Received March 1, 2020, accepted March 16, 2020, date of publication March 25, 2020, date of current version April 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983335

Security Analysis of CPS Systems Under Different Swapping Strategies in IoT Environments

HAO PENG[1,3], CAN LIU[1], DANDAN ZHAO[1], HONGXIA YE[1], ZIAN FANG[1], AND WEI WANG[2]

[1]College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China
[2]Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China
[3]Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China

Corresponding author: Wei Wang (wwzqbx@hotmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61902359, Grant 61602418, Grant 61872323, and Grant 61672468, in part by the Social Development Project of Zhejiang Provincial Public Technology Research under Grant 2016C33168, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY16F030002, in part by the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security under Grant AGK2018001, and in part by the Ministry of Education in China (MOE) Project of Humanities and Social Science under Grant 15YJCZH125.

ABSTRACT In this paper, we give attention to the robustness of the Cyber-Physical System, which consists of interdependent physical resources and computational resources. Numerous infrastructure systems can evolve into the Cyber-Physical System, e.g., smart power grids, traffic control systems, and wireless sensor and actuator networks. These networks depend on their interdependent networks, which provide information or energy to function. In a Cyber-Physical System, a small failure could trigger serious cascading failures within the entire interdependent networks. In this paper, we try to alleviate these cascading failures between interdependent networks to reduce losses. We discuss the robustness of systems for random attacks by calculating the size of functioning components in entire networks. We change the inter-links topology of the coupled networks to enhance the reliability of the entire system. Then we get the most effective swapping strategy in enhancing the robustness of the Cyber-Physical System compared to previous studies. Different systems' structures would influence the performance of swap inter links strategies on improving the reliability of networks. Moreover, our work could guide how to optimize a Cyber-Physical System topology by reducing the influence of cascading failures.

INDEX TERMS Cyber-physical system, interdependent networks, cascading failures, swap inter-links strategy, robustness, giant component.

I. INTRODUCTION

With the rapid development of the economy and society, the Internet has been widely used in our daily life and society. Since the networks bring great convenience and economic benefits, more and more companies and countries are focusing on them. Meanwhile, the networks have further grown from single small-scale to complex large-scale. The network plays an increasingly important role in our everyday life. Over the last decade, extensive research on complex networks has been conducted. This research demonstrates that many critical properties of the network's organization, growth, and robustness. More recently, research on network robustness has been pushed further. Nodes organize networks, but the network does not occur in isolation. These depend on the way in which nodes are interconnected and relatively independent with each node [1]. More networks are interdependent to function properly [1]–[10]. A representative interdependent networks example is Cyber-Physical Systems(CPS).

Cyber-Physical Systems are designed to seamlessly integrate computing components, networks, and physical devices into well-defined environments for specific purposes [11]–[15]. It is deeply embedded in cyber capabilities in the physical world to transform interactions with the physical world [16], [17]. A CPS typically consists of physical elements, a communication network, and a computation and control unit. The communication network can exchange data with other systems. A control unit is necessary to interact with the real world and process the data obtained [18]–[20]. Data exchange is the essential feature of the CPS since the data can be linked and evaluated centrally. In other words, the CPS is an embedded system that can send and receive data

The associate editor coordinating the review of this manuscript and approving it for publication was Yuyu Yin.

over networks [19]. More and more infrastructure systems evolve into CPSs in daily life. For example, we usually regard the smart grid system [12], [21]–[23] and radar system [24] as a typical representative of a CPS. If a failure occurs in an infrastructure system, it can cause property damage or even loss of human life. Therefore, the reliability of CPS is one of the leading indicators to be considered by designers and maintainers. It is especially important to prevent large-scale failures of a CPS and enhance its robustness. We have known that a small fault in an interdependent network could easily lead to severe failures in entire networks, which have shown in previous research work [2]. In this way, understanding how to improve the ability of a CPS to resist cascading failures poses a significant challenge, which is vital for understanding the resilience of natural systems [1].

In order to maintain a healthy daily life and promote social development, many researchers pay more attention to enhance the robustness of the CPS. In this paper, we abstract the concrete CPS into an unweighted and undirected network graph are made up of points and lines. We achieve the enhancement of CPS system reliability by changing the topology relationship of the dependent edges. The main contributions of this paper are listed as following:

(i) First, we simulate a variety of system models and attack proportions to get as comprehensive as possible the effects of different strategies on changing system reliability.

(ii) Second, we get the high eigenvector centrality swapping inter-links strategy has the best effect on enhancing network reliability in all our situations. This strategy performs better than the interlinking of nodes by their intralayer degrees in the monotonic order, which is discussed in [25] in enhancing network reliability.

The outline of this work is as follows: we introduce the review literature in Section II. In Section III, we propose our functional model for CPS and the different swapping strategies. Section IV performs the results of the simulation and analysis points. Conclusions and summarized in Section V.

II. LITERATURE REVIEW

A. RELATED WORK

Cyber-Physical Systems are becoming increasingly critical for daily life. Maintaining the reliability of CPS has become an important research direction. Many scholars have explored this topic from the hardware direction [24], [26]–[29]. Pennekamp *et al.* [22] study that CPS will lead to a plethora of new dataflows on the Internet of Production (IOP). Zhang *et al.* [30] investigate the security implications of multistate channel implementation and symbol energy, considering their effect on the CPS acceptance threshold. Many scholars are gradually applying machine learning to enhance the reliability of CPS [24], [26]. There are some researches on CPS reliability based on software [29], [31]. This method aims at changing the system state through software to ensure that the system is always in a safe state. In addition to changing network reliability from hardware and software, some scholars have also promoted research on CPS reliability from the direction of assessing the security of CPS [32].

The above approaches are always considered the physical device and the cyber components. Another direction of studying the reliability of the CPS is to abstract a CPS system into an interdependent network. This direction ignores the differences between devices and treats all devices and components as objects with similar functions. It pays attention to the point-to-point topological relationship between the networks. Since the specifics of actuation and physical world reaction, a unique CPS model is infeasible [33]. The challenge of establishing this model is to identify common ingredients and components of a CPS present in a variety of scenarios, models, and investigate them. To resolve this challenge, Zhang *et al.* [34] propose a classification for CPS. In a Cyber-Physical System, physical devices such as batteries and sensors seem to be physical components. The cyber components include embedded computers and communication networks. The interaction and relation between physical components and cyber components are essential to maintain the operation of the system. Thus, combining and applying these components and ingredients to certain categories of CPS and corresponding concrete systems are other challenges to building a CPS model. To model the interconnection and interconnection between cyber components and physical components, Wang *et al.* [35] and Derler *et al.* [36] have proposed different algorithms for focusing on the above interaction and related challenges.

Based on the above CPS models, researchers propose various theories to enhance the robustness of networks. The first approach is to protect critical nodes [37], [38]. However, Nguyen *et al.* [38] proved that finding critical nodes is an NP-hard problem. The second approach is to make nodes autonomous, which is concluded by Shao *et al.* [39]. However, this approach is likely to cost millions of dollars [40]. The third approach is to refigure the topology of the network by rewiring [21], [41], [42]. However, it is difficult to come true in a factual existing network. The fourth approach is adding links in networks. Cui *et al.* [40], Ji *et al.* [43], Jiang *et al.* [44], and Beygelzimer *et al.* [45] discussed the effects on the robustness of interdependent networks after different addition strategies. The approach described in [25] and [46] is to adjust the dependency links allocation. This approach might not increase or even reduce costs. It takes into account the structure of the existing networks for optimization. This approach is feasible if we consider the topology of existing networks and the costs of entire networks. In [43], some adding intra-links strategies are proposed. Through adding intra-links by different strategies, researchers find that the interdependent networks can get the best reliability by adding intra-links in the order of low IDD values.

Tu *et al.* [47] study the robustness of a single network with different values of network centralities. They find the optimal network topology to achieve the best network robustness. They do not mention how to change the topological network metrics. However, they conclude that the metrics will change when the network gets better robustness.

Changing the relationship of interdependent networks will not influence the links in one single network. Thus, this method has less impact on network topology. Based on the above favorable factors, we think swapping dependency links as a better method to improve interdependent networks reliability.

B. INTERDEPENDENT NETWORKS

Complex networks have been investigated extensively since the 1960s. Both of Erdös-Rényi networks(ER networks) and scale-free networks(SF networks) are briefly described to depict the real-world networks. The compositions and characteristics of these networks have been well studied. In a single network, intra-links of nodes satisfy a certain degree distribution. For example, nodes follow binomial distribution in ER networks while following power-law degree distribution in SF networks. Every node in the ER network has the same number of intra-links [33]. Therefore, all nodes in the ER network have the same degree [48]. Different from the ER network, the SF network is a network whose degree distribution follows a power-law distribution. SF network is a skewed degree distributed network [46], which means that most nodes have a few intra-links, and a few of the nodes have lots of intra-links.

To model interdependent networks, Buldyrev *et al.* [2] proposed a 'one-to-one' correspondence model, where two interdependent networks A and B have the same number of nodes which means that $N_A = N_B$. The inter-link represents an interdependent relationship between the two nodes which are in different networks. This model could reflect one kind of corresponding relationship of real networks, and it has been deeply studied. Different from Shao *et al.* [39] consider real networks as mutually dependent networks. One node in network A depends on more than one node in network B, and vice versa. This is the 'multiple-to-multiple' correspondence model. But the 'multiple-to-multiple' correspondence model has some limitations which don't have solutions yet [33].

C. CASCADING FAILURES

The cascading failures are always caused by a small failure in one network. The failure can lead to fragmentation of the entire interdependent networks. Percolation theory is a useful method to explore the reliability of networks. The giant component is the largest connected subnetwork in all interdependent networks. Generally, it is thought to be the normal working part of the networks [21], [42], [47]. Thus, the giant component is usually used to reflect network reliability when cascading failures stop. The giant component is the most widely used and persuasive measure of network robustness. One node in interdependent networks can operate after cascading failures only if it satisfies two conditions:

(i) The node has at least one inter-link with a node that functions;
(ii) It belongs to the giant component of its network.

We assume that the cascading failures are triggered by randomly removing $(1-p)$ fraction of nodes in network A. After removing $(1-p)\cdot|N_A|$ of nodes in network A, both of intra-links and inter-links of these nodes are removed. In the next stage, some nodes in network B are removed if they lose inter-links from network A. Since nodes and links are removed, network B fragments into several components. As the conditions of nodes can operate, we have shown above, except the giant component that can still operate, and the rest is removed. This stage results in network B split-up and some nodes in network A have no inter-links from network B. Then network A breaks up again. The cascading failures recurse between network A and B. These cascading failures processes will not stop until the interdependent networks reach one of the two stable states:

(i) All nodes in the two networks are completely failed;
(ii) The networks are divided into giant components without further cascading failures.

Fig 1 gives an example of failure propagation in interdependent networks. In the initial stage, there are seven nodes in network A and B. Then, node A_3 is attacked and triggers cascading failures. When the cascading stops, only two nodes remain functioning in the network A and B, respectively.

After cascading failures, the giant component might disappear. The number of giant components N'_A and N'_B is 0. The relative size of the giant component G is 0 too. If there exists the giant component in interdependent networks, G could be calculated by:

$$G = \frac{N'_A + N'_B}{N_A + N_B} \tag{1}$$

If $(1-p)$ is big enough, G will decrease to 0.

III. METHODOLOGY

In this section, we briefly introduce our CPS models and strategies of swapping inter-links. We construct CPS models by the most popular network models in recent research. After that, we use the 'one-to-one' correspondence model to interact with physical components and cyber components together. Then we sort nodes by three kinds of centralities values: degree centrality, betweenness centrality, and eigenvector centrality. Based on the above centralities, seven kinds of swapping links approaches are simulated in our models.

A. CPS MODELS

Previous studies show that the ER network and SF network could accurately simulate certain characteristics of natural networks. In this way, the simulation results will be more persuasive and real-world usable. Depending on this, we select one or two from the ER network and SF network to build interdependent networks to construct a CPS model. There are four kinds of CPS structures: ER network couples ER network(ER-ER), ER network couples SF network(ER-SF), SF network couples ER network(SF-ER) and SF network couples SF network(SF-SF).

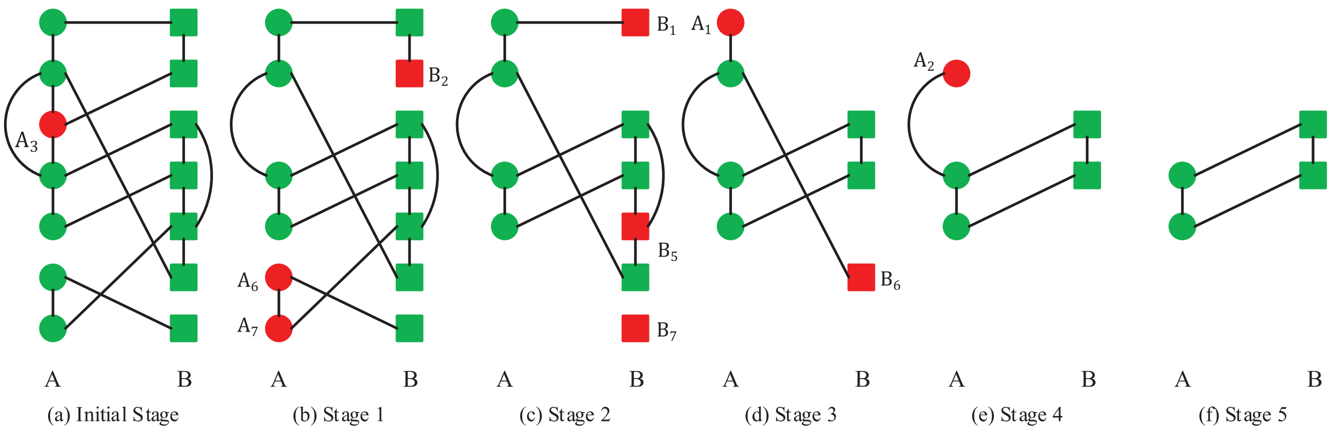


FIGURE 1. Cascading failures in interdependent networks. Initially, network *A* and *B* have seven nodes in their own network. The random attack upon network *A* causes failure of node A_3. In stage 1, we remove all intra-links and inter-links with node A_3. Thus, A_6 and A_7 are disconnected from the giant component in the network *A*. As a result, B_2 is removed since it loses its inter-link from network *A*. In stage 2, A_6, A_7 and B_2 are removed with their all links. Consequently, three nodes of network *B* fail, while node B_1 is excluded from giant component and B_5 and B_7 lose supporting links. Therefore, in stage 3, all of the node B_1, B_5, B_7, and their links are removed, network *B* fragments into components, while node B_6 is disconnected from the giant component, so fails. Node A_1 fails as it doesn't have a supporting link. In stage 4, A_2 fails because it doesn't connect to the giant component. In the final stage, the remaining nodes of this interdependent network reach one stable situation without further cascading failures.

Considering the two connection models mentioned in section II-B, we apply a more mature ‘one-to-one’ correspondence as to the model of interdependence in our simulation CPS models. We define N_A and N_B as the number of nodes in network A and network B. Each node in network A has function depending on exactly only one node in network B, and vice versa. In other words, one node in network A only has one inter-link from network B. This also applies to network B. We apply the ‘one-to-one’ correspondence model between networks to link inter-links to represent the interdependent relationships. To conform to this model, we presume the coupled networks have the same number of nodes.

B. SORT NODES BY CENTRALITY 1: DEGREE CENTRALITY

The degree is the simplest but important centrality to estimate the significance of nodes in a network. If one node locals in the center of the network, it has a high value of degree and be considered as a crucial node [43], [48]. When high degree nodes are attacked, a large number of nodes will be affected. In this way, the network has worse reliability than destroying low degree nodes. In an undirected network, a node degree is equal to the number of nodes’ intra-links [43]. Sorting single network nodes by their degrees, there are an ascending order and a descending order.

Low degree swapping links algorithm (LD) defines as ranking the nodes of network A and B with their degrees in ascending orders, respectively. We select nodes in the top array of increasing orders that are nodes A_i and B_j. Then we determine if there is an inter-link between the two nodes which we selected. There are two situations about connection:

(i) The first is that an inter-link does not link node A_i and B_j;

(ii) The second is that node A_i and B_j have linked by an inter-link.

When the second case occurs, we check whether the next array nodes of the two orders connect with an inter-link. In the first case, we have to change the inter-links in A_i and B_j. Firstly, we find there are two inter-links between A_i and B_n and A_m and B_j in the interdependent networks. Thus, these two nodes A_i and B_j do not link by one inter-link. Then, we remove all inter-links between A_i, B_n, A_m, and B_j. Finally, we link A_i and B_j and connect A_m and B_n with a new inter-link, respectively. After that, we complete a onetime swapping inter-link operation. This swapping procedure repeats until the demanded number appears.

The other algorithm which is based on the degree values is the high degree swapping links algorithm(HD). It sorts nodes in a descending sequence of nodes degree values. The swapping inter-link process takes place between the nodes with the highest degrees values. In [25], Chattopadhyay et al. simulate that linking nodes with inter-links in HD order leads to maximal ‘one-to-one’ interdependent network robustness.

In the interdependent networks, inter-similarity could effectively reflect the degree differences of connected nodes in coupled networks. Inter degree-degree difference(*IDD*) [43], [49] is to quantitatively evaluate the inter-similarity of interdependent networks. *IDD* is defined as:

$$IDD_{AB}(u, v) = k_u^A - k_v^B \tag{2}$$

where $IDD_{AB}(u, v)$ is the degree difference between node u in network A and its dependent node v in network B. k_u^A and k_v^B are the degree of node u and v. To ensure the inter-links distribution, we need to calculate all A nodes *IDD* for each node in network B. When N_A is the same as N_B, we set $|N_A|^2$ times subtraction calculation to get all *IDD* values.

Low inter degree-degree difference swapping links algorithm(LIDD) is to sort nodes in ascending order by *IDD* values. Then we swap links that satisfy the first situation which we described in LD. We do not swap links in high

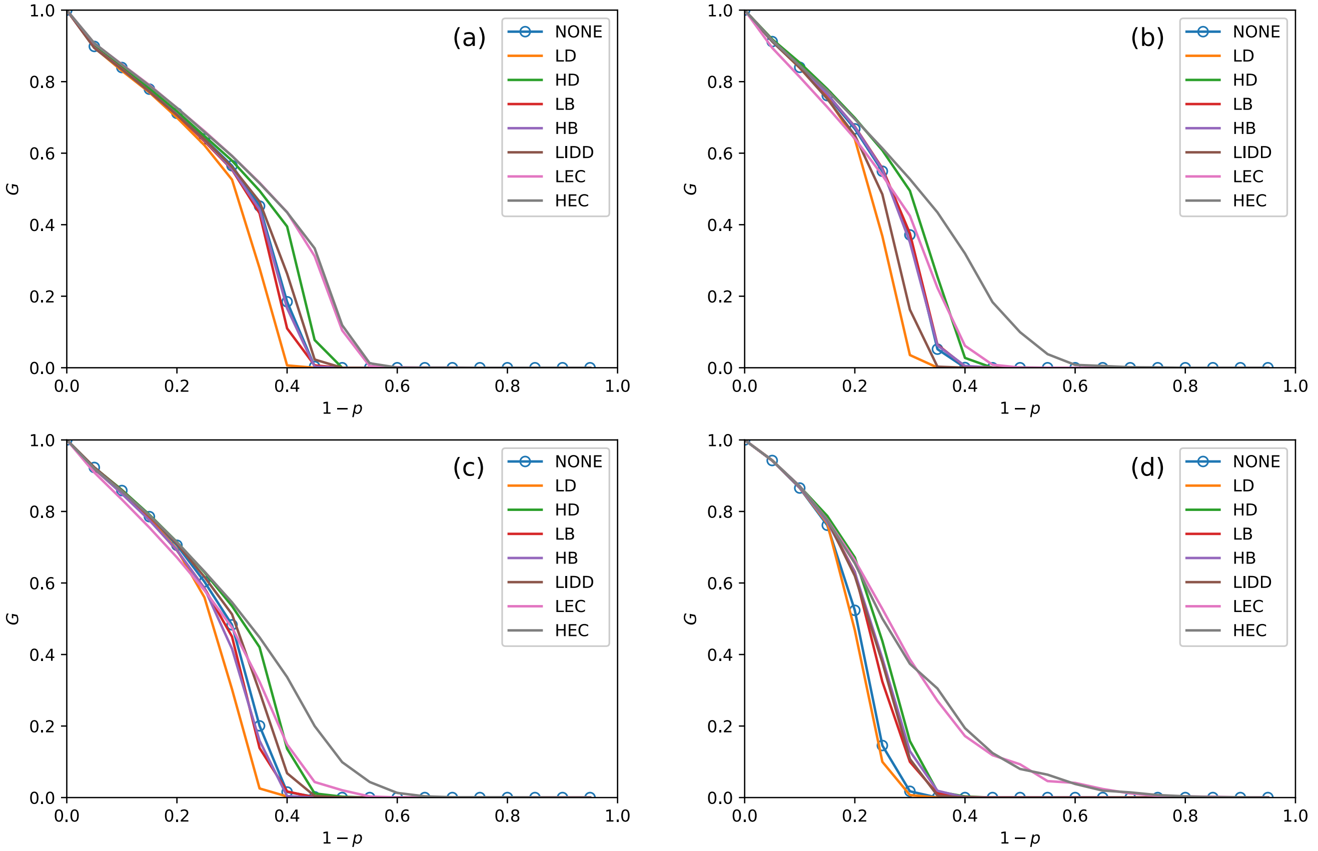


FIGURE 2. The fraction of function nodes in systems when $f_s = 30\%$. Figure (a), (b), (c), and (d) are the systems that are coupled by ER-ER, ER-SF, SF-ER, and SF-SF, respectively. Seven exchange strategies are compared with original independent networks in different systems structures. In (a) and (d), LEC and HEC are the best strategies in enhancing G and p_c, which have similar advantages. The structures of (a) and (d) are coupled by the same network. (b) and (c) show the results of random attack in ER-SF and SF-ER systems. HEC shows better performance to the other strategies. There is an intersection between the LEC and NONE curves in (b) and (c). In four figures, LD yields the worst performance. LB and HB can be regarded as equivalent.

inter degree-degree difference since it will be similar to HD. As described in [43], if $IDD > 0$, swapping inter-links with the values of high inter degree-degree is similar to the high degree swapping links algorithm. We have measured the robustness of networks by HD in the preceding. Thus, we take LIDD as our swapping strategy. This swapping process will be repeated a set number of times.

C. SORT NODES BY CENTRALITY CENTRALITY 2: BETWEENNESS CENTRALITY

The betweenness centrality is a metric that reflects the routing performance in one network. If one node sites in a large number of the shortest paths in the network, the node is more important than other nodes. Betweenness centrality is defined as:

$$B(v) = \sum_{i \neq j} \frac{\sigma_{ij}(v)}{\sigma_{ij}} \tag{3}$$

where σ_{ij} is the number of shortest paths going from node i to node j and $\sigma_{ij}(v)$ is the number of shortest paths going from node i to node j through node v [43], [48]. We calculate nodes betweenness centralities by Eq 3 and order nodes in ascending order and descending order. Low betweenness swapping links algorithm(LB) is swapping inter-links between the value of the lowest betweenness centrality.

High betweenness swapping links algorithm(HB) is ranking nodes in descending order. The process of swapping link occurs between the nodes with the highest betweenness values in their respective networks. If the nodes with highest betweenness values have connected with an inter-links, we judge whether there are edges between the nodes with the second highest degree. We swap inter-links between the nodes which are not linked by an inter-link. The specific swapping process we have explained in LD. This process of HB and LB will be repeated a set number of times.

D. SORT NODES BY CENTRALITY CENTRALITY 3: EIGENVECTOR CENTRALITY

The eigenvector centrality is an extension of degree centrality [48]. In degree centrality, all nodes importances are regarded as equivalent. But the importance of nodes is affected by their neighbors. If neighbor nodes are important, then this node will be considered important, too. This characteristic has been found in many realistic networks.

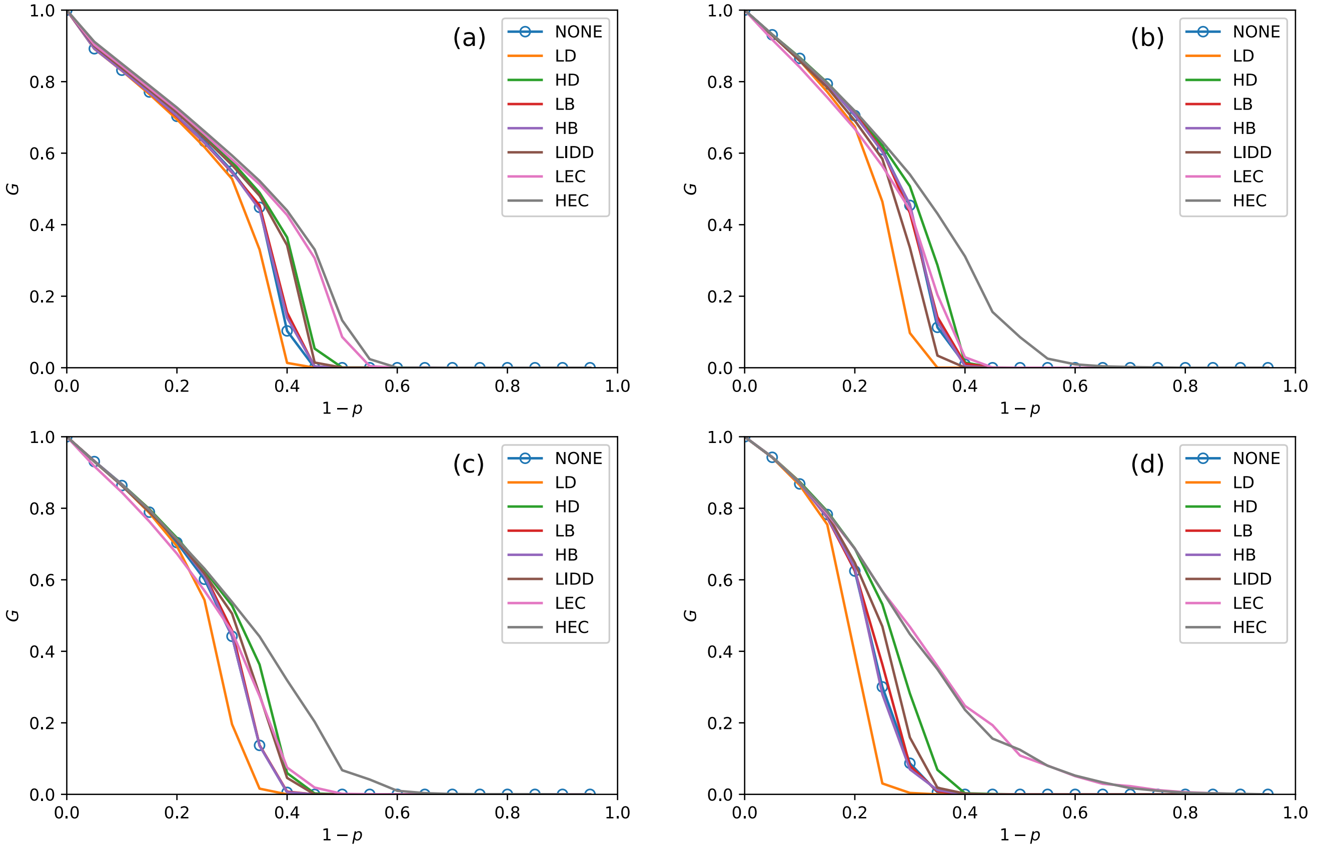


FIGURE 3. The fraction of function nodes in systems under $f_s = 50\%$. These four figures represent the systems we build, which are ER-ER, ER-SF, SF-ER, and SF-SF, respectively. In (a) and (d), LEC and HEC are the best strategies in enhancing G and p_c, which have similar results. p_c increases to 0.63. The structures of (a) and (d) are coupled by the same network. (b) and (c) are systems established by the ER network and SF network. These two figures perform the results after a random attack. HEC has the best results in improving robustness. When $1 - p = 0.3$, LEC and NONE have an intersection in (b). The value of G in LEC is smaller than NONE as $1 - p < 0.3$. While $1 - p > 0.3$, LEC is better than NONE in (b). The intersection of LEC and NONE appears at $1 - p = 0.4$ in (c). In all figures, LD yields the worst performance. LB and HB can be regarded as equivalent.

x_i means the eigenvector centrality of node i. The initial values of all x_i are set to 1. This is not a useful measure of network centrality. Thus we use x_i to calculate a better one x_i', which we define to be the sum of the centralities of i's neighbors thus: [48]:

$$x_i' = \kappa_1^{-1} \sum_j A_{ij} x_j \tag{4}$$

where A_{ij} is an element of the adjacency matrix. In one network, all A_{ij} can be written as a matrix notation A. κ_1 is the largest eigenvector value of A.

We calculate the eigenvector centrality of nodes in two interdependent networks. Then we sort nodes by the values of the eigenvector centrality in increasing order and descending order separately. The high eigenvector centrality swapping strategy (HEC) is that we choose the nodes with the highest eigenvector centrality values in two networks. Low eigenvector centrality swapping strategy (LEC) is swapping links between nodes that have the lowest value of eigenvector centrality in the network A and B. The specific swapping processes we have explained in LD. This process of HEC and LEC will be repeated a set number of times.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

To simulate a CPS model, we adopt two types of popular networks, which are Erdös-Rényi networks(ER networks) and scale-free networks(SF networks) to couple an interdependent system. ER network orders Poisson distribution and SF network obey power-law degree distribution. In order to comply with the generality, we construct the ER network with the size of the network $N = 1000$ and the average degree $\langle k \rangle = 4$. In SF network, the parameter $\gamma = 3$, the average degree $\langle k \rangle = 4$ and network size is $N = 1000$. After distributing two single networks, we randomly assign 'one-to-one' correspondence interdependencies between single networks. All of the intra-links and inter-links are bidirectional in our models. After the above setting, we have built a CPS completely.

We randomly remove $(1-p)N_A$ nodes to represent random failures in a CPS. Then we calculate the fraction of working nodes G in every $(1-p)$ with $(1-p)$ increasing 0.05 in each step. So we simulate one kind of swapping link strategies for 20 times in a specified model. To obtain an accurate result, we simulate 100 times in each $(1 - p)$. We use NONE as a comparative strategy with other strategies, which means

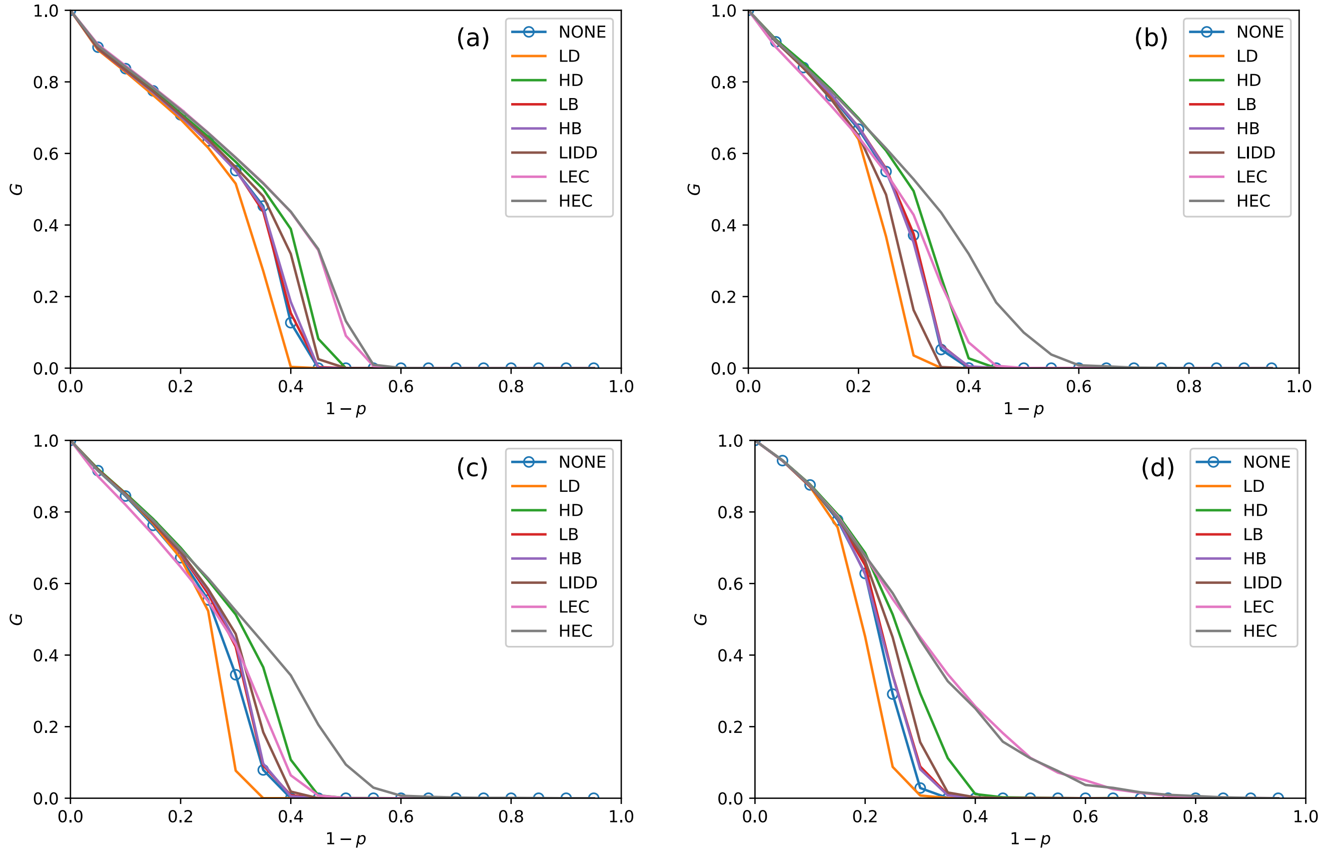


FIGURE 4. The fraction of function nodes in systems when $f_s = 70\%$ and the systems are coupled by ER-ER, ER-SF, SF-ER, and SF-SF respectively in figure (a), (b), (c) and (d). As shown in (a) and (d), it's clearly finding that the best strategies are LEC and HEC to enhance not only G but also p_c. Especially in (d), the value of p_c is increased to 0.8. (a) and (d) are systems that are the same network correspondence. According to the results shown in (a) and (d), we easily concluded that when network A and B are in one type network, HEC and LEC are the best choices to swap inter-links to improving robustness. (b) and (c) show the results of random attack in different coupled systems. HEC is the first selection to enhance reliability. There is an intersection between the LEC and NONE curves in each figure. As $1-p = 0.25$ and $1-p = 0.35$, LEC and NONE have an intersection in each figure. There is a negligible gap between LB and HB.

we do not change any inter-link. We assume the fraction of swapping inter-links as f_s:

$$f_s = L'/L \tag{5}$$

where L' is the number of swapping inter-links, and L means the total number of inter-links in one CPS. Since our systems follow 'one-to-one' correspondence interdependent and the inter-links are bidirectional, the number of inter-links should be equal to the number of nodes $N_A(N_B)$. Therefore, Eq 5 could be written as $f_s = L'/1000$.

In [25], scholars find that the interlinking of nodes by HD to maximal network robustness. However, they only simulated ER-ER interdependent networks to verify this conclusion. Thus, we construct five different kinds of CPS models to verify our proposed swapping inter-links strategies and compare the results with the HD algorithm. To compare the effects of different inter-links swapping strategies, we evaluate the reliability of a CPS by G and p_c. p_c represents the maximum tolerant ability against random failures. G and p_c are bigger, the reliability of CPS is better.

Here we compare different performances of the swapping inter-links strategies shown in Section III when $f_s = 30\%$, $f_s = 50\%$ and $f_s = 70\%$. From Fig 2, Fig 3 and Fig 4, we observe the following conclusions:

(i) Not all swapping strategies can enhance CPS reliability. In all of the above figures, we find that the network reliability of using LD to change the connection relationship of inter-links is worse than that of the original network.

(ii) Under the same experimental environment, the difference between HB and LB in enhancing the reliability of CPS can be ignored. This finding can be concluded as different betweenness centrally values have little effect on system reliability.

(iii) Under one particular centrality, swapping nodes inter-links with large values have a better influence on improving network robustness than with small values. The values of pc are not smaller in swapping nodes inter-links with large values than with small values. For example, in figure 4(a), the values of p_c in LD and HD are 0.45 and 0.5. In figure 4(c), the p_c values of LEC and HEC are 0.5 and 0.62.

When nodes have high centrality values linked by inter-links, the giant components in two single networks are huge. Although nodes are not operating since they lose inter-links, the other nodes in the giant component which connect the above-failed nodes can operate. This swapping inter-links operation will make a large number of nodes that can still work after cascading failure. In contrast, when we choose to swap inter-links with low values of nodes, the nodes connect with failed nodes with intra-links is easier to be apart from the giant component after randomly attacking nodes. As a result, the system is easier to collapse. This finding is in agreement with the finding of [25].

(iv) For the same number of swapping inter-links, we find that the LEC strategy has opposite results for enhancing G at ER-SF and SF-ER interdependent networks for different $(1 - p)$ values. In ER-ER and SF-SF systems, LEC and HEC have a negligible difference in improving G. Under the situation of $f_s = 30\%$ and ER network couples SF network situation, LEC has worse performance than NONE in increasing G value at $(1 - p) < 0.25$. This phenomenon is reversed when $(1 - p) > 0.25$. The abscissa of the intersection of LEC and NONE in SF-ER interdependent networks is 0.3. When the value of f_s is fixed, the size of G in LEC and NONE always have intersections in ER-SF and SF-ER simulation diagrams. This shows that different network structures and different attack ratios play critical roles in choosing the swapping link strategy.

(v) HEC has the best effect on enhancing network reliability in all situations. It also performs a clear advantage in increasing the value of p_c. In figure 4(b), the value of HEC is bigger than 0.6 and the other strategies p_c values are around 0.4. Compared with HEC and HD, both of the values of G and p_c have obvious advantages. In the case of f_s determination, the differences values of p_c between HEC and other strategies are most evident in ER-SF and SF-ER interdependent networks. Besides, HEC yields a clear advantage in relieving a sharply dropping of G when p closes to p_c. It means that the system could be controlled to prevent the system from completely collapsing.

Above all, the HEC strategy is the primary choice for improving system robustness under a given number of swapping inter-links. If we get one certain centrality value of interdependent networks, we can swap inter-links with nodes that have high centrality values. To ensure the best results in enhancing system reliability, we need to figure out the system structure and the fraction of attacks when determining the swapping strategy. We considered three topological metrics to quantify the location centrality of the nodes. When the two nodes which are in the central position are connected, there will be a large number of nodes in the central position of the entire system. The giant component gets bigger and bigger. After the random attack, the number of the giant component will also be relatively large. Based on the above explanation, our experimental conclusions are easy to understand.

V. CONCLUSION

To study the effect of cascading failures and robustness in real social networks, we construct different CPS models which consist of interdependent physical-resources and computational-resource networks. Meanwhile, we analyze the reliability of an interdependent CPS by measuring the value of the relative size of the giant component after cascading failures. Based on three kinds of network centralities, we design seven swapping inter-links strategies to change the topology of interdependent CPS. By comparing the performance of these strategies in a CPS, we find that it is more advantageous to transform inter-links with high-values centrality nodes than with low-values. At the same time, the simulation results show that the high eigenvector centrality swapping strategy is superior to the other strategies in enhancing the reliability of a CPS. This finding can help network builders to design a better network structure that can survive random network attacks.

However, our proposed models have some limitations, which could be our future work. In this study, we only consider the ‘one-to-one’ correspondence as a relationship in different networks. While some researchers build the ‘one-to-multiple’ correspondence to represent inter-links topology in a CPS [33], this paper still selects giant components as the functional part. The small and isolated components could also operate locally in reality. Furthermore, we will try to find some schemes to maximize the number of the giant component in forthcoming work.

REFERENCES

[1] S. D. S. Reis, Y. Hu, A. Babino, J. S. Andrade, Jr, S. Canals, M. Sigman, and H. A. Makse, “Avoiding catastrophic failure in correlated networks of networks,” *Nature Phys.*, vol. 10, no. 10, pp. 762–767, Oct. 2014.

[2] 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, Apr. 2010.

[3] R. G. Little, “Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures,” *J. Urban Technol.*, vol. 9, no. 1, pp. 109–123, Apr. 2002.

[4] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. D. Porcellinis, and R. Setola, “Modelling interdependent infrastructures using interacting dynamical models,” *Int. J. Crit. Infrastruct.*, vol. 4, nos. 1–2, p. 63, 2008.

[5] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, “Networks formed from interdependent networks,” *Nature Phys.*, vol. 8, no. 1, pp. 40–48, Jan. 2012.

[6] E. A. Leicht and R. M. D’Souza, “Percolation on interacting networks,” 2009, *arXiv:0907.0894*. [Online]. Available: http://arxiv.org/abs/0907.0894

[7] Y. Yin, J. Xia, Y. Li, Y. Xu, W. Xu, and L. Yu, “Group-wise itinerary planning in temporary mobile social network,” *IEEE Access*, vol. 7, pp. 83682–83693, 2019.

[8] J. Yu, J. Li, Z. Yu, and Q. Huang, “Multimodal transformer with multi-view visual representation for image captioning,” 2019, *arXiv:1905.07841*. [Online]. Available: http://arxiv.org/abs/1905.07841

[9] J. Yu, M. Tan, H. Zhang, D. Tao, and Y. Rui, “Hierarchical deep click feature prediction for fine-grained image recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, early access, Jul. 30, 2019, doi: 10.1109/TPAMI.2019.2932058.

[10] H. Peng, Z. Kan, D. Zhao, and J. Han, “Security assessment for interdependent heterogeneous cyber physical systems,” *Mobile Netw. Appl.*, 2019, doi: 10.1007/s11036-019-01489-z.

[11] F. Arafsha, F. Laamarti, and A. E. Saddik, “Development of a wireless CPS for gait parameters measurement and analysis,” in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (I2MTC)*, May 2018, pp. 1–5.

[12] L. Xuhong and L. Muhai, "Application of CPS in the complex network," in *Proc. 4th Int. Conf. Intell. Comput. Technol. Autom.*, Mar. 2011, pp. 1067–1069.

[13] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, "Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services," *IEEE Internet Things J.*, early access, Dec. 2, 2019, doi: 10.1109/JIOT.2019.2956827.

[14] H. Gao, Y. Duan, L. Shao, and X. Sun, "Transformation-based processing of typed resources for multimedia sources in the IoT environment," *Wireless Netw.*, vol. 11, pp. 1–17, Nov. 2019.

[15] W. Wang, M. Tang, H. Yang, Y. Do, Y.-C. Lai, and G. Lee, "Asymmetrically interacting spreading dynamics on complex layered networks," *Sci. Rep.*, vol. 4, no. 1, p. 5097, May 2015.

[16] R. Poovendran, "Cyber–Physical systems: Close encounters between two parallel worlds [Point of View]," *Proc. IEEE*, vol. 98, no. 8, pp. 1363–1366, Aug. 2010.

[17] Y. Yin, L. Chen, Y. Xu, J. Wan, H. Zhang, and Z. Mai, "Qos prediction for service recommendation with deep feature learning in edge computing environment," *Mobile Netw. Appl.*, 2019, doi: 10.1007/s11036-019-01241-7.

[18] H. Koc, S. S. Shaik, and P. P. Madupu, "Reliability modeling and analysis for cyber physical systems," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0448–0451.

[19] N. Jazdi, "Cyber physical systems in the context of industry 4.0," in *Proc. IEEE Int. Conf. Autom., Qual. Test., Robot.*, May 2014, pp. 1–4.

[20] W. Wang, Q.-H. Liu, J. Liang, Y. Hu, and T. Zhou, "Coevolution spreading in complex networks," *Phys. Rep.*, vol. 820, pp. 1–51, Aug. 2019.

[21] J. Zhang, E. Yeh, and E. Modiano, "Robustness of interdependent random geometric networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 3, pp. 474–487, Jul. 2019.

[22] J. Pennekamp, M. Henze, S. Schmidt, P. Niemietz, M. Fey, D. Trauth, T. Bergs, C. Brecher, and K. Wehrle, "Dataflow challenges in an Internet of production: A security & privacy perspective," in *Proc. ACM Workshop Cyber-Phys. Syst. Secur. Privacy CPS-SPC*, 2019, pp. 27–38.

[23] S. F. Mihalache, E. Pricop, and J. Fattahi, "Resilience enhancement of cyber-physical systems: A review," in *Power Systems Resilience*. 2019, doi: 10.1007/978-3-319-94442-5_11.

[24] S. Cohen, T. Gluck, Y. Elovici, and A. Shabtai, "Security analysis of radar systems," in *Proc. ACM Workshop Cyber-Phys. Syst. Secur. Privacy CPS-SPC*, 2019, pp. 3–14.

[25] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3847–3862, Sep. 2017.

[26] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, 2019.

[27] A. Prathiba and V. S. K. Bhaaskaran, "Hardware footprints of S-box in lightweight symmetric block ciphers for IoT and CPS information security systems," *Integration*, vol. 69, pp. 266–278, Nov. 2019.

[28] N. O. Tippenhauer and A. Wool, "Cps-spc 2019: Fifth workshop on cyber-physical systems security and privacy," in *Proc. 2019 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 2695–2696.

[29] J. Gardiner, B. Craggs, B. Green, and A. Rashid, "Oops i did it again: Further adventures in the land of ICS security testbeds," in *Proc. ACM Workshop Cyber-Phys. Syst. Secur. Privacy - CPS-SPC*, 2019, pp. 75–86.

[30] J. Zhang, A. Yang, Q. Hu, and G. P. Hancke, "Security implications of implementing multistate distance-bounding protocols," in *Proc. ACM Workshop Cyber-Physical Syst. Secur. Privacy - CPS-SPC*, 2019, pp. 99–108.

[31] R. Romagnoli, B. H. Krogh, and B. Sinopoli, "Design of software rejuvenation for CPS security using invariant sets," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 3740–3745.

[32] J. H. Castellanos and J. Zhou, "A modular hybrid learning approach for black-box security testing of CPS," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Bogota, Colombia: Springer, Jun. 2019, pp. 196–216.

[33] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Trans. Comput.*, vol. 64, no. 8, pp. 2158–2168, Aug. 2015.

[34] F. Zhang, Z. Shi, and S. Mukhopadhyay, "Robustness analysis for battery-supported cyber-physical systems," *ACM Trans. Embedded Comput. Syst.*, vol. 12, no. 3, pp. 1–27, Mar. 2013.

[35] Z. Wang, A. Scaglione, and R. J. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 28–39, Jun. 2010.

[36] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[37] S. Ruj and A. Pal, "Analyzing cascading failures in smart grids under random and targeted attacks," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, May 2014, pp. 226–233.

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

[39] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 83, no. 3, Mar. 2011, Art. no. 036116.

[40] P. Cui, P. Zhu, K. Wang, P. Xun, and Z. Xia, "Enhancing robustness of interdependent network by adding connectivity and dependence links," *Phys. A, Stat. Mech. Appl.*, vol. 497, pp. 185–197, May 2018.

[41] D. Zhou, H. E. Stanley, G. D'Agostino, and A. Scala, "Assortativity decreases the robustness of interdependent networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 86, no. 6, Dec. 2012, Art. no. 066103.

[42] K. Kamran, J. Zhang, E. Yeh, and E. Modiano, "Robustness of interdependent geometric networks under inhomogeneous failures," in *Proc. 16th Int. Symp. Model. Optim. Mobile, Ad Hoc, Wireless Netw. (WiOpt)*, May 2018, pp. 1–6.

[43] X. Ji, B. Wang, D. Liu, G. Chen, F. Tang, D. Wei, and L. Tu, "Improving interdependent networks robustness by adding connectivity links," *Phys. A, Stat. Mech. Appl.*, vol. 444, pp. 9–19, Feb. 2016.

[44] Z. Jiang, M. Liang, and D. Guo, "Enhancing network performance by edge addition," *Int. J. Modern Phys. C*, vol. 22, no. 11, pp. 1211–1226, Nov. 2011.

[45] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Phys. A, Stat. Mech. Appl.*, vol. 357, nos. 3–4, pp. 593–612, 2005.

[46] Y. Kazawa and S. Tsugawa, "Robustness of networks with skewed degree distributions under strategic node protection," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 14–19.

[47] H. Tu, Y. Xia, H. H.-C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 1, pp. 126–130, Jan. 2019.

[48] M. Newman, *Network*. London, U.K.: Oxford Univ. Press, 2018.

[49] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, "Inter-similarity between coupled networks," *EPL (Europhys.Lett.)*, vol. 92, no. 6, Dec. 2010, Art. no. 068002.

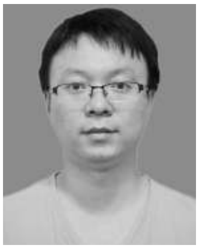
HAO PENG received the Ph.D. degree from Shanghai Jiao Tong University, in 2012. He is currently an Associate Professor with the Department of Computer Science and Engineering, Zhejiang Normal University. His main research interests include the Internet of Things (IoT) security, distributed system security, and CPS system security.

CAN LIU received the B.S. degree in computer science and technology from Jiangxi Normal University, in 2017. Since 2017, she has been studying in computer science and engineering with Zhejiang Normal University. Her main research interests include network and information security and CPS system security.

DANDAN ZHAO received the Ph.D. degree from Shanghai Jiao Tong University, in 2012. She is currently a Lecturer with the Department of Computer Science and Engineering, Zhejiang Normal University. Her main research interests include network and information security, distributed system security, and complex system security.

HONGXIA YE is currently pursuing the bachelor's degree with the Department of Software Engineering, Zhejiang Normal University. Her main research is network and information security.

ZIAN FANG is currently the bachelor's degree with the Department of Software Engineering, Zhejiang Normal University. Her main research is complex system security.



WEI WANG received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2017. He is currently an Associate Professor with Sichuan University, Chengdu. He has published more than 70 articles in the field of network science and spreading dynamics. His research interests include investigating the spreading mechanisms of information, epidemic, rumor, and associated critical phenomena in complex networks.