ORIGINAL RESEARCH
published: 17 November 2020
doi: 10.3389/fphy.2020.604595

Structural Vulnerability Analysis of Partially Interdependent Networks: The Joint Influence of Interdependence and Local Worlds

Jiawei Wang[1,2], *Shiwen Sun*[1,2]*, *Li Wang*[1,2] *and Chengyi Xia*[1,2]

[1]*Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, Tianjin, China,* [2]*Engineering Research Center of Learning-Based Intelligent System, Ministry of Education, Tianjin, China*

Previous studies have verified that the local-world mechanism can greatly affect the structural properties and dynamical processes occurring on isolated complex networks; however, the impact of local-world mechanism on structural vulnerability of interdependent systems is still not efficiently explored. Therefore, in this study, the joint influence of interdependence and local worlds on attack vulnerability of interdependent networks is addressed. First, a partially interdependent system model is proposed, consisting of two networks which are dependent on each other with different types of interdependence preference. In particular, each network evolves according to the local-world model with an adjustable parameter to control the size of local worlds during network evolution. Next, the cascading failure process induced by intentional attack on high-degree nodes is presented. Then, the responses of interdependent systems after cascading failures are investigated through large quantities of numerical simulations. The results show that the emergence of local worlds during network evolution plays an important role in the structural vulnerability of both single and interdependent networks; that is, networks with larger size of local worlds are found to be more vulnerable against attacks. Moreover, interdependent links make the entire system much more fragile, especially when the networks are with max–max assortative interdependence and the strength is enhanced. These results are beneficial to the deep understanding of the intrinsic connection between attack robustness and underlying structure of large-scale interdependent systems.

Keywords: interdependent networks, complex networks, structural vulnerability, cascading failures, local worlds, network attack

OPEN ACCESS

Edited by:
Mahdi Jalili,
RMIT University, Australia

Reviewed by:
Yongxiang Xia,
Hangzhou Dianzi University, China
Michele Bellingeri,
University of Parma, Italy

Correspondence:
Shiwen Sun
sunsw@tjut.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *09 September 2020*
Accepted: *29 September 2020*
Published: *17 November 2020*

Citation:
Wang J, Sun S, Wang L and Xia C (2020) Structural Vulnerability Analysis of Partially Interdependent Networks: The Joint Influence of Interdependence and Local Worlds. Front. Phys. 8:604595. doi: 10.3389/fphy.2020.604595

1 INTRODUCTION

In the past two decades, network science has been developed rapidly and enriched fruitful results in many fields [1–3]. Among all the active topics, due to the importance of network models in characterizing the structural properties and dynamics of complex large-scale systems, the study on a variety of network models is of great significance. For example, many real-world systems can be classified into and modeled as scale-free networks, such as Internet, World Wide Web, movie actor collaboration networks, and paper citation networks [4]. Let $p(k)$ represent the probability that a randomly selected node has k connections with its direct neighbors in the entire network, the typical feature of scale-free networks is that their node degree distributions follow a power-law form:

$p(k) \sim k^{-\gamma}$, which cannot be characterized by widely recognized Erdős and Rényi(ER) random model in graph theory [5].

In order to interpret the underlying formation mechanism of the abovementioned scale-free property, Barabási and Albert proposed the classical BA scale-free model [4], which includes two important ingredients: I) network growth, which means that new nodes and links are added into the network continuously, and II) preferential attachment in linking new-added nodes and old nodes. These two ingredients are thought to be responsible for the appearance of power-law degree distributions in many systems. However, during the evolution of many real-world complex networks, preferential attachment mechanism is found to only take effect in the local worlds, not the entire network [6]. Therefore, considering the local-world effect during network evolution, Li and Chen proposed the local-world evolving model [7]. An adjustable parameter, M, is introduced into the evolution of networks, which controls the size of the local worlds of the new-added nodes in which the preferential attachment mechanism works. As M increases, that is, the local world becomes larger, the resultant networks can show transitional behaviors between exponential and scale-free networks with respect to node degree distributions.

Motivated by this pioneering work, subsequent studies have been focused on local-world effect in modeling real-world complex networks, characterizing underlying structures and analyzing important dynamical processes occurring in complex systems. Some variants of local-world models are continually proposed to better understand the structural and functional properties of real systems, such as wireless communication networks [8], power grids [9], and energy supply–demand system [10]. Also, localization mechanism has been incorporated into the construction of other models in describing the structures of hypernetworks [11], bipartite networks [12], and weighted networks [13]. In addition, several important topological properties, such as clustering [14], community [15], hierarchical structures [16], and local neighborhood [17], are combined with the local-world effect to comprehensively uncover the underling structure of large-scale systems. Furthermore, previous findings have revealed that local-world effect can greatly affect the dynamical processes and collective behaviors of complex networks, including attack robustness [18], synchronization [19], epidemic spreading [20], cascading failures [21], consensus [22], and structural controllability [23].

In reality, many natural, technological, and social systems are composed of fully or partially interdependent networks [24, 25], which are becoming increasingly dependent on each other since no particular network can exist in isolation. Take the interdependence between three modern critical infrastructures, for instance, considering water supply system, communication network, and power grids, communication network and water supply system require power grids to provide power support for normal operations, power grids and water supply system need communication network to transmit control signals, and power grids require water supply system to cool down the electric generators. Particularly, due to the dependencies between networks, interdependent systems are extremely vulnerable to damage; that is, a small disturbance can result in a cascade of failures propagating through the interdependent connections between networks [26–28]. Hence, understanding the vulnerability of interdependent systems is of vital importance [29–37]. Attack vulnerability is regarded as one fundamental problem in many artificial and real-world interdependent networks, which has attracted extensive attention in the academic communities [38–42].

Although localization has been considered as an indispensable mechanism in modeling and analyzing isolated complex systems, the combined study of interdependence and local-world mechanism is not sufficiently explored by far. Especially for attack vulnerability, isolated [18] and fully interdependent local-world networks [43] have been investigated, and it is found that the existence of local worlds during network evolution can have a great impact on networks' performance-resisting attacks. These results motivate us to extent the study to partially interdependent networks to future explore the joint influence of interdependence and local-world effect on attack vulnerability. First, a partially interdependent system model is constructed, consisting of two networks which are dependent on each other with different coupling preference. In particular, each network is evolved according to the local-world model with an adjustable parameter to control the size of local worlds. Then, after the attack on a small fraction of nodes, the process of cascading failures of nodes and links in partially interdependent system is described. Moreover, different from random attack simulated by selecting and removing nodes randomly, an important and realistic attacking strategy in real world—intentional attack on high-degree nodes—is considered in this study.

The structure of the article is organized as follows. In **Section 2**, a partially interdependent system model is presented, consisting of two networks which are dependent on each other. Then, the cascading failure process induced by intentional removal of a small fraction of high-degree nodes is described in detail. In **Section 3**, through large quantities of numerical simulations, the impacts of local worlds and interdependence on system's performance after cascading failures are investigated. **Section 4** includes the conclusion of the whole article and the perspective on future works.

2 MODELS AND VULNERABILITY METRICS

2.1 Interdependent Local-World Networks

In order to further investigate the joint influence of both interdependence and local worlds on structural vulnerability of interdependent networks, a partially interdependent system model with two networks, that is, networks A and B, is established based on the fully interdependent system model proposed by Buldyrev et al. [24]. This model considers both interdependence strength and preference. In the meantime, to explore the effect of local-world mechanism during network evolution, A and B are constructed according to the *local-world* evolving model [7].

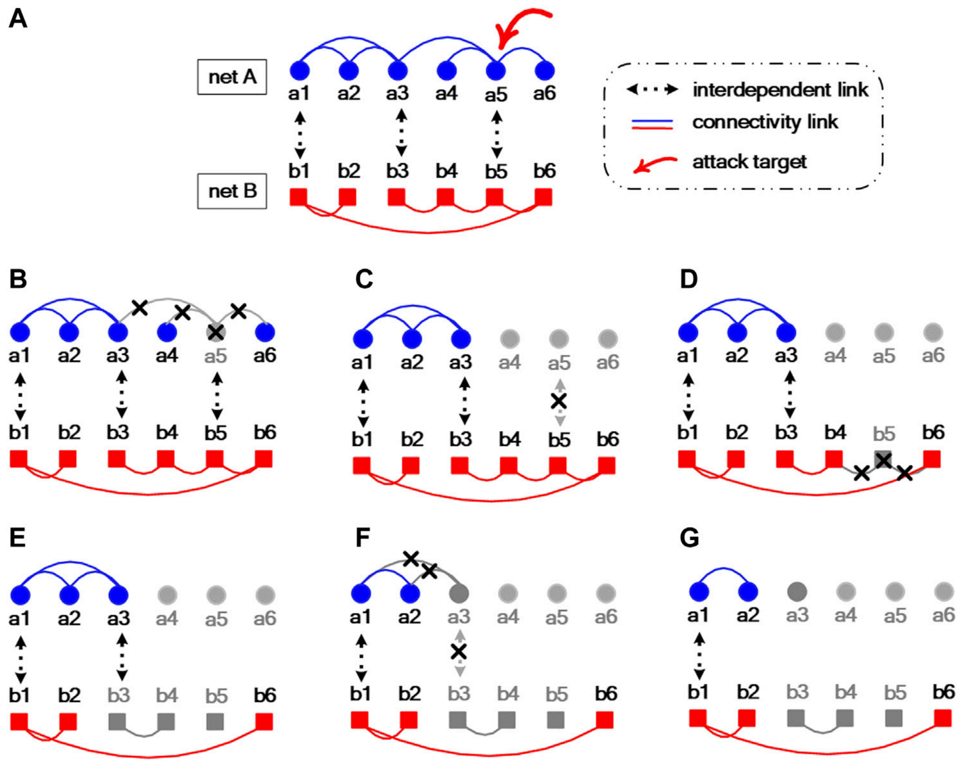

FIGURE 1 | (Color online) Schematic illustration of a partially interdependent system with two networks (*A* and *B*) and the cascade process of successive failures of nodes and links of both networks induced by single node removal (a_5) due to the existence of interdependence. **(A)** A partially interdependent system with network *A* and *B*. Nodes $\{a_i|1 \le i \le 6\}$ in network *A* and nodes $\{b_j|1 \le j \le 6\}$ in *B* are represented by solid circles and squares, respectively. The connectivity links, such as link (a_1-a_2) and link (b_1-b_5), are represented by solid lines. The dependency links, such as link (a_5-b_5), are represented by dashed lines. **(B–F)** Schematic illustration of the back-and-forth propagating process of cascading failures of nodes and links between two networks after node a_5 (one of nodes with highest degree in network *A*) is selected and attacked externally. The failure of node a_5 induces the damage on connectivity integrity of network *A*. Furthermore, due to the interdependence between networks, the removal of nodes and links in network *A* triggers the failures of nodes and links in network *B*. This propagating process between networks stops only until no further node and link are eliminated. **(G)** Finally stabilized system, network *A* is with largest connected component $\{a_1, a_2\}$ and *B* is with $\{b_1, b_2, b_6\}$, respectively.

An example of such interdependent system is exhibited in **Figure 1A**, which is composed of two networks A ($\{a_i|1 \le i \le 6\}$) and B ($\{b_j|1 \le j \le 6\}$). There are two types of links in interdependent networks, namely, connectivity links and interdependent links. Connectivity links are the links connecting nodes belonging to the same network, such as link (a_1-a_2) and link (b_1-b_5). However, the interdependent links indicate that one endpoint node of a link depends on the node at the other end, such as link (a_5-b_5). The functioning of node a_5 depends on the functioning of node b_5 and *vice versa*. Once node a_5 fails, its interdependent partner node b_5 in network B will also fail. The connectivity and interdependent links are represented by solid and dashed lines in **Figure 1**, respectively. Regarding the interdependence pattern between network A and B, several important factors should be considered, which are listed as follows:

2.1.1 Interdependence Strength

Even in real-world interdependent systems, there exist some nodes which have no dependency on other networks. To this end, different from fully interdependent networks, the partially interdependent model involves an important parameter, q, to define the fraction of nodes in one network which have interdependent links. Thus, q ($0 \le q \le 1$) characterizes the interdependence strength between networks A and B. When q approaches 0, the interdependence between two networks becomes weaker, where failures of nodes and links cannot easily spread from one network to another. On the contrary, when q approaches 1, the interdependence becomes stronger, and more interdependent links are added in the system. As two special cases, $q = 0$ corresponds to isolated networks without interdependence on each other, while when $q = 1$, it corresponds to the strongest interdependence, that is, the previous fully interdependent system model [24].

2.1.2 Interdependence Preference

Two kinds of interdependent interaction preference, that is, assortative and disassortative mixing, are usually considered in previous studies. Assortative mixing means that nodes with similar degree tend to be connected, and disassortative mixing indicates that nodes with different degree are connected. However, since only a fraction q of nodes have dependency relationships in partially interdependent networks, it is necessary to redefine assortative and disassortative interdependence as following.

Random interdependence

Random interdependence means randomly selecting nodes from networks A and B, respectively, and setting up interdependent links between them.

Assortative interdependence: *max–max* and *min–min*

First, sort nodes in networks A and B in the descending order of node degree, respectively, then, in the case of *max–max* interdependence, bidirectional interdependent links are set up between the fraction q of high-degree nodes in A and the fraction q of high-degree nodes in B. While, in the mode of *min–min* interdependence, the fraction q of low-degree nodes in one network are preferentially dependent on low-degree nodes in other network.

Disassortative interdependence: *max–min* and *min–max*

Here, *max–min* and *min–max* stand for two different kinds of disassortative interdependence. Considering *max–min* interdependence between networks A and B, it means that bidirectional interdependent links exist between high-degree nodes in A and low-degree nodes in B. On the contrary, in the case of *min–max* interdependence, the fraction q of low-degree nodes in A depend on the fraction q of high-degree nodes in B and *vice versa*.

For simplicity, only symmetric and *one-to-one* interdependence is considered, and two networks are with the same numbers of nodes and links in this study. *One-to-one* interdependence indicates that node a_i is dependent on only one node in network B, while *one-to-multiple* interdependence means that node a_i is dependent on more than one nodes in network B. As for *symmetric* interdependence, it means that node a_i is dependent on node b_j and *vice versa*. Otherwise, it is called *asymmetric* interdependence. Both networks in the interdependent system are constructed according to the *local-world* evolving model [7]. The construction algorithm can be described briefly as follows.

- Network growth

The network evolves with m isolated nodes initially; then, at each time step $t\,(t > 0)$, a new node is added into the network, and m links are added between this new node and m existing nodes. After T time steps, the resultant network has $N = m + T$ nodes and $E = mT$ links.

- Locally preferential attachment

At each time step t, $M\,(M \geq m)$ nodes are randomly chosen from the existing network and regarded as the local world of the new-added node. Afterward, the new node will connect to m nodes in this selected local world. Let Φ denote the set of nodes in this local world. Then, the linking probability l_i of any node $i \in \Phi$ and the new node is defined as $l_i \sim k_i/\sum_{j \in \Phi} k_j$. Obviously, l_i is valued over all the nodes $j \in \Phi$. Also, l_i is proportional to node degree k_i. However, this preferential attachment only takes effect locally, which is different from globally preferential attachment proposed in BA scale-free model [4].

The adjustable parameter M controls the extent to which locally preferential mechanism takes effect. If M is equal to the size of existing network at each time step, which is indicated by $M > N$ in the following numerical simulations, the local world of the new-added node does not exist and the preferential attachment mechanism actually works in the whole network-wide; thus, it corresponds to the BA scale-free model, and the degree distribution of the resultant network follows a power-law form: $p(k) \sim k^{-3}$ [4]. If $M = m$, the new-added node will connect all the nodes in the selected local world. It will result in an exponential network with degree distribution following an exponential form: $p(k) \sim \mathrm{e}^{-k/\mathrm{m}}$. By tuning the parameter $M\,(m \leq M < N)$ in the *local-world* model, networks can represent transitional behaviors between these two special cases.

2.2 Iterative Process of Cascading Failures under Intentional Attacks

In reality, targeted attacks on vital nodes are usually considered as effective strategies to destroy networked systems rather than random attacks. Therefore, it is of practical significance to investigate the performance of interdependent systems against intentional attacks. In this study, high-degree nodes are deliberately selected and removed from the system. For simplicity, nodes only in one network are initially attacked. Take the system shown in **Figure 1A** as an example; if network A is selected as the target, intentional attack can be simulated by sorting all the nodes in the descending order of degree and sequentially removing the nodes with the highest degree from network A.

Because of the interdependence between networks, once a small fraction of nodes are removed from one network, the damage may not be limited therein. The cascading failures of nodes and links can propagate between networks, just resulting in the collapse of the entire system. **Figures 1B–G** illustrate the propagating process of cascading failures of nodes and links which are caused by the removal of node a_5 (**Figure 1A**). After node a_5 is attacked and removed from network A, not only a_5 but also all its immediate links (a_5-a_3), (a_5-a_4) and (a_5-a_6) are destroyed (**Figure 1B**). Consequentially, this makes nodes a_4 and a_6 lose connection with the main body of network A (**Figure 1C**). Since node b_5 in network B depends on node a_5, the removal of a_5 leads to the failures of node b_5 and links (b_5-b_4) and (b_5-b_6) (**Figure 1D**), thus triggering the disconnection of nodes b_3 and b_4 from the main body of network B consequently (**Figure 1E**). Due to the existence of dependency link (b_3-a_3), the failure of nodes b_3 induces the elimination of nodes a_3 and two links (a_3-a_1) and (a_3-a_2) (**Figure 1F**). Thus, the failures cascade back and forth between networks A and B. This iterative process will not stop until no further node and link are eliminated (**Figure 1G**). In the finally stabilized system, network A is with the largest connected component $\{a_1, a_2\}$ and B is with $\{b_1, b_2, b_6\}$.

2.3 Structural Vulnerability Metrics

Generally speaking, after one network suffers attack on nodes and/or links, the structural vulnerability can be evaluated from two aspects, the damage on connectivity integrity and the loss of communication efficiency. Several widely used robustness measures are listed as follows:

(1) S, relative size of the largest connected component

For an unconnected network, considering all the components, that is, the subnetworks of connected nodes, the largest connected component (*LCC*) represents the component which has the maximum number of connected nodes [44]. Let N' and N_0 denote the number of nodes that remain in the *LCC* and the total number of nodes in the initial undamaged network, respectively. The relative size S is defined as $S = N'/N_0$, which is usually used as the main measure of the damage level caused by the elimination of nodes and links from the network, thus characterizing the performance of networks against attacks. Usually, the network is considered to be more robust with a larger value of S since more nodes remain connected in the largest component.

(2) η, residual communication efficiency

Communication efficiency is an important quantity to characterize how efficiently the information is transmitted between node pairs over the whole network [45]. Assume that information is always exchanged along the shortest paths, let d_{ij} represent the length of shortest paths between node i and j, and communication efficiency ε_{ij} is defined to be inversely proportional to the shortest distance, that is, $\varepsilon_{ij} = 1/d_{ij}$. Thus, global communication efficiency ε of the entire network is the average of ε_{ij} over all node pairs, that is, $\varepsilon = \sum_{i\neq j}\varepsilon_{ij}/(N(N-1))$. After nodes and links are removed, let ε_0 and ε_r denote the communication efficiency of the initial and residual network, respectively, the extent of communication efficiency loss can be defined as $\eta = \varepsilon_r/\varepsilon_0$, which can be used to evaluate the damage induced by node attack as well.

(3) f_c, critical fraction of removed nodes

The critical threshold f_c is the minimum fraction of nodes that must be eliminated to provoke the avalanche of the whole system. At $f = f_c$, the whole network is nearly destroyed with $S \approx 0$ and residual communication efficiency $\eta \approx 0$. Thus, f_c is another widely used quantity measuring the vulnerability of networks. A smaller value of f_c indicates that corresponding network is more easily to be destroyed and more vulnerable against attacks.

3 NUMERICAL SIMULATION RESULTS AND ANALYSIS

To explore the influence of both local-world mechanism and interdependence on structural vulnerability of interdependent systems, in the following numerical simulations, partially interdependent systems composed of two networks are established with different interdependence strength q and preference. According to the *local-world* evolving model, all the networks are constructed with different parameter M. Intentional attack is initiated by the removal of a fraction f of high-degree nodes in one network, indicated as the *target* network, which induces the cascading failures of nodes and links throughout both networks. When the system reaches the steady state after cascading failures, the damage on connectivity integrity and loss of communication efficiency of the *target* network are evaluated by monitoring the changes of S, η, and f_c with increasing f.

3.1 Effect of Local-World Mechanism

First, the influence of local-world mechanism on vulnerability of isolated networks is investigated, which is corresponding to the special case of strength $q = 0$ of interdependent systems proposed in **section 2.1**. All the networks are constructed with parameters $N = 10,000$, $m = 3$, average degree $\langle k\rangle = 6$ for different $M(M = 3, 5, 7, 9, 20$ and $M > N)$. **Figures 2 A and B** show the relative size S and residual communication efficiency η *versus* the fraction f of initially removed nodes for networks with different M, respectively. $M = m$ (curves with solid ●) and $M > N$ (curves with solid ◄) correspond to two special cases of *local-world* model, exponential and scale-free network, respectively.

From **Figure 2A**, with the increasing of f, the values of S inevitably are reduced to near 0. However, S is observed to decline more sharply in networks with the increasing of M. The rapid decrease of the size of largest connected component implies that nodes break off from the main body and all the connected components break into small pieces quickly, just accelerating the collapse of the whole network. For example, at $f = 0.3$, $S \approx 0.6$ with $M = m$; however, when $f = 0.3$ and $M > N$, S drops to $S \approx 0.0$, indicating the avalanche of the entire network.

Meanwhile, after cascading failures, the residual communication efficiency η of networks is also examined (**Figure 2B**). As more nodes are attacked and removed from the network, that is, η monotonically decreases, with the increasing of the fraction f of eliminated nodes. However, as M increases (from top to bottom), under the same level of external damage, that is, with the same f, η declines more rapidly in networks with higher values of M. For example, when $f = 0.2$, the residual efficiency of network with $M = m$ is $\eta \approx 0.8$, which is larger than $\eta \approx 0.2$ in the network with $M > N$. Also, as shown in **Figure 2**, f_c is observed to become smaller in networks as M increases. For instance, when $M = m$, $f_c \approx 0.44$, however, f_c is observed to be about 0.26 when $M > N$ (**Figure 2A**). As mentioned above, a smaller f_c means corresponding network is more fragile and can be destroyed more easily.

Second, the impact of local-world mechanism on structural vulnerability of fully interdependent *local-world* networks is also explored, which can be regarded as a special case of partially interdependent system with strength $q = 1.0$. In the numerical experiments, based on *local-world* model, all the networks are constructed with parameters $N = 2000$, $m = 3$, average degree $\langle k\rangle = 6$ for different M. As for fully interdependent systems, N

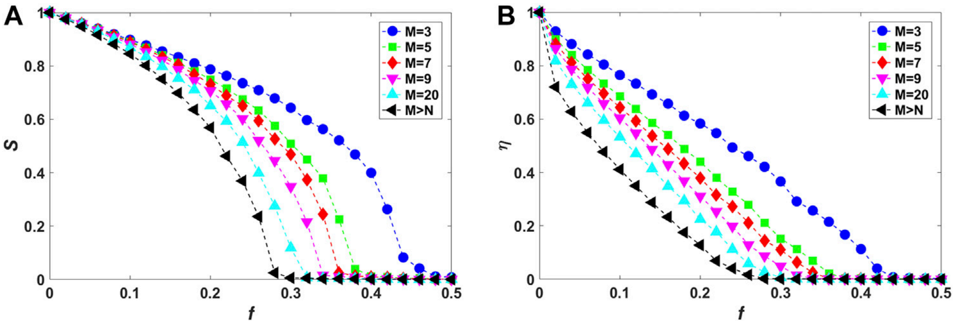

FIGURE 2 | (Color online) Vulnerability analysis of isolated *local-world* networks (corresponding to interdependence strength $q = 0.0$) after intentional attack on a fraction f of high-degree nodes. **(A)** Relative size S of the *local-world* networks as a function of the fraction f of removed nodes; **(B)** residual communication efficiency η *versus* the fraction f of removed nodes. Results are obtained by averaging over 50 independent realizations on *local-world* networks, which are constructed with size $N = 10,000$, $m = 3$, and average degree $\langle k \rangle = 2m = 6$ for different M ($M = 3, 5, 7, 9, 20$ and $M > N$). $M = 3$ and $M > N$ correspond to two special cases of *local-world* model, exponential and scale-free network, respectively.

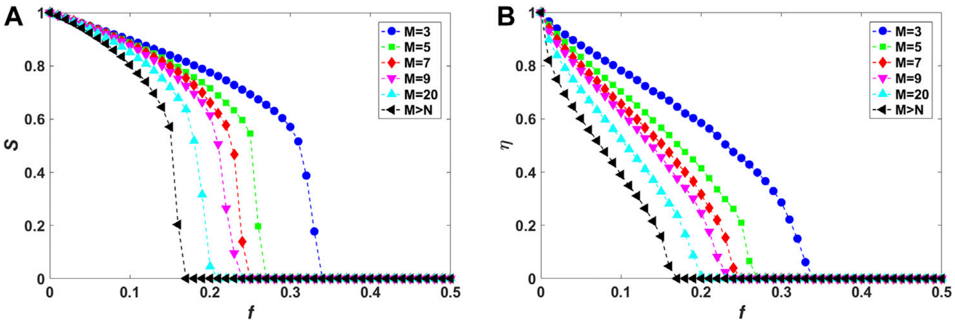

FIGURE 3 | (Color online) Vulnerability analysis of fully interdependent *local-world* networks (corresponding to interdependence strength $q = 1.0$) after cascading failures caused by intentional removal of high-degree nodes from one network in the case of random interdependence. **(A)** Relative size S of the largest connected component as a function of the fraction f of removed nodes; **(B)** residual communication efficiency η as a function of the fraction f of removed nodes. Results are obtained by averaging over 50 independent realizations on interdependent systems consisting two *local-world* networks, which are separately constructed with $N = 2000$, $m = 3$, and $\langle k \rangle = 2m = 6$ for different M ($M = 3, 5, 7, 9, 20$ and $M > N$).

interdependent links are set up between all the nodes of both networks, indicating that each node in the system is dependent on one and only one node in the other network. Note that, since q equals to 1, *max–max* are identical with *min–min* for assortative interdependence and *max–min* are identical with *min–max* for disassortative interdependence.

Figures 3–5 show the relative size S of the largest connected component and the residual communication efficiency η as functions of the fraction f of initially removed high-degree nodes for fully interdependent *local-world* networks in the case of random, assortative and disassortative interdependence, respectively. It can be observed from **Figures 3A, 4A, 5A** that, as M is increased, the decline of S becomes more drastically with increasing f, implying that corresponding networks are more vulnerable against cascading failures. Also, as shown in **Figures 3B, 4B, 5B**, residual communication efficiency η decreases more rapidly in networks with higher values of M. Note that, these behaviors are consistent with those of isolated *local-world* networks (**Figure 2**).

In summary, the simulation results demonstrate that the emergence of local worlds during network evolution has great influence on structural vulnerability of both single and interdependent networks. Deliberate attacks on highly connected nodes can induce more damage and sequentially more easily lead to abrupt collapse on networks with larger size M of local worlds. In other words, networks with larger size of local worlds are found to be more vulnerable against attacks.

3.2 Influence of Interdependence Preference

Previous study has verified that interdependent links accelerate the cascading spreading of node and link failures between networks, thus greatly enhancing the fragility of entire system against cascading failures [24]. This can be proved by the following observation of the simulation results. From **Figures 3–5**, compared with isolated networks (**Figure 2**), S decreases

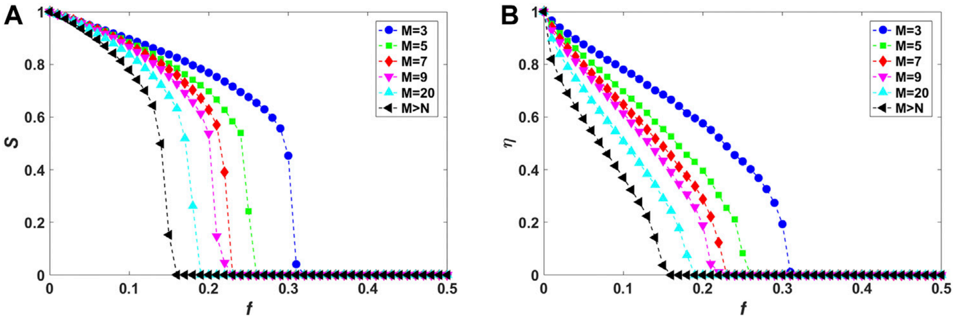

FIGURE 4 | (Color online) Vulnerability analysis of fully interdependent *local-world* networks (corresponding to interdependence strength q = 1.0) after cascading failures caused by intentional removal of high-degree nodes from one network in the case of assortative interdependence. **(A)** Relative size S of the largest connected component as a function of the fraction f of removed nodes; **(B)** residual communication efficiency η as a function of the fraction f of removed nodes. Results are obtained by averaging over 50 independent realizations on interdependent systems consisting two *local-world* networks, which are separately constructed with N = 2000, m = 3, and $\langle k\rangle = 2m = 6$ for different M (M = 3, 5, 7, 9, 20 and $M > N$).

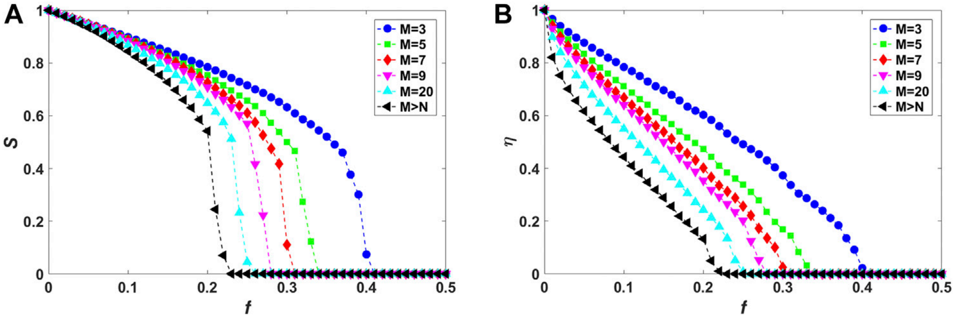

FIGURE 5 | (Color online) Vulnerability analysis of fully interdependent *local-world* networks (corresponding to interdependence strength q = 1.0) after cascading failures caused by intentional removal of high-degree nodes from one network in the case of disassortative interdependence. **(A)** Relative size S of the largest connected component as a function of the fraction f of removed nodes; **(B)** residual communication efficiency η as a function of the fraction f of removed nodes. Results are obtained by averaging over 50 independent realizations on interdependent systems consisting two *local-world* networks, which are separately constructed with N = 2000, m = 3, and $\langle k\rangle = 2m = 6$ for different M (M = 3, 5, 7, 9, 20 and $M > N$).

more drastically and f_c becomes lower in fully interdependent networks. For example, $f_c \approx 0.44$ for isolated network with $M = m$ (**Figure 2A**), while $f_c \approx 0.34$ for networks with $M = m$ in random case (**Figure 3A**).

Considering the effect of different interdependence preference, systems with assortative interdependence (**Figure 4**) are found to be the most vulnerable resisting cascading failures compared with random (**Figure 3**) and disassortative (**Figure 5**) cases. As M is fixed, the relative size S declines most rapidly and drops to $S \approx 0$ at the lowest values of f_c in the case of assortative interdependence. For instance, in networks with $M > N$ (curves with solid ◀), S drops more drastically to $S \approx 0$ at the lowest $f_c \approx 0.15$ with assortative interdependence (**Figure 4A**), however, $f_c \approx 0.17$ and $f_c \approx 0.24$ in networks with random (**Figure 3A**) and disassortative interdependence (**Figure 5A**), respectively. The same phenomena can be observed in networks with $M = m$ (curves with solid ●), f_c is the smallest in assortative case ($f_c \approx 0.32$), while the values f_c in random coupling and disassortative cases are $f_c \approx 0.35$ and $f_c \approx 0.40$, respectively.

Moreover, the effect of interdependence preference can also be verified by exploring the loss of communication efficiency induced by the elimination of nodes and links at the end of a cascading process. The changes of residual communication efficiency η versus the fraction f of initially removed high-degree nodes are shown in **Figures 3B, 4B, 5B**, which are corresponding to systems with random, assortative, and disassortative interdependence, respectively. In **Figure 4B**, for interdependent networks with assortative interdependence and local world size $M > N$ (curves with solid ◀), at $f = 0.1$, which means that 10% of high-degree nodes are initially eliminated from the network, the residual efficiency is $\eta \approx 0.4$, while at $f = 0.1$, the residual efficiency is approximately $\eta \approx 0.5$ in networks with random (**Figure 3B**) and disassortative interdependence. All the simulation results strongly confirm that compared with random and disassortative interdependence, interdependent networks coupled in an assortative way are more easily to be destroyed.

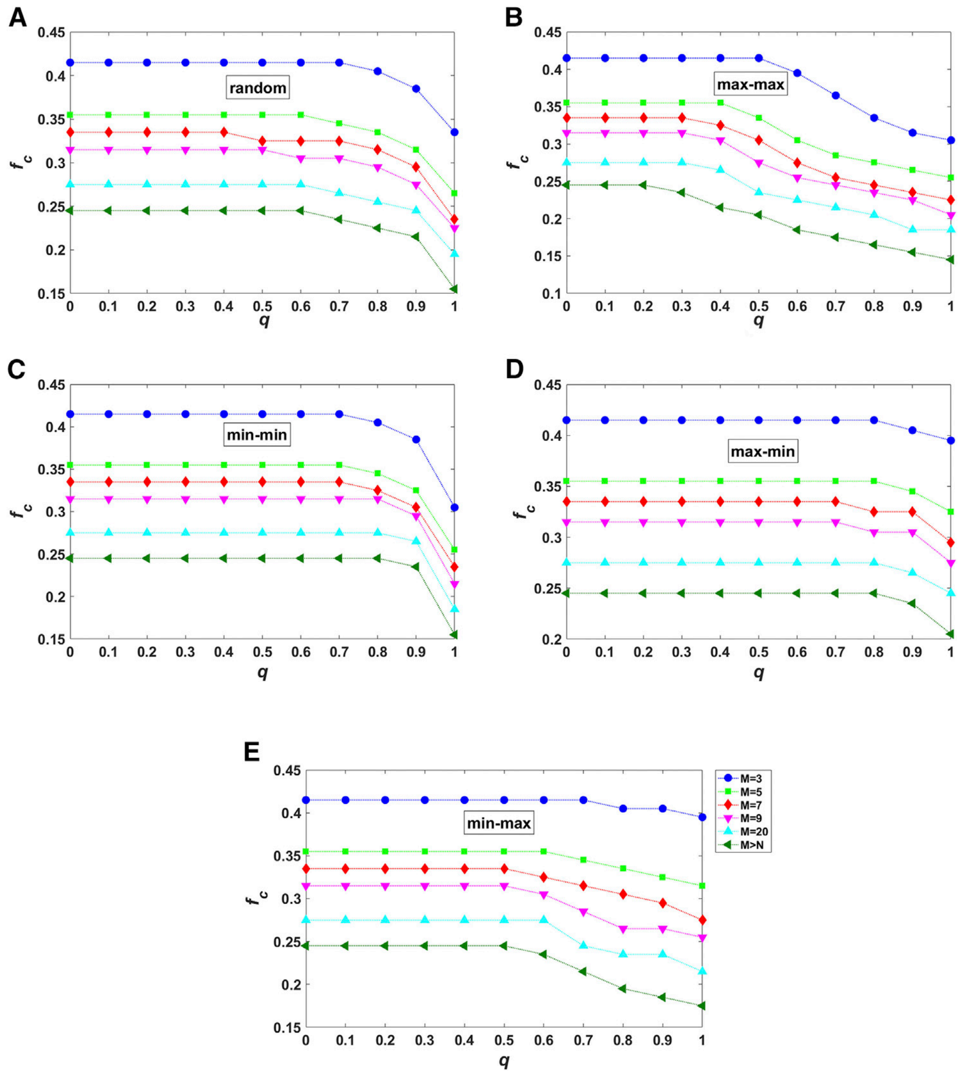

FIGURE 6 | (Color online) Vulnerability analysis of partially interdependent *local-world* networks after cascading failures caused by intentional removal of high-degree nodes from one network. Both interdependence preference and strength are considered: **(A)** *random*; **(B)** *max–max*; **(C)** *min–min*; **(D)** *max–min*; **(E)** *min–max*. All the plots show the joint effect of interdependence strength q and local world size M on the critical threshold values of f_c. f_c is the minimum fraction of nodes that must be removed to trigger the avalanche of the entire system. At $f = f_c$, the whole network is nearly destroyed with the relative size of the largest connected components $S \approx 0$ and the residual communication efficiency $\eta \approx 0$. A smaller f_c indicates that corresponding networks are more fragile against attacks and *vice versa*. The results are obtained by averaging over 50 independent realizations on interdependent systems consisting two *local-world* networks, which are separately constructed with $N = 2000$, $m = 3$, and $\langle k \rangle = 2m = 6$ for different M ($M = 3, 5, 7, 9, 20$ and $M > N$).

3.3 Impact of Interdependence Strength

Sequentially, in the following simulations, the vulnerability of partially interdependent networks after cascading failures is investigated by monitoring the joint influence of interdependence strength q, interdependence preference, and local world size M on the values of critical node threshold f_c (**Figure 6**). Here, f_c indicates the minimum number of nodes whose removal can trigger the cascade process of failure of nodes and links in both networks and lead to the abrupt collapse of the entire system. Meanwhile, different types of interdependence preference, namely, *random*, *max–max*, *min–min*, *max–min* and *min–max*, are considered. The results are obtained by averaging over 50 independent realizations on interdependent systems consisting two *local-world* networks, which are separately constructed with $N = 2000$, $m = 3$, and $\langle k \rangle = 2m = 6$ for different M ($M = 3, 5, 7, 9, 20$ and $M > N$).

In all the plots of **Figure 6**, from top ($M = m$) to bottom ($M > N$), with the same interdependence strength q, as M increases, f_c is observed to decrease monotonically, implying that partially interdependent systems composed of networks with relatively larger size M of local worlds become more vulnerable once cascading failures of nodes and links occur. Also, the results illustrate that interdependent networks

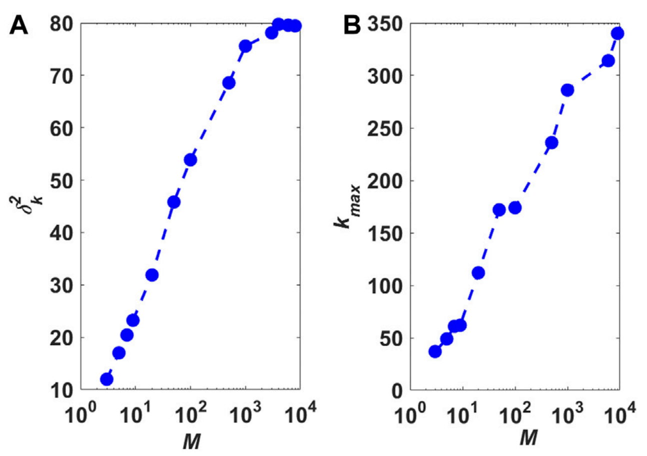

FIGURE 7 | (Color online) Heterogeneity analysis of node degree distribution of *local-world* evolving networks with different parameter *M*. **(A)** σ_k^2; **(B)** k_{max}. All the networks are with $N = 10,000$ nodes and average node degree $\langle k \rangle = 6$. Each data point is the average of 50 independent runs. The values of σ_k^2 and k_{max} increase monotonously with *M*, implying that corresponding networks become more heterogeneous in connectivity.

become more fragile with enhanced coupling strength. When M is fixed, f_c is observed to decrease with the increasing of q, indicating that the emergence of more interdependent links makes both networks more vulnerable against attacks.

Compared with random interdependence (**Figure 6A**), f_c drops more rapidly at relatively smaller values of q in networks with assortative *max–max* interdependence (**Figure 6B**). This reveals that *max–max* interdependence makes interdependent system more fragile resisting cascading failures. After targeted attacks occur in one network, since high-degree nodes of each network are depend on each other, the failures of high-degree nodes can not only trigger the breakdown of their neighbors in the same network but also lead to the failures of counterpart nodes in other networks. Especially, when q becomes larger, that is, $q > 0.5$, the propagation of failures will lead to the quick collapse of both networks. On the contrary, in networks with *min–min* interdependence (**Figure 6C**), interdependent links preferentially connect low-degree nodes of both networks; thus, the failures induced by interdependence are limited to low-degree nodes. Therefore, networks with *min–min* interdependence are more robust than other cases under attacks, especially when the interdependence strength is relatively small (**Figure 6C**).

As q is increased, for example, $q > 0.7$, it can be observed from **Figures 6 D and E** that, with the same M, the values of f_c in networks with *max–min* interdependence are relatively larger than those in networks with *min–max* interdependence. In other words, compared with *max–min* interdependence, networks with *min–max* interdependence are more fragile against cascading failures. Qualitatively, this can be explained as follows: *max–min* and *min–max* are two different types of disassortative interdependence between networks. For interdependent system with networks A and B, in the case of *max–min* interdependence, high-degree nodes in A and low-degree nodes in B are dependent on each other, while, in the case of *min–max* interdependence, low-degree nodes in A depend on high-degree nodes in B and *vice versa*. If A is selected as the attacking target, a fraction f of high-degree nodes in A are intentionally removed from the network, which triggers the cascading failures of nodes and links in both networks. In the case of *max–min* interdependence, the removal of high-degree nodes in A can only directly destroy low-degree nodes in B. The failures of low-degree nodes in B can bring less damage on connectivity compared with the failures of high-degree nodes in B in the case of *min–max* interdependence, thus suppressing the propagation of failures of nodes and links in both networks.

In previous studies, it has been revealed that node degree distribution and degree heterogeneity are essentially important for attack robustness of complex networks [46–49]. Two basic topological metrics, k_{max} and σ_k^2, are introduced to characterize the extent of heterogeneity of node degree distribution. k_{max} is defined to be the maximal value of degrees among all the nodes. And σ_k^2 denotes the variance of the entire node degree sequence, that is, $\sigma_k^2 = \langle k \rangle^2 - \langle k^2 \rangle$. **Figures 7 A and B** exhibit σ_k^2 and k_{max} as a function of M in *local-world* networks, respectively. As observing from **Figure 7A**, σ_k^2 increases monotonously with M, implying that corresponding networks become more heterogeneous in connectivity. As well, k_{max} becomes larger with increasing M (**Figure 7B**), indicating that *hub* nodes with more links emerge in resultant networks.

The results in **Figure 7** demonstrate that with the increasing of size M of local worlds, the local-world characteristic of the network decreases, especially when $M > N$ the local-world mechanism loses effect thoroughly and the resultant network reduces to the classic BA scale-free model [4]. The losing of local-world feature makes the network become more heterogeneous in connectivity, that is, the emergence of hub nodes and increased degree variance. Also, the network becomes more fragile against attacks. Intentional attack on high-degree nodes can lead to more drastic damage on connectivity integrity in more heterogeneous networks. This is the reason why isolated and interdependent networks with increased M are more fragile to be destroyed. In particular, in systems with *max–max* assortative interdependence, hub nodes in both networks depend on each others, when targeted attack is initiated, the removal of hub nodes in one network can cause the failures of hub nodes in the other network, just accelerating the propagation of node and link failures between networks. Thus, compared with other types of preference, systems with *max–max* interdependence are the most vulnerable against cascading failures caused by the attack on highly connected nodes.

4 CONCLUSION

To give a deep insight into the joint influence of interdependence and local worlds on complex interdependent networks with respect to the structural vulnerability after cascading failures, an interdependent system composed of two networks is established incorporating the consideration of both interdependence strength and preference. Especially, based on the *local-world* model, both networks are constructed with an adjustable parameter which controls the size of local worlds during network evolution. Through numerical simulations, it has been revealed that local-world mechanism can greatly affect the vulnerability of both isolated and interdependent networks. As the size of local world increases, corresponding networks are found to be more vulnerable after cascading failures induced by node removal. Additionally, the research results strongly verify that interdependent links can accelerate the collapse of the entire system. Comparing different interdependence preference, networks with *max–max* assortative interdependence are the most fragile against cascading failures. These results suggest that protecting highly connected nodes and weakening the interdependence between high-degree nodes can be effective for enhancing the robustness of interdependent systems. Especially, from the viewpoint of network evolution, controlling the extent of preferential attachment can be quite beneficial to preventing the drastic catastrophic failures of isolated and interdependent networks.

In this study, the investigation on network vulnerability against cascading failures is mainly focused on a simple binary networked system model, where links between nodes are only with two states, that is, present or absent. Nonetheless, most real-world networks are naturally weighted with some interaction values associated to the links (i.e., the link weight) [13, 44]. Thus, in the following work, the study on the relationships between local-world effect and network attack will be extended to weighted interdependent networks and real-world networks. Recently, many protection approaches have been developed to improve attack robustness and avoid abrupt collapse of complex systems, including setting reinforced nodes to support their neighborhood [50], targeted node recovery [51–53], and introducing node repair after collapse [54]. Therefore, local-world mechanism should be incorporated into the robustness improvement of interdependent systems, which remains as an interesting topic to be explored extensively. Moreover, several important dynamical behaviors, such as system crash behavior [36], epidemic dynamics [55] and structural controllability [56], have been extended into multiple networked systems. The effect of local worlds on these dynamic behaviors in interdependent systems deserves further study as well.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary materials; further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

JW and SS conceived and conducted the numerical experiments. LW and CX proposed the advice. All the authors analyzed the research results and together wrote the first version of the manuscript.

FUNDING

This work is partially supported by the Natural Science Foundation of Tianjin under Grant No. 18JCYBJC87800 and the National Natural Science Foundation of China under Grant No. 61773286.

ACKNOWLEDGMENTS

We would like to thank all the anonymous reviewers for their helpful suggestions to improve the quality of our manuscript.

REFERENCES

1. Albert R, Barabási AL. Statistical mechanics of complex networks. *Rev Mod Phys* (2002) 74:47–97. doi:10.1103/RevModPhys.74.47
2. Newman MEJ. The structure and function of complex networks. *SIAM Rev* (2003) 45:167–256. doi:10.1137/S003614450342480
3. Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang D. Complex networks: structure and dynamics. *Phys Rep* (2006) 424:175–308. doi:10.1016/j.physrep.2005.10.009
4. Barabási AL, Albert R. Emergence of scaling in random networks. *Science* (1999) 286:509–12. doi:10.1126/science.286.5439.509
5. Erdős P, Rényi A. On the evolution of random graphs. *Publ Math Inst Hung Acad Sci* (1960) 5:17–61. doi:10.1515/9781400841356.38
6. Li X, Ying Jin Y, Chen G. Complexity and synchronization of the world trade web. *Phys Stat Mech Appl* (2003) 328:287–96. doi:10.1016/S0378-4371(03)00567-3
7. Li X, Chen G. A local-world evolving network model. *Physica A* (2003) 328: 247–86. doi:10.1016/S0378-4371(03)00604-6
8. Ding Y, Li X, Tian YC, Ledwich G, Mishra Y, Zhou C. Generating scale-free topology for wireless neighborhood area networks in smart grid. *IEEE Trans Smart Grid* (2019) 10:4245–52. doi:10.1109/TSG.2018.2854645
9. Xing YF, Chen X, Guan MX, Lu ZM. An evolving network model for power grids based on geometrical location clusters. *IEICE Trans Info Syst* (2018) E101.D:539–42. doi:10.1587/transinf.2017EDL8177
10. Sun M, Han D, Li D, Fang C. The general evolving model for energy supply-demand network with local-world. *Int J Mod Phys C* (2013) 24:1350070. doi:10.1142/S0129183113500708
11. Yang GY, Liu JG. A local-world evolving hypernetwork model. *Chin Phys B* (2014) 23:018901. doi:10.1088/1674-1056/23/1/018901
12. Tian L, He Y, Huang Y. A novel local-world-like evolving bipartite network model. *Acta Phys Sin* (2012) 61:228903. doi:10.7498/aps.61.228903.
13. Li P, Zhao Q, Wang H. A weighted local-world evolving network model based on the edge weights preferential selection. *Int J Mod Phys B* (2013) 27:1350039. doi:10.1142/S0217979213500392
14. Zhang Z, Rong L, Wang B, Zhou S, Guan J. Local-world evolving networks with tunable clustering. *Phys Stat Mech Appl* (2007) 380:639–50. doi:10.1016/j.physa.2007.02.045
15. Xie Z, Li X, Wang X. A new community-based evolving network model. *Phys Stat Mech Appl* (2007) 384:725–32. doi:10.1016/j.physa.2007.05.031
16. Wang LN, Guo JL, Yang HX, Zhou T. Local preferential attachment model for hierarchical networks. *Phys Stat Mech Appl* (2009) 388:1713–20. doi:10.1016/j.physa.2008.12.028
17. Mu J, Zheng W, Wang J, Liang J. A novel edge rewiring strategy for tuning structural properties in networks. *Knowl Base Syst* (2019) 177:55–67. doi:10.1016/j.knosys.2019.04.004
18. Sun S, Liu Z, Chen Z, Yuan Z. Error and attack tolerance of evolving networks with local preferential attachment. *Phys Stat Mech Appl* (2007) 373:851–60. doi:10.1016/j.physa.2006.05.049

19. Sun S, Liu Z, Chen Z, Yuan Z. On synchronizability of dynamical local-world networks. *Int J Mod Phys B* (2008) 22:2713–23. doi:10.1142/S0217979208039770
20. Xia C, Liu Z, Chen Z, Sun S, Yuan Z. Epidemic spreading behavior with time delay on local-world evolving networks. *Front Electr Electron Eng China* (2008) 3:129–35. doi:10.1007/s11460-008-0033-3.
21. Bao Zj, Cao Yj. Cascading failures in local-world evolving networks. *J Zhejiang Univ-Sci* (2008) 9:1336–40. doi:10.1631/jzus.A0820336
22. Wu ZP, Guan ZH, Wu X. Consensus problem in multi-agent systems with physical position neighbourhood evolving network. *Phys Stat Mech Appl* (2007) 379:681–90. doi:10.1016/j.physa.2006.12.026
23. Sun S, Ma Y, Wu Y, Wang L, Xia C. Towards structural controllability of local-world networks. *Phys Lett* (2016) 380:1912–17. doi:10.1016/j.physleta.2016.03.048
24. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature* (2010) 464:1025–28. doi:10.1038/nature08932
25. Kivelä M, Arenas A, Barthelemy M, Gleeson JP, Moreno Y, Porter MA. Multilayer networks. *Journal of Complex Networks* (2014) 2:203–71. doi:10.1093/comnet/cnu016
26. Boccaletti S, Bianconi G, Criado R, del Genio CI, Gómez-Gardeñes J, Romance M. The structure and dynamics of multilayer networks. *Phys Rep* (2014) 544: 1–122. doi:10.1016/j.physrep.2014.07.001
27. Li J, Wang Y, Huang S, Xie J, Shekhtman L, Hu Y, et al. Recent progress on cascading failures and recovery in interdependent networks. *Internat J Disaster Risk Reduction* (2019) 40:101266. doi:10.1016/j.ijdrr.2019.101266
28. Jiang W, Liu R, Fan T, Liu S, Lu L. Overview of precaution and recovery strategies for cascading failures in multilayer networks. *Acta Phys Sin* (2020) 69:088904. doi:10.7498/aps.69.20192000.
29. Albert R, Jeong H, Barabási AL. Error and attack tolerance of complex networks. *Nature* (2000) 406:378–82. doi:10.1038/35019019
30. Podobnik B, Horvatic D, Lipic T, Perc M, Buldú JM, Stanley HE. The cost of attack in competing networks. *J R Soc Interface* (2015) 12:20150770. doi:10.1098/rsif.2015.0770
31. Qiu T, Liu J, Si W, Han M, Ning H, Atiquzzaman M. A data-driven robustness algorithm for the internet of things in smart cities. *IEEE Commun Mag* (2017) 55:18–23. doi:10.1109/MCOM.2017.1700247
32. Zhou M, Liu J. A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks. *IEEE Trans Cybern* (2016) 47:1–14. doi:10.1109/TCYB.2016.2520477
33. Lin Y, Burghardt K, Rohden M, Noël P-A, D'Souza RM. Self-organization of dragon king failures. *Phys Rev E* (2018) 98:022127. doi:10.1103/PhysRevE.98.022127
34. Kornbluth Y, Barach G, Tuchman Y, Kadish B, Cwilich G, Buldyrev SV. Network overload due to massive attacks. *Phys Rev E* (2018) 97:052309. doi:10.1103/PhysRevE.97.052309
35. Yang Y, Nishikawa T, Motter AE. Vulnerability and cosusceptibility determine the size of network cascades. *Phys Rev Lett* (2017) 118:048301. doi:10.1103/PhysRevLett.118.048301
36. Yu Y, Xiao G, Zhou J, Wang Y, Wang Z, Kurths J, et al. System crash as dynamics of complex networks. *Proc Natl Acad Sci USA* (2016) 113:11726–31. doi:10.1073/pnas.1612094113
37. Yang Y, Nishikawa T, Motter AE. Small vulnerable sets determine large network cascades in power grids. *Science* (2017b) 358:eaan3184. doi:10.1126/science.aan3184
38. Duan D, Lv C, Si S, Wang Z, Li D, Gao J. Universal behavior of cascading failures in interdependent networks. *Proc Natl Acad Sci USA* (2019) 116: 22452–7. doi:10.1073/pnas.1904421116
39. Cai Y, Cao Y, Li Y, Huang T, Zhou B. Cascading failure analysis considering interaction between power grids and communication networks. *IEEE Trans Smart Grid* (2016) 7:530–8. doi:10.1109/TSG.2015.2478888
40. Chen Z, Wu J, Xia Y, Zhang X. Robustness of interdependent power grids and communication networks: a complex network perspective. *IEEE Trans Circuits Syst II* (2018) 65:115–19. doi:10.1109/TCSII.2017.2705758
41. Zhang H, Peng M, Guerrero JM, Gao X, Liu Y, Liu Y. Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks. *Energies* (2019) 12:3439. doi:10.3390/en12183439
42. Zhou D, Bashan A. Dependency-based targeted attacks in interdependent networks. *Phys Rev E* (2020) 102:022301. doi:10.1103/PhysRevE.102.022301
43. Wu Y, Sun S, Wang L, Xia C. Attack vulnerability of interdependent local-world networks: the effect of degree heterogeneity. In: Proc. IEEE IECON 2017 - 43rd Ann. Conf. of the IEEE Ind. Elect. Soc. 2017 (2017). p. 8763–7. doi:10.1109/IECON.2017.8217540
44. Bellingeri M, Bevacqua D, Scotognella F, Alfieri R, Nguyen Q, Montepietra D, et al. Link and node removal in real social networks: a review. *Front Physiol* (2020) 8:228. doi:10.3389/fphy.2020.00228
45. Latora V, Marchiori M. Efficient behavior of small-world networks. *Phys Rev Lett* (2001) 87:198701. doi:10.1103/PhysRevLett.87.198701
46. Yuan X, Shao S, Stanley HE, Havlin S. How breadth of degree distribution influences network robustness: comparing localized and random attacks. *Phys Rev E* (2015) 92:032122. doi:10.1103/PhysRevE.92.032122
47. Sun S, Wu Y, Ma Y, Wang L, Gao Z, Xia C. Impact of degree heterogeneity on attack vulnerability of interdependent networks. *Sci Rep* (2016) 6:32983. doi:10.1038/srep32983
48. Buldyrev SV, Shere NW, Cwilich GA. Interdependent networks with identical degrees of mutually dependent nodes. *Phys Rev E* (2011) 83:016112. doi:10.1103/PhysRevE.83.016112
49. Zhou D, Stanley HE, D'Agostino G, Scala A. Assortativity decreases the robustness of interdependent networks. *Phys Rev E* (2012) 86:066103. doi:10.1103/PhysRevE.86.066103
50. Yuan X, Hu Y, Stanley HE, Havlin S. Eradicating catastrophic collapse in interdependent networks via reinforced nodes. *Proc Natl Acad Sci USA* (2017) 114:3311–15. doi:10.1073/pnas.1621369114
51. Majdandzic A, Podobnik B, Buldyrev SV, Kenett DY, Havlin S, Eugene Stanley H. Spontaneous recovery in dynamical networks. *Nat Phys* (2014) 10:34–8. doi:10.1038/NPHYS2819
52. Gong M, Ma L, Cai Q, Jiao L. Enhancing robustness of coupled networks under targeted recoveries. *Sci Rep* (2015) 5:8439. doi:10.1038/srep08439
53. Zhou D, Elmokashfi A. Network recovery based on system crash early warning in a cascading failure model. *Sci Rep* (2018) 8:1–9. doi:10.1038/s41598-018-25591-6
54. Majdandzic A, Braunstein LA, Curme C, Vodenska I, Levy-Carciente S, Eugene Stanley H, et al. Multiple tipping points and optimal repairing in interacting networks. *Nat Commun* (2016) 7:1–10. doi:10.1038/ncomms10850
55. Wang Z, Guo Q, Sun S, Xia C. The impact of awareness diffusion on sir-like epidemics in multiplex networks. *Appl Math Comput* (2019) 349:134–47. doi:10.1016/j.amc.2018.12.045
56. Xiang L, Chen F, Ren W, Chen G. Advances in network controllability. *IEEE Circ Syst Mag* (2019) 19:8–32. doi:10.1109/MCAS.2019.2909446

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.