]. In this paper, we model the IIoT system composed of computing resources and physical resources as two interdependent complex networks and elaborate the cascading failure dynamics of the cyber-physical system under the intentional attack strategy. We define the coupling relationship between physical resource networks and information resource networks through the model proposed in this paper. The specific contributions are as follows:

(i) We apply the percolation theory to the cascading failure of interdependent networks. Percolation theory is a process of removing network vertices and edges. We consider that both physical resource networks and computational resource networks are scale-free networks, and their degree distribution obeys power-law distribution. We analyze the robustness of our model in intentional attack strategy by calculating the proportion of functional nodes after cascading failure stops.

(ii) We use a mathematical method to analyze the cascading failure process of the coupling network in detail. The results show that, given the power-law exponent and initial attack parameters of the coupled network, there is always a threshold for the network to collapse and form a steady state. Beyond this threshold, the network will no longer have functional nodes. Within the threshold range, there are still functional nodes in the coupling network after cascading failure stops.

(iii) We further verify the accuracy of the theoretical and experimental results through simulation experiments. In addition, we analyze several essential parameters in the simulation phase, such as power-law index, attack parameters, etc. We find that the percolation threshold decreases with the increase of the power-law exponent of the network, which improves the robustness of the surface network. This work speeds up the understanding of the relationship between the online world and the physical world.

The essay proceeds as follows. The related work of this paper is addressed in Section 2. Section 3 presents the concept of the interdependent network model and the detailed cascading failure dynamics. In Section 4, the whole cascading failure dynamics is interpreted by the theoretical method. In Section 5, we solve the theoretical equation in Section 4 by numerical analysis and get the theoretical solution to give the simulation results. Section 6 summarizes the relevant conclusions and gives some possible works in the future.

2. Related Work

The Industrial Internet of Things system, composed of CPS, has always been the focus of scholars. We will mainly analyze and study the two critical theories of the security of the Industrial Internet of Things, namely the interdependent network and percolation theory.

2.1. Interdependent Networks. The scholarly study of the interdependent network mainly concentrates on the evolutionary dynamics and network structure's robustness [32–34]. The robustness of the network structure here refers to the integrity of network topology after some nodes fail. When a network in the cyber-physical system is attacked, it will split into a more extensive cluster and smaller groups. From the research of scholars [33, 35–37], it can be concluded that a node holds its function only if it meets two conditions as follows:

(i) Nodes in the current network must combine with those in another network.

(ii) The node should be part of the most extensive set of connected clusters.

Those who satisfy the conditions mentioned above are considered as functional nodes and features prominently in the entire network. When an attack comes, only these can remain. Once there exist no function nodes, the network would collapse completely.

In 2010, a "one-to-one correspondence" theoretical model was put forward by Buldyrev et al. [38] to abstract the robustness of coupled networks cascading failures into a model, and they found that the interdependent network under random attack is more fragile than the single network. This brings more scholars' attention to the coupled networks. Huang et al. [31] and others examined and put forward the interdependent networks' robustness model when being deliberately attacked. They transformed the targeted-attack model into a random attack model. They found that in an entirely random coupled scale-free network, even if the attack probability on a large vertex in one of the networks is reduced, the system is still fragile, which shows that it is complicated to protect the entirely random coupled scale-free network. Since then, Dong et al. [30] have also studied the degree-based attack of partial interdependent systems.

Parshani et al. [39] used the mathematical research method proposed by Buldyrev to study the partially interacted network. It was found when the degree of interdependence between the two subnetworks decreased, the network robustness would be enhanced; that is, the former first phase transition of network seepage is now transformed into the second phase transition. In 2014, Danziger studied a system of partially coupled spatial networks and presented cascade dynamics measurements. Chattopadhyay and Dai [40] researched some interdependent networks and established mathematical equations. Combining two attack models, random attack and target attack, we can learn more regarding the robustness of coupled interdependent networks.

In 2012, Gao et al. [34] jointly published a network paper on the interdependent network in the Journal of Nature Physics. They developed a more general mathematical method based on Buldyrev and others' mathematical framework, which further opened a new milestone for individuals to study the interdependence network.

In 2014, Shao et al. [41] researched the robustness of interdependent networks with clustering properties and noticed that the lower the clustering coefficient, the better the network robustness. In the same year, Zhou et al. [42] and others conducted an in-depth study on the cascading failure dynamics and found that a spontaneous second-order phase transition happened in the first-order phase transition point.

In recent years, experts and scholars have studied how to slow down coupled networks' cascading failure. Tootaghaj [43] had a comprehensive knowledge of failure location and focused on recovery strategies after failures. In this way, he developed two methods to solve the continuous cascading failure.

2.2. Percolation Theory. There are many theories in the research process of complex networks, such as game theory, communication theory, and percolation theory [42]. In network science, percolation theory becomes a significant part of the complex network structure's research evolution [39, 44]. Callaway et al. [45] first proposed the concept of percolation in 1957. Percolation theory is a method to estimate network reliability. There are two standard percolation modes: bond percolation and site percolation. In an $n * n * n$ mesh, the edges between nodes are preserved with probability p. Given a probability p, what is the probability of a path from the top to the bottom of the grid, called bond percolation [45]? If the mesh vertex is retained with probability p, then there is a question concerning the probability of a path from the top to the bottom of the mesh, called site percolation [46].

In [35, 38], the seepage theory is used to measure the coupled network's characteristics. In a single network, Cohen et al. [46] used percolation theory [47] to study network robustness and vulnerability.

In 2010, the percolation theory was used by Buldyrev et al. [38] to explore the robustness of interdependent networks. In 2013, Zhou et al. [48] researched the percolation phenomena of similar interdependent networks. In 2015, Dong et al. [49] and others delved into the percolation problem of the interdependent network with feedback dependent edges and found that in the case of strong coupling, the system with feedback dependent edges is more vulnerable.

The percolation research of interdependent networks mainly designs the network random evolution rules and the network seepage application [50, 51]. So far, there are a host of areas worth studying network seepage.

We will systematically analyze and study the security of IIoT by using the two methods of interdependent network theory and seepage theory. Compared with the above work, this paper's difference is that it analyzes the interdependent network's cascading failure dynamics based on the intentional attack mode, and the network type is closer to reality. We can better evaluate CPS's network security performance and industrial Internet of things through the combination of theory and simulation.

3. Proposed Model and Concepts

We propose a new modeling and analysis method of IIoT environment security from the two aspects of modeling and simulation. Figure 1 shows the primary process of our method. At the modeling level, we start with analyzing the network's cascading failure dynamics, studying the process of cascading failure mathematically, and proving when the network will come to an end. Furthermore, we get the critical value equation of network collapse. We find this threshold by image fitting. In the simulation, we build a cyber-physical network model of coupled networks. We will simulate the network's process being attacked deliberately, get the number of nodes remaining in the most connected group after the network crash, and find the network's critical value by drawing graphs. By analyzing these two levels, the emulation results can be fed back to the modeling results to analyze further the network security performance of the industrial Internet of things.

3.1. Modeling Level. In real life, the IIoT system is often based on CPS architecture, usually composed of a coupled computational-resource and physical-resource networks. As shown in Figure 2, these scenarios show the IIoT system based on CPS architecture. Many research and empirical data show that the number of nodes in a physical resource network is less than that in a computing resource network. Therefore, at the modeling level, we set the number of nodes of the two coupled networks to be 3 : 1. We use S and I to represent the two networks of computing and physical resources. The number of nodes is N_S and N_I, respectively. We call the connecting edge between S and I as internetwork connection and the connecting edge of the nodes in two networks as intranetwork connection. Both intranetwork and inter network connections are random. Nodes from different networks depend on each other by connecting edges. Failure of either party will result in the failure of the other party. It can be found that only a few nodes are linked to a large number of nodes, while most nodes are only connected with a small amount. We usually call the network with this distinct scale-free network. For the convenience of research, we consider the two coupled networks as scale-free networks. The degree distribution of scale-free networks follows the power-law distribution. In other words, $P(k) \propto k^{-\lambda}$ where $P(k)$ is the probability that a node has k edges and λ is a power-law exponent.

The computing and physical resources in IIoT are composed of many components, such as control devices, network devices, computers, and batteries. In the whole system, the damage of some devices has little effect on the network cascading failure. Therefore, in this paper, we only consider the impact of critical nodes on cascading failure of coupled networks. For example, in a smart grid, the power control node that provides power for communication network operation and the communication node that ensures the regular operation of the power network are the key nodes.

Some natural factors or emergencies may lead to some nodes' failure in the network in real life. However, more often than not, the network is deliberately attacked due to human factors. Therefore, in this paper, we assume that some computing resource network nodes suffer from intentional destruction. We use a deliberate attack strategy to delete the number of nodes in the network S, and the ratio is $1 - p$. The internetwork connection and intranetwork connection of these deleted nodes will be deleted. Due to interdependence, some nodes in the network I lose their connection, leading to dysfunction. As mentioned above, due to the coupling and interdependence between computing resource networks and physical resource networks, node failure in one network will affect another network. The node failure in another network will affect this network in turn, leading to the node failure in the network coupled with it. Therefore, it is a cycle process. We call this process a professional term: cascading failures, as shown in Figure 3.

The cascading failure dynamics have been described clearly, and we need to determine when it will stop. When the nodes in the two networks no longer fail or the coupled network collapses completely, we think the network has reached a stable state. At this point, cascading failures stop. We stipulate that only the nodes that meet the requirements of maintaining function in at least another network and belong to the largest connected cluster are called function nodes. Therefore, the functional nodes eventually survive. The following section will detailedly analyze the cascading failure dynamics by using mathematical methods.

3.2. Simulation Level. At the simulation level, the experimental data are used to verify the above theoretical results' accuracy. We will build two scale-free networks that are coupled and interdependent. The number of nodes in the two networks is set to 3000 and 9000, respectively. We know that three network nodes S establish a connection relationship with one network I. The nodes of network S and network I will also be connected randomly. Hence, we can compare the two networks. According to the targeted-attack model, intentional attacks between networks are skillfully transformed into equivalent random attacks. Referring to the above probability equations, which indicate targeted attacks, each node's failure probability is determined, and then nodes are deleted randomly. Due to the cascading failure, the nodes in one network are deleted, which will cause the nodes in another network to be affected and fail. In each step of the cascading failure dynamics, we will save the remaining nodes in the current network until there is no cascading failure in the network. The storage of these data will help us analyze the changes of network nodes. Algorithm 1 shows our simulation steps.

4. Mathematical Analysis of Cascading Failure Dynamics

In this section, we will use some mathematical methods to describe the process of cascading failures in coupled networks. Since the direct calculation of an intentional attack

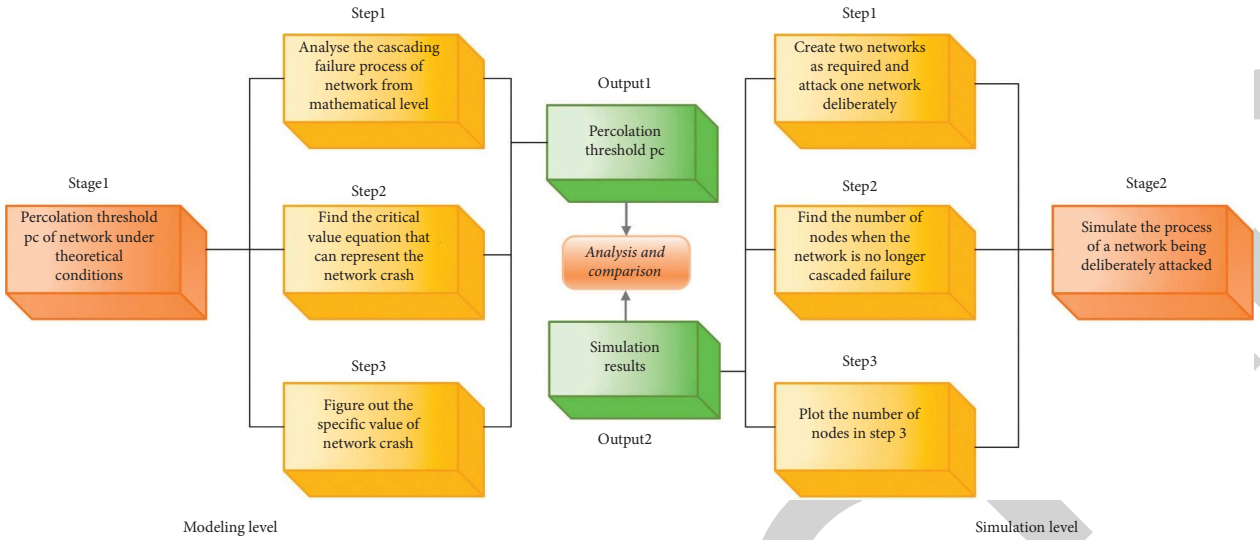

Figure 1: Process of the proposed method.

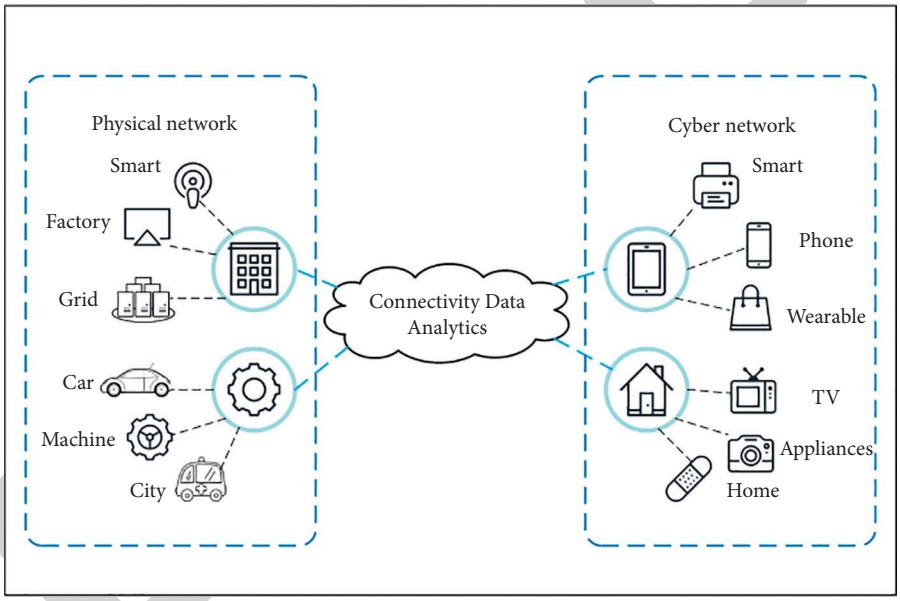

Figure 2: A conceptual view of industrial Internet of things system based on interdependent CPS architecture.

will increase the difficulty, we will use some scientific methods to convert an intentional attack into a random attack. After the transformation, we will analyze the process of network cascading failure step by step. Finally, we get the expression that the network finally reaches a steady state. The related symbols are defined in Table 1.

4.1. Stage 1: Intentional Attack in Network S. Various nodes in a network have different weights. Some nodes are crucial in the connectivity of the network. The criteria for evaluating node importance are not unique, and here we choose a more general one. Gallos et al. [36] proposed the influence of the degree of any vertices on network robustness. In Ref. [36], a family of functions is defined as follows:

$$Q_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=0}^{N} k_i^\alpha}. \quad (1)$$

Assign $Q_\alpha(ki)$ to each node i with a corresponding degree of k_i, where $Q_\alpha(ki)$ implies the likelihood of nodes' failure caused by being attack.

By observing the function, we can know that when $\alpha < 0$ and the node degree is 0, the formula will become meaningless. From this, to keep the nodes with node degree 0 from being excluded and make them conform to the situation of the coupled system in real life, we improve the function equation and get the following functions:

$$Q_\alpha(k_i) = \frac{(k_i + 1)^\alpha}{\sum_{i=0}^{N} (k_i + 1)^\alpha}. \quad (2)$$

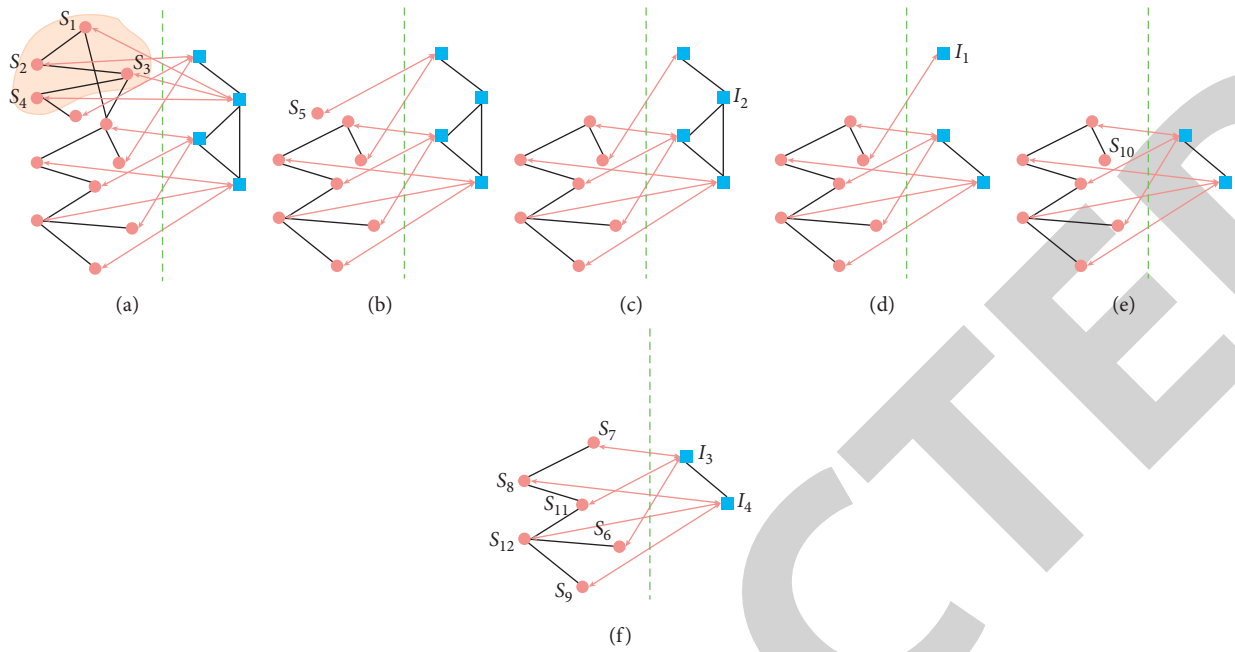

Figure 3: The process of cascading failure. (a) The left and right sides represent a computational-resource network and a physical-resource network, and the nodes are connected randomly. The shadow nodes S_1 S_2 S_3 S_4 indicate the deliberately damaged nodes of network S. (b) The damaged nodes are disconnected from network S and network I. Those belonging to the largest connected cluster in S will be preserved. Consequently, the node S_1 will be deleted. (c) Because of the node's failure in the network S, the node I_2 in the network I has no interlinks. I_2 also fails. (d) It demonstrates that the node I_1 does not belong to the giant network I and fails. (e) The nodes' failure occurs in the network I, and the interlink is disconnected from S_{10}. Thus, S_{10} fails. (f) The nodes of both networks do not fail anymore and reach a stable state.

```
(1) for each i ∈ [0, 1] do
(2)   for i = 1 to 50 do
(3)     Target attack network S;
(4)     Remove the node of the attacked node network S;
(5)     int step;
(6)     while The number of network nodes is still changing do
(7)       step++;
(8)       if step% = 2 then
(9)         Delete the node in network S that has lost its normal function due to the failure of the node in network I;
(10)      else
(11)        Delete the node in network I that has lost its normal function due to the failure of the node in network S;
(12)      end if
(13)    end while
(14)  end for
(15)  Save the number of remaining nodes in the network;
(16) end for
```

Algorithm 1: Network cascading failure against intentional attack simulation.

When $\alpha < 0$, it is more vulnerable to fail low degree nodes, and those with high degrees are better protected. When $\alpha > 0$, the nodes with high degrees are more vulnerable to failure, and the nodes with a low degree are better protected. When $\alpha = 0$, $W_0 = 1/N$, all nodes have the same probability of failure, which is equivalent to being converted into a random attack. When $\alpha \longrightarrow +\infty$, the nodes with degrees from high to low are deleted in turn. On the contrary, when $\alpha \longrightarrow \infty$, the nodes with degrees from low to high are deleted in turn.

According to the previous description, our main method is to construct a network S', which is equivalent to the original network S. Therefore, the intentional attack on network S can be transformed into a random attack on network S'. According to Huang et al. [31] method, target attack is mapped to random attack. In the first step, according to equation (1), we first remove the $(1 - p)$ scale nodes from the network. The edges between the remaining nodes and the removed nodes are preserved. Then, the degree distribution of the remaining nodes $P_p(k)$ is as follows:

Table 1: Symbol definition.

Symbol	Explanation
N_S, N_I	The initial nodes of scale-free network S and I.
N'_{S_i}, N'_{I_i}	Number of nodes that have supporting interlink in the network S and I at stage i and j.
N_{S_i}, N_{I_i}	The giant components that remain functional in N'_{S_i} and N'_{I_i}.
μ_i, μ_j	The fraction corresponding to N_{S_i} and N_{I_i}.
μ'_i, μ'_j	The fraction corresponding to N'_{S_i} and N'_{I_i}
λ_S, λ_I	Parameters of the degree distribution of network S and I.

$$P_p(k) = \frac{Q_p(k)}{pN_S}. \tag{3}$$

We assume $Q_p(k)$ describes the number of k-degree nodes among the resting part.

After deleting another node, $Q_p(k)$ will become as follows:

$$Q_{(p-1/N)}(k) = Q_p(k) - \frac{P_p(k)(k+1)^\alpha}{\sum_k P_p(k)(k+1)^\alpha}. \tag{4}$$

When $N \longrightarrow \infty$, equation (4) could be changed into a derivative of $Q_p(k)$ with respect to p:

$$\frac{dQ_p(k)}{dp} = \mathrm{N}\frac{P_p(k)(k+1)^\alpha}{\sum_k P_p(k)(k+1)^\alpha}. \tag{5}$$

When $N \longrightarrow \infty$ combining equation (3) with equation (5), it can be seen that

$$-p\frac{dQ_p(k)}{dp} = P_p(k) - \frac{P_p(k)(k+1)^\alpha}{\sum_k P_p(k)(k+1)^\alpha}. \tag{6}$$

To better find a solution concerning the equation (6), a new function $G_\alpha(x) = \sum_k P(x)x^{(k+1)^\alpha}$ is defined and $d = G_\alpha^{-1}(p)$ [39], then we can solve equation (6) to get the following:

$$P_p(k) = \frac{1}{p}P(k)d^{(k+1)^\alpha}, \tag{7}$$

$$\sum P_p(k)(k+1)^\alpha = \frac{dG'_\alpha(d)}{G_\alpha(d)}. \tag{8}$$

Accordingly, the generating function of $P_p(k)$ is as follows:

$$G_{Sb}(x) \equiv \sum_k P_p(x)x^k = \frac{1}{p}\sum_k P(x)d^{(k+1)^\alpha}x^k. \tag{9}$$

Since network S is randomly connected, the probability that an edge ends at the remaining nodes is equal to the ratio of the number of edges sent from the remaining nodes to the total number of edges from all nodes of the original network:

$$\widetilde{p} \equiv \frac{p\mathrm{N}\langle k(p)\rangle}{N\langle k\rangle} = \frac{\sum_k P(k)kd^{(k+1)^\alpha}}{\sum_k P(k)k}. \tag{10}$$

Here, we define $\langle k\rangle$ as the original network's average degree, and set $\langle k(p)\rangle$ as the remaining nodes' average degree after the network being intentionally attacked. With the method in Ref. [38], we obtain the remaining nodes' generating function as follows:

$$G_{Sc}(x) \equiv G_{Sb}(1 - \widetilde{p} + \widetilde{p}x). \tag{11}$$

Our goal is to transform the target attack on network S into random attack on network S'. Through some theoretical research, it can be found that the difference between a target attack and a theoretical attack is only in the first step of cascading failure. Therefore, as long as we seek out a network S', its generating function $G_{Sc}(x)$ and $\widetilde{G}_{S0}(x)$ are equal after randomly deleting nodes with $(1-p)$ ratio. Then, the random attack analysis of network S' can replace the intentional attack analysis of network S. Based on the experience of Ref. [38], we use $\widetilde{G}_{S0}(1 - p + px) = G_{Sc}(x)$ to get the following formula:

$$\widetilde{G}_{S0}(x) = G_{Sb}\left(1 + \frac{\widetilde{p}}{p}(x-1)\right). \tag{12}$$

Next, we use the random attack analysis process to continuously analyze the process of cascading failure under targeted attack, mainly searching the iterative process detailedly with the generation function and percolation theory. Then, we analyze the ratio of the current network's functional nodes amounts to the total quantity of nodes in the original network after each step of failure. The generating function of network S' has been obtained, as shown in equation (12). In light of the above generating function of network S', the generating function of the underlying branching process $\widetilde{G}_{S1}(z)$ is as follows:

$$\widetilde{G}_{S1}(z) = \frac{\widetilde{G}'_{S0}(z)}{\widetilde{G}'_{S0}(1)}. \tag{13}$$

When S' is randomly attacked to remove the nodes with the ratio of $(1-p)$, the remaining nodes' degree distribution will change while affecting the corresponding degree distribution in generating function. Therefore, the degree distribution of the remaining nodes in S' is $N'_{S1} = p * N_S$. The proportion of function nodes is as follows:

$$g_S(p) = 1 - \widetilde{G}_{S0}[1 - p(1 - f_S)], \tag{14}$$

where we define f_S as the function of p, fs meets the following:

$$f_S = \widetilde{G}_{S1}[1 - p(1 - f_S)]. \tag{15}$$

Next, we will analyze the cascading failure dynamics step by step.

4.2. Stage 2: Equivalent Failure Under Random Attack in Network S'. In the previous paper, we have analyzed the process from intentional attack to random attack. Therefore, we think that the initial attack is a random attack on network S'. The $(1-p)$ ratio of node failure. The quantity of remaining nodes is as follows:

$$N'_{S1} = p \cdot N_S = \mu'_1 \cdot N_S. \tag{16}$$

From equation (16), we could get $\mu'_1 = p$. Based upon the previous analysis, the quantity of nodes in the giant component in N'_{S1} is as follows:

$$N_{S1} = g_S(\mu'_1) \cdot N'_{S1} = \mu'_1 \cdot g_S(\mu'_1) \cdot N_S = \mu_1 \cdot N_S. \tag{17}$$

From equation (17), we obtain the following:

$$\mu_1 = \mu'_1 \cdot g_S(\mu'_1). \tag{18}$$

4.3. Stage 3: Cascading Failures in Network I Caused by S-Node Failures. Through the analysis of the CPS system, we know that the nodes in the coupling network S' and I' are interdependent. Therefore, the failure of nodes in network S' may lead to the nodes crash in network I'. In our model, one node in network I' connects with three nodes of network S', and the internetwork connection and intranetwork connection are random. Consequently, the quantity of nodes remaining in network I' is as follows:

$$N_{I2}' = \left[1-(1-\mu_1)^3\right] \cdot N_I = \left(\mu_1^3 - 3\cdot\mu_1^2 + 3\cdot\mu_1\right) \cdot N_I = \mu_2' \cdot N_I, \tag{19}$$

$$\mu_2' = \mu_1^3 - 3\cdot\mu_1^2 + 3\cdot\mu_1 = \mu_1' \cdot g_S(\mu_1') \cdot \left(\mu_1^2 - 3\cdot\mu_1 + 3\right). \tag{20}$$

Using the same analysis theory before, we can get the number of nodes in N'_{I2} that belongs to the huge connectivity component:

$$N_{I2} = g_I(\mu_2') \cdot N'_{I2} = \mu_2' \cdot g_I(\mu_2') \cdot N_I = \mu_2 \cdot N_I. \tag{21}$$

From equation (21), we obtain the following:

$$\mu_2 = \mu_2' \cdot g_I(\mu_2'). \tag{22}$$

4.4. Stage 4: Further Fragment in Network S'. From the previous theoretical derivation of cascading failure, it is found that the number of nodes with dependency in those that remained and belonging to network S'. In the first step of random failure, it is derived that a node in network I may have a random connection to one to three nodes in network S'. In Table 2, we list the proportion of different connections.

According to our previous model, intralinks connection and interlinks connection are completely independent, which is a completely random event. Consequently, we get the quantity of nodes with dependency in S':

$$N_{S3}' = \mu_2 \cdot N_I \cdot \frac{\left[C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2 \cdot 1 + C_3^2 \cdot \mu_1^2 \cdot (1-\mu_1) \cdot 2 + \mu_1^3 \cdot 3\right]}{\left[1-(1-\mu_1)^3\right]}. \tag{23}$$

So

$$N'_{S3} = \mu_1 \cdot g_I(\mu_2') \cdot N_S. \tag{24}$$

From N_{S1} to N'_{S3}, we know that

$$N_{S1} - N'_{S3} = \left(1 - g_I(\mu_2')\right) \cdot N_{S1}. \tag{25}$$

Based upon the theory in Ref. [52], the nodes removed in the initial stage do not belong to N_{I2}, N_{S1} and N'_{S1}, so from the proportion of nodes removed in N_{S1} has the identical ratio with those nodes removed from N'_{S1}. So

$$\begin{aligned} N_{S1} - N'_{S3} &= \left(1 - g_I(\mu_2')\right) \cdot N_{S1} \\ &= \left(1 - g_I(\mu_2')\right) \cdot N'_{S1}. \end{aligned} \tag{26}$$

The fraction of the total nodes removed to the original network S' is as follows:

$$1 - \mu_1' + \left(1 - g_I(\mu_2')\right) \cdot \mu_1' = 1 - \mu_1' \cdot g_I(\mu_2'). \tag{27}$$

From equation (27), we know the following:

$$\mu_3' = \mu_1' \cdot g_I(\mu_2'). \tag{28}$$

So, the quantity of nodes in the massive component in N'_{S3} is as follows:

$$N_{S3} = \mu_3' \cdot g_I(\mu_3') \cdot N_S = \mu_3 \cdot N_S. \tag{29}$$

So,

$$\mu_3 = \mu_3' \cdot g_S(\mu_3'). \tag{30}$$

4.5. Stage 5: Cascading Failures in I Once Again. Because of the coupled CPS system, the network's nodes would occur breakdown caused by the previous failure of relevant nodes in the network S'. As in the second step, the quantity of dependent nodes in I is obtained.

$$N'_{I4} = \left[1-(1-\mu_3)^3\right] \cdot N_I = \left(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3\right) \cdot N_I. \tag{31}$$

From N_{I2} to N'_{I4}, we can obtain the following:

$$N_{I2} - N'_{I4} = \left[\frac{1-\left(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3\right)}{\mu_2}\right] \cdot N_{I2}. \tag{32}$$

Same as the previous analysis, we get the following:

$$N_{I2} - N'_{I4} = \left[\frac{1-\left(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3\right)}{\mu_2}\right] \cdot N'_{I2}. \tag{33}$$

Table 2: The proportion of different nodes.

0	1	2	3
$(1-\mu_1)^3$	$C_3^1 \cdot \mu_1 \cdot (1-\mu_1)^2$	$C_3^2 \cdot \mu_1^2 \cdot (1-\mu_1)$	μ_1^3

Thus, we know the fraction of the nodes that failed in network I is as follows:

$$1-\mu_2' + \mu_2' \cdot \left[\frac{1-\left(\mu_3^3 - 3\cdot\mu_3^2 + 3\cdot\mu_3\right)}{\mu_2}\right] = 1-\mu_1' \cdot \left(\mu_3^2 - 3\cdot\mu_3 + 3\right)\cdot g_S(\mu_3'). \tag{34}$$

So,

$$\mu_4' = \mu_1' \cdot \left(\mu_3^2 - 3\cdot\mu_3 + 3\right)\cdot g_S(\mu_3'). \tag{35}$$

It is found that the quantity of nodes in the largest component in N_{I4}' is as follows:

$$N_{I4} = \mu_4' \cdot g_I(\mu_4') \cdot N_I. \tag{36}$$

So,

$$\mu_4 = \mu_4' \cdot g_I(\mu_4'). \tag{37}$$

Following the prior conclusions of the cascading failure dynamics method, we can identify the node size after each step of the process, which could be expressed by the following equations:

$$\begin{cases} \mu_{2i}' = \mu_1' \cdot \left(\mu_{2i-1}^2 - 3\cdot\mu_{2i-1} + 3\right)\cdot g_S(\mu_{2i-1}'), \\ \mu_{2i+1}' = \mu_1' \cdot g_I(\mu_{2i}'), \end{cases} \tag{38}$$

where $\mu_1' = p$.

In the next section, we will use numerical simulation and other methods to find Eq's solution (38). Thus, we can get the critical threshold of the coupled network.

5. Performance Analysis

5.1. Formula Calculation. Through the analysis in the previous section, it is clearly known that cascading failures will not occur again when the nodes in the coupled network are no longer in failure. Table 3 shows the specific state equations of the two networks at each stage. Therefore, in the coupled system, we can obtain the following equations when the cascading failure dynamics comes to an end:

$$\begin{cases} \mu_{2i}' = \mu_{2i-2}' = \mu_{2i+2}', \\ \mu_{2i+1}' = \mu_{2i-1}' = \mu_{2i+3}'. \end{cases} \tag{39}$$

In order to solve the above equations more efficiently, we define variables x, y:

$$\begin{cases} y = \mu_{2i}' = \mu_{2i-2}' = \mu_{2i+2}', \\ x = \mu_{2i+1}' = \mu_{2i-1}' = \mu_{2i+3}'. \end{cases} \quad (0 \le x, y \le 1). \tag{40}$$

Consequently, equation (38) can be shown as follows:

$$\begin{cases} y = p\cdot\left(\left(x\cdot g_S(x)\right)^2 - 3\cdot x\cdot g_S(x) + 3\right)\cdot g_S(x), \\ x = p\cdot g_I(y). \end{cases} \tag{41}$$

Simplify equation (41) to get the following:

$$x = p\cdot g_I\left[p\cdot\left(\left(x\cdot g_S(x)\right)^2 - 3\cdot x\cdot g_S(x) + 3\right)\cdot g_S(x)\right]. \tag{42}$$

In the process of solving the seepage threshold of a scale-free network, it is hard to directly replace the degree distribution of the network into the equation. Therefore, we need to rewrite equation (42) into two equations and make them infinitely approximate by drawing. Let's rewrite equation (42) into the following two equations:

$$\begin{cases} z = x, \\ z = p\cdot g_I\left[p\cdot\left(\left(x\cdot g_S(x)\right)^2 - 3\cdot x\cdot g_S(x) + 3\right)\cdot g_S(x)\right]. \end{cases} \tag{43}$$

According to the above equations, we draw the two equations in the figure. When the curve equation is tangent to the straight line, the intersection point is the seepage threshold as shown in Figure 4.

In Figure 4, we can see that when α is 1, the percolation threshold of the network is 0.5, while α is 2, it is 0.59. So far, we have solved the seepage threshold of the coupled network under different conditions. In order to verify the accuracy of the theoretical results, we will do some simulation experiments.

5.2. Case Results and Analysis. Simulation experiments in this section verify the correctness of the theoretical value. We analyze and verify the correctness of the theoretical data from several different dimensions. We write a C++ program to simulate the whole cascading failure process of interdependent networks in order to obtain the proportion of surviving nodes in the final steady state. Considering the actual situation, the power-law exponent of a scale-free network with power-law distribution is not a fixed value. We set this value between 2.0 and 3.0 to adapt and study different interdependent network systems. Whether the size of the network node affects the change of the experimental threshold is also the focus of our research. We set the network node size to different values. In addition to attack

Table 3: The stage of network S and network I.

	Network S	Network I
Stage 1	$\mu_1' = p\ \mu_1 = \mu_1' \cdot g_S(\mu_1')$	
Stage 2		$\mu_2' = \mu_1' \cdot g_S(\mu_1') \cdot (\mu_1^2 - 3 \cdot \mu_1 + 3)\ \mu_2 = \mu_2' \cdot g_I(\mu_2')$
Stage 3	$\mu_3' = \mu_1' \cdot g_I(\mu_2')\ \mu_3 = \mu_3' \cdot g_S(\mu_3')$	
Stage 4		$\mu_4' = \mu_1' \cdot g_S(\mu_3') \cdot (\mu_3^2 - 3 \cdot \mu_3 + 3)\ \mu_4 = \mu_4' \cdot g_I(\mu_4')$
...	...	...
Stage $2i$		$\mu_{2i}' = \mu_1' \cdot (\mu_{2i-1}^2 - 3 \cdot \mu_{2i-1} + 3) \cdot g_S(\mu_{2i-1}')\ \mu_{2i} = \mu_{2i}' \cdot g_I(\mu_{2i}')$
Stage $2i+1$	$\mu_{2i+1}' = \mu_1' \cdot g_I(\mu_{2i}')\ \mu_{2i+1} = \mu_{2i+1}' \cdot g_S(\mu_{2i+1}')$	

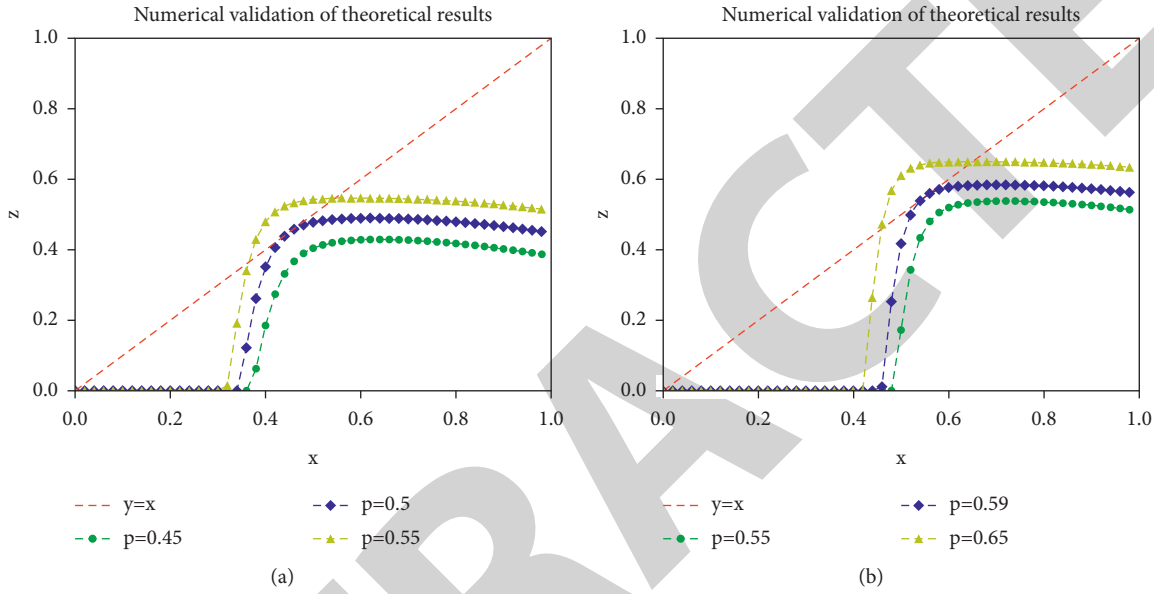

Figure 4: Solving iterative equations. We set the parameter λ of the network to 2.8 and change the value of α. (a) The intersection of a curve and a line stands for the critical threshold of the coupled system in the case of $\alpha = 1$. (b) The intersection of a curve and a line describes the critical threshold of the coupled system obtained with $\alpha = 2$.

parameters α, it is also essential to study cascading failure of coupled networks. We will set α between −1.0 and 2.0.

5.2.1. System Robustness. In Figure 5, we analyze the remaining nodes' proportion when the failure comes to an end in two networks with different p. From these three graphs, we can find that as p goes from $pc + \varepsilon$ to $pc - \varepsilon$, the value of the ordinate suddenly drops from a nonzero finite value to 0, where ε is a value tending to 0. This shows that when the value of p is in this range, the remaining nodes' scale will reduce to an exceedingly small value by deleting one node in the network. Moreover, we can observe that the abscissa's value corresponding to the network's remaining nodes' phase transition corresponds to the theoretical value, verifying the formula's theoretical value.

From Figure 5, it is found that with the change of abscissa, the changing trend of network S and I is the same. Both networks are generic nodes or crash at the same time. When p approaches the critical threshold, the maximum connected component in the network will rise linearly, this indicates that when p exceeds the critical threshold, some nodes may exist, or the coupled system may collapse. This is consistent with our theoretical analysis.

In Figures 5(a) and 5(b), we set the attack parameter α to the same value and change the power-law index λ of a scale-free network to 2.6 and 2.8, respectively. Comparing the two graphs, we get that the greater the λ is, the smaller the percolation threshold is, and the more reliable the network is. The larger the λ of the scale-free network, the higher the likelihood that a few network nodes have the most connections. That is, the network connections are closed. So, the reliability of the network will be improved. In Figures 5(b) and 5(c), we change the attack parameter α of the network, one is set to 1, and the other is set to 2. The scale-free network is invariant. By comparison, we find that the larger the α, the bigger the pc. This shows that the reliability of the coupled network is getting worse. The larger the α, the more vulnerable the nodes are to attack, so the network reliability is reduced. These analyses correspond to our previous theoretical analysis.

From Figure 5, it can be seen that the blue line representing the percentage of the nodes that remained in network I is almost invariably above the red one, which represents that proportion in network S. Due to the initial attack in network S, every node in network I was linked with three nodes in network S, the network I receives a certain degree of protection. This has a particular significance for us

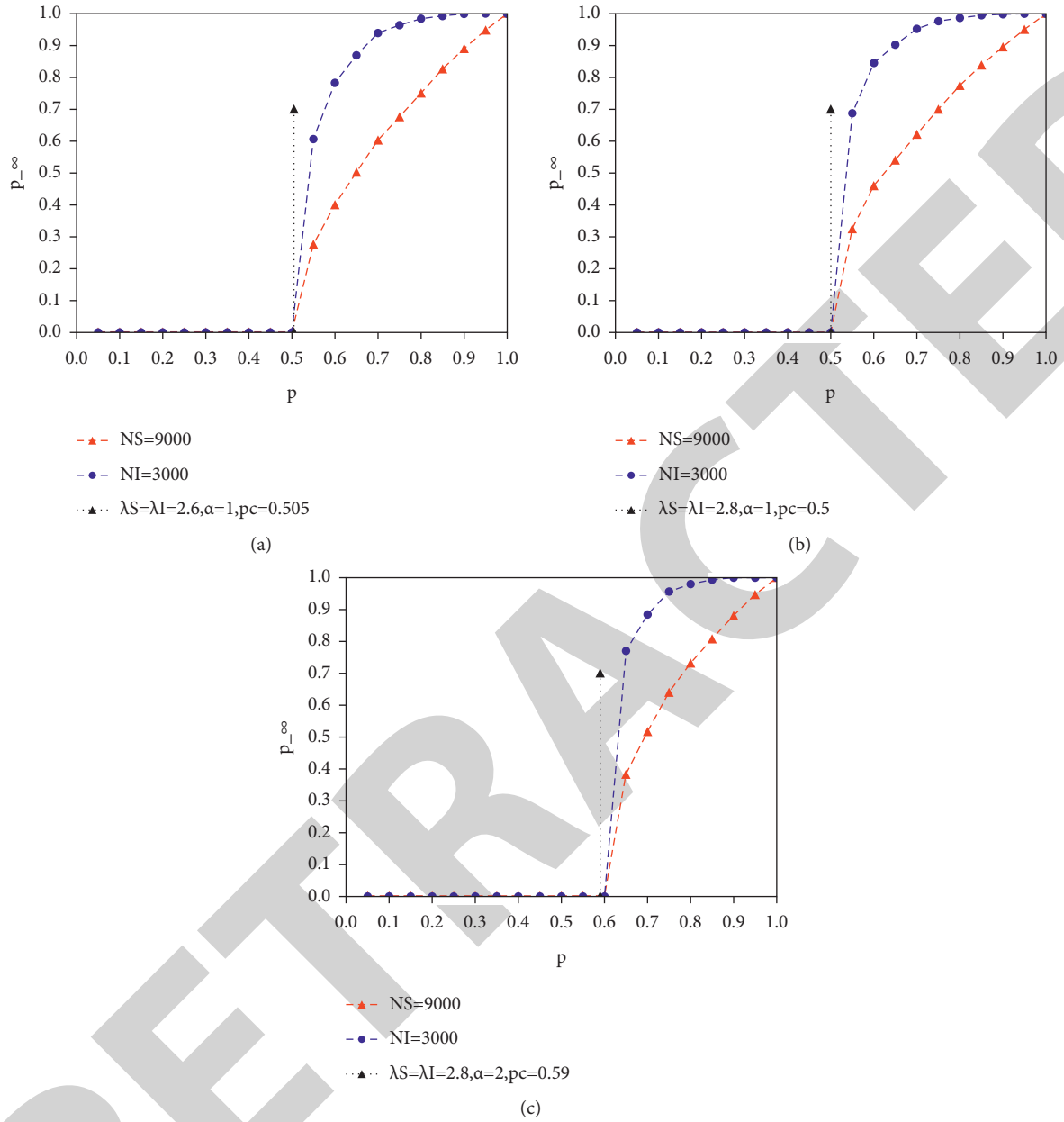

Figure 5: The fraction of survival nodes in network S and I. Abscissa p represents the proportion of nodes that are not attacked in the targeted-attack process and $1 - p$ represents the percentage of the attacked nodes. Ordinate p_∞ indicates the proportion of remaining nodes when cascading failure stops after the coupled network receives a targeted attack. The red line represents network S, the blue line represents network I, and the abscissa corresponding to the black line represents the theoretical value of the critical threshold when the networks fail.

in the construction of real-life infrastructure. We can connect more critical nodes in the coupled system to multiple dependent sides to improve its security.

5.2.2. Influence of Network Size. In Figure 6(a), various values of p are selected in the range [0.485, 0.545] near $pc = 0.5$, and we conduct 60 experiments at each point to calculate more accurately the times that the coupled system has not entirely failed. The same method is applied in Figure 6(b), except that the value of α is changed. By observing Figure 6, we can see that the curve is steadily approaching critical importance as nodes' size increases. When network nodes' scale reaches a specific value, the first-order phase transition occurs near the critical threshold, distinct from the second-order phase transition of single networks.

5.2.3. Comparison between Different λ and α. Figure 7 compares the change of percolation threshold under different λ. We keep the other parameters unchanged. The abscissa represents the power-law index λ of the scale-free network, and the ordinate stands for the critical threshold pc

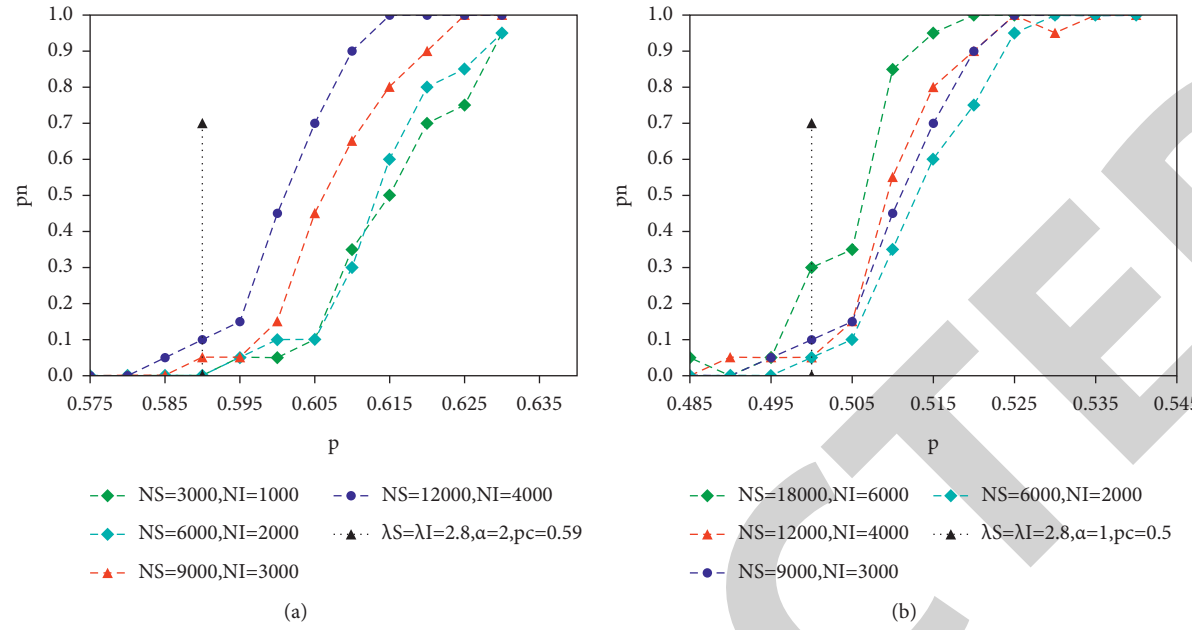

Figure 6: The existence probability of the huge component. We select several groups of points around the critical threshold for comparative analysis.

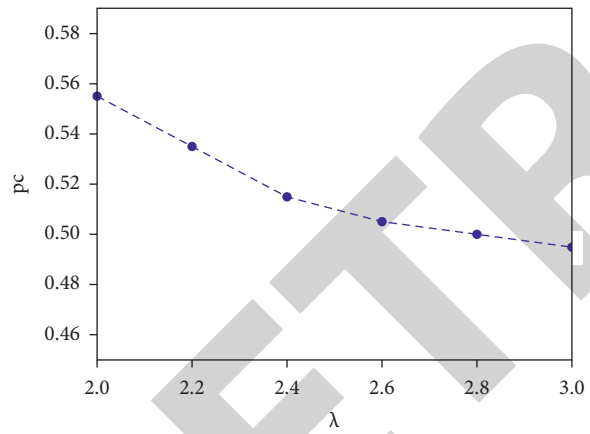

Figure 7: The relationship between pc and λ. We compare the transforming of pc in the case of different power-law indexes λ.

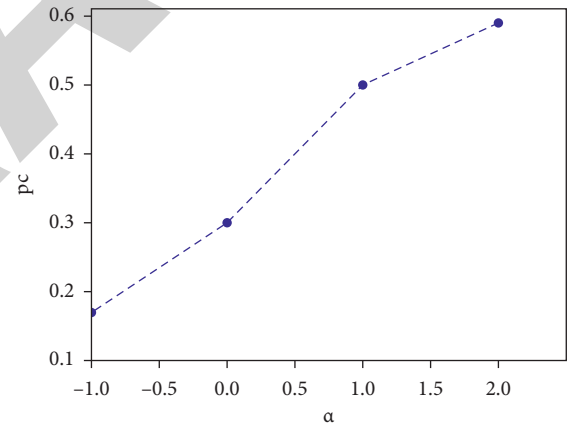

Figure 8: The relationship between pc and α. We compare different α with different critical threshold pc. The abscissa represents α, and the ordinate represents the essential threshold pc.

of the network. It can be found from the figure that the seepage threshold decreases with the increase of λ. This reduction is relatively small. This shows that the power-law index of scale-free networks is not a factor that significantly changes coupled networks' robustness. This has an efficient significance for us to analyze CPS.

In Figure 8, for comparison purposes, we set the rest of the network's parameters to the same, only changing the value of α. The λ of the network is 2.8, and the minimum degree of network is 3. We can see that the critical threshold pc increases with an increase of α. This implies that the robustness of the network is reduced. The greater α is, the more vulnerable the nodes with high degrees are. Hence, the network's robustness decreases. This also verifies the previous theoretical results. We can also find that the percolation threshold pc is not alike when the scale-free network faces various targeted attacks. This is because of the characteristic that the least nodes of the scale-free network have the most connections, which leads to the difference between percolation thresholds in the face of different attacks. This is beneficial for us to protect the coupled network in real life. Correspondingly, we should analyze different situations according to the actual network structure.

5.3. Engineering Applications. As a typical CPS application, the smart grid provides us with many conveniences in real life [53]. Figure 9 shows a vast power grid system with isolated grids connected by long-distance transmission lines. A smart grid system is composed of a power grid network and communication network coupled and interdependent [35]. The power grid is controlled by the communication

Figure 9: A huge power grid system with isolated grids connected by long-distance transmission lines.

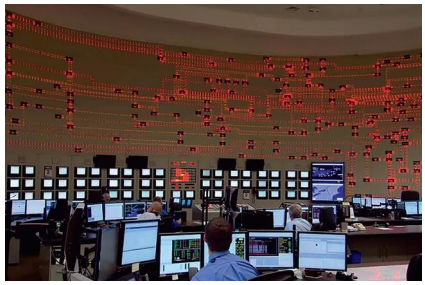

Figure 10: The grid nodes appear red in a large area.

network, which also needs power from the power grid [54]. This interdependence will increase the risk of the power grid, and the failure of a network node will cause the collapse of the whole power grid [55, 56].

The most classic blackout in the United States was in 2003 [45]. A circuit line is entangled with the roots of the trees growing under it. Due to the lack of timely measures, nearly 20 high-voltage lines were out of control. This led to more severe consequences. The interruption of one line made other high-voltage lines overburdened, and eventually, the entire New York State Grid collapsed. As shown in Figure 10, it can be seen that the power grid collapses in a large area, and the grid nodes appear red in large areas. Therefore, it is necessary to study the cascading failure dynamics of coupled networks.

We can use the network model to abstract the smart grid system into a system composed of two coupled networks. We can take the real power grid's data scale and the average degree of network nodes to study the cascading failure dynamics caused by partial node failure. According to the power grid failure process simulation, we can purposefully study the critical nodes in the network and study network nodes' influence and network size on the cascading failure dynamics. According to this data, we can improve the robustness of the smart grid more effectively.

6. Conclusion

The research work addressed the emerging IIoT concept and its cybersecurity concerns with probable outcomes. The security risk analysis is not yet developed, and various strategies, conceptual design, and technical implementations are expected in this paperwork. The cascading failure theory was suggested for providing risk assessment services at the regional level by improving effectiveness, accessibility, and expandability. The risk analysis scheme proposed for security service corresponds to the interdependent IIoT application environment. The key risk factor is an essential part of ensuring IIoT system security; however, the research study addressed the mathematical mechanism analysis details of the emerging IIoT systems. We propose a novel risk analysis scheme for security modeling and analysis of such interdependent IIoT environments in the design. This method aims to support the development of secure IIoT environments at the modeling and simulation levels framework, and risk factors were hacked at the basic level itself. The methods utilized resistance and risk alleviation techniques. In the future, we plan to examine the environment of other complex application scenarios of our proposed risk analysis method, such as connected cars and houses, wearable devices, and smart medical care in intelligent interdependent IIoT applications. This will give us an in-depth understanding of the risks and challenges faced in these environments. They must be addressed to protect the security of interdependent distributed devices and all connected service-related participants, thereby limiting the risk elements that may affect the entire interdependent IIoT environment. Besides, we also aim to extend our work by including privacy requirements during the modeling and the analysis of such systems by including other risk requirements such as privacy protection and ciphertext retrieval in the modeling process. Through this extension, we will be able to protect user data security in interdependent IIoT systems and identify key risk factors that may affect user security requirements, such as anonymity, interconnectivity, unobservability, and undetectability, etc. Finally, we plan to introduce artificial intelligence and game theory methods for comparative analysis to determine the attacker's attack path mitigation technology.

Data Availability

All the data has been explained in detail in the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under grant nos. 62072412, 61902359, 61702148, and 61672468, in part by the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security under grant AGK2018001.

References

[1] K. Huang, Q. Zhang, C. Zhou, N. Xiong, and Y. Qin, "An efficient intrusion detection approach for visual sensor networks based on traffic pattern learnings," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 10, pp. 2704–2713, 2017.

[2] W. Wu, N. Xiong, and C. Wu, "Improved clustering algorithm based on energy consumption in wireless sensor networks," *IET Networks*, vol. 6, no. 3, pp. 47–53, 2017.

[3] 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 & Engineering Management*, Selangor, Malaysia, December 2015.

[4] Z. You and L. Feng, "Integration of industry 4.0 related technologies in construction industry: a framework of cyber-physical system," *IEEE Access*, vol. 8, pp. 122908–122922, 2020.

[5] A. Villalonga, G. Beruvides, F. Castaño, and R. E. Haber, "Cloud-based industrial cyber-physical system for data-driven reasoning: a review and use case on an industry 4.0 pilot line," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5975–5984, 2020.

[6] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[7] M. Canizo, A. Conde, S. Charramendieta, R. Miñón, R. G. Cid-Fuentes, and E. Onieva, "Implementation of a large-scale platform for cyber-physical system real-time monitoring," *IEEE Access*, vol. 7, pp. 52455–52466, 2019.

[8] B. M. Lee and H. Yang, "Massive MIMO for industrial Internet of things in cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 2641–2652, 2017.

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

[10] D. B. Rawat, C. Bajracharya, and G. Yan, "Towards intelligent transportation cyber-physical systems: real-time computing and communications perspectives," in *Proceedings of the SoutheastCon 2015*, pp. 1–6, Fort Lauderdale, FL, USA, April 2015.

[11] E. Bartocci, J. Deshmukh, A. Donzé et al., "Specification-based monitoring of cyber-physical systems: a survey on theory, tools and applications," in *Lectures on Runtime Verification*, pp. 135–175, Springer, Berlin, Germany, 2018.

[12] X. Yuan, C. J. Anumba, and M. K. Parfitt, "Cyber-physical systems for temporary structure monitoring," *Automation in Construction*, vol. 66, pp. 1–14, 2016.

[13] Y. Lu, "Cyber physical system (CPS)-based industry 4.0: a survey," *Journal of Industrial Integration and Management*, vol. 2, no. 3, Article ID 1750014, 2017.

[14] R. M. Murray, K. J. Astrom, S. P. Boyd, R. W. Brockett, and G. Stein, "Future directions in control in an information-rich world," *IEEE Control Systems*, vol. 23, no. 2, pp. 20–33, 2003.

[15] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: automation networks in the era of the Internet of things and industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[16] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 46, pp. 1429–1444, 2017.

[17] S. Aamir, L. Malrey, Y. K. Lee et al., "Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information," *Symmetry*, vol. 7, no. 3, pp. 1176–1210, 2015.

[18] H. I. AL-Salman and M. H. Salih, "A review cyber of industry 4.0 (cyber-physical systems (CPS), the internet of things (IoT) and the internet of services (IoS)): components, and security challenges," in *Proceedings of the 2nd International Conference on Advance & Scientific Innovation*, vol. 1424, Medan, Indonesia, July 2019.

[19] J. Herwan, S. Kano, R. Oleg, H. Sawada, and N. Kasashima, "Cyber-physical system architecture for machining production line," in *Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, St. Petersburg, Russia, May 2018.

[20] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, pp. 2375–2385, 2017.

[21] E. Pavlenko and D. Zegzhda, "Sustainability of cyber-physical systems in the context of targeted destructive influences," in *Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 830–834, St. Petersburg, Russia, May 2018.

[22] L. Ribeiro and M. Björkman, "Transitioning from standard automation solutions to cyber-physical production systems: an assessment of critical conceptual and technical challenges," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3816–3827, 2017.

[23] C. Lu, A. Saifullah, B. Li et al., "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1013–1024, 2016.

[24] L. Guo, B. Yang, J. Ye et al., "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3335–3347, 2021.

[25] 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, pp. 83–92, 2018.

[26] L. Ding and M. Tan, "Robustness of random scale-free networks against cascading failure under edge attacks," *Journal of Communications*, vol. 11, pp. 1088–1094, 2016.

[27] F. Imbault, M. Swiatek, R. D. Beaufort, and R. Plana, "The green blockchain: managing decentralized energy production and consumption," in *Proceedings of the IEEE International Conference on Environment & Electrical Engineering & IEEE Industrial & Commercial Power Systems Europe*, Milan, Italy, June 2017.

[28] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," *IEEE Network*, vol. 27, no. 1, pp. 19–24, 2013.

[29] M. Rungger and P. Tabuada, "A notion of robustness for cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2108–2123, 2016.

[30] G. Dong, J. Gao, L. Tian, R. Du, and Y. He, "Percolation of partially interdependent networks under targeted attack," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 85, no. 1 Pt 2, Article ID 016112, 2012.

[31] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 83, no. 6 Pt 2, Article ID 065101, 2011.

[32] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

[33] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in

Proceedings of the 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), Melbourne, VIC, Australia, June 2013.

[34] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, 2012.

[35] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures, and robustness," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1708–1720, 2012.

[36] L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, "Stability and topology of scale-free networks under attack and defense strategies," *Physical Review Letters*, vol. 94, Article ID 188701, 2005.

[37] J. Shao, S. V. Buldyrev, L. A. Braunstein, S. Havlin, and H. E. Stanley, "Structure of shells in complex networks," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 80, Article ID 036105, 2009.

[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] R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition," *Physical Review Letters*, vol. 105, Article ID 048701, 2010.

[40] S. Chattopadhyay and H. Dai, "Estimation of robustness of interdependent networks against failure of nodes," in *Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, December 2016.

[41] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Robustness of a partially interdependent network formed of clustered networks," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 89, Article ID 032812, 2014.

[42] 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, Statistical, Nonlinear, and Soft Matter Physics*, vol. 90, Article ID 012803, 2014.

[43] D. Z. Tootaghaj, N. Bartolini, H. Khamfroush, T. He, N. R. Chaudhuri, and T. L. Porta, "Mitigation and recovery from cascading failures in interdependent networks under uncertainty," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 501–514, 2019.

[44] S. W. Son, G. Bizhani, C. Christensen, P. Grassberger, and M. Paczuski, "Percolation theory on interdependent networks based on epidemic spreading," *EPL (Europhysics Letters)*, vol. 97, no. 1, Article ID 16006, 2011.

[45] 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.

[46] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," *Physical Review Letters*, vol. 85, no. 21, pp. 4626–4628, 2000.

[47] V. K. S. Shante and S. Kirkpatrick, "An introduction to percolation theory," *Advances in Physics*, vol. 20, no. 85, pp. 325–357, 1971.

[48] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 87, Article ID 052812, 2013.

[49] G. Dong, R. Du, L. Tian, and R. Liu, "Percolation on interacting networks with feedback-dependency links," *Chaos*, vol. 25, no. 1, Article ID 013101, 2015.

[50] F. Radicchi, "Percolation in real interdependent networks," *Nature Physics*, vol. 11, no. 7, 2015.

[51] S. Havlin, H. E. Stanley, A. Bashan, J. Gao, and D. Y. Kenett, "Percolation of interdependent network of networks," *Chaos, Solitons & Fractals*, vol. 72, pp. 4–19, 2015.

[52] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "DDOA: a dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, 2016.

[53] M. Parandehgheibi, E. H. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," in *Proceedings of the IEEE International Conference on Smart Grid Communications*, Venice, Italy, November 2014.

[54] L. Martins, R. Girao-Silva, L. Jorge, A. Gomes, F. Musumeci, and J. Rak, "Interdependence between power grids and communication networks: a resilience perspective," in *Proceedings of the DRCN 2017-Design of Reliable Communication Networks; 13th International Conference*, Munich, Germany, March 2017.

[55] Z. Huang, C. Wang, T. Zhu, and A. Nayak, "Cascading failures in smart grid: joint effect of load propagation and interdependence," *IEEE Access*, vol. 3, pp. 2520–2530, 2015.

[56] P.-Y. Kong, "Optimal configuration of interdependence between communication network and power grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4054–4065, 2019.