Hindawi
Discrete Dynamics in Nature and Society
Volume 2021, Article ID 9965707, 12 pages
https://doi.org/10.1155/2021/9965707

Research Article

A Comprehensive Analysis of Robustness in Interdependent Mechatronic Systems under Attack Strategies

Gang Xu,[1] Yanhui Wang,[2,3,4,5] Yucheng Hao,[2,3] Limin Jia,[2,3,4,5] Zeyun Yang,[6] and Zhichao He[2,3]

[1]*CRRC Academy (Qingdao), Qingdao 266111, China*
[2]*State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China*
[3]*School of Traffic and Transportation, Beijing Jiaotong University, Beijing 100044, China*
[4]*Beijing Research Center of Urban Traffic Information Sensing and Service Technology, Beijing Jiaotong University, Beijing 100044, China*
[5]*Research and Development Center of Transport Industry of Technologies and Equipment of Urban Rail Operation Safety Management, Beijing 100044, China*
[6]*CRRC Qingdao Sifang Co., Ltd., Qingdao 266111, China*

Correspondence should be addressed to Yanhui Wang; wangyanhui@bjtu.edu.cn and Yucheng Hao; 18114021@bjtu.edu.cn

Received 6 March 2021; Accepted 14 May 2021; Published 12 June 2021

Academic Editor: Binxiang Dai

With the development of mechatronic systems, different kinds of subsystems within them are highly correlated to each other due to the demand for the special function. To assess the robustness in the mechatronic system under various disturbances, we build an interdependent mechatronic system as an interdependent machine-electricity-communication network (IMECN) and adopt the improved cascading failure model where the occurrence of the failure propagation is decided by a proportion threshold δ. In order to fully explore the robustness under different disturbances, we develop attack strategies concerning nodes, edges, and interdependent links by considering measures for a node. Then, we also define the robustness metric to quantify the performance of IMECN during the entire attack process. The mass transit vehicle is taken as an example to investigate the impact of attack strategies on the robustness at different δ in a real-world mechatronic system. It is found that each subnetwork in this IMECN has a scale-free property. Based on simulation results, we obtain the most efficient attack strategies to remove nodes, edges, and interdependent links for different possibilities of triggering the failure propagation. In addition, we find that the attacks on nodes and interdependent links make IMECN more vulnerable compared with the ones on edges. This work provides theoretical insights into the comprehensive analysis of the robustness in interdependent mechatronic systems.

1. Introduction

Interdependent mechatronic systems, such as a mass transit vehicle and an airplane, are the backbone of modern society as they provide essential services for our life. These systems consist of a tremendous amount of equipment and there exist complex interactions between units. Moreover, different kinds of subsystems are not isolated but highly dependent on each other in order to perform the specific function in reality. Complex networks have been widely studied and applied in various fields as an effective analytical approach; therefore, we adopt this theory to model the interdependent mechatronic system and explore its robustness under disturbances in detail.

The topology structure is a key parameter to characterize the property of networks. As a result, the robustness of scale-free and small-world networks against targeted attacks and random failures was explored [1–3]. As we all know, the more important the attacked node, the more vulnerable the network [4]. Although the degree is a basic measure, the significance of a node for an entire network is hardly quantified by it. As a consequence, the attack strategy with

regard to the betweenness was presented to remove the critical node [5]. Nie et al. gave a new attack strategy that combines the degree and the betweenness [6]. Optimal attack strategies for undirected and directed networks were given based on the tabu search [7, 8], respectively. There have been a large number of works focusing on attack strategies in artificial networks. However, the behavior of the artificial network subjected to attacks hardly reflects that of the real-world network. To this end, Bellingeri et al. investigated the impact of attack strategies to remove nodes and edges on the robustness of real-world networks [9–11].

One or several failed components may cause the breakdown of the adjacent node or even the collapse of the whole system in some cases. Typical examples are the blackout of the western United States power grid that took place on August 10, 1996, and the congestion of the Internet [12]. As a result of the impact of cascading failures, Motter et al. developed a cascading model where the load on the node is dependent on the total number of shortest paths passing through it [13, 14]. Additionally, the degree [15, 16], the betweenness [17], and the harmonic closeness [18, 19], as metrics of nodes to quantify their characteristics, have been widely adopted to obtain the load. Similarly, in order to define the cascading failure model concerning the edge, these measures have also been further studied [20–24]. On the basis of the comparison of different definitions of the load, Hao et al. found that the networks where the loads on the node and edge are defined as the harmonic closeness have a higher level of robustness [18, 19, 24]. Different from the cascading failure induced by overloads, Newman et al. employed the generating function formalism to study the failure process of nodes and edges by means of percolation theory from another perspective [25].

With the deepening of the study of network robustness, many instances have demonstrated that the behavior of modern systems is interdependent on each other. In particular, once a system breaks down, the other system is likely to be affected by it due to the lack of interdependency. Enlightened by this, Buldyrev et al. presented a framework for capturing the response of the entire system during the failure propagation between subsystems [26]. In the past decade, there have been a large number of works paying attention to the robustness analysis of interdependent networks. The interdependency makes interdependent networks vulnerable to attacks; thus, Brummitt et al. analyzed the change of the robustness of interdependent networks for different coupling probabilities [27]. In a similar way, more in-depth studies on partially interdependent networks were conducted [28–31]. In addition to the number of interdependent links, the robustness of interdependent networks with the coupling preferences according to the node load [32], the node degree [33], and the harmonic closeness [34], has also been thoroughly explored. In addition, in consideration of the vulnerability of the single network subjected to targeted attacks, the attack strategies aiming at removing the key nodes and edges for interdependent networks were proposed [35–37]. Many works have revealed that the interdependent network is more vulnerable than the single network; thus, Chattopadhyay et al. presented an optimization framework for the maximization of the robustness of interdependent networks by optimizing the distribution of interdependent links [38]. Based on the study on the interdependent network, Gao et al. developed an analytical framework for a network of networks and pointed out that its robustness is deeply affected by the interdependence with other networks [39].

In practice, based on network science, many studies have conducted the vulnerability assessment of the transportation system [40–43], the power grid [44, 45], and so on. In addition, the interdependent networks have also been widely applied in the robustness analysis of the real-life system. As typical interdependent systems, the evaluation of the robustness and the dynamics analysis of cascading failures for the interdependent cyber-physical networks [46], the interdependent energy-physical networks [47], and the interdependent transportation-power network [48] have been discussed.

As discussed above, although the research on interdependent networks has attracted great attention, there is a relative lack of investigation on the mechatronic system from the aspect of complex networks. Up to now, the works [49, 50] have studied the reliability of mechatronic systems on the basis of the network theory, but they neglect the difference among various kinds of components. Moreover, the response of the robustness in the mechatronic system under different attack strategies (i.e., the removal of nodes, edges, and interdependent links) has not yet been thoroughly analyzed. To address these issues, we construct an interdependent machine-electricity-communication network model to characterize the relationship between units in the interdependent mechatronic system. Taking into account different measures for a node, we developed the attack strategies to destroy nodes, edges, and interdependent links. Furthermore, the case study whose data is obtained by a real-world interdependent mechatronic system is conducted to explore the response of the robustness in this system subjected to the above attack strategies in consideration of the improved cascading failure model. According to the simulation results, we analyze the efficiency of attack strategies to impair the robustness.

2. Model

2.1. Interdependent Machine-Electricity-Communication Networks. There have been many methods to model the complex system up to now, such as empirical methods, agent based methods, system dynamics based methods. In this paper, we adopt the network science to analyze the robustness of the interdependent mechatronic system; therefore, it is modeled as an interdependent machine-electricity-communication network (IMECN) composed of three subnetworks, that is, a machine network (MN), an electricity network (EN), and a communication network (CN). For each subnetwork, a node stands for a minimum maintenance unit and an edge stands for the functional relationship between units. If fasteners (e.g., bolt, screw, welding) connect equipment p (corresponding node i) with

equipment q (corresponding node j), node i has an edge with node j within the machine network. In a similar way, when there exists an electric current (a packet) between two units, corresponding nodes are connected by an edge within the electricity network (the communication network). Note that if nodes i and j within different subnetworks represent the same equipment, node i has an interdependency link with node j and is the dependent node of node j and vice versa. That is to say, we build an interdependent network with the one-to-one correspondence.

2.2. Cascading Failure Model in IMECN. The existing cascading failure model in interdependent networks is based on the percolation theory; however, this theory only takes into account the cluster with the largest size, that is, the giant component. For this purpose, we adopt the extended cascading failure model [51], which considers the fact that the nongiant component may also keep working in the special condition in reality even though the network is split into some clusters. In this improved model, the active component has two conditions to be satisfied: (1) It has at least an interdependency link with the other two subnetworks, respectively, and (2) its size proportion p_{c_i} is not smaller than the proportion threshold δ, where the size proportion p_{c_i} of the component c_i equals the proportion of its size in the subnetwork size. If a component has a small size proportion or does not have the two interdependency links from the other two subnetworks, it will break down and the cascading failure will be triggered, which leads to the removal of the nodes and edges (including the intralink and interdependent link) within it. Due to the absence of the interdependent link, the dependent node of a failed node is also considered to be inactive. The cascading failure process stops until no inactive component occurs. Obviously, the larger δ is, the more likely the cascading failure is to be triggered.

2.3. Attack Strategies. In terms of an interdependent network, we can attack three kinds of elements, that is, the node, the edge, and the interdependent link. Generally speaking, the more important the attacked node, edge, and interdependent link, the more vulnerable the network against cascading failures induced by their failures. To this end, we quantify the importance of nodes, edges, and interdependent links by the degree, the betweenness, and the PageRank of nodes. This is because these three metrics capture the characteristics of a node from different aspects. The degree and the betweenness can reflect the local and global information on a node, respectively, and the PageRank can reflect the knowledge of the adjacent node. Because the existing measures for a node only reflect its importance in the subnetwork, we adopt the interdependent measures combining the significance of a node and its dependent node. The interdependent degree ik_i, the interdependent betweenness ib_i, and the interdependent PageRank ipr_i are given as follows, respectively:

$$\begin{aligned} ik_i &= k_i + \sum_{m\in\Phi_i} k_m, \\ ib_i &= b_i + \sum_{m\in\Phi_i} b_m, \\ ipr_i &= pr_i + \sum_{m\in\Phi_i} pr_m, \end{aligned} \tag{1}$$

where k_i, b_i, pr_i are the degree, the betweenness, and the PageRank of node i, respectively. Φ_i is the set of dependent nodes of node i.

According to the work [35], we calculate the priority $pn(i)$ of attacked node i, which is defined as follows:

$$pn(i) = \alpha\frac{ik_i}{\sum_i ik_i} + \beta\frac{ib_i}{\sum_i ib_i} + \gamma\frac{ipr_i}{\sum_i ipr_i}, \tag{2}$$

where α, β, γ are parameters to control the strength of the interdependent degree, the interdependent betweenness, and the interdependent PageRank of node i, respectively. According to the work [36], we propose the priority $pe(ij)$ of attacked edge ij in the light of interdependent measures of end nodes, which is defined as follows:

$$pe(ij) = \alpha\frac{ik_i ik_j}{\sum_i\sum_j ik_i ik_j} + \beta\frac{ib_i ib_j}{\sum_i\sum_j ib_i ib_j} + \gamma\frac{ip_i ip_j}{\sum_i\sum_j ip_i ip_j}. \tag{3}$$

Based on the definitions of the priority of the attacked node, edge, and interdependent link, corresponding attack strategies are described in detail as follows. By varying the parameters of equations (2) and (3), we can obtain different attack strategies which are listed in Table 1.

Nodes and edges under the corresponding attack strategies are, respectively, one by one removed in the descending order of their priorities at each simulation step t. For the interdependent link attack strategies, one of the end nodes of the interdependent link is attacked in the descending order of the priority of this end node at each simulation step t.

2.4. Metric for Robustness. In the field of complex networks, existing studies have proposed many metrics to quantify the robustness of networks. It is well known that the robustness of interdependent networks is measured by the size of the giant component. Considering that the size of interdependent networks under edge attack strategies may keep a certain value, we use the natural connectivity (NC) [52] to reflect the robustness of IMECN, which is shown as follows:

$$nc = \ln\left(\frac{1}{n}\sum_{k=1}^{n} e^{\lambda_k}\right), \tag{4}$$

where λ_k is the kth eigenvalue of the adjacent matrix A and n is the number of nodes in a subnetwork. For simplicity, the natural connectivity of networks after attacks is normalized by the one of initial network. Therefore, the robustness R during the attack strategies is defined as follows:

Table 1: Attack strategies for different values of parameters.

Kind of attack strategies	Parameters	Considered measures	Attack strategies
Node attack strategies obtained by equation (2)	$\alpha = 1, \beta = 0, \gamma = 0$	ik	ND
	$\alpha = 0, \beta = 1, \gamma = 0$	ib	NB
	$\alpha = 0, \beta = 0, \gamma = 1$	ip	NP
	$\alpha = 1, \beta = 1, \gamma = 0$	ik and ib	NDB
	$\alpha = 1, \beta = 0, \gamma = 1$	ik and ip	NDP
	$\alpha = 0, \beta = 1, \gamma = 1$	ib and ip	NBP
	$\alpha = 1, \beta = 1, \gamma = 1$	ik, ib and ip	NDBP
Edge attack strategies obtained by equation (3)	$\alpha = 1, \beta = 0, \gamma = 0$	ik	ED
	$\alpha = 0, \beta = 1, \gamma = 0$	ib	EB
	$\alpha = 0, \beta = 0, \gamma = 1$	ip	EP
	$\alpha = 1, \beta = 1, \gamma = 0$	ik and ib	EDB
	$\alpha = 1, \beta = 0, \gamma = 1$	ik and ip	EDP
	$\alpha = 0, \beta = 1, \gamma = 1$	ib and ip	EBP
	$\alpha = 1, \beta = 1, \gamma = 1$	ik, ib and ip	EDBP
Interdependent link attack strategies obtained by equation (2)	$\alpha = 1, \beta = 0, \gamma = 0$	ik	ILD
	$\alpha = 0, \beta = 1, \gamma = 0$	ib	ILB
	$\alpha = 0, \beta = 0, \gamma = 1$	ip	ILP
	$\alpha = 1, \beta = 1, \gamma = 0$	ik and ib	ILDB
	$\alpha = 1, \beta = 0, \gamma = 1$	ik and ip	ILDP
	$\alpha = 0, \beta = 1, \gamma = 1$	ib and ip	ILBP
	$\alpha = 1, \beta = 1, \gamma = 1$	ik, ib and ip	ILDBP

$$R = \int_0^n \frac{1}{3}\left[\frac{nc_{\mathrm{MN}}(t)}{nc_{\mathrm{MN}}} + \frac{nc_{\mathrm{EN}}(t)}{nc_{\mathrm{EN}}} + \frac{nc(t)}{nc_{\mathrm{CN}}}\right]\mathrm{d}t, \tag{5}$$

where $nc_{\mathrm{MN}}(t), nc_{\mathrm{EN}}(t), nc_{\mathrm{CN}}(t)$ stand for the values of the natural connectivity of the machine network, the electricity network, and the communication network after t nodes, edges, or interdependent links are attacked, respectively. Obviously, the larger R, the more robust the IMECN during the attack process.

3. Case Studies

Taking the subway is one of the main choices to travel in the city. The mass transit vehicle (MTV) is a key system to transport passengers for the subway. To explore the robustness of MTV, we build the interdependent networks consisting of a machine network, an electricity network, and a communication network based on the real-world data, whose data are shown in Table 2. We can find that the size of MN is the largest while the one of CN is the smallest. It shows that MTV is mainly composed of mechanical units. In addition, we use the Pearson correlation coefficient r to analyze the distribution of interdependent links. The value of r between MN and EN is approximately equal to zero, indicating that the node in MN randomly connects with the one in EN. However, the value of r between MN and CN is greatly larger than zero and shows that the degrees of end nodes of interdependent links between MN and CN are similar to each other. Furthermore, the distribution of interdependent links between EN and CN is similar to the one between MN and CN. According to the topology of subnetworks, the cumulative distribution $P(k)$ of the degree is shown in Figure 1.

As shown in Figure 1, we can find that most of the nodes have a small degree, while a few nodes have the high degree in three subnetworks. Moreover, the distribution of the degree is approximately linear in the log-log plot, which means that the distributions of the degree in three subnetworks obey the power-law distribution. Therefore, the result shows that MN, EN, and CN have a scale-free property. According to the previous studies, it is found that MN, EN, and CN are vulnerable to targeted attacks, while robust to random attacks.

On the basis of the cascading failure model used in this paper, it is clear that the larger δ, the more serious the impact of the cascading failure on the whole interdependent network, so our aim is to investigate the robustness under attack strategies to remove the node, the edge, and the interdependent link for different values of δ. Here, we carry out the simulations under attacks on nodes at $\delta = 0$, $\delta = 0.1$, and $\delta \geq 0.2$.

In Figure 2(a), it is evident that the value of NC in IMECN under ND significantly decreases in the range of $t \leq 7$, but the one under NDB is smaller than others and decreases to zero when t is just 11. The result at $\delta = 0$ indicates that when the cascading failure does not widely spread, removing the node with the high degree is more harmful to the robustness of the network at the early stage of attacks, while the failure of the node with the high degree and betweenness is crucial to the robustness. From Figure 2(b), we can observe that the efficient node attack strategy is ND in the range of $t \leq 6$, and the values of NC in IMECN subjected to NB and NBP decrease to zero first. When δ increases to a large value (i.e., $\delta \geq 0.2$), Figure 2(c) depicts that the curve of ND is lower than others no matter what t is and the IMECN becomes paralyzed after just five nodes with the high degree are attacked, which implies that the degree is a key measure for identifying the crucial node whose failure has a negative effect on the robustness in the case of the wide spread of failures. The main reason is that

Table 2: Data of IMECN.

Networks	Number of nodes	Number of edges	r
MN	119	158	−0.12 between MN and EN 0.54 between MN and CN
EN	63	91	−0.12 between EN and MN 0.42 between EN and CN
CN	27	30	0.54 between MN and CN 0.42 between EN and CN

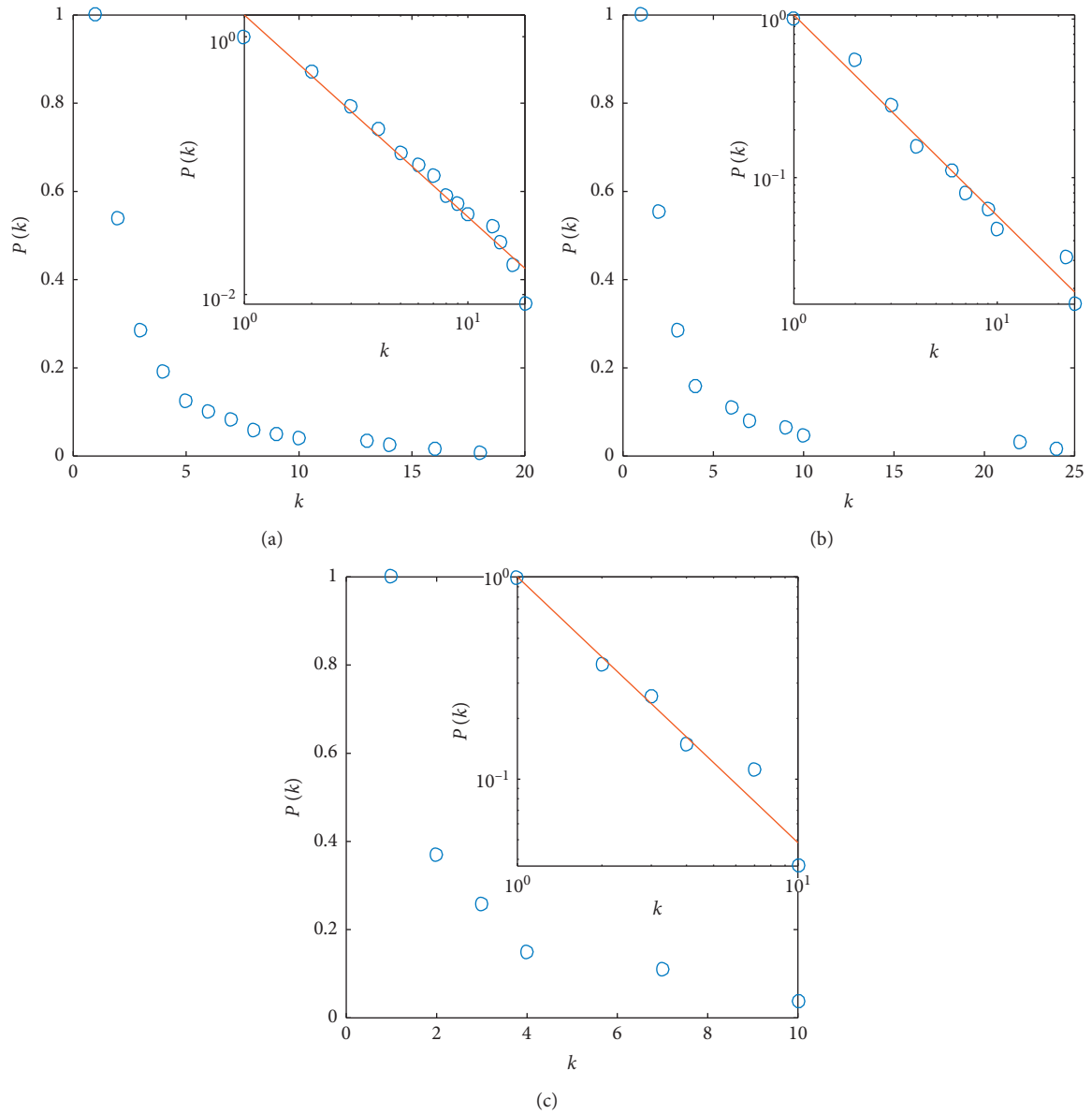


Figure 1: Cumulative distribution $P(k)$ of the degree in (a) MN, (b) EN, and (c) CN.

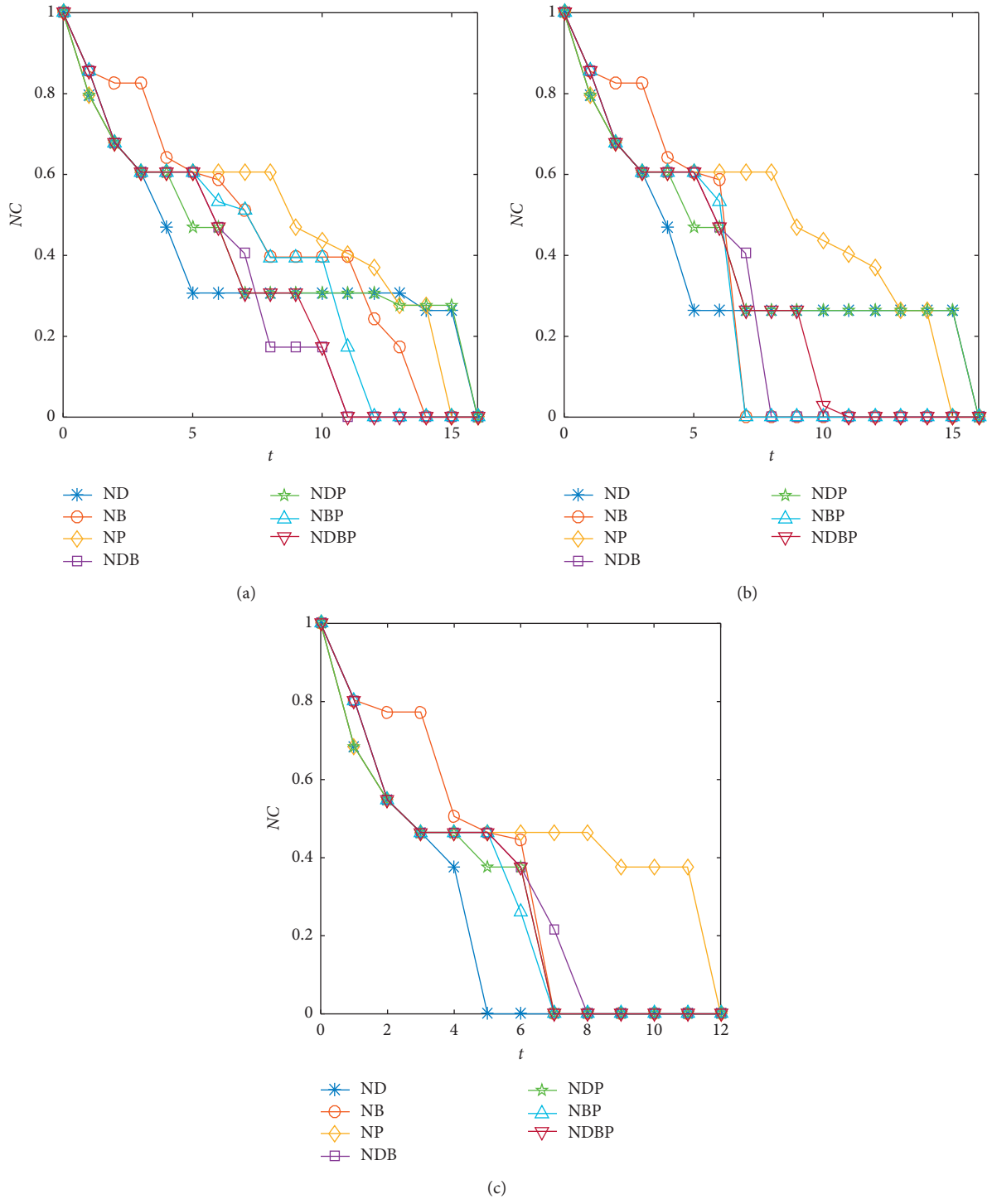


Figure 2: Comparison of NC of IMECN under node attack strategies at (a) $\delta = 0$, (b) $\delta = 0.1$, and (c) $\delta \geq 0.2$.

the breakdown of the high degree node is prone to split these three subnetworks with the scale-free property into some clusters so that the cluster may fail to work due to the small size proportion or lack of interdependent links. In addition, as can be seen in Figure 2, for different values of δ, the IMECN with NB (NP) has the large NC at the early (late) period of attacks. This illustrates that the measures that quantify the importance of the node in the whole interdependent network do not accurately reflect the impact of its failure on the robustness. Based on the above discussion, we find that it is effective to maintain the robustness by preventing the node with the high degree from failing, especially for the cases of serious cascading failures and the start of attacks.

In addition to NC, we also pay attention to the evaluation of the robustness during the whole process of attacks, that is,

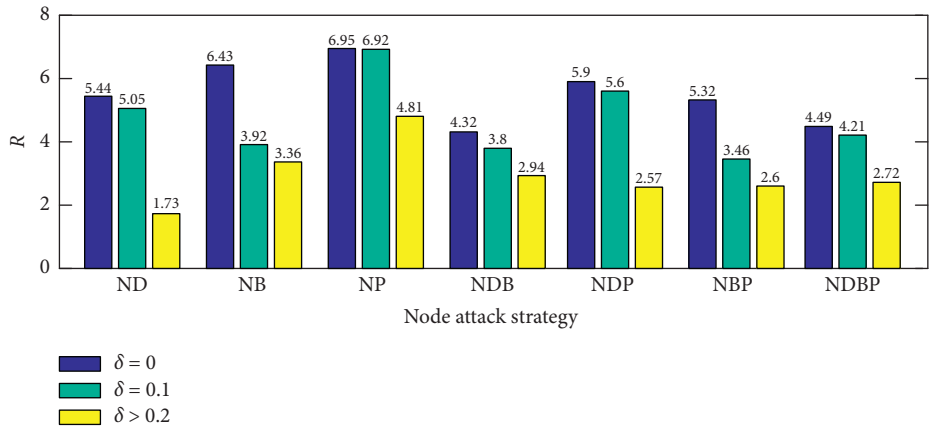


Figure 3: Comparison of R of IMECN under node attack strategies at $\delta = 0$, $\delta = 0.1$, and $\delta \geq 0.2$.

R. The value of R is shown for different δ and attack strategies in Figure 3. It is obvious that the values of R in IMECN under NDB, NBP, and ND are the smallest at $\delta = 0$, $\delta = 0.1$, and $\delta \geq 0.2$, respectively, which is also in accordance with the analysis of NC. Furthermore, there is a common ground that regardless of δ, the robustness of IMECN under NP is the strongest. This is because the high PageRank nodes tend to connect with each other. In this case, though the high PageRank node malfunctions, its adjacent node is likely to still connect with the functional cluster and maintain the normal operation.

In this section, we discuss the robustness of IMECN under attacks on the edges within subnetworks for different δ. In Figure 4(a), we can see that there is little difference among edge attack strategies in the range of $t \leq 30$ at $\delta = 0$. However, with the increase of t, the value of NC in IMECN under EP first decreases to zero, indicating that attacks on the edge between nodes with the high PageRank more easily result in the total collapse of IMECN compared with attacks on the ones between nodes with other high measures. Additionally, IMECN subjected to EB still keeps high connectivity when $\delta = 0$. Interestingly, in Figures 4(a) and 4(b), we find that as the values of δ increase to 0.2 and 0.4, respectively, the curve of EB is greatly lower than others when $t \geq 10$. This phenomenon demonstrates that the edge between the high betweenness nodes plays a key role in the robustness in the case of the large-scale propagation of cascading failures. This is due to the fact that the high betweenness node serves as the bridging node that links different clusters in most cases. Once the edge between these nodes breaks down, it is likely to split the subnetworks and trigger the cascading failure. In terms of ED, because the high degree node is still active without a few edges, it is found that regardless of δ the removal of the edge of the high degree node does not cause a significant reduction of the robustness on the whole in Figure 4.

In Figure 5, we can observe that the value of R under EP at $\delta = 0$ is the smallest, while at $\delta = 0.2$ and $\delta \geq 0.4$, EB makes the value of R smaller, which also agrees with the result of Figure 4. Additionally, for every edge attack strategy, the result of $\delta = 0.2$ is similar to the one of $\delta \geq 0.4$. This is due to the reason that attacking edges within the subnetwork in a particular order tends to form clusters with a small size. Moreover, the size proportions of these clusters are smaller than 0.2 in general. Therefore, this cluster is likely to fail to work for the slightly large δ, which leads to similar results at $\delta = 0.2$ and $\delta \geq 0.4$. Moreover, edge attack strategies make the value of R larger in comparison with node attack strategies (see Figure 3). That is to say, the IMECN in the face of attacks on edges has a stronger robustness compared with the one in the face of attacks on nodes, which is also in agreement with our intuition.

Previous studies have illustrated that the interdependent links play a vital part in the robustness in interdependent networks. For this reason, we analyze the change of the value of NC according to different attack strategies to remove interdependent links. From Figure 6(a), it is found that the value of NC in IMECN under ILD is the smallest in the range of $3 \leq t \leq 5$, while there is a slight difference of values of NC for interdependent link attack strategies in the other range of t. As δ increases to 0.1 in Figure 6(b), it is clear that the removal of just five interdependent links leads to the total collapse of IMECN, which implies that IMECN subjected to ILD exhibits the obvious vulnerability. Moreover, from Figure 6(c), we can find that in the case of $\delta \geq 0.2$, the value of NC in IMECN under ILD is still the smallest. The above result shows that the robustness of IMECN is significantly affected by removing interdependent links between the nodes with the high degree no matter what the possibility of triggering cascading failures is.

In this part, we compare the values of R in IMECN under interdependent link attack strategies for different δ. From Figure 7, it can be found that the value of R under ILD is the smallest regardless of δ, which is similar to the analysis of NC. In addition, in terms of ILD, the values of R at $\delta = 0.1$ do not significantly differ from the ones at $\delta \geq 0.2$. This result means that the size proportions of most of the inactive components in IMECN under ILD are between 0 and 0.1. On the contrary, for the other six interdependent link attack strategies, the values of R at $\delta = 0$ are similar to the ones at $\delta = 0.1$, different from the ones at $\delta \geq 0.2$. This result shows

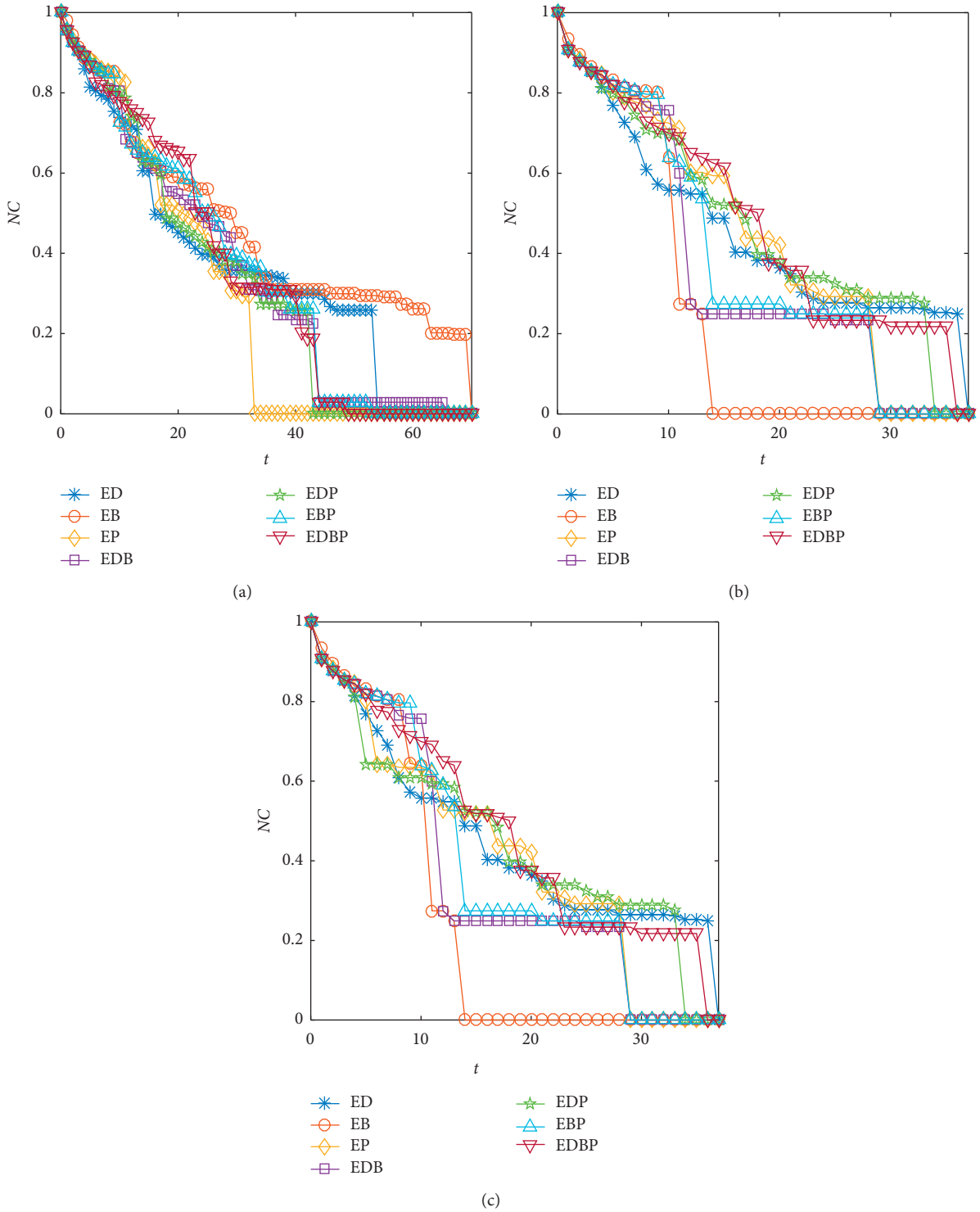


Figure 4: Comparison of NC of IMECN under edge attack strategies at (a) $\delta = 0$, (b) $\delta = 0.2$, and (c) $\delta \geq 0.4$.

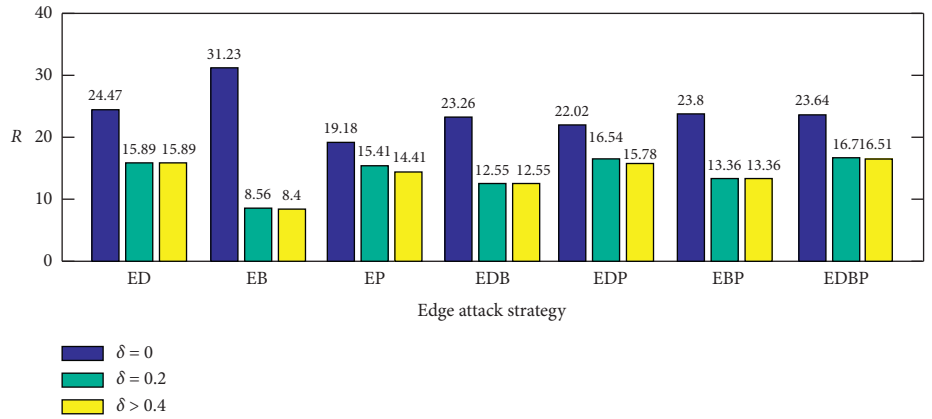


Figure 5: Comparison of R of IMECN under edge attack strategies at $\delta = 0$, $\delta = 0.2$, $\delta \geq 0.4$.

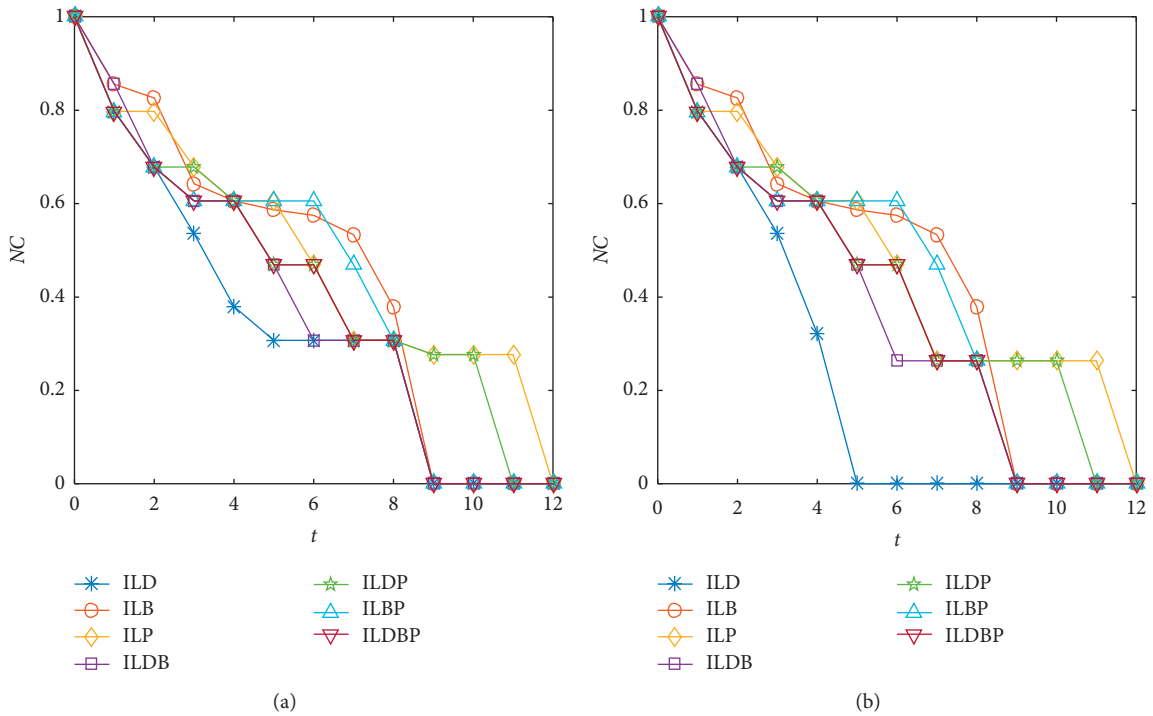
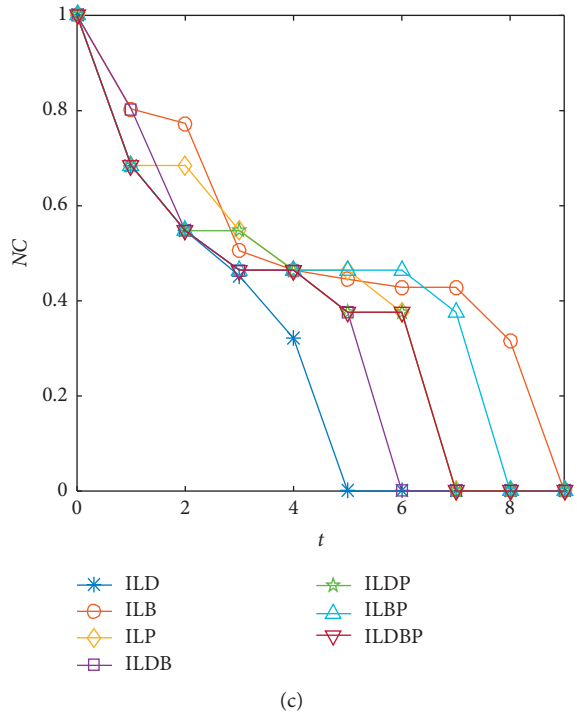


Figure 6: Continued.



(c)

Figure 6: Comparison of NC of IMECN under interdependent link attack strategies at (a) $\delta = 0$, (b) $\delta = 0.1$, and (c) $\delta \geq 0.2$.

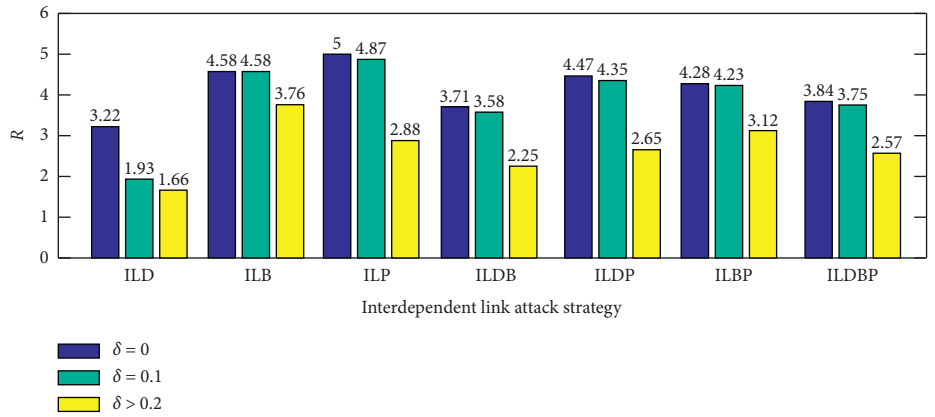


Figure 7: Comparison of R of IMECN under interdependent link attack strategies at $\delta = 0$, $\delta = 0.1$, and $\delta \geq 0.2$.

that the size proportions of almost all of the failed components under these attack strategies range from 0.1 to 0.2, which are larger than the case under ILD.

Based on the comparison of R under attack strategies with regard to the node, the edge, and the interdependent link (see Figures 3, 5, and 7), we find that the values of R under attack strategies concerning the node and the interdependent link are smaller than the ones under attack strategies concerning the edge for different δ, indicating that the robustness of IMECN is more sensitive to the attack on the node and the interdependent link. The major reason is that the attack on a node causes the failures of more than one edge in general and equates to attacks on several edges. Besides, in the matter of the attack strategy defined as the same measure, the value of R under the interdependent link attack strategy is slightly smaller than the one under the corresponding node attack strategy in most conditions, which reveals that the removal of nodes with the interdependent links makes the reduction of the robustness of IMECN greater in contrast to the one of nodes that may have interdependent links or not.

4. Conclusions

The ability of interdependent mechatronic systems to maintain the normal function after failures is directly related to every aspect of our lives. This paper models an interdependent network including a machine network, an electricity network, and a communication network to represent this system. Furthermore, in consideration of the

characteristics of interdependent mechatronic systems, we adopt the improved cascading failure model. In order to investigate the impact of the failures of different kinds of elements on the robustness, we propose attack strategies concerning nodes, edges, and interdependent links based on the degree, the betweenness, and the PageRank. Based on a real-world interdependent mechatronic system with the scale-free property, case studies are performed. Simulation results show that the most efficient node attack strategies are NDBP, NBP, and ND when $\delta = 0$, $\delta = 0.1$, and $\delta \geq 0.2$, respectively. In the matter of edge attack strategies, EP and EB make IMECN more vulnerable in the cases of $\delta = 0$ and $\delta > 0$, respectively. In addition, we also find that attacks on the interdependent links between the high degree nodes are more harmful to the robustness regardless of δ. Based on the comparison of different kinds of attack strategies, the removal of nodes and interdependent links significantly increases the vulnerability of IMECN. In the future work, we will try to take the physical parameters (such as the voltage, the current, and so on) into account for the evaluation of the robustness, the attack strategies, and the cascading failure model. Although the case study is carried out in the MTV, the method we propose also can be applied to the robustness analysis in other real-world mechatronic systems, for example, aerospace industry and manufacturing industry. To sum up, our research may be useful to identify the key element and design the robust interdependent mechatronic system against the failure propagation.

Data Availability

The data used to support the findings of this study are available from the corresponding authors upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the State Key Laboratory of Rail Traffic Control and Safety (contract no. RCS2019ZT007), Beijing Jiaotong University.

References

[1] R. Albert, H. Jeong, and A. L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 1, pp. 378–382, 2000.

[2] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of scale-free networks: error and attack tolerance," *Physica A: Statistical Mechanics and Its Applications*, vol. 320, pp. 622–642, 2003.

[3] M. Jalili, "Error and attack tolerance of small-worldness in complex networks," *Journal of Informetrics*, vol. 5, no. 3, pp. 422–430, 2011.

[4] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Physical Review Letters*, vol. 86, no. 16, pp. 3682–3685, 2001.

[5] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 340, no. 1-3, pp. 388–394, 2004.

[6] T. Nie, Z. Guo, K. Zhao, and Z.-M. Lu, "New attack strategies for complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 424, pp. 248–253, 2015.

[7] Y. Deng, J. Wu, and Y.-J. Tan, "Optimal attack strategy of complex networks based on tabu search," *Physica A: Statistical Mechanics and Its Applications*, vol. 442, pp. 74–81, 2016.

[8] Y. Yu, Y. Deng, S.-Y. Tan, and J. Wu, "Efficient disintegration strategy in directed networks based on tabu search," *Physica A: Statistical Mechanics and Its Applications*, vol. 507, pp. 435–442, 2018.

[9] M. Bellingeri, D. Bevacqua, F. Scotognella, R. Alfieri, and D. Cassi, "A comparative analysis of link removal strategies in real complex weighted networks," *Scientific Reports*, vol. 10, no. 1, p. 3911, 2020.

[10] M. Bellingeri, D. Cassi, and S. Vincenzi, "Efficiency of attack strategies on complex model and real-world networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 414, pp. 174–180, 2014.

[11] M. Bellingeri, D. Bevacqua, F. Scotognella, Z.-M. LU, and D. Cassi, "Efficacy of local attack strategies on the Beijing road complex weighted network," *Physica A: Statistical Mechanics and Its Applications*, vol. 510, pp. 316–328, 2018.

[12] A. Arenas, A. Díaz-Guilera, F. Giralt, and R. Guimerà, "Dynamical properties of model communication networks," *Physical Review E*, vol. 66, no. 2, p. 26704, 2002.

[13] A. E. Motter, "Cascade control and defense in complex networks," *Physical Review Letters*, vol. 93, no. 9, p. 98701, 2004.

[14] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 2, p. 65102, 2002.

[15] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 387, no. 26, pp. 6671–6678, 2008.

[16] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[17] Y. Xia, J. Fan, and D. Hill, "Cascading failure in Watts-Strogatz small-world networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 389, no. 6, pp. 1281–1285, 2010.

[18] Y. Hao, L. Jia, and Y. Wang, "Robustness of weighted networks with the harmonic closeness against cascading failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 541, Article ID 123373, 2020.

[19] Y. Hao, L. Jia, Y. Wang, and Z. He, "Modelling cascading failures in networks with the harmonic closeness," *PLoS One*, vol. 16, no. 1, Article ID e243801, 2021.

[20] J.-W. Wang and L.-L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Safety Science*, vol. 49, no. 6, pp. 807–812, 2011.

[21] W. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E*, vol. 77, p. 26101, 2008.

[22] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari, "Cascaded failures in weighted networks," *Physical Review E*, vol. 84, p. 46114, 2011.

[23] R. Yang, W. X. Wang, Y. C. Lai, and G. R. Chen, "Optimal weighting scheme for suppressing cascades and traffic

congestion in complex networks," *Physical Review E*, vol. 79, no. 2, p. 26112, 2009.

[24] Y. Hao, Y. Wang, L. Jia, and Z. He, "Cascading failures in networks with the harmonic closeness under edge attack strategies," *Chaos, Solitons & Fractals*, vol. 135, Article ID 109772, 2020.

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

[26] 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.

[27] C. D. Brummitt, R. M. D'Souza, and E. A. Leicht, "Suppressing cascades of load in interdependent networks," *Proceedings of the National Academy of Sciences*, vol. 109, no. 12, pp. E680–E689, 2012.

[28] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Robustness of a partially interdependent network formed of clustered networks," *Physical Review E*, vol. 89, no. 3, p. 32812, 2014.

[29] G. Dong, J. Gao, L. Tian, R. Du, and Y. He, "Percolation of partially interdependent networks under targeted attack," *Physical Review E*, vol. 85, no. 2, p. 16112, 2012.

[30] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review E*, vol. 87, no. 5, p. 52812, 2013.

[31] G. Dong, L. Tian, Z. Di, R. Du, X. Jiang, and H. E. Stanley, "Robustness of n interdependent networks with partial support-dependence relationship," *Europhysics Letters*, vol. 102, no. 102, p. 68004, 2013.

[32] F. Tan, Y. Xia, W. Zhang, and X. Jin, "Cascading failures of loads in interconnected networks under intentional attack," *EPL (Europhysics Letters)*, vol. 102, no. 2, p. 28009, 2013.

[33] R.-Q. Li, S.-W. Sun, Y.-L. Ma, L. Wang, and C.-Y. Xia, "Effect of clustering on attack vulnerability of interdependent scale-free networks," *Chaos, Solitons & Fractals*, vol. 80, pp. 109–116, 2015.

[34] Y. Hao, L. Jia, and Y. Wang, "Cascading failures in interdependent scale-free networks of different coupling preferences with the harmonic closeness," *EPL (Europhysics Letters)*, vol. 127, no. 3, p. 38003, 2019.

[35] Y.-L. Gao, S.-M. Chen, S. Nie, F. Ma, and J.-J. Guan, "Robustness analysis of interdependent networks under multiple-attacking strategies," *Physica A: Statistical Mechanics and Its Applications*, vol. 496, pp. 495–504, 2018.

[36] Y. Hao, L. Jia, and Y. Wang, "Edge attack strategies in interdependent scale-free networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 540, Article ID 122759, 2020.

[37] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 2, p. 65101, 2011.

[38] S. Chattopadhyay, H. Dai, and D. Young Eun, "Maximization of robustness of interdependent networks under budget constraints," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1441–1452, 2020.

[39] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Physical Review Letter*, vol. 107, no. 19, Article ID 195701, 2011.

[40] Y. T. Mohmand, A. Wang, and B. Paternoster, "Complex network analysis of Pakistan railways," *Discrete Dynamics in Nature and Society*, vol. 2014, Article ID 126261, 2014.

[41] Y. T. Mohmand, A. Wang, and Z. Jin, "Weighted complex network analysis of Pakistan highways," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 862612, 2013.

[42] Y. Xing, J. Lu, S. Chen, and J. R. Torregrosa, "Weighted complex network analysis of shanghai Rail transit system," *Discrete Dynamics in Nature and Society*, vol. 2016, Article ID 1290138, 2016.

[43] J. Feng, X. Li, B. Mao, Q. Xu, Y. Bai, and R. López-Ruiz, "Weighted complex network analysis of the different patterns of metro traffic flows on weekday and weekend," *Discrete Dynamics in Nature and Society*, vol. 2016, Article ID 9865230, 2016.

[44] J. M. Reynolds-Barredo, D. E. Newman, B. A. Carreras, and I. Dobson, "The interplay of network structure and dispatch solutions in power grid cascading failures," *Chaos*, vol. 26, no. 11, pp. 643–652, 2016.

[45] X. Zhang and C. K. Tse, "Assessment of robustness of ower systems from a network erspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 456–464, 2015.

[46] X. Gao, M. Peng, C. K. Tse, and H. Zhang, "A stochastic model of cascading failure dynamics in cyber-hysical ower systems," *IEEE Systems Journal*, vol. 14, no. 3, pp. 1–12, 2020.

[47] X. Lu, K. Hinkelman, Y. Fu et al., "An open source modeling framework for Interdependent energy-transportation-communication infrastructure in smart and connected communities," *IEEE Access*, vol. 7, pp. 55458–55476, 2019.

[48] M. H. Amini, J. Mohammadi, and S. Kar, "Distributed holistic framework for smart city infrastructures: tale of interdependent electrified transportation network and power grid," *IEEE Access*, vol. 7, pp. 157535–157554, 2019.

[49] S. Lin, L. Jia, Y. Wang, and H. Zhang, "A new function-topology-based method for assessing assive safety of mechatronics systems," *IEEE Access*, vol. 8, pp. 9312–9324, 2020.

[50] M. Li, Y. Wang, and L. Jia, "A research into the eliability of equipment-integrated system egarding high-speed train based on network model," *IEEE Access*, vol. 7, pp. 186328–186339, 2020.

[51] Y. Hao, Y. Wang, L. Jia, and Z. He, "Analysis of resilience under repair strategy in nterdependent mechatronic system," *IEEE Access*, vol. 9, pp. 12717–12729, 2021.

[52] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 41, no. 6, pp. 1244–1252, 2011.