PLOS | ONE

RESEARCH ARTICLE

Optimization of robustness of interdependent network controllability by redundant design

Zenghu Zhang[☯], **Yongfeng Yin**[☯]*, **Xin Zhang**[☯], **Lijun Liu**[☯]

School of Reliability and System Engineering, Beihang University, Beijing, China

☯ These authors contributed equally to this work.
* yyf@buaa.edu.cn

Abstract

Controllability of complex networks has been a hot topic in recent years. Real networks regarded as interdependent networks are always coupled together by multiple networks. The cascading process of interdependent networks including interdependent failure and overload failure will destroy the robustness of controllability for the whole network. Therefore, the optimization of the robustness of interdependent network controllability is of great importance in the research area of complex networks. In this paper, based on the model of interdependent networks constructed first, we determine the cascading process under different proportions of node attacks. Then, the structural controllability of interdependent networks is measured by the minimum driver nodes. Furthermore, we propose a parameter which can be obtained by the structure and minimum driver set of interdependent networks under different proportions of node attacks and analyze the robustness for interdependent network controllability. Finally, we optimize the robustness of interdependent network controllability by redundant design including node backup and redundancy edge backup and improve the redundant design by proposing different strategies according to their cost. Comparative strategies of redundant design are conducted to find the best strategy. Results shows that node backup and redundancy edge backup can indeed decrease those nodes suffering from failure and improve the robustness of controllability. Considering the cost of redundant design, we should choose BBS (betweenness-based strategy) or DBS (degree based strategy) for node backup and HDF(high degree first) for redundancy edge backup. Above all, our proposed strategies are feasible and effective at improving the robustness of interdependent network controllability.

OPEN ACCESS

Citation: Zhang Z, Yin Y, Zhang X, Liu L (2018) Optimization of robustness of interdependent network controllability by redundant design. PLoS ONE 13(2): e0192874. https://doi.org/10.1371/journal.pone.0192874

Editor: Lidia Adriana Braunstein, Universidad Nacional de Mar del Plata, ARGENTINA

Received: June 14, 2017

Accepted: January 21, 2018

Published: February 13, 2018

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: This work was partially supported by Beihang University Innovation and Practice Fund for Graduate under grant No. YCSJ-02-2016-09, National Aerospace Science Foundation of China under grant No.20140751008. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Introduction

With the increasingly wide and deep research into complex networks, such as traffic networks, energy networks, power networks and social networks, complex networks have drawn more and more attention in recent years. The control of complex networks is the focus and the ultimate purpose of studying them. Controlling complex networks means to make the networks reach the desired state by appropriate signal inputs. The first question is to ensure whether the complex networks are controllable or not.

Competing interests: The authors have declared that no competing interests exist.

Real systems are coupled by multiple networks and thus construct interdependent networks [1–4]. For example, the communication networks describe the networks where the vertex is one person in real world and the edge is one kind of communication between two persons. In fact, the communication networks are composed of online application network, email network and telephone network. As another example, the Internet network and the power network are mutually dependent. The failure of nodes in one network will lead to the failure of nodes that depend on the former in the other network. In fact, less research focuses on the controllability of interdependent networks.

Because of interactions of nodes in interdependent networks, the failure of a small fraction of nodes will cause the crash of the whole system. The network will then be out of control. Therefore, the robustness of interdependent network controllability is another topic that should be studied. This paper will analyse the robustness of interdependent network controllability and find methods to optimaze it.

A significant shortcoming of solving the controllability for complex networks by classical control theory is that it is a computationally prohibitive job for large scale networks, resulting from the need for brute-force search of all combinations of the rank of W [5, 6]. To bypass the requirement of measuring all combinations, Liu et al. proposed an analysis framework for the structural controllability of a single network [7]. As long as the network is structurally controllable, it will always be controllable by adjusting appropriate parameters of the network [8]. However, this framework can only solve the controllability of a single network without considering multiple networks.

With the development of the research in the field of controllability for complex network, a general question is what type of role each node plays. Based on the framework of controllability, Menichetti et al. [9] discussed the determined effect of nodes with minimal in-degree and out-degree on the controllability of the network. By comparing the controllability between an ER network and the maximum entropy network, Hou et al. found that the latter had a higher controllability [10]. This paper determined that the controllability of one node is influenced by the properties of its neighbors. Jia and Barabasi [11] put forward the concept of control capacity for nodes by calculating the frequency of a single node in all minimum matching sets. The author described a method that could be used to analyze the relationship between the control capacity and the degree of the nodes.

To measure the importance of nodes in the driver node set, Jia et al. [12] considered the classification of driver nodes based on the structural controllability of a complex network. This classification can successfully determine the role of one node on the controllability of a single network. However, although useful for the controllability of a single network, the research above has not considered the robustness of controllability for networks.

The model of cascading failure in a random network that includes only overload failures was presented by Watts DJ [13]. In this model, the load of a failed node will be reallocated to other functional nodes. Buldyrev et al. [14] studied the interdependent failure process in interdependent networks without considering overload failures. The failure of one node in one network will lead to the failure of a node in another network. Therefore, a small fraction of failures of nodes will crash the whole network. We will consider a cascading process including both the overload and the interdependent failures in our work.

Cohen et al. [15] was the first to consider theoretically failures in the structure via percolation theory. Most of the research on the robustness of complex networks focused on the structure of the network without considering controllability [14, 16–19]. To measure the robustness of controllability and global connectivity for a single network, a parameter was presented based on the maximum weakly connective components [20]. The result for the robustness of controllability based on edge attack shows the accuracy and usability of this parameter [21], giving an instructive idea for obtaining the parameter to evaluate the robustness of the interdependent network controllability.

Liu et al. [22] proposed a method of redundant design to optimize the structure of interdependent networks. To achieve the terminal purpose of optimizing the robustness of interdependent network controllability, we improved the redundant design by analyzing the factors which determine the process of cascading failures and proposing different strategies.

Based on the previous research results, this paper solves the optimization question of robustness for interdependent network controllability as the following idea: first, we construct the model of the interdependent networks. Second, we determine the process of cascading process including both overload and interdependent failures in interdependent networks under different proportions of node attacks. Then, we analyze the robustness of interdependent network controllability. Finally, a redundancy design and sevaral strategies are proposed to optimize the robustness of interdependent network controllability.

Materials and methods

Structural controllability of networks

In an N-dimensional space, the state of the nodes in a system can be described by an N-dimensional vector that is $x(t) = (x_1(t), x_2(t), \cdots, x_N(t))^T$. The system is controllable if it can reach any expected state from any initial state within a finite time [23].

For a nonlinear system, many aspects act similarly to time-invariant dynamics:

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{1}$$

where $x(t) = (x_1(t), x_2(t), \cdots, x_N(t))^T$ denotes the state of the nodes at time t, $A = [a_{ik}]_{N\times N}$ is the adjacency matrix of N nodes, $B = [b_{ik}]_{N\times M}$ is the input matrix that identifies nodes driven by input signals, and $u(t) = (u_1(t), u_2(t), \cdots, u_N(t))^T$ is the vector of input signals.

Kalman controllability rank condition [23] says that the system expressed by Eq (1) is controllable if and only if the controllability matrix satisfies as follows:

$$\mathrm{rank}(W) = N, \tag{2}$$

where $W = [B, AB, \cdots, A^{N\text{-}1}B]$.

To overcome the shortcomings of computationally prohibitive tasks to calculate Eq (2) for large networks, the notion of structural controllability [8] is proposed. The system described by Eq (1) is structurally controllable if the non-zero weights in A and B can be replaced by some parameters so that the system satisfies Eq (2). A system that is structurally controllable can be controlled in most circumstances [8]. The least number of input signals that can be used to control a network is denoted by N_D. Therefore, N_D can describe the controllability of the network, where a higher N_D means more input signals to control the network. Liu et al. [7] proposed a controllability analysis framework for a complex network based on the maximum matching theory to solve the minimum set of driver nodes that are the unmatched nodes of the maximum matching set in the directed network.

The undirected network can be regarded as a directed network where there are two edges between any nodes. Moreover, the directed network can also be regarded as a bipartite network. In the bipartite network, $H(A) = (V_A^+, V_A^-, \Gamma)$, where $V_A^+ = \{x_1^+, \cdots, x_N^+\}$ and $V_A^- = \{x_1^-, \cdots, x_N^-\}$ denote the node sets in the complex network and $\Gamma = \{(x_j^+, x_i^-)|a_{ij} \neq 0\}$ denotes the set of edges. Fig 1 shows the bipartite network of a directed network $G(A)$ and the process to calculate the minimum set of driver nodes. The minimum set of driver nodes can be obtained by solving the maximum matching of the bipartite networks where the

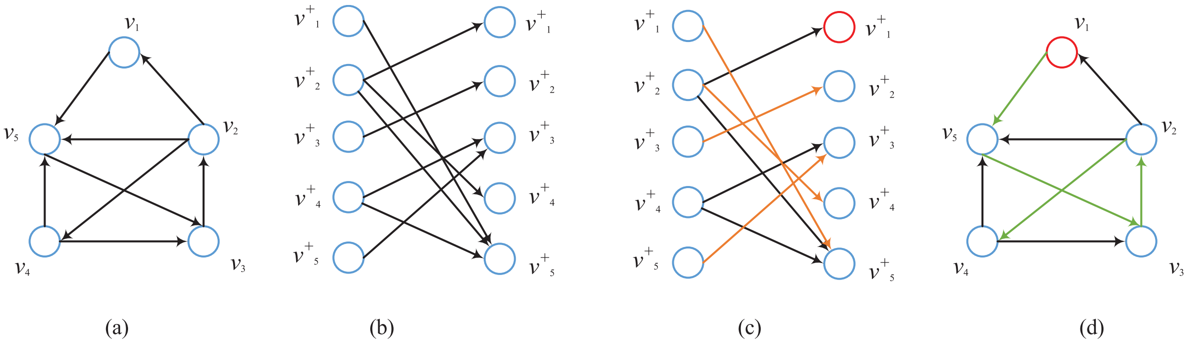

Fig 1. Demonstration of calculating the minimum set of driver nodes. (a) The directed network topology with five nodes. (b) The bipartite network of the directed network. Each connection in the bipartite network is related to an edge in the directed network. (c) The max matching set of the bipartite network. The set of red edges is the max matching set where any additional edge will make some vertex matched more than one time. The red vertex is the minimum set of driver nodes. (d) The max matching and minimum set of driver nodes in the directed network.The red vertex is the minimum set of driver nodes.The set of green edges is the max matching set in the directed network.

https://doi.org/10.1371/journal.pone.0192874.g001

unmatched nodes are exactly the minimum set of driver nodes to make the network structurally controllable.

Each node in the complex network can be classified into three different types according to its role in maintaining controllability [7]: (1) critical if it will always exist in all minimum sets of driver nodes; (2) redundant if will never exist in any minimum set of driver nodes; and (3) ordinary if it is neither critical nor redundant.

Cascading process of interdependent networks

Suppose that a single network G is composed of a vertex set V and an edge set E, where V is $\{v_1, v_2, \cdots, v_N\}$ and E is $\{e_1, e_2, \cdots, e_N\}$. A path between node v_i and node v_j is a subset of consecutive edges that can be expressed as $P(v_i, v_j)$. So $|P(v_i, v_j)|$ is the length of path $P(v_i, v_j)$. Moreover, d_{ij} is defined as the shortest length between node v_i and node v_j. There may exist several paths $P(v_i, v_j)$ whose length is equal to d_{ij}.

According to the topology of a complex network, network failures on a global scale can be caused by local node failures through the cascading mechanism. The initial load on each node of a complex network can be denoted by its betweenness centrality, which means the total number of the shortest paths passing through it. Its formula is expressed as follows:

$$B^0(v_k) = \sum_{i \neq j = 1}^{N} \frac{N_{ij}(k)}{N_{ij}} \tag{3}$$

where $N_{ij}(k)$ denotes the number of the shortest paths $P(v_i, v_j)$ that passes through node v_k, and N_{ij} means the number of the shortest paths between node v_i and node v_j.

Because the capacity of a node is limited, the loads of nodes in the complex network will be reallocated and exceed their limits as a result of attacks on the complex network. Kim and Motter [24] found that there is a nonlinear relationship between the load of a node and capacity. Dou B. [25] proposed a nonlinear load-capacity model for real systems that can be expressed as follows:

$$Cap(v_k) = B^0(v_k) + \beta(B^0(v_k))^\alpha, k = 1, 2, \cdots, N \tag{4}$$

where $\alpha > 0, \beta > 0$. When $\alpha = 1$, this model degenerates to linear load-capacity model. Suppose that the load of a failed node will be assigned to other functional nodes on average which can be expressed as follows:

$$B^{t}(v_j) = B^{t-1}(v_j) + \frac{\sum B^{t-1}(v_i)}{|V_{functional}|}, v_i \in V_{failed}, v_j \in V_{functional} \tag{5}$$

where $V_{\text{functional}}$ and V_{failed} are sets of nodes that remain functional and failed, respectively. $|V_{\text{functional}}|$ denotes the number of nodes in $V_{\text{functional}}$. If the load of a node is larger than its capacity, this node will cause overload failure. Moreover, to measure the cost of a network, we define the cost of the network according to the capacities of the nodes. The greater the value of α and β, the more resources that should be allocated on the network. The cost of a network is defined as follows:

$$\text{Cost} = \sum_{i=1}^{N} Cap(v_i) \tag{6}$$

Real systems are always coupled together by multiple networks and should be regarded as interdependent networks. For example, the power network and the Internet network are coupled together so that the power stations rely on Internet nodes for control and vice versa. The significant feature of interdependent networks is that the failure of nodes in one network will lead to interdependent failures of nodes in the other network [14]. Removal of a small fraction of nodes in one network will cause a considerable fraction of interdependent failures in the whole network.

This paper considers both the overload failures and the interdependent failures in the cascading process of interdependent networks. We begin by removing a fraction of nodes in one network and all the edges connected to the removed nodes. Then, the process of interdependent failures happens, which leads to the removal of all edges that are connected to different clusters in the other network, and removal of edges and isolated nodes in the other network will cause further interdependent failures until no nodes fail. As a result of removing nodes in the network, the load of failure nodes will be reallocated to those remaining nodes. Once the load of a node exceeds its capacity and fails, the process of overload failures will occur. This is another failure mode of nodes in the interdependent networks which in turn causes further interdependent failures of the network.

Fig 2 illustrates the process of cascading failures under node attacks in interdependent networks. We consider for simplicity, and without loss of generality, two networks, N_A and N_B, with the same number of four nodes as depicted in Fig 2(a). The black dashed lines that cannot transfer traffic are dependency edges between two isolated networks. However, the blue and green lines in two networks that can transfer traffic are connective edges. At the first stage, node C in network N_A is attacked and fails. After the process of interdependent failures, nodes A, D in network N_B and nodes B, C in network N_A will fail and lose their functions. Then, their loads will be reassigned to nodes that are still functional in their own network, as shown in Fig 2(b). In the next stage, the load of node C in network N_B exceeds its capacity and fails. Then, node D fails in the same way as C. This is the process of overload failures of the networks. The result after overload failures can be seen in Fig 2(c). Then, another process of interdependent failures occurs. Nodes A, D in network N_A fail. Finally, all nodes fail and lose their functions as shown in Fig 2(d).

Robustness of interdependent network controllability

The robustness of a complex network has become a hot topic in recent years [15, 21, 25, 26]. Previous work has mainly focused on the connectivity of complex networks. Some topological

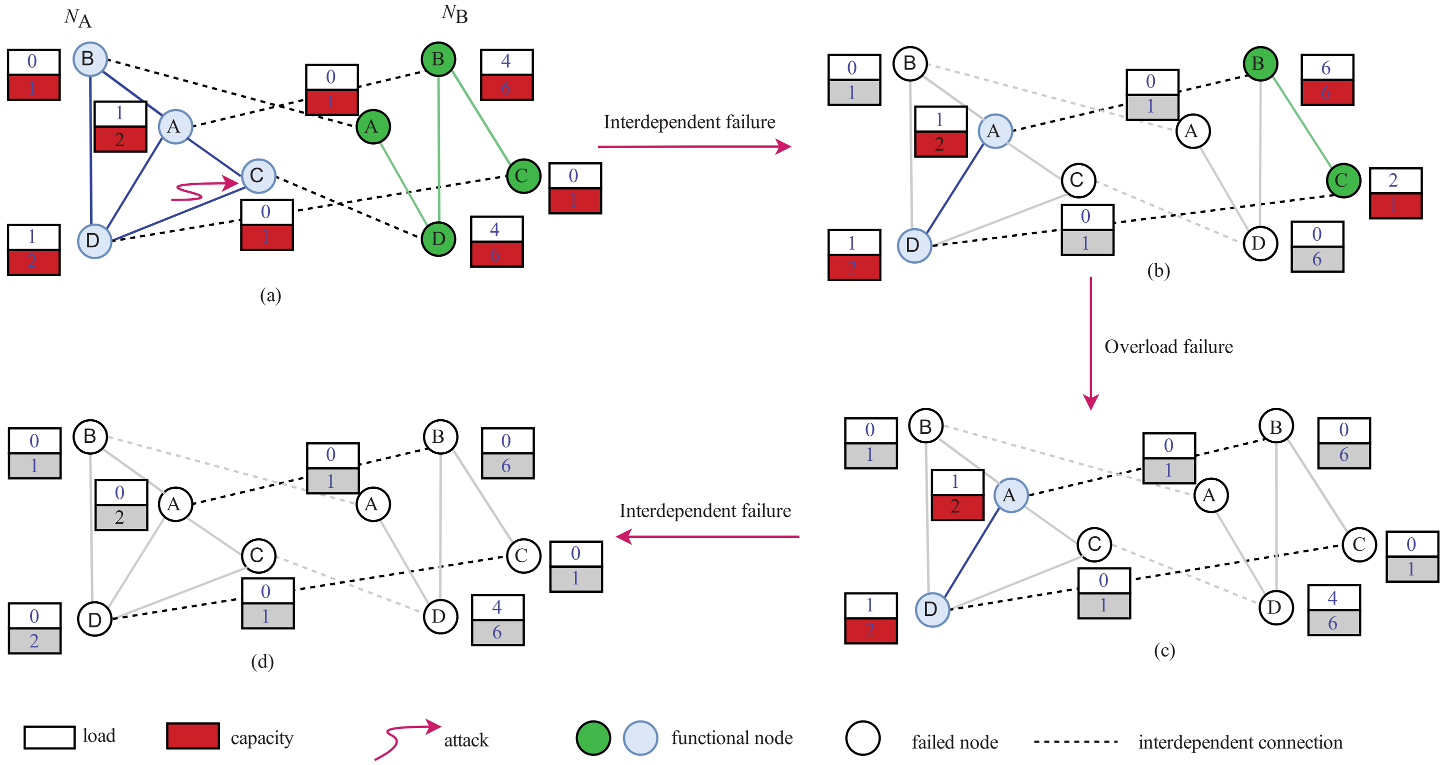

Fig 2. Cascading process of interdependent networks under node attacks. (a) The topology of interdependent networks with eight nodes. The initial attack set of nodes is *C*. (b) The topology of the networks after the process of interdependent failure. Nodes *A*, *D* in network N_B and nodes *B*, *C* in network N_A fail and lose their functions. (c) The topology of the networks after the process of overload failure. Node *C* in network N_B fails as the load exceeds its capacity. So is node *B*. (d) The terminal state of the interdependent networks. All nodes fail and lose their functions.

https://doi.org/10.1371/journal.pone.0192874.g002

properties of the network will change after some nodes are attacked and fail. These properties are parameters for evaluating the robustness of the complex networks, such as the connectivity, the largest connected component, and the average shortest path. With the development of research on the controllability of complex networks, more attention is attracted by the robustness of the controllability of a complex network.

When a different fraction of nodes in interdependent networks is attacked, the network will reach a stable state in the end. Then, we analyze the controllability of the interdependent networks under different proportions of attacks to obtain the robustness of controllability in the interdependent networks. The parameter to evaluate the robustness of controllability in the interdependent networks can be calculated as follows:

$$CR = \frac{1}{|N_A| + |N_B|} \sum_{q=1/N_A}^{1} \frac{s_A(q) + s_B(q)}{N_D^A(q) + N_D^B(q)}, \tag{7}$$

where $|N_A|$, $|N_B|$ are the number of nodes in networks N_A and N_B, respectively. A directed network is called weakly connected if replacing all of its directed edges with undirected edges produces a connected (undirected) network. $s_A(q)$ is the fraction of the largest weakly connected component nodes of network N_A in the whole network after removing qN_A nodes in network N_A and qN_B nodes in network N_B, and $s_B(q)$ is the fraction of the largest weakly connected component nodes of network N_B in the whole network. $N_D^A(q)$ is the number of minimum driver nodes of network N_A after removing nodes. $N_D^B(q)$ is the number of minimum driver nodes of network N_B.

Redundant design in interdependent networks

The more important purpose of studying the robustness of controllability of interdependent networks is to find methods to improve it [27, 28]. As the properties of interdependent networks are determined by the topology of each isolated network and the dependency edges between the networks, the robustness of controllability can be improved by node backup for each isolated network and dependency edge backup between each isolated network. This is a redundancy design of the interdependent networks [22].

Node backup. The overload failures exist in the cascading process of interdependent networks. When a node is attacked, its failure will lead to a higher load of the functional nodes in the network and cause overload failure. If nodes are backed up, they can stand more loads and enlarge their capacity. Therefore, node backup will suppress the process of overload failures and decrease the proportion of failure nodes. Furthermore, fewer minimum driver nodes to maintain the networks structurally controllable are required. At last, we can improve the robustness of controllability for interdependent networks.

Fig 3 shows the model for node backup. Fig 3(a) is the topology of the nodes without backup. This paper assumes that the backup nodes will not be activated until necessary. Therefore, the initial loads of the nodes will not increase as shown in Fig 3(b), but the capacities of the nodes will increase. When node *C* fails, its load will allocate to its functional neighbors, which may cause overload failures. If we back up node *C* and its backup nodes has been activated, the overload failures will not happen as shown in Fig 3(c). Furthermore, the cost of the node *C* will also increase because of node backup. Clearly, the capacity of node v_k can be calculated as follows [22]:

$$CC(v_k) = n \times Cap(v_k), n \in \mathbb{N}, k = 1, \cdots, N, \tag{8}$$

where *Cap* (v_k) is the initial capacity of node v_k, and *n* is the number of backup nodes for node v_k. The cost of the network after node backup is $\sum_{i=1}^{N} CC(v_k)$.

The strategy to determine the set of backup nodes has a significant effect on the optimization of robustness of interdependent network controllability. This paper compares five different strategies to backup nodes in interdependent networks, which are random-based (RBS), low frequency of overload failures first (LFOF), high frequency of overload failures first (HFOF), degree based (DBS) and betweenness-based (BBS).

RBS strategy randomly selects nodes of interdependent networks to backup nodes. DBS strategy and BBS strategy select nodes that have a higher degree and a higher betweenness, respectively.

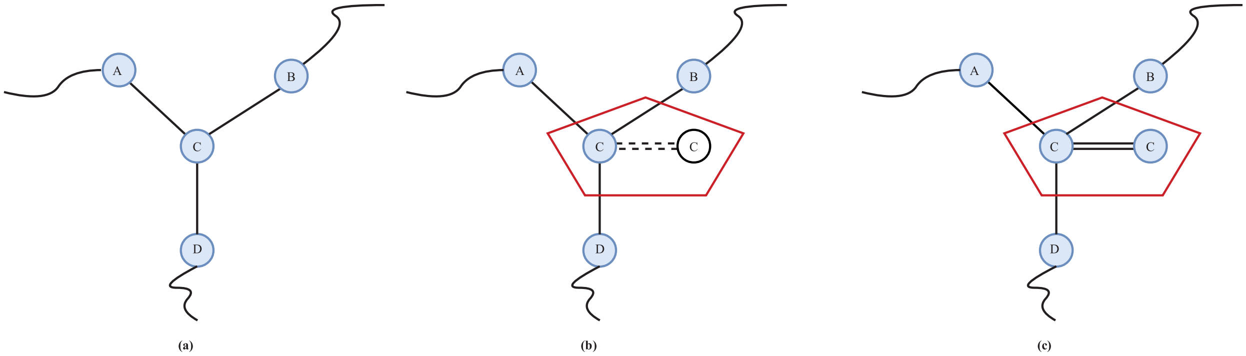

Fig 3. Model of node backup. (a) The topology of networks without node backup. (b) The node backup will not be activated if nodes *C* works. (c) The node backup will be activated if nodes *C* fails.

https://doi.org/10.1371/journal.pone.0192874.g003

LFOF strategy prefers to select nodes that have a low frequency of overload failures that can be obtained by large scale simulation of cascading failures over in interdependent networks. In fact, the frequency data of overload failure nodes shall be obtained before we choose a strategy to select nodes to backup. The structure of the interdependent networks which produce the frequency data is the same as the structure of networks which will have redundancy design. To obtain the frequency data of failure nodes including overload failures and interdependent failures, attack proportion and enough simulations shall be choose appropriately as shown in S1 Mat and S2 Mat. Similarly, HFOF strategy prefers to select nodes that have a higher frequency of overload failures.

Dependency edge backup. Interdependent failure is another failure mode in the cascading process of interdependent networks. The removal of a node in network N_A will fail the node that depends on it in network N_B. Fig 4 shows the mode of dependency edges backup. Node A in network N_A is attacked and node A in network N_B will fail if no dependency edges backup exists. However, if node A in network N_B has a dependency edge, as the red dashed line shows, it will activate this edge and depend on node C in network N_A. Therefore, node A in network N_B will remain working. This redundancy design will suppress the interdependent failure process and increase the robustness of interdependent network controllability.

The dependency edge backup will not increase the initial loads and capacities of nodes in the network. However, some additional resources will be added to the network. Therefore, the cost of the dependency edges can be calculated as follows [22]:

$$Cost(l_{ij}) = \max\{Cap(v_i), Cap(v_j)\}, v_i \in V(N_A), v_j \in V(N_B) \tag{9}$$

where $Cost(l_{ij})$ is the cost of dependency edge l_{ij}. The total cost of dependency edges is $\sum Cost(l_{ij})$.

The strategy to determine those nodes that have dependency edges plays a key role in the result of optimizing the robustness of controllability. This paper has studied seven strategies, which are random selected (RSB), low frequency of interdependent failures first (LFIF), high frequency of interdependent failures first (HFIF), across low and high frequency of interdependent failures (AFIF), high degree first (HDF), low degree first (LDF) and across high and low degree (ADF).

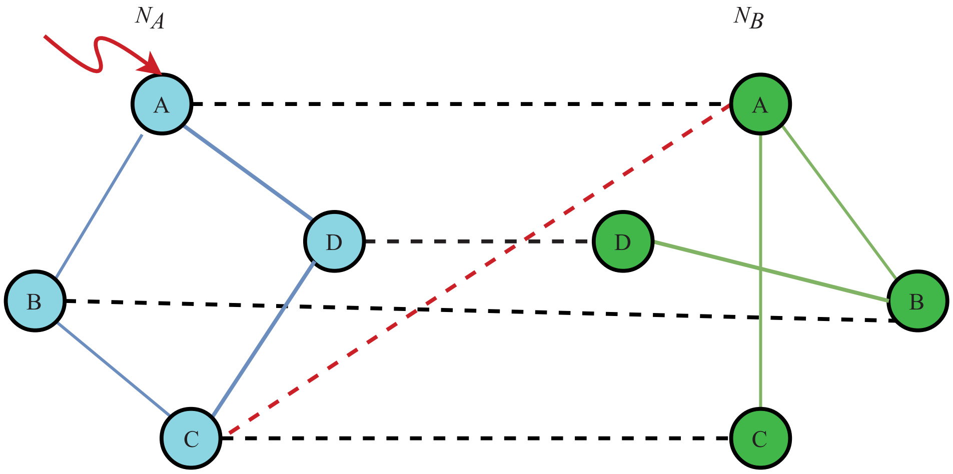

Fig 4. Dependency edge backup. If node A is attacked, node A in another network will not fail because of its dependency edge backup strategy.

https://doi.org/10.1371/journal.pone.0192874.g004

RSB strategy randomly selects nodes and makes redundancy edges between them. LFIF strategy prefers to select a lower frequency of interdependent failure nodes in both networks and backup their redundancy edges. Similarity, HFIF prefers to select a higher frequency of interdependent failure nodes. AFIF selects one node with a higher frequency of interdependent failures in a network and a lower node in another network. HDF and LDF selects nodes with high and low degree in both networks, respectively. ADF strategy select a higher degree node in a network and a lower degree node in another.

The procedure of the optimization algorithm for robustness

Redundancy design is a method to improve the robustness of controllability of interdependent networks. The process of the method is described as follows:

Step 1. Initiate the interdependent networks.
In this stage, the topology of the interdependent networks will be initialized, including the scale of networks, the degree distribution of the network and the dependency edges between the networks. Therefore, we can get the initial loads and capacities of nodes in interdependent networks. One of the redundancy design strategies is also determined to optimize the robustness of controllability. According to the strategy, some changes will be made in the topology of networks.

Step 2. Obtain the frequency data of failure nodes including overload failures and interdependent failures in large scales simulation in interdependent networks.
In this stage, the attack proportion shall be determined in order to produce sufficient frequency data of failure nodes. Then we randomly select the set of nodes in both networks to attack. Nodes which are attacked will fail and so will the nodes which depend on the former. This is the process of interdependent failures. The load of failure nodes will be reallocated to the nodes that are still functional. Once the load of a node exceeds the capacity of that node, the node will fail. Therefore, the process of overload failures will begin. Interdependent failures alternate with overload failures until no nodes fail. Then we obtain the frequency data of failure nodes including overload failures and interdependent failures by repeating this simulation for enough times.

Step 3. The cascading process of interdependent networks under different proportions of attack nodes.
Firstly, we initialize the parameters of interdepenedent networks by step 1. The proportion of attack nodes is continuously obtained from the interval [0, 1]. We randomly select the set of nodes in both networks to attack. The cascading process, including the interdependent failures and overload failures, will alternately happen until the networks reach a stable state. Then, we calculate the minimum driver node set of the networks that are left and collect data in the cascading process such as the proportion of interdependent failures and overload proportion, the proportion of minimum driver nodes in both interdependent networks and the cost of the strategy. Repeated simulations are conducted under diffrent attack proportions. At last, we can obtain the robustness of interdependent network controllability by Eq (7) under different strategies from these data.

Step 4. Compare the effect of different strategies on optimization of the robustness of interdependent network controllability.

Results

To verify the feasibility and effect of our proposed strategy on the optimization of the robustness of interdependent network controllability, we conduct a series of comparative experiments in this section. Without the loss of generality, the two isolated directed networks labeled N_A and N_B are ER networks that are widely used in the research of complex networks and have the same number of nodes that can be denoted by $|N_A| = |N_B| = 300$. The probabilities of two nodes that are connected are $p_A = 0.02$ and $p_B = 0.02$ in networks N_A and N_B, respectively. This paper randomly selects initial dependency edges with one node in network N_A and and one in network N_B. This is the initial topology of interdependent networks that is used in all simulations. For the load-capacity model, we use a nonlinear load-capacity model, where the parameter α is set to 0.97, and β is 6. For LFOF and HFOF strategies that are used to optimize the redundant design in node backup, we shall gather the frequency information of overload failures for each node in the interdependent networks. Similarity, HFIF, LFIF and AFIF strategies that can improve the performance of dependent edges

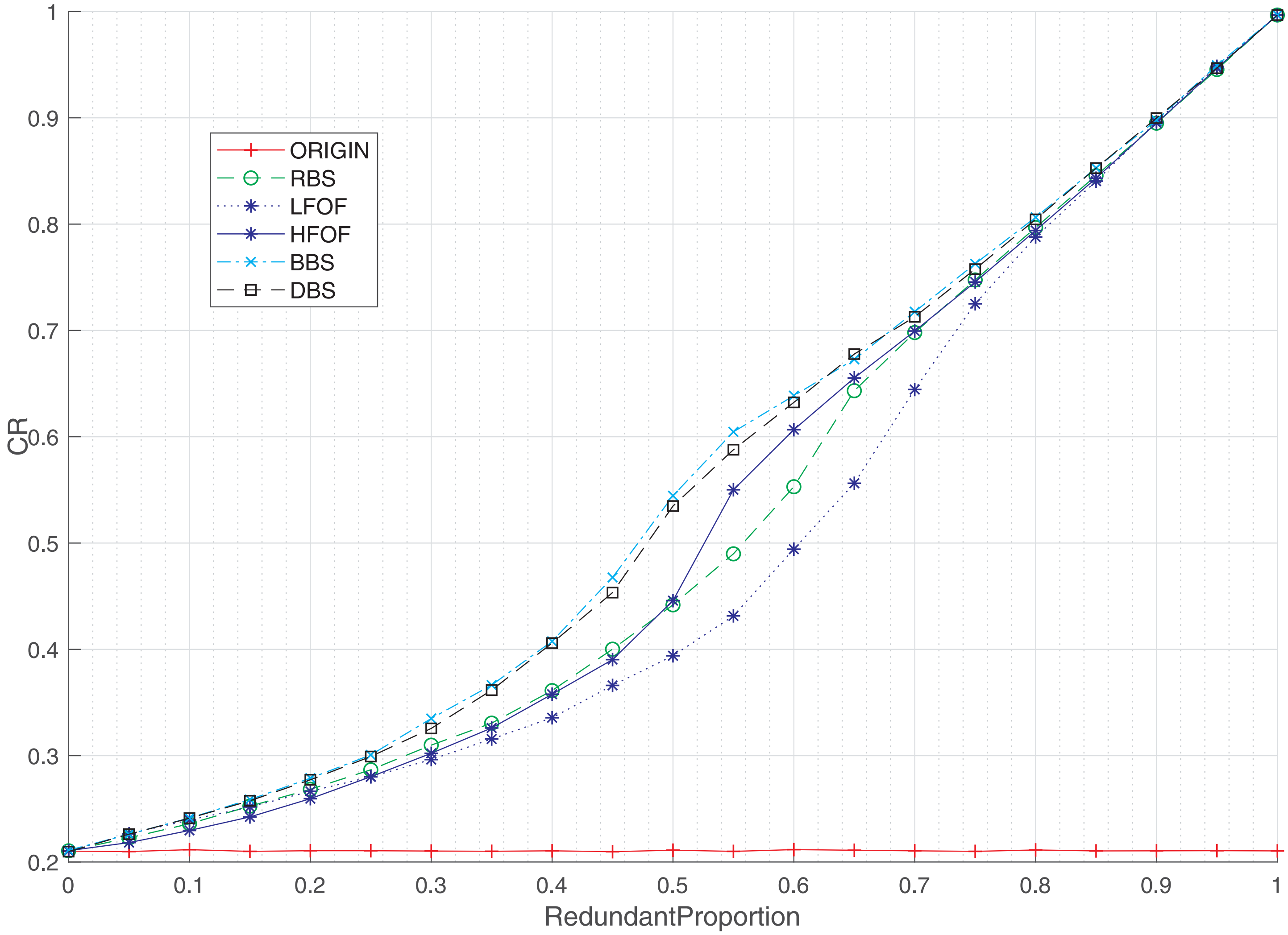

Fig 5. Relationship between the robustness of interdependent network controllability and the proportion of node backup under different backup strategies. CR is a parameter to evaluate the robustness of interdependent network controllability.

https://doi.org/10.1371/journal.pone.0192874.g005

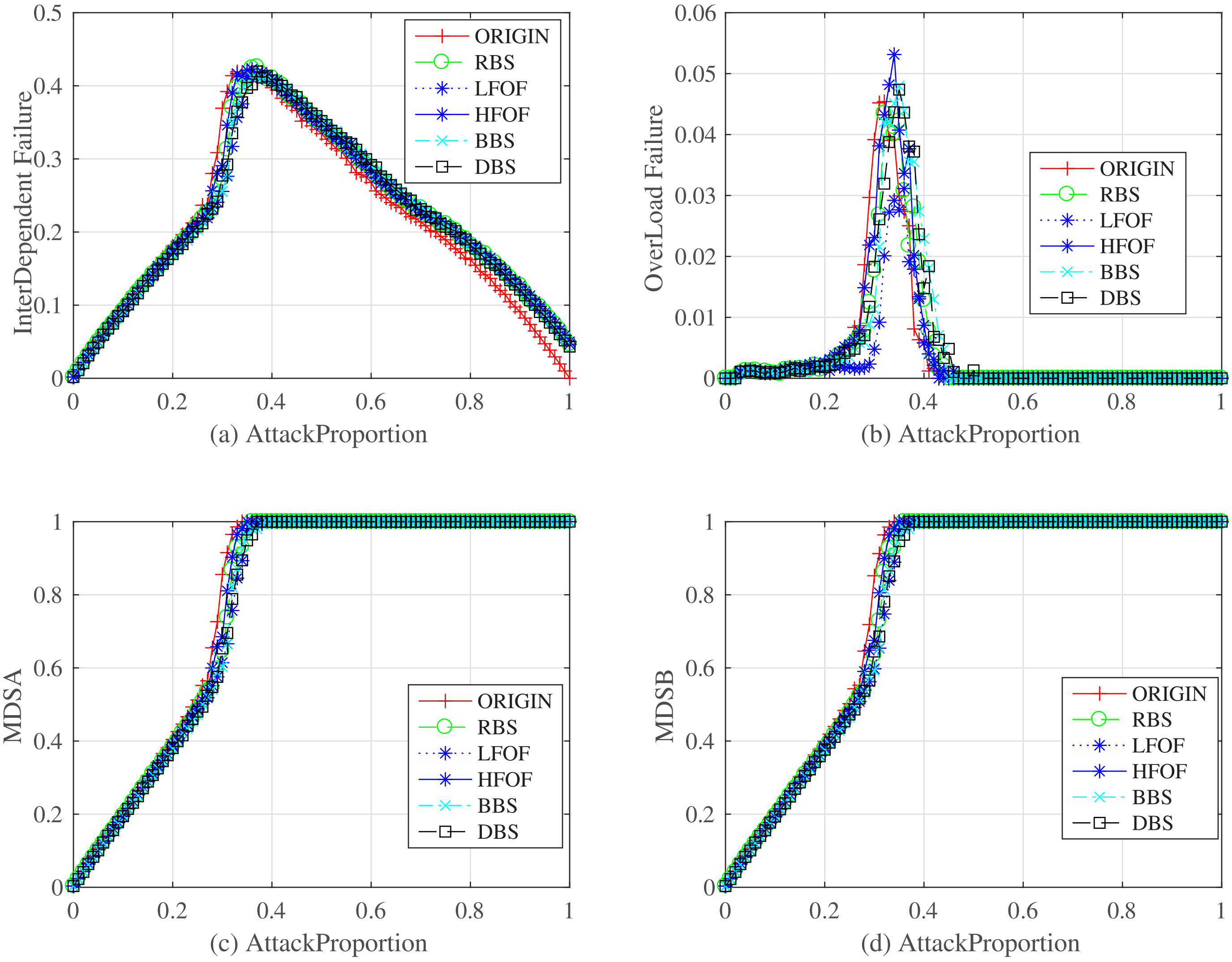

Fig 6. Statistical data for the network under the node backup proportion of 10% for different strategies.

https://doi.org/10.1371/journal.pone.0192874.g006

backup require the frequency information of interdependent failures. To obtain the frequency data of the failure nodes, we simulate 100,000 times under the same conditions when the attacked proportion is 30%.

To compare the performance of strategies over the node backup mechanism, experiments based on the five strategies (RBS, LFOF, HFOF, BBS, and DBS) are conducted as depicted in Figs 5–8. The red line labeled as ORIGN in each figure shows the result without redundant design. For different proportions of node backup, the robustness of interdependent networks under different strategies is shown in Fig 5. The robustness of controllability increases slowly as the redundant proportion is small and speeds up when the redundant proportion increases, showing the feasible method of node backup to optimize the robustness. From another perspective, BBS and DBS strategies can make interdependent networks more roubust and work better than other strategies in the same condition. Therefore, nodes with higher degree and load urgently need backups. Furthermore, node backup for lower failure frequency (LFOF) is worse than node backup for higher nodes (HFOF) and even worse than the RBS strategy,

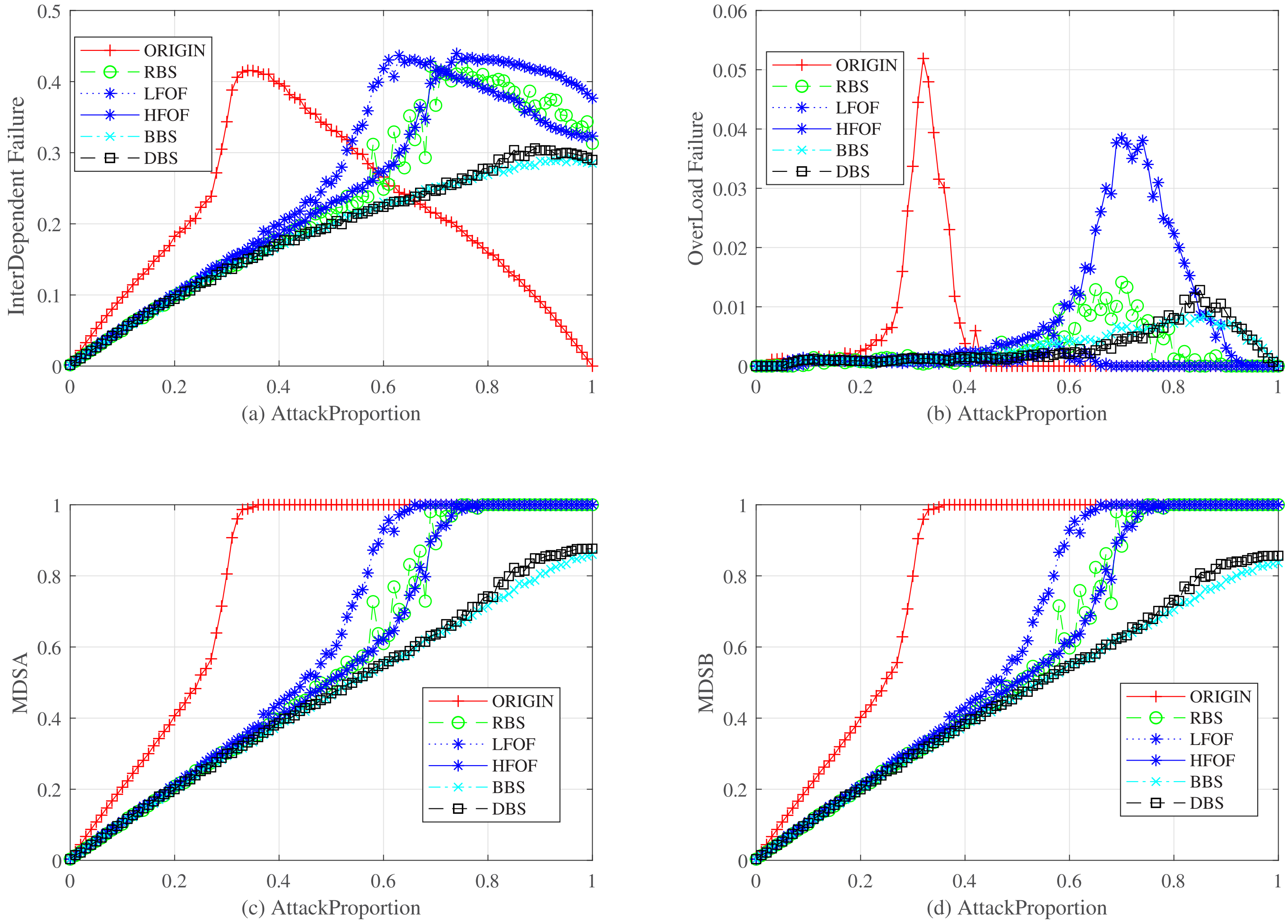

Fig 7. Statistical data for the network under the node backup proportion of 55% for different strategies.

https://doi.org/10.1371/journal.pone.0192874.g007

demonstrating that we shall allocate more resources to nodes that failed more in the past. Therefore, LFOF strategy is a bad choice to optimize the robustness of interdependent networks.

Figs 6 and 7 shows statistical data including interdependent failures and overload failures for the network under the node backup proportions of 10% and 55% for different strategies. MSDA and MSDB are the proportions of driver nodes in network N_A and N_B, respectly. We can ensure that the node backup strategy can indeed decrease those nodes suffering from failure and improve the robustness of controllability. It will delay the appearance of a phase transition behavior as the attack proportion grows. The cost of different strategies is described in Fig 8 where we can observe that DBS and BBS will have a high cost though they can improve the robustness of controllability at the same time. We must take care that the HFOF strategy costs nearly the same as the DBS and the BBS strategies. Under these conditions, HFOF is not a good strategy, nor is LFOF. Therefore, we should choose the BBS or DBS strategy for node backup.

By comparing the performance of strategies over the redundancy edges backup mechanism, we carry out our simulation based on the seven strategies (RSB, LFIF, HFIF, AFIF, ADF, HDF,

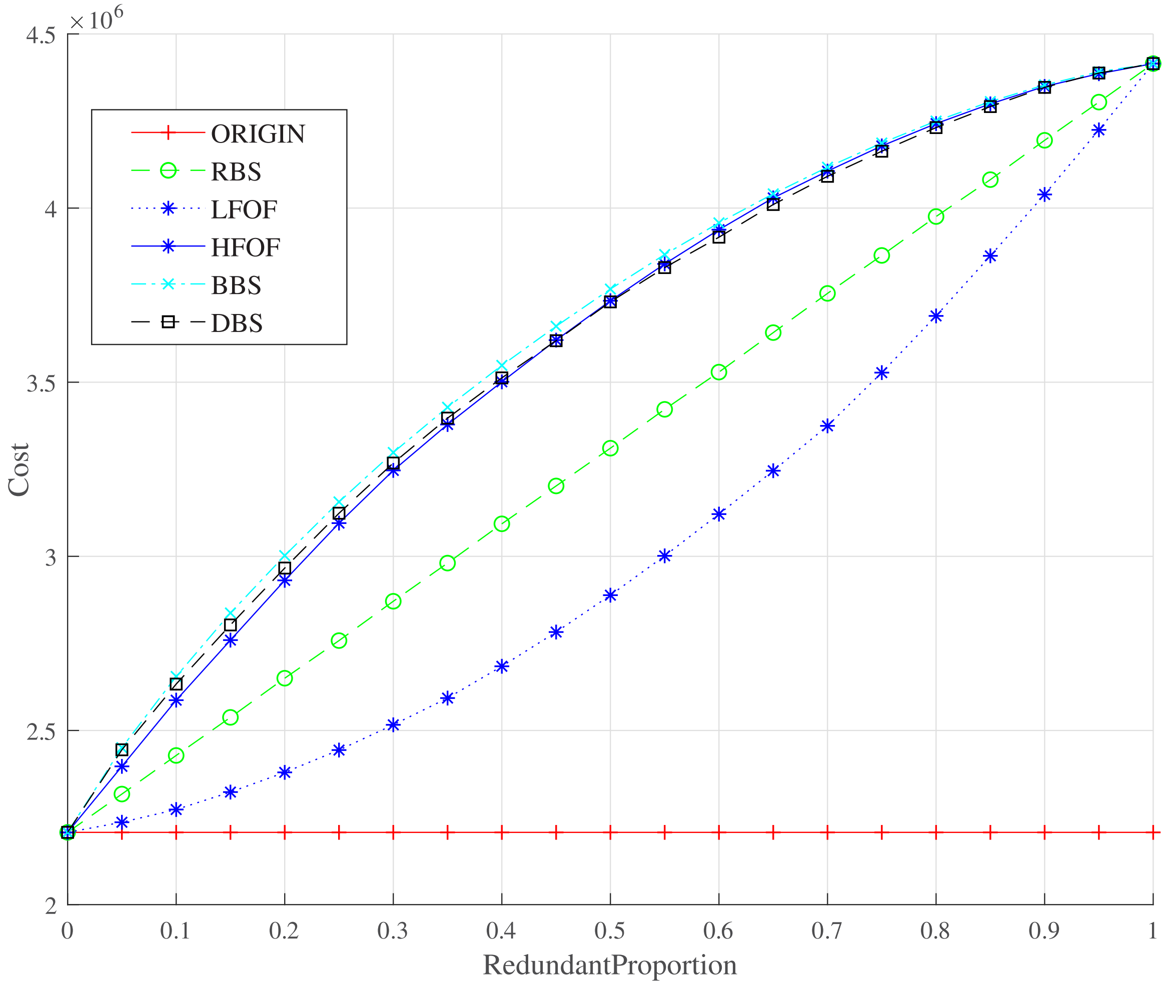

Fig 8. Relationship between the cost and the proportion of node backup under different backup strategies. The total cost of the interdependent networks with node backup can be obtained by Eq (8).

https://doi.org/10.1371/journal.pone.0192874.g008

and LDF) as shown in Figs 9 and 10. For different redundant proportions, Fig 9 presents the relationship between the robustness of controllability and redundancy edges backup strategies. The HFIF and HDF strategies work better than the others. Therefore, we shall choose redundancy edges that have nodes with higher degree or higher failure frequency. LDF and LFIF are not good choices to optimize the robustness of controllability. They work even worse than the RSB strategy. The cost of all strategies for redundancy edges backup is demonstrated in Fig 10. We can see that HDF costs more than HFIF when the redundant proportion ranges from 0 to 0.55. However, HDF will cost less when the redundant proportion is larger than 0.55. The robustness of all redundancy edge backup strategies converges to 0.32 when redundant proportion is close to 1 because redundancy edges backup cannot suppress the process of overload failure, which can fail the isolated network. Therefore, dependency edge backup can only optimize the interdependent failure process and improve partial robustness but not all robustness.

Discussion

Controllability of networks has become hot topic in recent years. The cascading process of interdependent networks, including interdependent failure and overload failure, could make a

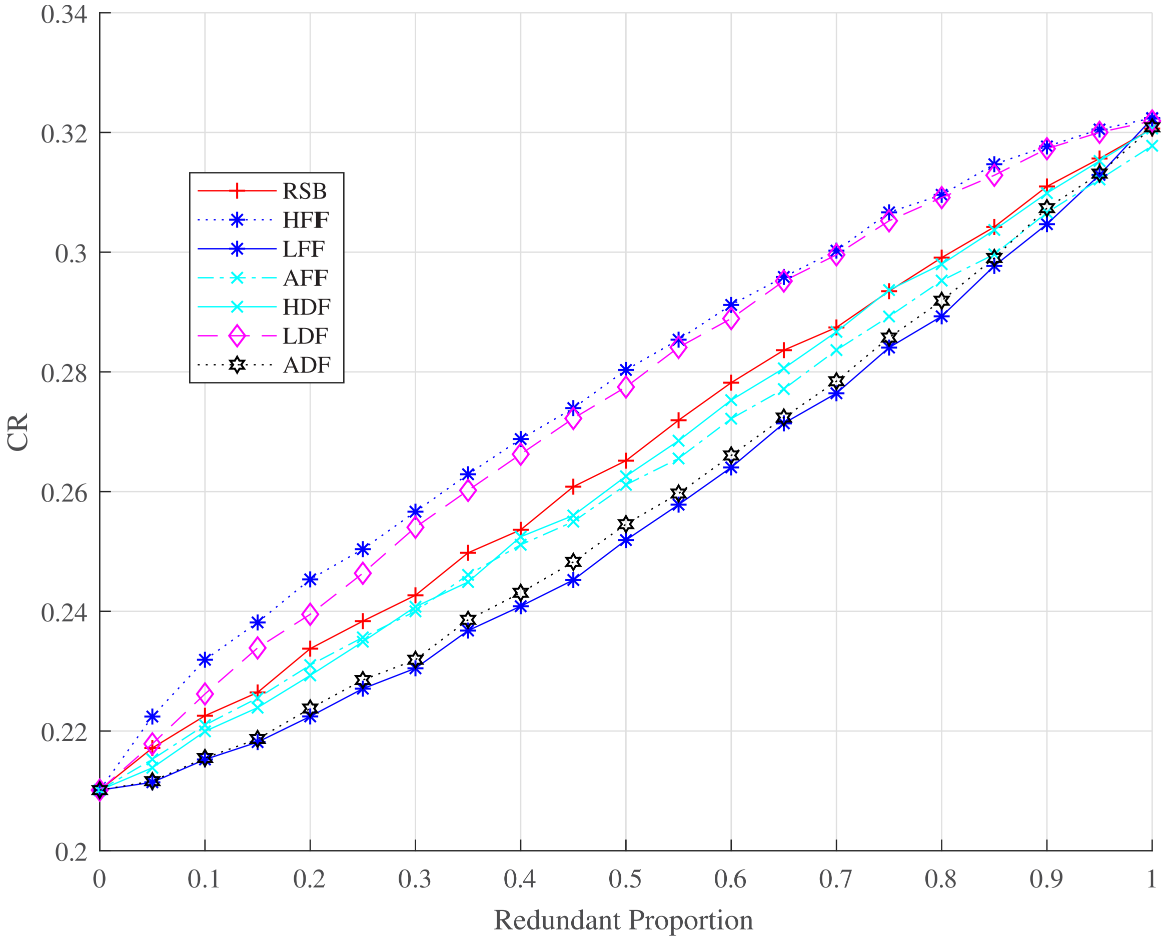

Fig 9. Relationship between the robustness of interdependent network controllability and the proportion of redundancy edge backup under different backup strategies. CR is a parameter to evaluate the robustness of interdependent network controllability.

https://doi.org/10.1371/journal.pone.0192874.g009

whole network cascade when only a small fraction of the nodes fail in fault. In this paper, we have studied the cascading process based on the non-linear load-capacity model. We analyze the factors which determine the process of cascading failures and proposing a redundant design including node backup and dependency edge backup to optimize the robustness of interdependent network controllability. The redundant design is feasible and effective at improving the robustness of interdependent networks. As the strategy to determine the set of backup nodes and denpendency edges has a significant effect on the optimization of robustness of interdependent network controllability, this paper compares five node backup strategies and seven dependency edge backup strategies in interdependent networks. We also considered the cost of all the strategies.

Among the strategies which are proposed in this paper, the BBS and DBS strategies are good choices for node backup, even though they cost more than the other strategies. Similarity, the HFIF and HDF strategies are best choices of redundancy edges backup. Considering the cost of the strategy, HDF is better than HFIF when the redundant proportion of redundancy edges is small, and HFIF is the best when the redundant proportion of redundancy edges is large.

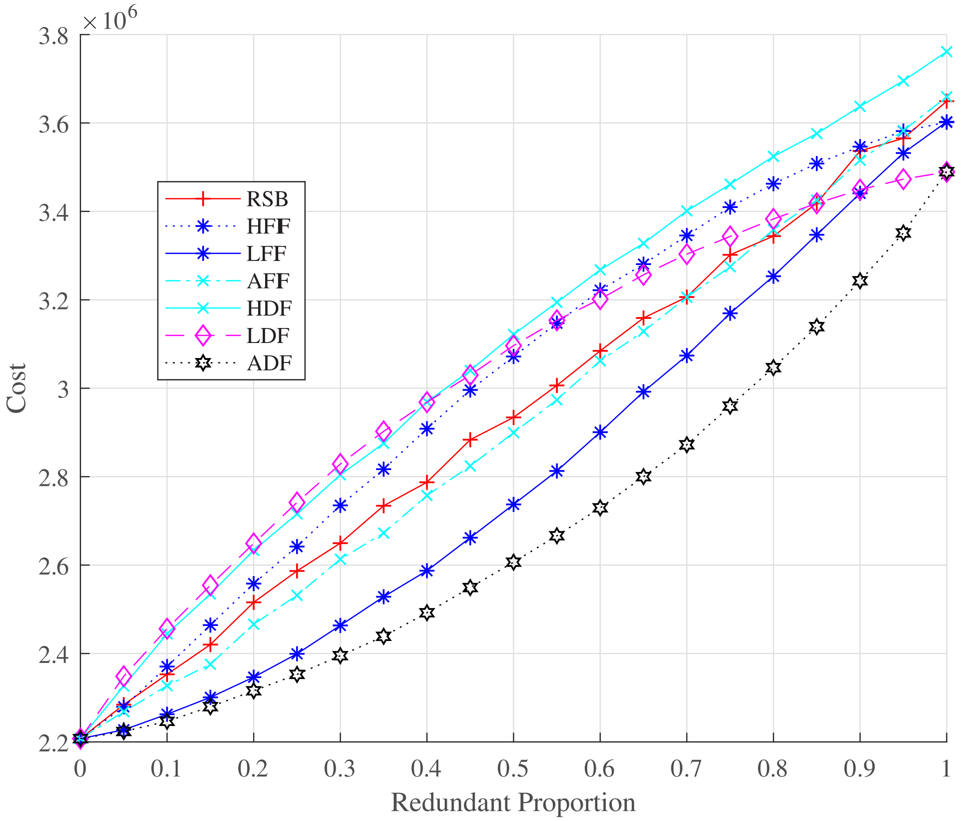

Fig 10. Relationship between the cost and the proportion of redundancy edge backup under different backup strategies. The total cost of the interdependent networks with redundancy edge backup can be obtained by Eq (9).

https://doi.org/10.1371/journal.pone.0192874.g010

Supporting information

S1 Fig. The structure of interdependent networks without redundant design under different attack proportions. The parameters of the ER interdependent networks is $\alpha = 0.97$, $\beta = 2$, 6, 10, $N = 300$, $p_a = 0.02$, $p_b = 0.03$, MDSA is the number of minimum driver nodes in network N_A, so is MSDB.
(FIG)

S2 Fig. The structure of interdependent networks for different α when attack proportions is 5%. The parameters of the ER interdependent networks is $\beta = 2$, 6, 10, $N = 300$, $p_a = 0.02$, $p_b = 0.03$.
(FIG)

S1 Mat. The structure of the interdependent networks. The parameters of the ER interdependent networks is $N = 300$, $p_a = 0.02$, $p_b = 0.03$.
(MAT)

S2 Mat. The failure frequency data of nodes after simulation for 100000 times when the attack proportion is 30%. The parameters of the ER interdependent networks is $\beta = 6$, $\alpha = 0.97$, $N = 300$, $p_a = 0.02$, $p_b = 0.03$. Sufficient frequency data of failure nodes can be obtained under the attack proportion.
(MAT)

Acknowledgments

We thank Lijun Liu for his critical reading of the manuscript and useful suggestion in the experiments design.

Author Contributions

Conceptualization: Zenghu Zhang, Yongfeng Yin.

Data curation: Zenghu Zhang, Yongfeng Yin, Xin Zhang, Lijun Liu.

Formal analysis: Zenghu Zhang, Xin Zhang, Lijun Liu.

Funding acquisition: Zenghu Zhang, Yongfeng Yin.

Investigation: Zenghu Zhang, Yongfeng Yin, Lijun Liu.

Methodology: Zenghu Zhang, Yongfeng Yin.

Project administration: Yongfeng Yin.

Resources: Yongfeng Yin, Lijun Liu.

Software: Zenghu Zhang, Yongfeng Yin, Xin Zhang.

Supervision: Yongfeng Yin.

Validation: Yongfeng Yin, Xin Zhang, Lijun Liu.

Visualization: Zenghu Zhang.

Writing – original draft: Zenghu Zhang.

Writing – review & editing: Zenghu Zhang, Yongfeng Yin, Xin Zhang, Lijun Liu.

References

1. Gao JX, Buldyrev SV, Stanley HE, Havlin S. Networks formed from interdependent networks. Nature Physics. 2012 Dec; 8(1):40–48. https://doi.org/10.1038/nphys2180
2. Gomez S, Diaz-Guilera A, Gomez-Gardenes J, Perez-Vicente CJ, Moreno Y, Arenas A. Diffusion Dynamics on Multiplex Networks. Physical Review Letters. 2013; 110(2). https://doi.org/10.1103/PhysRevLett.110.028701
3. Menichetti G, Dall'Asta L, Bianconi G. Control of Multilayer Networks. Scientific Reports. 2016; 6:8. https://doi.org/10.1038/srep20706
4. Boccaletti S, Bianconi G, Criado R, del Genio CI, Gomez-Gardenes J, Romance M, et al. The structure and dynamics of multilayer networks. Physics Reports. 2014; 544(1):1–122. https://doi.org/10.1016/j.physrep.2014.07.001
5. Wang XW, Nie S, Wang WX, Wang BH. Controlling complex networks with conformity behavior. EPL. 2015; 111(6):68004. https://doi.org/10.1209/0295-5075/111/68004
6. Nie S, Wang XW, Wang BH, Jiang LL. Effect of correlations on controllability transition in network control. Scientific reports. 2016; 6:23952. https://doi.org/10.1038/srep23952 PMID: 27063294
7. Liu YY, Slotine JJ, Barabasi AL. Controllability of complex networks. Nature. 2011; 473(7346):167–173. https://doi.org/10.1038/nature10011 PMID: 21562557
8. Lin CT. Structural controllability. IEEE Transactions on Automatic Control. 1974; 19(3):201–208. https://doi.org/10.1109/TAC.1974.1100557
9. Menichetti G, Dall'Asta L, Bianconi G. Network Controllability Is Determined by the Density of Low In-Degree and Out-Degree Nodes. Physical Review Letters. 2014; 113(7). https://doi.org/10.1103/PhysRevLett.113.078701 PMID: 25170736
10. Hou LL, Small M, Lao SY. Maximum entropy networks are more controllable than preferential attachment networks. Physics Letters A. 2014; 378(46):3426–3430. https://doi.org/10.1016/j.physleta.2014.09.057

11. Jia T, Barabasi AL. Control Capacity and A Random Sampling Method in Exploring Controllability of Complex Networks. Scientific Reports. 2013; 3. https://doi.org/10.1038/srep02354

12. Jia T, Liu YY, Csoka E, Posfai M, Slotine JJ, Barabasi AL. Emergence of bimodality in controlling complex networks. Nature Communications. 2013; 4. https://doi.org/10.1038/ncomms3002

13. Watts DJ. A simple model of global cascades on random networks. Proceedings of the National academy of Sciences of the United States of America. 2002; 99(9):5766–5771. https://doi.org/10.1073/pnas.082090499 PMID: 16578874

14. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature. 2010; 464(7291):1025–1028. https://doi.org/10.1038/nature08932 PMID: 20393559

15. Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the internet to random breakdowns. Physical review letters. 2000; 85(21):4626. https://doi.org/10.1103/PhysRevLett.85.4626 PMID: 11082612

16. Callaway DS, Newman MEJ, Strogatz SH, Watts DJ. Network robustness and fragility: Percolation on random graphs. Physical Review Letters. 2000; 85(25):5468–5471. https://doi.org/10.1103/PhysRevLett.85.5468 PMID: 11136023

17. Schwartz N, Cohen R, ben Avraham D, Barabasi AL, Havlin S. Percolation in directed scale-free networks. Physical Review E. 2002; 66(1). https://doi.org/10.1103/PhysRevE.66.015104

18. Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex networks. Physical Review E. 2002; 65(5). https://doi.org/10.1103/PhysRevE.65.056109

19. Albert R, Jeong H, Barabasi AL. Error and attack tolerance of complex networks. Nature. 2000; 406 (6794):378–382. https://doi.org/10.1038/35019019 PMID: 10935628

20. Wang BB, Gao L, Gao Y, Deng Y. Maintain the structural controllability under malicious attacks on directed networks. Epl. 2013; 101(5). https://doi.org/10.1209/0295-5075/101/58003

21. Nie S, Wang X, Zhang H, Li Q, Wang B. Robustness of controllability for networks based on edge-attack. PLoS One. 2014; 9(2):e89066. https://doi.org/10.1371/journal.pone.0089066 PMID: 24586507

22. Liu LJ, Yin YF, Zhang ZH, Malaiya YK. Redundant Design in Interdependent Networks. PLoS One. 2016; 11(10). https://doi.org/10.1371/journal.pone.0164777

23. Kalman RE. Mathematical description of linear dynamical systems. Journal of the Society for Industrial and Applied Mathematics, Series A: Control. 1963; 1(2):152–192. https://doi.org/10.1137/0301010

24. Kim DH, Motter AE. Resource allocation pattern in infrastructure networks. Journal of Physics A Mathematical and Theoretical. 2008; 41(22). https://doi.org/10.1088/1751-8113/41/22/224019

25. Dou BL, Wang XG, Zhang SY. Robustness of networks against cascading failures. Physica A Statistical Mechanics and Its Applications. 2010; 389(11):2310–2317. https://doi.org/10.1016/j.physa.2010.02.002

26. Pu CL, Pei WJ, Michaelson A. Robustness analysis of network controllability. Physica A Statistical Mechanics and Its Applications. 2012; 391(18):4420–4425. https://doi.org/10.1016/j.physa.2012.04.019

27. Hou LL, Lao SY, Bu J, Bai L. Enhancing Complex Network Controllability by Rewiring links. 2013 Third International Conference on Intelligent System Design and Engineering Applications. 2013; p. 709–711.

28. Hou L, Lao SY, Small M, Xiao YD. Enhancing complex network controllability by minimum link direction reversal. Physics Letters A. 2015; 379(20–21):1321–1325. https://doi.org/10.1016/j.physleta.2015.03.018