Robustness Analysis of Interdependent Networks under Grey Information Attack

Zhe Wang 1,2, Jianhua Li 2, Dong Kang 1,2, Haodan Ran 2

1 Information and Navigation College, Air Force Engineering University, Xi’an 710077, China
2 College of Information and Communication, National University of Defense Technology, Xi’an 710100, China
wangzhe798@nudt.edu.cn

Abstract. In modern society, many infrastructures are interdependent owing to functional and logical relations among components in different systems, and they can be characterized as complex interdependent networks. Interdependency makes network so fragile that even a slight initial disturbance may lead to a cascading failure of the entire systems. Previous research on interdependent networks has focused on two types of initial attack: random attack and degree-based targeted attack. In this paper, a grey information attack strategy with the information incompleteness and complexity by adjusting the tunable parameters was designed, and a cascading failure process is studied considering their effects on failure propagation. Moreover, the robustness of two types of interdependent networks (BA – BA, ER – ER) is evaluated under grey attacking strategies. Interesting conclusions could be obtained. The simulation results show that the proposed method can identify the key nodes more effectively, and the robustness of the network decreases with the increase of the grey attack coefficient. In addition, the relation between weight coefficient and robustness under various strategy is quite different. Our results can be very useful for safety design and protection of interdependent networks.

1. Introduction

With the rapid development of economy and science and technology, the coupling and service dependence between various infrastructure systems are getting higher and higher. The service dependency relationship between different types of infrastructure systems makes them jointly constitute interdependent systems[1]. For example, advanced information and communication technologies are widely used in power grid systems, which has deepened the fusion of communication information systems and power physical networks[2]. Due to the interdependence between systems, once system encounters extreme events such as extreme weather, earthquakes, and terrorist attacks, the interaction caused by the interdependence will amplify the coupling of disaster effects and cause cascading failures. For example, 2010, Stuxnet hit about 30,000 Internet terminals in Iran, infecting more than 100,000 hosts[3], the large-scale power outage in Venezuela in 2019[4], and the worldwide outbreak of COVID-19 in 2020 are all closely related to cascading failures[5]. This article focuses on cascading failures in interdependent networks. The real attention began with the work of Buldyrev et al.[6] in 2010, and they proposed a theoretical framework for solving the cascading failure of interdependent networks.

In recent years, the research on the robustness of networks has been extensively carried out under the theoretical framework, various research results have shown that the behaviours of networks are
different from the single network. At present, the research on the robustness of interdependent networks mainly includes three aspects. First, some studies focus on the robustness of different structural models. Parshani et al. explored the effect of coupling strength on the robustness of interdependent networks[7]. Chen and Gao et al. studied the robustness of interdependent networks from the perspective of a coupling model[8]. Other researchers have studied the robustness of interdependent networks from the perspective of network weights[9], types, interdependent directions, and malicious attacks[10-12]. However, the cascading fault seepage model only considers the topology characteristics of the network. In view of the fact that the actual interdependent system has the function of carrying the load, literature[13] considers the load coupling factors in the interdependent network, such as the amount of electricity transmitted in the power network, the passengers and materials transported in the transportation network, and the traffic transmitted by the Internet Package, etc., to establish a cascading failure model of a load-interdependent network. Second, there are some research on the robustness analysis with different failure strategies, Liu[14] study the robustness of partially networks when suffering attack combinations of random, targeted, and localized attacks. Hao[15] propose fourteen edge attack strategies by two edge importance functions. Then, BA networks with assortative coupling (AC), disassortative coupling (DC), and random coupling (RC) are constructed, whose robustness is quantified by the relative size of the giant component under varying a fraction $f$ of removed edges. The third is the robustness under different measurement indicators. The measures of the robustness of traditional interdependent networks include maximal connected subgraphs[16], average failure scale[17], algebraic connectivity[18-20], natural connectivity[21], and seepage threshold[22].

However, previous studies on interdependent networks mainly focused on a single attack type such as random failure or degree-based malicious attacks which means that one can obtain the all information of nodes or not, but the attack information may be imprecise in the real world and not only random or malicious, and different failure strategies have different effects on the network. In this paper, we consider another important scenario of imperfect attack information, i.e., one can obtain the information of all nodes, but the attack information may be imprecise. Our study focuses on the exact value of the critical removal fraction of nodes for the disintegration of interdependent networks. We find that decreasing the precision of attack information can enhance the attack robustness of interdependent networks remarkably.

The rest of this paper is organized as follows. In Sec.2, we describe the model of cascading failures and the relative size of the giant connected component $S$ used to characterize the robustness of interdependent networks. In Sec.3, a general grey attack strategy is proposed. In Sec.4, the results of our simulations are illustrated and discussed. Finally, conclusions are summarized in Sec.5.

2. Model Definitions

2.1. Network model

In this paper, without loss of generality, our model is assumed in a pair of interdependent networks formed by layers $A$ and $B$ whose size is $N$, and the two networks have the same size $N^A = N^B$. $N^A = N/2$ and $P_A(k)$ represent the size and degree distribution of network $A$, meanwhile, $N^B = N/2$ and $P_B(k)$ represent the size and degree distribution of network $B$. There are two kinds of links in the model, which one is called inner-link and the other is called dependence-link. Inner-link is the link that connect the nodes belong to same layer, and the dependence-link is some links that connecting one node in layer $A$ and another node in layer $B$. In initial stage (stage 0), there are $q_0^{A-B} N^A$ dependence-links from nodes in network $A(B)$ to nodes in network $B(A)$. $q_0^{A-B}$ quantifies the fraction of nodes having interdependency links in models. For simplicity, we set $q_0^{A-B} = 1$, that’s mean each node in network $A$ depends only on one node in network $B$ and vice versa, which establishes a one-to-one bidirectional dependent relation. The one-to-one bidirectional dependent links are established randomly to avoid any correlations among the two networks.
The interdependent network can be viewed as a triple form $\Theta(G_A, G_B, G_R)$, where $G_A$ is the network $A$, which is represented as simple undirected graph $G_A = (V_A, E_A)$. $G_B$ is the network $B$, which is represented as $G_B = (V_B, E_B)$. $G_R$ is the coupling network, which is represented as $G_R = (V_R, E_R)$, where $V_R \in \{V_A, V_B\}$ and $E_R = V_A \times V_B$. We will use these two artificial networks to construct two kinds of interdependent networks ($BA - BA$, $ER - ER$).

2.2. Cascading failure model

We adopt the cascading failure model defined in[23], where a node of interdependent networks is removed from one network, two types of failures occur: internal failure and coupling failure. Among them, internal failure means that the removal of a node in sub-network A will affect the change of the connection degree of the neighbour node in the current layer. The failure of the neighbour node will cause the failure of the node in a larger range, and will be broken into several fragments, where the nodes not belonging to the giant connect component would lose their functionality. In order to change the topology of the entire single-layer network; coupling failure refers to the failure of a node in sub-network B that has a coupling relationship after a node in sub-network A is removed. At the same time, this failed node in sub-network B will also cause the coupling node in sub-network A to fail. The failure repeatedly oscillates between the two sub-networks to form a cascading failure process until the steady state is reached, when there are no more nodes being removed. The process of cascading failure is shown in Fig. 2.

In Fig. 2, we believe that the nodes in the interdependent networks should simultaneously meet the following conditions to survive: 1. The nodes connected to it in this layer have not failed; 2. The nodes
coupled with it in the dependent layer have not failed; 3. Theses nodes that belongs to the Giant connect component (GCC).

In this paper, the different attacking strategies are performed on interdependent networks with different coupling network $(BA – BA, ER – ER)$. The cascading failure mechanism will be comprehensively investigated, which is caused by the interaction of the interdependent network. As a result, the influence of different attacking strategies on the robustness of the network can be thoroughly revealed.

2.3. Evaluation indicators

For convenience, we only discuss $G$ as the measurement of the robustness of networks[24], where $G$ represents the relative size of the giant connect component (GCC). Due to the one to-one dependence-links between network $A$ and network $B$, $G$ can be described as follow:

$$S = \frac{N_{GCC}^A + N_{GCC}^B}{N^A + N^B}$$

Where $N_{GCC}^A$ and $N_{GCC}^B$ represent the number of remaining GCC nodes of sub-network $A$ and sub-network $B$, respectively, and $N^A$ and $N^B$ represent the initial number of nodes of subnetwork $A$ and $B$ respectively. It should be noted that the interdependent network suffers a failure and reaches a steady state, $N_{GCC} > 2$ and $N_{GCC} > 2$ are considered to exist; otherwise, it is regarded as a crash. In other words, when $S \approx 0$, it indicates that the network has almost completely collapsed; when $S = 1$, it indicates that the network has not been attacked. The network performance is the best; the performance of the network is positively correlated with the $S$ value. In order to measure the robustness of the network, the critical removal ratio $p_c$ of nodes when the network collapses is introduced, which represents the critical removal ratio of nodes when the network is close to collapse.

3. Methodologies

3.1. Node importance

Node importance is used to measure the key nodes in the network. The key nodes refer to certain core nodes that can affect the system structure and performance to a greater extent than other nodes in the system. The number of key nodes is generally small, but the impact can quickly spread to most nodes in the system. Existing key node metrics based on degree centrality[25] and intermediary[26] are mainly used in single-layer complex networks, which have certain limitations for interdependent networks. According to the characteristics of the two-layer interdependent network structure of the system, the importance of nodes should not only depend on the single-sided network, but also on its coupling network. For example, in the power information physical system, the power network and the communication network support each other, and the importance of the nodes affects each other. Therefore, this paper believes that the importance of the nodes in the dependent network is affected by the following three factors: one is the local importance of the node in the single-layer network; the second is the global importance of the node in the coupled network; the third is the coupling effect between the subnets. To this end, this paper draws on the literature method, and proposes a weighted evaluation method based on node contraction (WEMNC). Suppose the comprehensive importance of the node is $I_i$, there is

$$I_i = \beta I^p_i + (1 - \beta)I^c_j$$

Where $I^p_i$ and $I^c_i$ represent the important index of the nodes in sub-network $A$ and the important index of the nodes coupled to it in sub-network $B$ respectively, $\beta$ is the weight adjustment parameter and $\beta \in [0,1]$. When $\beta = 1$, the node importance is the node importance index in sub-network $A$; when $\beta = 0$, the node importance is the node importance index in sub-network $B$. When $0 < \beta < 1$, it reflects the weight of the node important index of different layers in the node importance. The larger the value of $\beta$, the more the current node layer important index is considered, and the coupling layer
node important index is considered less. In order to facilitate the calculation, the parameter \( f = \beta/(1 - \beta) \) is used to quantify the proportion relationship between the two connected edges. If the parameter \( f = 1 \), that is, the value of \( \beta \) is equal to 0.5, it means that the nodes at both ends of the coupling edge are equally important in terms of measuring the overall importance of the node. For the discussion of parameters, please refer to the case analysis below. Here, it is simple and without loss of generality. The parameter \( f \) is defaults set to 1 in this paper.

In order to evaluate the node important index \( I^{\ast}_i \) of the single-layer network, proposed the node contraction \( \partial(G^+_i) \) as follow,

Let \( V_i \) be a node in the graph \( G = (V, E) \), and merge the node \( V_i \) with \( k_i \) nodes connected to it, that is, replace this \( k_i + 1 \) with a new node Nodes, the edges originally associated with them are now associated with the new node, and the graph \( G^+_i \) is formed after contraction. Then the node cohesion \( \partial(G^+_i) \) can be expressed as the reciprocal of the product of the number \( N \) of nodes and the average path length \( L \),

\[
\partial(G^+_i) = \left\{ \begin{array}{ll}
\frac{1}{N \cdot L} &= \frac{1}{N \cdot \sum_{i \in V \cup V_j} d_{ij}} = \frac{N-1}{\sum_{i \in V \cup V_j} d_{ij}}, N \geq 2 \\
1, N &= 1
\end{array} \right.
\]  
(3)

Where, \( d_{ij} \) represents the shortest path length between node \( V_i \) and \( V_j \). Obviously, there is \( 0 < \partial(G^+_i) \leq 1 \), when there is only one node in the network, \( \partial(G^+_i) = 1 \). On this basis, define the node importance index \( I^{\ast}_i \),

\[
I^{\ast}_i = 1 - \frac{\partial(G)}{\partial(G^+_i)} = \frac{N \cdot d(G) - (N-k_i) \cdot d(G^+_i)}{N \cdot d(G)}
\]

(4)

It can be seen from above that under the same conditions, if the connection degree \( k_i \) of the node \( V_i \) is larger, the number of nodes in the network after shrinking the node is smaller, the greater the degree of network cohesion, the more important the node. In addition, if the node \( V_i \) is at the critical position of the information flow path, the more the shortest path through the node, the average path length of the network after contraction will be greatly reduced, resulting in a greater degree of cohesion. The recognition of node importance based on cohesion is consistent with intuitively judging the importance of a node.

3.2. Attacking strategies

At present, the processing of incomplete information mainly includes grey system theory, fuzzy mathematics and rough set theory[27]. Among them, the grey system theory has certain effectiveness in dealing with the uncertainty of weak data and poor information. Therefore, this paper uses the grey theory design to generate network attack strategies.

Under the condition of grey information, suppose the observed importance degree of node \( V_i \) is \( I_i \), and the observed importance degree is \( p_{i \rightarrow j}(k) \). Assume that the attacker attacks in descending order of the importance of nodes \( \hat{I}_i \) in the network. To describe the uncertainty of the attack information, this article assumes that the importance \( \hat{I}_i \) of a node observed by the attacker is a random variable, subject to \( [I_i - (I_i - I_{min})(1 - \alpha), I_i + (I_{max} - I_i)(1 - \alpha)] \) with uniform distribution, then \( \hat{I}_i \) can be expressed as,

\[
\hat{I}_i = I_i + (I_i - I_{min})(1 - \alpha) + (I_{max} - I_{min})(1 - \alpha) \delta \\
= I_i \alpha + I_{min}(1 - \alpha) + (I_{max} - I_{min})(1 - \alpha) \delta \\
= \Psi + \Delta.
\]

(5)

Where \( \Psi = I_i \alpha \), \( \Delta = I_{min}(1 - \alpha) + (I_{max} - I_{min})(1 - \alpha) \delta \), \( \delta \) is a random variable that satisfies a uniform distribution in the interval [0,1], \( \alpha (\alpha \in [0,1]) \) adjust the parameters for the accuracy of attack information. Obviously, there are two extreme cases: when \( \alpha = 0 \), \( \hat{I}_i = \Delta \) is a uniformly distributed random variable in the interval \([I_{min}, I_{max}]\), which is equivalent to the random failure of the network; when \( \alpha = 1 \), \( \hat{I}_i = I_i \) which corresponds to Intentional attacks on the network. On this
basis, considering the importance of the nodes in the single-layer network and the comprehensive importance of the two-layer coupling nodes, the following three network failure strategies are proposed:

Strategy 1: Random Attack of Double Contraction (RADC): Randomly select \( p \) nodes on a single-layer network to fail, and the remaining nodes in the layer to \( 1 - p \) survive, corresponding to random failures in the network (\( \alpha = 0 \)).

Strategy 2: Malicious Attack of Double Contraction (MADC): According to the actual importance of the node from large to small, remove the node with the ratio \( p \), and the remaining ratio in the layer is \( 1-\rho \) The node survives (\( \alpha = 1 \)).

Strategy 3: Grey Information Attack of Double Contraction (GIADC): When \( 0 < \alpha < 1 \), the nodes in the network are sorted according to the importance of the grey information, and the nodes with the proportion \( p \) are removed according to the sorting result. Nodes with a remaining ratio of \( 1-p \) survive. Here, the parameter \( p \) can be used to adjust the attack intensity to the networks.

4. Simulation Results

BA networks and ER networks are selected to form two types of interdependent networks: BA – BA, ER – ER. Fig. 3 to Fig. 5 demonstrate the simulation results. To avoid the uncertainty of random attacks, the Monte Carlo method is used in the numerical simulation, and the data are the average results of independent repeats.

4.1. The effectiveness of the identification method of key nodes in the network

With the traditional single network key node identification (Single Degree, SD) based on node degree centrality, double network key node identification (Double Degree, DD) based on node degree centrality as a reference, comparative analysis of the key based on contraction degree proposed in this paper the effectiveness of node identification methods. Fig. 3 shows the changes in network performance after intentionally attacking BA – BA and ER – ER with different key node identification methods. Among them, the red curve is based on the single-layer node degree centrality malicious attack (MASD), the blue is based on the double-layer network degree centrality weighted malicious attack (MADD), and the pink is a malicious attack of single contraction (MASC) based on single-layer contraction, green is a malicious attack of double contraction (MADC) weighted based on two-layer contraction.

Fig. 3(a) show that the malicious attack strategy using different node importance recognition methods destroys the BA – BA, and all bring a second-order discontinuous phase transition. At the same time, before the network collapse occurs, the network performance is not much different under the same node failure rate. When the network is close to collapse, the phenomenon of \( MADS < MADD < MA \) occurs at the phase transition point. This indicates that the node-based
intentional attack effect based on the degree of cohesion is better than the node-based intentional attack effect based on degree-centrality. Observing the curve changes in Fig. 3(b), we can see that $MADD(MADS) < MASD(MASS)$, that is, the method based on double-layer weighted evaluation has better strike effect.

In addition, there are $MAS < MASD$ and $MADD < MADS$ in Fig. 3(b), which is opposite to the situation in Fig. 3(a). This is due to the small difference in the degree of nodes in the $ER - ER$, plus the random coupling between the networks Relationship, the overall distribution of interdependent networks is relatively uniform, and the key nodes based on cohesion are more effective in single-layer networks, but generally perform well in two-layer interdependent networks. In general, whether it is a single-layer network or a coupled network, the key node identification method based on node aggregation can accurately determine the important nodes in the network, which is of great value for the preparation of targeted and efficient NISoS attack strategies. For example, using this method can determine the centre of gravity of the enemy's combat system and implement precise strikes to promptly paralyze it with points and faces; it can also focus on protecting its own system to ensure the integrity of the system structure.

4.2. Analysis of network robustness under different attack strategies

In order to investigate the structural robustness of interdependent networks under different attack strategies, three modes of random attack $RADC(\alpha = 0)$, deliberate attack $MADC(\alpha = 1)$ and grey information attack $GIADC(0 < \alpha < 1)$ were used to attack the interdependent network model($BA - BA$). The results are shown in Fig. 4.

Fig. 4 The robustness analysis of interdependent network under different attack strategies

Fig. 4(a) and Fig. 4(c) show that the grey attack coefficient, namely the accuracy $\alpha$ of attack information, has a great influence on the robustness of the network. Under the two attack strategies for interdependent networks, the network performance decreases as the node failure rate $p$ increases. Fig.
4(b) and Fig. 4(d) compare the effect of the grey attack coefficient on the number of iteration steps \((NOI)\) of the interdependent models of different structures. \(NOI\) is used to indicate the number of iteration steps that the interdependent network has experienced when it suffered attack\([28]\). The peak number of iteration steps \((NOI)\) in the figure refers to the maximum number of iteration steps required for the network to reach steady state under different attack patterns. The maximum iteration steps of the network under different attack patterns are shown in Table 1. According to Fig. 4(b) and Table 1, in the BA – BA model, as the grey attack coefficient \(\alpha\) increases, the critical threshold of network collapse \(p_c\) gradually decreases, and the network is more vulnerable (equivalent to the network’s robustness gradually changing Small), and at the same time the maximum iteration number of the network \(NOI\) gradually increases. This is because the larger the grey attack coefficient \(\alpha\), the closer it is to malicious attacks, which can accurately destroy the key nodes of the system network, causing repeated oscillations between interdependent network layers within a short period of time, resulting in a sharp increase in the scale of dependent network cascading failures. The same situation also appears on the ER – ER model, as shown in Fig. 4(d). As show in Table 1, we can see that there is a negative correlation between the grey attack coefficient \(\alpha\) and the network robustness index \(p_c\). In other words, the network robustness can be changed by adjusting the grey attack coefficient \(\alpha\). Due to the control of attack information in real situations, it is easier to change the network structure and performance. The above conclusions have practical guiding significance for our goal of enhancing network robustness.

| Model   | \(\alpha\) | 0 | 0.2 | 0.4 | 0.6 | 0.8 | 1.0 |
|---------|------------|---|-----|-----|-----|-----|-----|
| BA-BA   | \(p_c\)    | 0.81| 0.74 | 0.65 | 0.54 | 0.44 | 0.34 |
|         | \(NOI\)    | 3.30| 3.50 | 3.70 | 4.10 | 5.00 | 7.00 |
| ER-ER   | \(p_c\)    | 0.75| 0.64 | 0.60 | 0.52 | 0.42 | 0.36 |
|         | \(NOI\)    | 2.10| 2.30 | 2.40 | 2.80 | 3.30 | 4.00 |

As show in Table 1, under the same grey attack coefficient, two dependent networks always have \(p_c^{BA-BA} > p_c^{ER-ER}\) and \(NOI^{BA-BA} > NOI^{ER-ER}\) phenomenon, that is, the BA – BA interdependent network is less robust than the ER – ER interdependent network. For example, under the same attack strategy, such as malicious attack \(MA (\alpha = 1)\) to destroy networks, the BA – BA interdependent network critical removal ratio \(p_c = 0.34\), when the node removal ratio \(p < p_c\), the network can maintain a scale of about 60% with only a few faulty nodes; however, while \(p \geq p_c\), the number of faulty nodes increases sharply, the scale of the maximum connected subgraph of the network drops sharply, and the network performance quickly collapses. Correspondingly, the critical removal ratio of the ER – ER interdependent network is \(p_c = 0.36\). Compared with the BA – BA model, the ER – ER network needs to remove more nodes to collapse, which means the robustness of \(ER – ER\) is better. This is because the importance distribution of nodes in the ER random network is relatively uniform and the overall deviation is not large. RA strategy will not cause large-scale network failures, and thus will not cause large-scale network failures that depend on them, resulting in more robustness.

4.3. Influence of different importance weight coefficients on network robustness

According to Section 2.3, the parameter \(f\), which represents the relationship between the coupling nodes and the importance ratio, is one of the key factors that affect the identification of key nodes in the network. In order to better observe the phase change of the performance curve of the network during the attack, the grey malicious attack strategy is selected to trigger the second-order phase change of the network, and the relationship between the parameter \(f\) and the network phase change point is discussed, as shown in Fig. 5. Among them, the ordinate \(p_c\) represents the phase transition point threshold of the proportion of failed nodes when there is a giant connect component\([29]\). The higher the \(p_c\), the better the network robustness.
In Fig. 5(a), it is found that under malicious attack on $BA-BA$ and $ER-ER$ interdependent network, the parameters and threshold $p_c$ overall show a U-shaped phenomenon with high at both ends and low at the middle: 1) Overall, $p_c^{ER-ER} > p_c^{BA-BA}$ is still alive regardless of the parameter $f$, which means that the robustness of the $ER-ER$ is better than that of the $BA-BA$; 2) For $ER-ER$, when the parameter $f = 0$ ($\beta = 0$), the robustness of both networks is the best, and at this time, $p_c = 0.46(0.42)$. This phenomenon shows the influence of the importance of the two types of coupling nodes during deliberate attacks. The role can not be compared; for this layer of nodes, its essential role is to measure the importance of the current layer of nodes, the impact of this type of node not only affects the network structure of this layer, but also affects the structure of the coupling layer; in contrast, the coupling layer node, this type of node The more important it is in the layer, and the greater the weight in the comprehensive evaluation of nodes, the greater the robustness of the entire network after its failure. 3) When $f = \infty$, that is, when $\beta = 1$ (only considering the importance of nodes in the current layer, completely ignoring the importance of nodes coupled with it), $p_c$ starts to rise from the minimum, this phenomenon shows the coupling edge again although the above two types of nodes are different, only a comprehensive consideration can fully measure the key role of nodes in the network. 4) When $f = 3(12)$, the robustness of the two networks is the worst. When $0 < f < 3$ or $0 < f < 12$, it is negatively correlated with $p_c$ within a certain range, and the network performance gradually deteriorates but does not decrease non-linearly. Similarly, when $3 < f < \infty$ or $12 < f < \infty$, $f$ is positively correlated with $p_c$ within a certain range, that is, the larger $f$ and the greater $p_c$, and the network robust performance gradually improves but is always less than $p_c$ ($f = 0$). 5) Further analysis shows that there is an approximate optimal value of the parameter $f$ that can make $p_c$ reach the trough position (lowest point), such as $(3,0.38)$ and $(12,0.32)$. However, the optimal value of $f$ still needs to be determined by further study of the structure and interaction of the coupled sub-networks. Fig. 5(b) shows the relationship between the weight coefficient and the critical removal ratio for two types of networks under random failure. Result shows that for the $BA-BA, p_c^{BA-BA} \in [0.72,0.80]$ exists under the random attack; for the $ER-ER, p_c^{ER-ER} \in [0.64,0.72]$, the critical removal ratio $p_c$ of the two types of networks shows a certain randomness in their respective intervals. However, in general, there is a $p_c^{ER-ER} \leq p_c^{BA-BA}$, that is to say, the robustness of the $BA-BA$ under random failure is always better than the $ER-ER$, which is due to the $BA-BA$, the contraction distribution is more uneven, and the random coupling relationship between two sub-networks make it difficult for random attacks to effectively destroy key nodes in the network, thereby showing better robustness.

5. Conclusions
This paper compares the cascading failure process and robust performance of two different types of interdependent network models $BA-BA$ and $ER-ER$ under the grey attack strategy. The research found that:
1) The key node identification method based on contraction has a better effect than the traditional key node identification method based on degree centrality;

2) It is more effective to consider the double-coupling node's attack on the contraction characteristics than the attack strategy that only considers the single-sided node's contraction characteristics.

3) The network robustness under different weight coefficients is closely related to the attack strategy. The two types of interdependent network models have the best and worst robustness phenomena under malicious attacks, while the two types of network robustness performance under random attacks is completely different, only random values within a certain range. This work not only helps to understand the relationship between the organizational form and function of complex systems, but also provides a useful reference for finding the weakness (or centre of gravity) of the system and make protection strategy.

Acknowledgments
This work was financially supported by the National Social Science Foundation of China (Grant No. 14GJ003-172), and Strategic Planning Project of China (Grant No. 19ZLXD04110110001).

References
[1] Gao Jianxi, Buldyrev V S, Stanley H E, et al. Networks formed from interdependent networks[J]. Nature Physics, 2012, 8(1): 323–328.

[2] Nguyen D T, Shen Y, Thai M T. Detecting critical nodes in interdependent power networks for vulnerability assessment[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 151–159.

[3] Zhang Jianian. Research on the fusion of security intelligence and strategic resilience from the perspective of national security assurance – implications of the Stuxnet virus attack on Iranian nuclear facilities[J]. Intelligence, 2016, 37(2): 8–14.

[4] Antian research institute. Guangdong province power system network security enterprise key laboratory. Preliminary analysis and reflections on large-scale power outage in Venezuela[J]. Information security and communication Privacy, 2019, 5(1): 28–39.

[5] Zhong Nanshan. Prevention and treatment of chronic respiratory diseases in China[J]. Chronic Diseases and Translational Medicine, 2019, 5(4): 209–213.

[6] Buldyrev S V, Prarshani R, Stanley H E, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464: 1025–1028.

[7] Parshani R, Rozenblat C, Ietri D, et al. Inter-similarity between coupled networks[J]. Europhysics Letters, 2011, 92(6): 68002.

[8] Chen Shiming, Dai Yaming, Cheng Yunhong. Study on adding edge strategy to improve the robustness of dependent networks[J]. Journal of university of electronic science and technology, 2019, 48(1): 103–109.

[9] Pan Zifang, Li Xi, Wang Xiaofang. Generalized local-world models for weighted networks[J]. Physical Review E, 2006, 73(5): 056109.

[10] Chen Shiming, Lu Hui, Xu Qinggang, et al. Degree based positive/negative correlation dependency network Studies on models and their Robustness[J]. Acta Phys. Sin, 2015, 64(4): 048902.

[11] Wang Xiaoyang, Zhou Weijun, Li Rui, et al. Improving robustness of interdependent networks by a new coupling strategy[J]. Physica A, 2018,492:1075–1080.

[12] Dong Zhengcheng, Fang Yijun, Tian Meng, et al. Cascading failures of interdependent networks with different k-core structures[J]. Modern Physics Letters B, 2017, 31(10): 1750112

[13] Zhou lin, Qi Xiaogang, Liu Lifang. The Robustness of Interdependent Networks with Traffic Loads and Dependency Groups[J]. IEEE Access, 2020, 8(1): 98449–98459.

[14] Liu Yangyang, Zhao Chengli, Yi Dongyun, et al. Robustness of partially interdependent networks under combined attack[J]. Chaos, 2019, 29(2):1054–1061.

[15] Hao Yuncheng, Jia Limin, Wang Yanhui. Edge attack strategies in interdependent scale-free
networks[J]. Physica A: Statistical Mechanics and its Applications, 2020, 540(1): 122759.

[16] Gao Jianxi, Buldyre S V, Stanley H E, et al. Networks formed from interdependent networks[J]. Nature Physics, 2012, 8(1): 40–48.

[17] Buldyrev S V, Parshani R, Gerald P. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464(7291): 1025–1028.

[18] Martin-hernandez J, Wang Hui, Mieghem P V, et al. Algebraic connectivity of interdependent networks[J]. Physica A Statistical Mechanics & Its Application, 2014, 404(1): 92–105.

[19] Shahrivar E M, Pirani M, Sundaram S. Robustness and algebraic connectivity of random interdependent networks[C]. IFAC-PaperOnLine. 2015, 48(1): 252–257.

[20] Shahrivar E M, Pirani M, Sundaram S. Spectral and structural properties of random interdependent networks[J]. Automatica. 2017, 83(1): 234–242.

[21] Wu Jun, Mauricio B, Tan Yuejin, et al. Spectral measure of structural robustness in complex networks[J]. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 2011, 41(6): 1244–1252.

[22] Dong Gaogao, Du Ruijin, Hao Huifang, et al. Shell attack on interdependent networks[C]//Proceeding of the 35th Chinese Control Conference. Chengdu, China. Institute of Electrical and Electronics Engineers Press, 2016: 1198–1201.

[23] Buldyrev V, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature 2010, 464(7291): 1025–1028.

[24] Motter A E. Cascade control and defense in complex networks[J]. Phys. Rev. Lett. 2004, 93(9): 098701.

[25] Chen Zhu, Wu Jun, Xia Yan, et al. Robustness of interdependent power grids and communication networks: a complex network perspective[J]. IEEE Trans Circ Syst II: Exp Briefs, 2018, 65(1): 115–119.

[26] Nogal M, Honfí D. Assessment of road traffic resilience assuming stochastic user behavior[J]. Reliability Engineering and System Safety, 2019, 185(1): 72–83.

[27] Li Jichao. Wu Jun. Li Ye, et al. Attack Robustness of Scale-Free Networks Based on Grey Information[J]. Chin. Phys. Lett. 2011, 28(5): 058904.

[28] Liu Yiyi, Zhao Cilun, Yi Daye, et al. Robustness of partially interdependent networks under combined attack[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019, 29(2): 021101.

[29] Chen Lun, Yue Dong, Dou Caixi, et al. Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters[J]. International Journal of Electrical Power & Energy Systems, 2020, 114(1): 105374.