Physica A 443 (2016) 58–69

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

# Complex interdependent supply chain networks: Cascading failure and robustness

Liang Tang [a,b,c,*], Ke Jing [d], Jie He [b], H. Eugene Stanley [c]

[a] Industrial Engineering Department, Shenyang Aerospace University, Shenyang, Liaoning 110136, PR China
[b] School of Transportation, Southeast University, Nanjing, Jiangsu 210096, PR China
[c] Department of Physics, Boston University, Boston, MA 02215, USA
[d] School of Economics and Management, Shenyang Aerospace University, Shenyang, Liaoning 110136, PR China

## HIGHLIGHTS

- We construct a theoretical model of interdependent supply chain network.
- A time-varied cascading failure model of failed loads propagation is developed.
- We present a priority redistribution strategy for failed loads propagation.
- The robustness of supply chain network is assessed in three node removal ways.
- The simulation results show a sudden collapse of interdependent supply chain network.

## ARTICLE INFO

*Article history:*
Received 31 May 2015
Received in revised form 17 September 2015
Available online 30 September 2015

*Keywords:*
Interdependent supply chain network
Cascading failure
Load propagation
Network robustness
Node removal

## ABSTRACT

A supply chain network is a typical interdependent network composed of an undirected cyber-layer network and a directed physical-layer network. To analyze the robustness of this complex interdependent supply chain network when it suffers from disruption events that can cause nodes to fail, we use a cascading failure process that focuses on load propagation. We consider load propagation via connectivity links as node failure spreads through one layer of an interdependent network, and we develop a priority redistribution strategy for failed loads subject to flow constraint. Using a giant component function and a one-to-one directed interdependence relation between nodes in a cyber-layer network and physical-layer network, we construct time-varied functional equations to quantify the dynamic process of failed loads propagation in an interdependent network. Finally, we conduct a numerical simulation for two cases, i.e., single node removal and multiple node removal at the initial disruption. The simulation results show that when we increase the number of removed nodes in an interdependent supply chain network its robustness undergoes a first-order discontinuous phase transition, and that even removing a small number of nodes will cause it to crash.



* Corresponding author at: Industrial Engineering Department, Shenyang Aerospace University, Shenyang, Liaoning 110136, PR China. Tel.: +86 13940217982.
*E-mail addresses:* tangericliang@gmail.com, erictang@bu.edu (L. Tang), chloe.jingke@gmail.com (K. Jing), hejie@seu.edu.cn (J. He), hes@bu.edu (H.E. Stanley).

http://dx.doi.org/10.1016/j.physa.2015.09.082
0378-4371/

## 1. Introduction

In recent years we have begun to understand the behavior of such phenomena as natural disasters, the breakdown of technological systems, epidemic propagation, and spreading social unrest in terms of their complex network structure. During these events, supply chain systems often collapse, e.g., during the 2011 earthquake in Japan the Toyota Motor Company was forced to stop operations in twelve assembly plants and absorb a production loss of 140,000 vehicles. The main cause of this problem was the disruption of the supply chain supporting the manufacturing subsystem. During disruptive events, supply chains are particularly vulnerable to propagating failure. A major cause of this is the connectivity and interdependent relationships between supply chain partners. Dependence relationships can cause the transmission of disruptions to "snowball" through a supply chain network or through a portion of it [1].

In order to develop effective countermeasures to these disruptions, we must understand the conditions that allow them to occur and the mechanisms that drive risk propagation. Linked relations are one precondition for cascading failures that collapse a supply chain system, but there are others. As information and network technology becomes increasingly sophisticated, supply chain systems increase in complexity and become ever more dependent on a collaborative network structure. Most real-world supply chain collaborative networks consist of two networks: an undirected cyber-layer network and a directed physical-layer network. As the two layers interact they guarantee the function of the supply chain system, but they also become less robust to attack and breakdown and more likely to facilitate global collapse. A significant amount of empirical and quantitative research has been done on supply chain risk management, including measuring global supply chain risk, planning for catastrophic events in supply chains, and increasing chain agility and risk mitigation [2]. These research have been of limited usefulness because they have been focused on the risk of cascading failure in single isolated networks and, in contrast, most real-world supply chain networks are geographically dispersed across regions and countries [3–5].

Most current studies of cascading failures in complex networks have focused on single networks [6–12]. Because it is difficult to depict real-world network systems using a single network model, e.g., a supply chain network with multiple attributes and multiple functions, some researchers have proposed a "super network" concept [13–16], and interdependent network models have also been proposed. A notable case is the work by Buldyrev et al. [17] in which they describe a one-to-one correspondence model for studying the ramifications of interdependence between two networks. Their analytical framework is based on a generating-function formalism widely used for studies of percolation and structure within a single network [7]. This framework for interdependent networks enables us to follow the dynamics of the cascading failures and derive analytic solutions for the final steady state. Inspired by the work of Buldyrev [17], many researchers have studied interdependent networks from different angles [18–26].

Most of the above researches especially those related to interdependent networks, do not consider the spreading of failed loads, and thus their determining whether neighbor nodes connecting with failed nodes will fail depends on the connectivity links and dependence links, and not on the capacity of the neighbor nodes. Unlike most of these previous works, which focuses on interdependent networks formed from undirected networks, we analyze the cascading failure process and the robustness of interdependent networks that are composed of both undirected and directed networks. We also take into account the flow constraints present when failed loads propagate through a directed layer network, which is an important factor in a supply chain network. We examine the cascading failure mechanism of an interdependent supply chain network subject to a one-to-one interdependence relation in order to measure its robustness against disruption when it is composed of an undirected cyber-layer network and a directed physical-layer network. Our results can provide a scientific basis for the structural optimization of an interdependent supply chain network and for the development of a robustness control strategy.

## 2. Theoretical model of interdependent supply chain networks

As described above, an interdependent supply chain network is composed of a physical-layer network $G^P$ and a cyber-layer network $G^L$. We assume all suppliers, production centers, distribution centers, and customers to be network nodes. Because the cyber-layer and the physical-layer of a supply chain network are interactive, failed nodes in one layer can propagate their failure through dependence links to nodes in both layers. The links between nodes in the same layer are connectivity links, and they can transfer failed loads. The links between nodes in different layers are dependence links. In this two-layered interdependent supply chain network, failures caused by disruption are redistributed.

Here both networks have $N$ nodes. Without loss of generality, we assume the nodes in network $G^P$ are connected with directed links using a degree distribution function $P_P(k)$, which contains an in-degree distribution $P_P(k_{in})$ and an out-degree distribution $P_P(k_{out})$. The nodes in network $G^L$ are similarly connected with undirected links using a degree distribution $P_L(k)$.

### 2.1. Supply chain physical-layer network

A supply chain physical-layer network is composed of suppliers, manufacturers, distributors, retailers, and customers, all of which can be denoted as nodes, and the connecting relationship between entities can be denoted as edges. A model of a physical-layer network can therefore be represented as

$$R^P = (V^P, E^P, W^P, L^P, C^P), \tag{1}$$

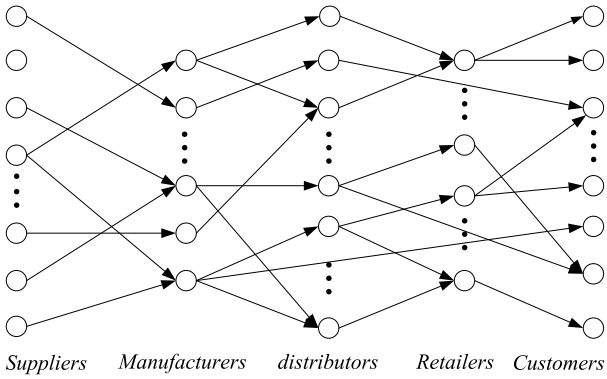


**Fig. 1.** Example of a supply chain physical-layer network.

where $V^P = \{v_1^P, v_2^P, \ldots, v_n^P\}$ is a set of nodes, and $E^P = \{(v_i^P, v_j^P) \mid e_{ij}^P = 1 \text{ or } 0\}$ is a set of connectivity links. Here, $e_{ij}^P = 1$ indicates that a directed connection from node $v_i^P$ to node $v_j^P$ exists; otherwise, $e_{ij}^P = 0$. In a supply chain physical-layer network, nodes of suppliers connect to nodes of manufacturers, nodes of manufacturers connect to nodes of distributors or customers, nodes of distributors connect to retailers or customers, and nodes of retailers connect to nodes of customers, as shown as Fig. 1. When a disruption occurs, the failed loads propagate via these directed connections. In addition, $W^P = \{w_{ij}^P \mid e_{ij}^P = 1, i, j = 1, 2, \ldots, n\}$ is a set of load constraints on connectivity links, and indicates the maximum permitted failed load that can be propagated. Each physical node thus usually employs countermeasures for risk prevention, e.g., improving inventory level, in order to reduce risk and restrict the size of failed loads that can be propagated through connectivity links.

In our network model, we define the initial degree of node $v_i^P$ as $K_i$ ($K_i = K_{i(in)} + K_{i(out)}$), where $K_{i(in)}$ is the in-degree of node $v_i^P$, and $K_{i(out)}$ is the corresponding out-degree. We define $L_{i(0)}^P$ as the initial load of node $v_i^P$, which is a function of the out-degree of node $v_i^P$ [27] represented by

$$L_{i(0)}^P = \alpha K_{i(out)}^{\beta}, \tag{2}$$

where $\alpha$ and $\beta$ are adjustable parameters, and $\alpha, \beta > 0$. For a supply chain physical-layer network, the initial load of a node is positively related to its out-degree. When node $v_i^P$ fails, its failure is redistributed to its neighbor node $v_j^P$ through out-degree connectivity link $e_{ij}^P$.

$C^P = \{c_1^P, c_2^P, \ldots, c_n^P\}$ is a set of node load constraints and denotes the largest load capacity allowed a node. If the load of a node exceeds its capacity, it fails. In a supply chain physical-layer network, the capacity $C_i^P$ of node $i$ is linearly correlated with its initial load $L_i^P$, and thus the node capacity is

$$C_i^P = (1 + \sigma) L_{i(0)}^P, \tag{3}$$

where $\sigma \geq 0$. When load $L_{i(t)}^P$ of node $v_i^P$ at time $t$ is larger than its capacity $C_i^P$, node $v_i^P$ will fail. When $L_{i(0)}^P \leq L_{i(t)}^P < C_i^P$, node $i$ is in a normal state. A higher node capacity usually indicates a higher cost. Consequently, $C_i^P$ is limited by the cost constraint.

### 2.2. Supply chain cyber-layer network

A supply chain cyber-layer network composed of cyber entities is undirected because the data can be transmitted in both directions. Here we assume that each physical enterprise entity possesses a corresponding cyber node, and thus the number of nodes in a cyber-layer network is the same as that of a physical-layer network. Similarly, a model of supply chain cyber-layer network can be represented by

$$R^L = (V^L, E^L, L^L, W^L, C^L), \tag{4}$$

where $V^L = \{v_1^L, v_2^L, \ldots, v_n^L\}$ is a set of cyber node entities, and $E^L = \{(v_i^L, v_j^L) \mid e_{ij}^L = 1 \text{ or } 0\}$ is a set of undirected connectivity links; $e_{ij}^L = 1$ denotes that data propagation between node $v_i^L$ and node $v_j^L$ exists; otherwise, $e_{ij}^L = 0$, as shown in Fig. 2. In a cyber-layer network, high-degree nodes function as hubs, and their failure when attacked has dire consequences. When a disruption occurs, the congestion data of a failed node will be propagated via these undirected connectivity links. $W^L = \{w_{ij}^L \mid e_{ij}^L = 1,\ i, j = 1, 2, \ldots, n\}$ is a set of flow constraints on undirected connectivity links, and indicates the maximum permitted data load that can be propagated.

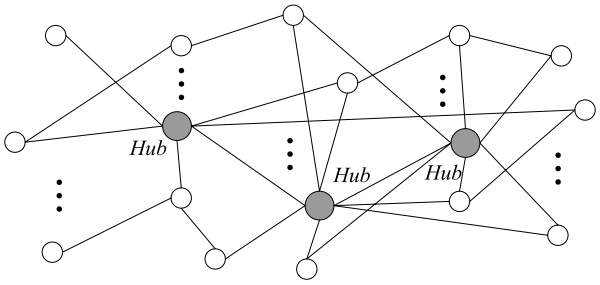


**Fig. 2.** Example of a supply chain cyber-layer network.

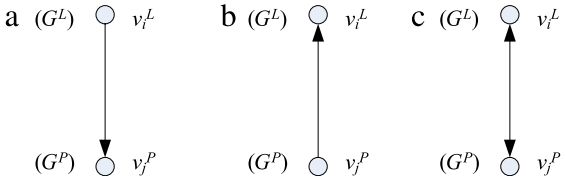


**Fig. 3.** One-to-one interdependence relations between nodes in an interdependent supply chain network. The arrows indicate the interdependence relations between nodes: (a) node $v_j^P$ in $G^P$ depends on node $v_i^L$ in $G^L$, and once node $v_i^L$ fails, node $v_j^P$ will also accordingly fail; (b) node $v_i^L$ in $G^L$ depends on node $v_j^P$ in $G^P$, and once node $v_j^P$ fails, node $v_i^L$ will also fail; and (c) node $v_i^L$ in $G^L$ depends on node $v_j^P$ in $G^P$, and vice versa. Once any one node fails, the other node will also fail.

In contrast to the physical-layer network, we define the initial degree of node $v_i^L$ in a cyber-layer network to be $K_i$, and the initial load of cyber node $v_i^L$ to be

$$L^L_{i(0)} = \alpha K_i^{\beta}. \tag{5}$$

Here the initial load $L^L_{i(0)}$ denotes the initial amount of data. In addition, $C^L = \{c_1^L, c_2^L, \ldots, c_n^L\}$ is the set of constraints on the cyber nodes and represents their maximum data capacity. When a cyber node fails due to attack, the resulting congestion data are propagated to the neighbor nodes through undirected connectivity links, and the capacity $C_i^L$ of cyber node $v_i^L$ is

$$C_i^L = (1+\sigma)L^L_{i(0)}. \tag{6}$$

### *2.3. Description of interdependence relations*

Because an interdependent supply chain network is composed of a physical-layer network and cyber-layer network, we need to know the interdependence relation between the nodes in the two layers in order to quantify the risk propagation facilitated by these interdependent relations. We here assume that each node in the physical-layer network has a one-to-one relationship with only one node in the cyber-layer network. Fig. 3 shows several different kinds of node interdependence.

Fig. 3 shows that each node in the cyber-layer network depends on only one node in the physical-layer network, and vice versa. The set of nodes in $G^L$ is $V^L = \{v_1^L, v_2^L, \ldots, v_n^L\}$, and in $G^P$ it is $V^P = \{v_1^P, v_2^P, \ldots, v_n^P\}$. We use $\Phi(v_i^L) = v_j^P$ to indicate that node $v_i^L$ in $G^L$ is mapped to node $v_j^P$ in $G^P$, and $\Phi^{-1}(v_j^P) = v_i^L$ to indicate that node $v_j^P$ in $G^P$ is conversely mapped to node $v_i^L$ in $G^L$. Since the mapping has a one-to-one relation, we obtain $\Phi(v_i^L) = v_j^P$ only when $\Phi^{-1}(v_j^P) = v_i^L$.

## 3. Cascading failure model of failed loads propagation

To analyze the process of a cascading failure in an interdependent supply chain network, we construct a model to describe failed loads propagation in an isolated network and in interdependent networks. As described above, a two-layer interdependent supply chain network has connectivity links within each layer and dependence links between them. The dependence link that connects one node in network $G^L$ with one node in network $G^P$ maintains the communication and collaboration between $G^L$ and $G^P$, and thus supports the functioning of the interdependent supply chain network.

We assume that there is a fraction $q_p$ of nodes in physical-layer network $G^P$ that depend on the nodes in cyber-layer network $G^L$, and a fraction $q_l$ of nodes in cyber-layer network $G^L$ that depend on the nodes in physical-layer network $G^P$. We use $R_{v_i^L v_j^P}$ and $R_{v_j^P v_i^L}$ to express the interdependence between nodes $v_i^L$ and $v_j^P$, respectively, which are given by

$$R_{v_i^L v_j^P} = \begin{cases} 0 & \text{no dependence between node } i \text{ in } G^L \text{ and node } j \text{ in } G^P \\ 1 & \text{node } i \text{ in } G^L \text{ depends on node } j \text{ in } G^P, \end{cases} \qquad v_i^L \in V^L,\ v_j^P \in V^P \tag{7}$$

$$R_{v_j^P v_i^L} = \begin{cases} 0 & \text{no dependence between node } i \text{ in } G^L \text{ and node } j \text{ in } G^P \\ 1 & \text{node } j \text{ in } G^P \text{ depends on node } i \text{ in } G^L, \end{cases} \quad v_i^L \in V^L,\ v_j^P \in V^P. \tag{8}$$

According to Eqs. (7) and (8), $q_l = \sum R_{v_i^L v_j^P}/n$, and $q_p = \sum R_{v_j^P v_i^L}/n$.

### 3.1. Process of a cascading failure in an interdependent supply chain network

We assume that when a node is not connected to a giant component [7] it is not functioning and has failed. When a fraction $1 - p$ of nodes in $G^L$ or $G^P$ is initially removed, the resulting cascading failure occurs as follows.

**Stage 1:** When a fraction $1 - p$ of nodes in $G^L$ or $G^P$ fails, the risk load of these failed nodes first propagates through connectivity links in the same layer network according to a priority redistribution strategy. This divides each layer into several components, and the valid nodes are those that have not failed after redistribution.

We construct the supply chain cascading failure model using a flow constraint and node capacity constraint, and through the giant component function $Y_{L,P}$ we can determine the probability that a surviving network node still belongs to an effective cluster after failure load propagation. We formulate the comprehensive efficiency index (robustness index) used to measure network robustness according to $Y_{L,P}$.

If node $v_i^P$ fails in directed network $G^P$, the failed load will be propagated to its neighbor nodes $v_s^P$ based on a priority redistribution strategy. The redistribution probability is defined as $P_s^P$, $P_s^P = \alpha K_{s(out)}^{\beta} / \sum_{s\in N_i} \alpha K_{s(out)}^{\beta}$, where $N_i$ is the set of nodes $s$ that are neighbors of node $v_i^P$. However, if node $v_i^L$ fails in undirected network $G^L$, the risk load propagates according to the probability $P_s^L = \alpha K_s^{\beta} / \sum_{s\in N_i} \alpha K_s^{\beta}$. A neighbor node $s$ receives an extra risk load $\Delta S = L_i P_s^{L,P}$, and when $L_s + \Delta S \le C_s$ node $s$ does not fail. When $L_s + \Delta S > C_s$, node $s$ fails and causes a cascading failure. We present failed load redistribution strategies based on parameters $\alpha$, $\beta$, and $\sigma$ for three cases. (i) Failed loads $\Delta S$ are no more than the flow constraints $w_{is}$ on the connectivity links, i.e., $\Delta S \le w_{is}$. Here the load on node $s$ is replaced by $L_s' = L_s + \Delta S$. Node $s$ will not fail while $K_{i(out)}^{\beta} / \sum_{s\in N_i} K_{s(out)}^{\beta} \le \sigma$ or $K_i^{\beta} / \sum_{s\in N_i} K_s^{\beta} \le \sigma$ inferred from a new value of $L_s$. Or node $s$ will fail and lead to a further propagation of the failure. (ii) Failed loads $\Delta S$ are larger than the flow constraints $w_{is}$ on the connectivity links ($\Delta S > w_{is}$). The loads $\Delta S - w_{is}$ are abandoned due to risk defense countermeasures, and the new load on node $s$ is $L_s' = L_s + w_{is}$. When $L_s' \le C_s$, node s does not fail. (iii) Some failed loads $\Delta S \le w_{is}$, and other failed loads $\Delta S > w_{is}$. For these failed loads $\Delta S$, when $\Delta S \le w_{is}$, $\Delta S_n$ is used and the corresponding flow constraint becomes $w_{isn}$. We determine the value of $L_s + \Delta S_n$ and $C_s$, and when $L_s + \Delta S_n > C_s$, the loads of node $s$ will be $C_s$ and propagate further. When $L_s + \Delta S_n \le w_{isn}$, nodes $s_n$ carry out a secondary redistribution. We define the extra failed loads when $\Delta S > w_{is}$ to be $\Delta S_o$, and $w_{iso}$ to be the flow constraints on the connectivity links. The failed loads $\Delta S_o - w_{iso}$ will be redistributed to the connectivity links that satisfy $\Delta S_n \le w_{isn}$ and $L_s + \Delta S_n < C_s$. The secondary redistribution strategy is given by

$$P_s = [C_s - (L_s + L_i P_s)] / \sum_{L_s + \Delta S_n \le C_s} [C_s - (L_s + L_i P_s)]. \tag{9}$$

Applying Eq. (9), the secondary failed loads $\Delta S_o - w_{iso}$ are delivered from node $i$ to nodes $s$ that satisfy the condition $L_s + \Delta S_n < C_s$ with probability $P_s$.

**Stage 2:** After the failed loads propagate through the same layer during stage 1, we find those nodes that have not failed based on the three redistribution strategies, and determine the ultimately functional nodes belonging to the giant components according to $Y_{L,P}$. We also identify those nodes that have not failed but do not belong to the giant components, and determine that they are only partially functional. All connectivity links of the failed nodes are then cut.

**Stage 3:** The failed nodes in the same layer in $G^L$ ($G^P$) affect the corresponding nodes in the other layer $G^P$ ($G^L$) through dependency links. We then identify the newly generated nodes that have failed in the other layer $G^P$ ($G^L$), and the failed loads of these newly failed nodes propagate further in the same network $G^P$ ($G^L$) in accordance with the redistribution strategies described in Stage 1.

**Stage 4:** We loop stages 1–3 until no more new node failures occur in the interdependent supply chain network.

Fig. 3 shows a simple example of the cascading failure process in a supply chain interdependent network. Both the directed physical-layer $G^P$ and the undirected cyber-layer $G^L$ have nine nodes, and the interdependence relations among the nodes are shown in Fig. 4, where $q_p = 6/9$, and $q_l = 6/9$. Undirected curves represent connectivity links within the same network $G^L$, and directed curves represent connectivity links within the same network $G^P$. The directed lines with arrows indicate the dependence links between networks $G^L$ and $G^P$. We assume that only one node is removed initially in network $G^L$, and thus $1 - p = 1/9$ initially.

In Fig. 4, the attack is on node $v_2^L$ (in yellow) in network $G^L$ at first. Under certain parameters $\alpha$, $\beta$, and $\sigma$, the nodes $v_5^L$ and $v_8^L$ in the same network may fail according to the risk load redistribution strategy in undirected network $G^L$. The connectivity links of failed nodes $v_2^L$, $v_5^L$, and $v_8^L$ are then removed (as shown in stage 1). At this time, though nodes $v_4^L$, $v_7^L$, and $v_9^L$ are still valid, they cannot function completely since they no longer belong to the giant components. We therefore mark these nodes in white (as shown in stage 2). The failed nodes $v_2^L$, $v_4^L$, $v_5^L$, $v_7^L$, $v_8^L$, and $v_9^L$ in network $G^L$ will lead to failures of the corresponding nodes in network $G^P$ according to the directed dependence links. Based on the dependence relations

shown in stage 1, the nodes $v_2^P$, $v_4^P$, $v_5^P$, and $v_9^P$ (in black) are failed in network $G^P$. With certain adjustable parameters $\alpha$, $\beta$, and $\sigma$, nodes $v_8^P$ (in blue) may fail according to the directed redistribution strategy. We then remove all connectivity links with failed nodes, and thus obtain the cascading failure shown in stage 2. At this point, nodes $v_1^P$, $v_3^P$, $v_6^P$, and $v_7^P$ have not failed in network $G^P$. However, since $v_1^P$ (in purple) does not belong to the giant components, and thus has yet to fail, it leads to a failure of the corresponding node $v_1^L$ (in green) in network $G^L$ according to dependence link. Here, if the adjustable parameters $\alpha$, $\beta$, and $\sigma$ cause node $v_3^L$ to not fail while the risk loads of node $v_1^L$ are redistributed to node $v_3^L$, the cascading failure propagation finishes; the final steady state of this is shown in stage 3. However, if adjustable parameters $\alpha$, $\beta$, and $\sigma$ cause node $v_3^L$ to fail, all nodes in networks $G^L$ and $G^P$ will then become isolated and fail, thereby causing an interdependent supply chain collapse. We therefore need to find the most suitable parameters leading to a minimal cascading failure.

### 3.2. Time-varied cascading failure equation

In order to understand the dynamic failure spread mechanism in an interdependent supply chain network, we construct time-varied cascading failure equations of load propagation based on the failure process described above. We assume that when a fraction $1-p$ of nodes fails in network $G^L$ after an initial removal of nodes, the remaining fraction of functional nodes in the network will be $\delta_1 = p$.

Removing these nodes will cause the nodes directly connected to them to disconnect from a giant component. Hence the remaining functional fraction of nodes in network $G^L$ becomes $\delta_1' = \delta_1 Y_L(\delta_1)$, where $Y_L(\delta_1)$ is the fraction of nodes belonging to a giant component.

Since a fraction $q_p$ of nodes in network $G^P$ depends on the nodes in network $G^L$, the non-functional nodes in network $G^P$ become $(1-\delta_1')q_p$ and the remaining functional nodes $\zeta_1 = 1-(1-\delta_1')q_p$. Here the fraction of functional nodes belonging to a giant component is $\zeta_1' = \zeta_1 Y_P(\zeta_1)$ in network $G^P$, and thus $1-\zeta_1'$ denotes the fraction of those nodes not belonging to a giant component. Thus the fraction of non-functional nodes newly occurring in network $G^L$ is $p(1-\zeta_1')q_l$ because a fraction $q_l$ of nodes in network $G^L$ depends on the nodes in network $G^P$. We recall that a fraction $1-p$ of the nodes in network $G^L$ has failed as a result of the initial attack, and we find that there is a total fraction $1-p+p(1-\zeta_1')q_l$ of nodes that has failed in network $G^L$ that can be transformed into $1-p[1-(1-\zeta_1')q_l]$. Consequently, the remaining fraction of functional nodes in network $G^L$ is $\delta_2 = p[1-(1-\zeta_1')q_l]$, and thus $\delta_2' = \delta_2 Y_L(\delta_2)$. It is easy to obtain the recursive relations of a cascading failure according to the above description, and the time-varied equations of functional nodes at each stage can be summarized as

$$\begin{aligned}
&L_1:\ \delta_1 = p \qquad \delta_1' = \delta_1 Y_L(\delta_1)\\
&P_1:\ \zeta_1 = 1-(1-\delta_1')q_p \qquad \zeta_1' = \zeta_1 Y_P(\zeta_1)\\
&L_2:\ \delta_2 = p[1-(1-\zeta_1')q_l] \qquad \delta_2' = \delta_2 Y_L(\delta_2)\\
&P_2:\ \zeta_2 = 1-(1-p\delta_2')q_p \qquad \zeta_2' = \zeta_2 Y_P(\zeta_2)\\
&\cdots\\
&L_t:\ \delta_t = p[1-(1-\zeta_{t-1}')q_l] \qquad \delta_t' = \delta_t Y_L(\delta_t)\\
&P_t:\ \zeta_t = 1-(1-p\delta_{t-1}')q_p \qquad \zeta_t' = \zeta_t Y_P(\zeta_t).
\end{aligned} \tag{10}$$

When $t \to \infty$, Eq. (10) arrives at a steady state, i.e., $\delta_{t+1} = \delta_t$ and $\zeta_{t+1} = \zeta_t$ because the giant components in an interdependent network stop the separation, and the fraction of removed nodes at step $t$ is equal to the fraction at step $t+1$. Here $\delta_t' = \delta_{t+1}'$ and $\zeta_t' = \zeta_{t+1}'$, and we obtain

$$L_t:\ \delta_t = p[1-(1-\zeta_t')q_l] \tag{11}$$

$$P_t:\ \zeta_t = 1-(1-p\delta_t')q_p. \tag{12}$$

We represent the giant components in networks $G^P$ and $G^L$ at the end of a cascading failure as $U_{L,\infty} = \delta_t Y_L(\delta_t)$ and $U_{P,\infty} = \zeta_t Y_P(\zeta_t)$, respectively.

## 4. Numerical simulation

To generalize our results, we numerically simulate a randomly generated supply chain physical-layer network $G^P$ (see Fig. 1) and cyber-layer network $G^L$ (see Fig. 2). We assume that there are 500 nodes in both networks $G^P$ and $G^L$, and that the average degree of networks $G^P$ and $G^L$ is $\langle k\rangle = 4$. Thus we know that the average in-degree $\langle k\rangle_{in}$ and out-degree $\langle k\rangle_{out}$ are the same at $0.5\langle k\rangle = 2$ in network $G^P$. One-to-one dependence links are randomly generated, and the values of the flow constraints of connectivity links are set to within 60 and 140. We simulate the cascading failure results for two cases: initial single and initial multiple node removal.

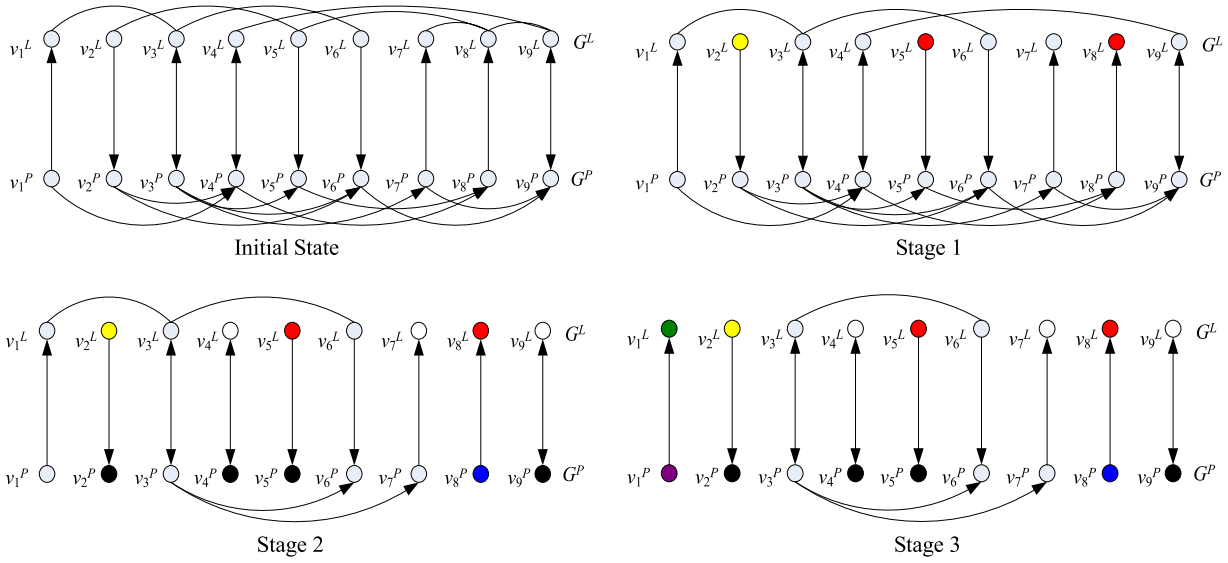


**Fig. 4.** Process of a cascading failure of an instance. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

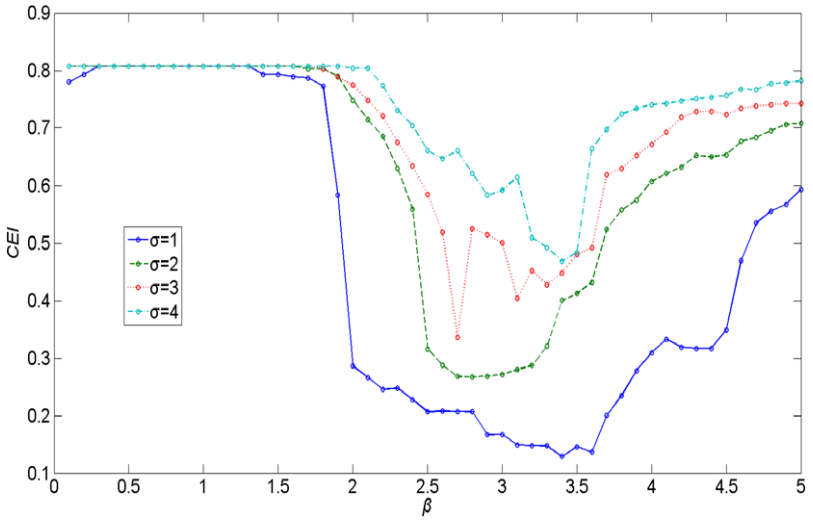


**Fig. 5.** CEI of an interdependent supply chain network under the conditions of single node removal in network $G^L$.

### 4.1. Network robustness of single node removal

We use a comprehensive effectiveness index (CEI) to indicate the average robustness of an interdependent supply chain network. For the single node removal case, $CEI = \sum_{i=1}^{N}(U^i_{L,\infty} + U^i_{P,\infty})/2N^2$, where $N$ is the number of nodes in a single network as discussed above, and $\sum_{i=1}^{N}(U^i_{L,\infty} + U^i_{P,\infty})$ is the sum of fractions when each single node in $G^P$ and $G^L$ is removed sequentially.

(1) Robustness of single node removal in network $G^L$.

We set the parameters to be $\alpha = 1$, $\beta$ changes from 0.1 to 5 with a step size of 0.1, and $\sigma = 1, 2, 3$, or 4. We simulate a cascading failure when initially a single node failure occurs in network $G^L$, and Fig. 5 shows the simulation results of the CEI.

As $\beta$ increases gradually, the CEI of an interdependent supply chain network first decreases, and then increases gradually. This indicates that the node loads will reach a certain extent with an increase of $\beta$, and thus the redistribution strategies (ii) and (iii) will be adopted, which lead to more failures. Nevertheless, when $\beta$ increases to a certain extent, although the node loads still increase in size, the speed increase of the node capacity becomes faster than that of the node loads. Consequently, the sum of the failed nodes becomes correspondingly smaller. Meanwhile, under the conditions of a same $\beta$ and different

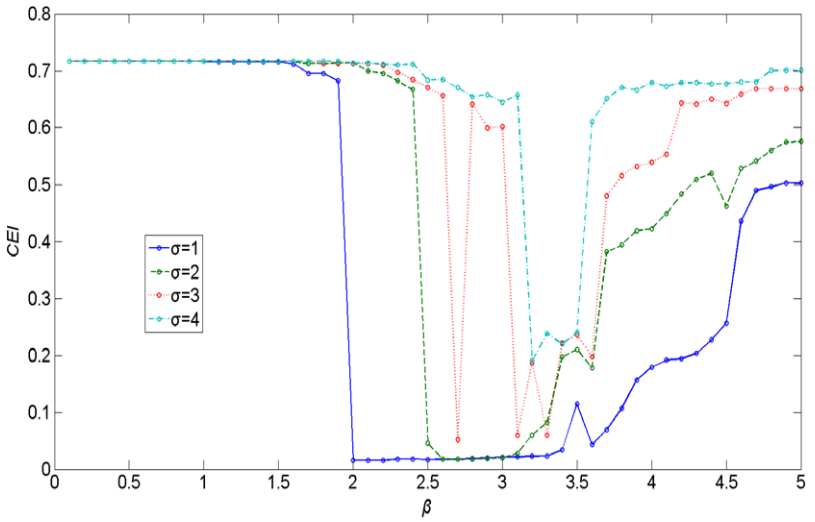


**Fig. 6.** CEI of an interdependent supply chain under the conditions of a single node removal in network $G^P$.

$\sigma$, CEI usually increases along with an increase in $\sigma$ from 1 to 4, which is due to the fact that the node capacity increases with an increase in $\sigma$ while $\alpha$ and $\beta$ remain unchanged, and the node failure probability becomes accordingly smaller.

(2) Robustness of single node removal in network $G^P$.

When a single initial node failure occurs in network $G^P$, we compare the CEI with that obtained from the simulation results when a single initial node removal occurs in network $G^L$. We find that the CEI is usually smaller at the same $\beta$ when a single initial node removal occurs in network $G^P$. As in the single node removal in network $G^L$, the CEI first decreases and then increases gradually as $\beta$ increases. When $\sigma$ increases from 1 to 4, the CEI also increases. Fig. 6 shows these simulation results.

From Fig. 6, CEI suddenly approaches zero while $\beta$ is at a certain value, which is different from the results obtained while a single node removal occurs in network $G^L$ initially. When $\sigma = 1$ and $\beta = 2$, the value of CEI is 0.015; when $\sigma = 2$ and $\beta = 2.5$, the value of CEI is 0.045; and when $\sigma = 3$ and $\beta = 2.7$, 3.1, and 3.3, the values of CEI are 0.0518, 0.0592, 0.0602, respectively. In particular, CEI will fluctuate when $\beta$ changes from 2.7 to 3.6. When $\sigma = 3$ and $\beta = 3.2$, the value of CEI is 0.1904, which indicates that with a growth of $\sigma$ to a certain extent, the corresponding increase in node capacity leads to a reduction of failed nodes, and CEI therefore becomes larger. Clearly, the growth of $\sigma$ is proportional to the costs.

### *4.2. Network robustness of multiple node removal*

To measure the robustness of an interdependent supply chain network when a fraction $1 - p$ of nodes is removed, we analyze the changes in the CEI when multiple nodes are initially removed from network $G^P$, and check to see whether a first-order phase transition occurs [17]. We can remove multiple nodes (1) by the degree of descending order, (2) by the degree of ascending order, or (3) randomly. We compare the results with the CEI obtained from single network $G^P$ under the condition of the same fraction of removed nodes. Here the CEI is given by $CEI = (U_{P,\infty}^{1-p} + U_{P,\infty}^{1-p})/2N$, which differs from that when a single node is removed.

(1) Node removal based on the degree of descending order.

Fig. 7 shows that when the fraction $1 - p$ of removed nodes in an interdependent supply chain network approaches 0.2, all nodes fail, i.e., the $CEI = 0$. This failure is abrupt, and thus is a first-order phase transition. In particular, the CEI suddenly becomes 0 from 0.57, and the removal fraction is 0.19. As $\beta$ grows from 0.5 to 2, the CEI becomes smaller at the same removal fraction. Because the node load increases with an increase in $\beta$, the number of failure nodes in the same network and the coupled network is larger.

The simulation results for the node removal in single network $G^P$ are shown in Fig. 8, where CEI is larger than that of in interdependent supply chain network at the same removal fraction, $1 - p$. That is, single network $G^P$ collapses while the removal fraction approaches 0.73. However, the interdependent supply chain network collapses while the removal fraction is approximately only 0.2.

(2) Node removal based on the degree of ascending order.

Fig. 9 shows the simulation results when multiple nodes in an interdependent supply chain network are removed by degree of ascending order. Here $\beta = 0.5$, $1 - p$ approaches 0.16, and 95% of the nodes fail. When the nodes are removed by degree of descending order, the CEI becomes 0 while $1 - p$ approaches 0.2 at the same value of $\beta$. The CEI obtained when the node removal is by degree of ascending order is smaller than when it is by degree of descending order because most of the small-degree nodes in network $G^P$ link to large-degree nodes in network $G^L$ randomly. When the node removal is by degree

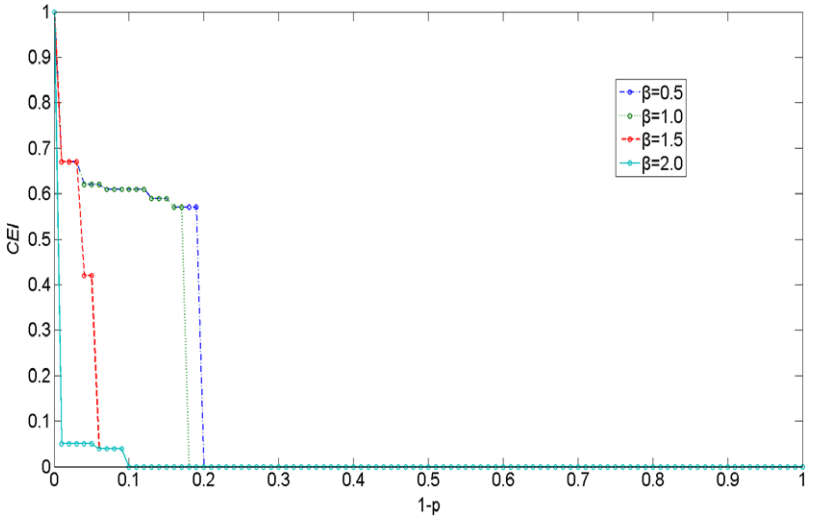


**Fig. 7.** CEI of an interdependent supply chain network according to the descending degree of removal.

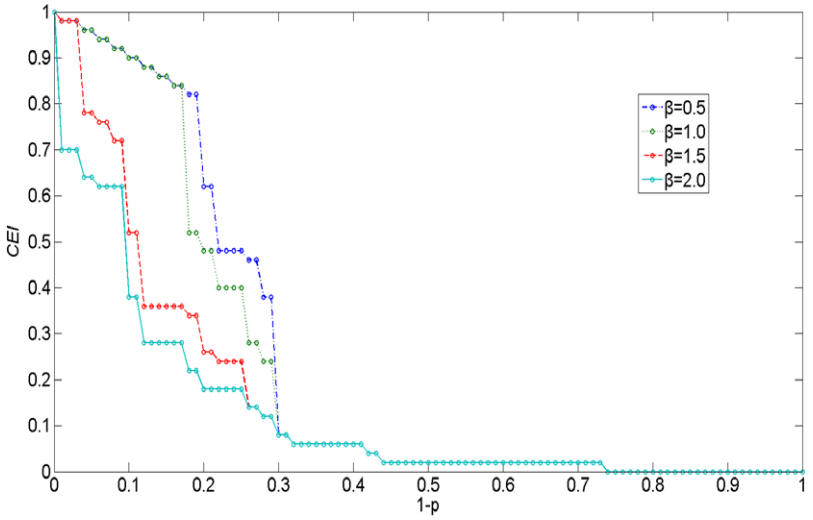


**Fig. 8.** CEI of single network $G^P$ according to the descending degree of removal.

of ascending order in single network $G^P$ (shown in Fig. 10), the CEI is larger when multiple nodes are removed in a single network. In single network $G^P$, the CEI increases as $\beta$ increases from 0.5 to 2. In an interdependent supply chain network, the CEI decreases as $\beta$ increases.

(3) Node removal based on the degree of random order.

Fig. 11 shows that when multiple nodes are randomly removed, CEI $= 0.05$ when $\beta = 0.5$ or $\beta = 1$, and the removal fraction $1 - p$ is approximately 0.14, and CEI $= 0.01$ when $\beta = 1.5$ or $\beta = 2$, and the removal fraction $1 - p$ approaches 0.04. The CEI obtained when node removal is random is smaller than when it is by descending degree order and larger than when it is by ascending degree order. In a single network $G^P$, the CEI approaches 0 when $1 - p$ approaches 0.8 (see Fig. 12), and is larger when multiple nodes are removed in an interdependent supply chain network.

### *4.3. Results and discussion*

(1) In the simulation results, when a single node is removed from an interdependent supply chain network the CEI changes with parameters $\alpha$, $\beta$, and $\sigma$, and failed loads propagate through the system. In both $G^L$ and $G^P$ when a single node is removed, the CEI first decreases and then increases because the redistribution strategies change from case (i) to case (iii) and then to case (ii). In particular, the node loads increase as $\beta$ increases and failures increase. When $\beta$ increases beyond a certain value the node loads still increase, but node capacity increases more rapidly than node load. Thus the CEI increases.

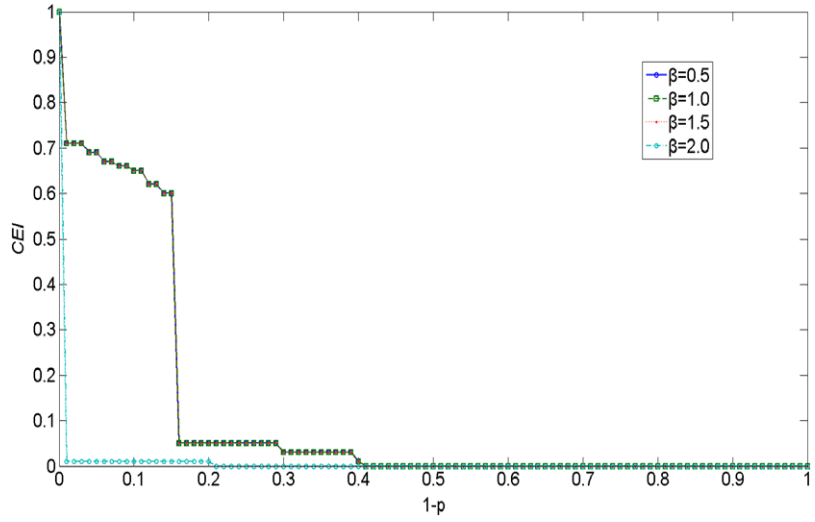


**Fig. 9.** CEI of an interdependent supply chain network according to the ascending degree of removal.

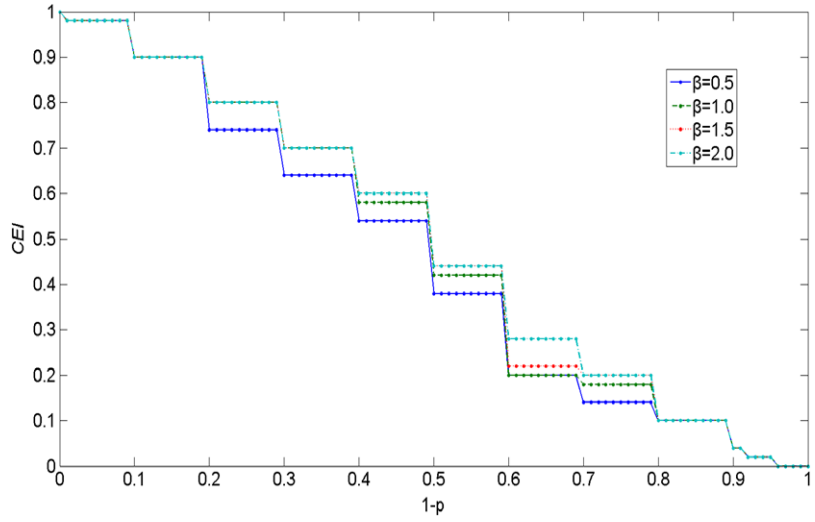


**Fig. 10.** CEI of single network $G^P$ according to ascending degree of removal.

This indicates that the risk defense strategies implemented by the entity nodes in an interdependent supply chain network enhance the CEI by making failed load propagation subject to $W^L$ or $W^P$. Because these risk defense strategies are costly, they are often applied only within a certain range and thus failed loads are not avoided completely.

(2) The degree of ascending order yields the worst CEI. Random removal yields a CEI that is larger than removal by ascending degree and smaller than removal by descending degree. Failure in an interdependent supply chain network is a first-order phase transition in all three methods of multiple node removal, and failure in a single network $G^P$ is a second-order phase transition. Following the characteristics of a directed physical network, failed loads propagate along the directed links in network $G^P$, which leads a CEI of 0 once a large number of nodes are removed.

(3) The simulation results show that removal by degree of ascending order yields the lowest robustness value of the three removal methods. This counterintuitive observation indicates that most of the dependence links connect small degree nodes in the cyber layer to large degree nodes in the physical layer, and vice versa. Parshani et al. [26] and Gu et al. [21] found that robustness increases as the similarity of the interdependent networks increases. Interdependent networks with a low structural similarity are thus weak and highly susceptional to cascading failure even when only a few nodes have failed. Although we can thus improve the robustness by adjusting the network structure, network structure adjustment is extremely costly, and a more practical method of regulation is optimizing the dependence links between the nodes in the different network layers. This topic will be the subject of a future paper.

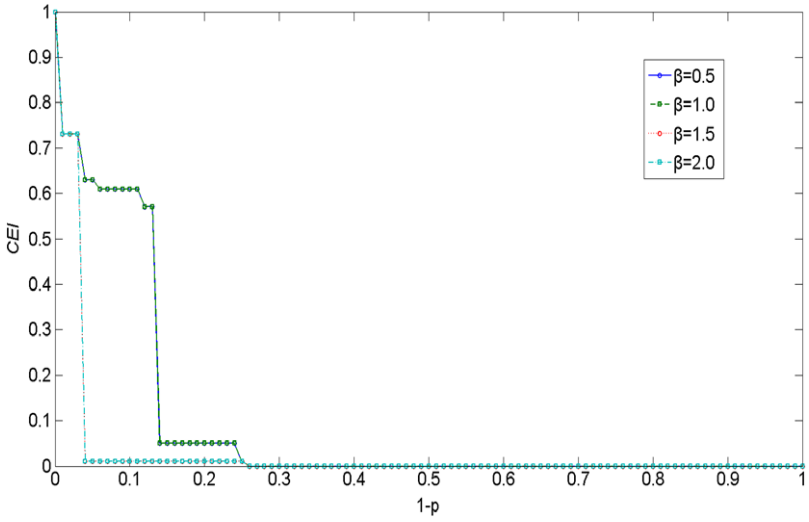


**Fig. 11.** CEI of an interdependent supply chain network according to the random degree of removal.

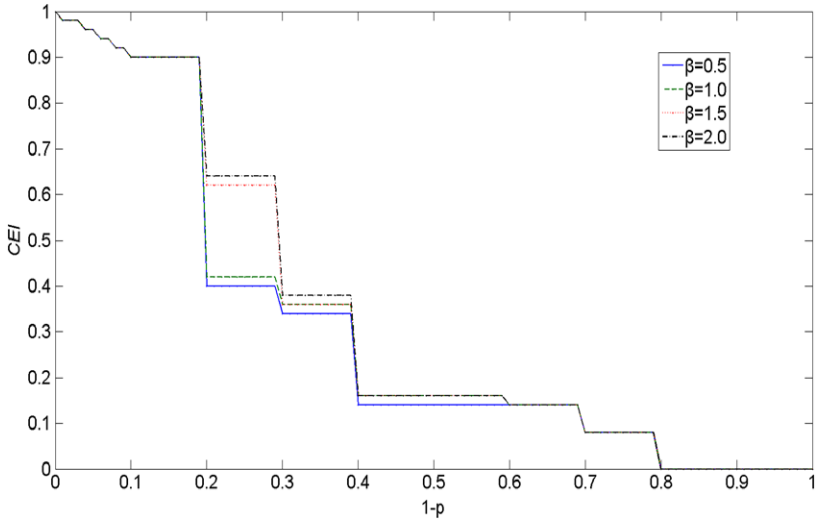


**Fig. 12.** CEI of single network $G^P$ according to the random degree of removal.

## 5. Conclusions

In this paper we describe the interdependent structure of an undirected cyber network and a directed physical network, two layers that constitute an interdependent supply chain network, and we construct models of a physical-layer network and a cyber-layer network using a risk-analysis conceptual framework. We describe node load, node capacity, and other factors using adjustable parameters $\alpha, \beta, \sigma$, and node degree. To measure the robustness of an interdependent supply chain network during an attack, we study the cascading failure mechanism of a single network and an interdependent supply chain network with a one-to-one dependence relation between physical network $G^P$ and cyber network $G^L$. We describe cascading failure using a time-varying cascading failure equation, which enables us to identify the nodes still functioning after the failed loads have ceased propagating.

To measure network robustness at parameters $\alpha = 1$, $\beta = 0.1$–5, and $\sigma = 1$, 2, 3, and 4, we simulate the CEI of an interdependent supply chain network and a single network with risk flow constraints. We simulate a cascading failure for two cases in an interdependent supply chain network: single node removal and multiple node removal. In multiple node removal we found that a first-order phase transition occurs, subject to three methods of removal: degree ascending, degree descending, and random. We compare the simulation results obtained using these three removal methods in an interdependent network and a single network. Our research provides a way of analyzing the robustness to attack of an interdependent supply chain network, and the scientific basis for network structure optimization and cascading failure control.

The significant difference between the undirected cyber network $G^L$ and the directed physical network $G^P$ causes a first-order phase transition. The random dependence links between nodes in network $G^L$ and network $G^P$ significantly lower the robustness. In a future paper we will build on the intra-network and inter-network link research described in the literature and develop strategies for optimizing the structure of an interdependent supply chain network.

## Acknowledgments

This work was partially supported by grant 71201106, 71371044 and 71301108 from the National Natural Science Foundation of China. We also thank the first-class General Financial Grant (2013M530228) and the Special Financial Grant (2014T70462) from the China Postdoctoral Science Foundation.

## References

[1] A. Świerczek, The impact of supply chain integration on the "snowball effect" in the transmission of disruptions: An empirical evaluation of the model, Int. J. Prod. Econ. 157 (2013) 89–104.
[2] R. Narasimhan, S. Talluri, Perspectives on risk management in supply chains, J. Oper. Manage. 27 (2009) 114–118.
[3] P.R. Kleindorfer, G.H. Saad, Managing disruption risks in supply chains, Prod. Oper. Manage. 14 (2005) 53–68.
[4] Y. Sheffi, The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, The MIT Press, Cambridge, MA, 2005.
[5] C.W. Craighead, J. Blackhurst, M.J. Rungtusanatham, R.B. Handfield, The severity of supply chain disruptions: design characteristics and mitigation capabilities, Decis. Sci. 38 (2007) 131–156.
[6] A.L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509–512.
[7] M.E.J. Newman, S.H. Strogatz, D.J. Watts, Random graphs with arbitrary degree distributions and their applications, Phys. Rev. E 64 (2001) 026118.
[8] P. Holme, B.J. Kim, Vertex overload breakdown in evolving networks, Phys. Rev. E 65 (2002) 066109.
[9] Y. Moreno, R. Pastor-Satorras, A. Vázquez, A. Vespignani, Critical load and congestion instabilities in scale-free networks, Europhys. Lett. 62 (2003) 292–298.
[10] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (2002) 065102.
[11] X.F. Wang, J. Xu, Cascading failures in coupled map lattices, Phys. Rev. E 70 (2004) 056113.
[12] J. Wang, Y.H. Liu, Y. Jiao, H.Y. Hu, Cascading dynamics in congested complex networks, Eur. Phys. J. B 67 (2009) 95–100.
[13] A. Nagurney, F. Toyasaki, Supply chain supernetworks and environmental criteria, Transp. Res. D 8 (2003) 185–213.
[14] A. Nagurney, M. Yu, Sustainable fashion supply chain management under oligopolistic competition and brand differentiation, Int. J. Prod. Econ. 135 (2012) 532–540.
[15] Z.T. Wang, Reflection on supernetwork, J. Univ. Shanghai Sci. Technol. 33 (2011) 229–237.
[16] Q. Dong, J. Ma, Recent development on supply chain supernetwork modeling, J. Univ. Shanghai Sci. Technol. 33 (2011) 238–247.
[17] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[18] S.V. Buldyrev, N.W. Shere, G.A. Cwilich, Interdependent networks with identical degrees of mutually dependent nodes, Phys. Rev. E 83 (2011) 016112.
[19] X.Q. Huang, J.X. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of interdependent networks under targeted attack, Phys. Rev. E 83 (2011) 065101(R).
[20] C.M. Schneider, N.A.M. Araujo, S. Havlin, H.J. Herrmann, Towards designing robust coupled networks, Sci. Rep. 3 (2013) http://dx.doi.org/10.1038/srep01969. article number: 1969.
[21] C.G. Gu, S.R. Zou, X.L. Xu, Y.Q. Qu, Y.M. Jiang, D.R. He, Onset of cooperation between layered networks, Phys. Rev. E 84 (2011) 026101.
[22] J. Shao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Cascade of failures in coupled network systems with multiple support-dependence relations, Phys. Rev. E 83 (2011) 036116.
[23] J.X. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (2012) 40–48.
[24] O. Yağan, D.J. Qian, J.S. Zhang, D. Cochran, Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures and robustness, IEEE Trans. Parallel Distrib. Syst. 23 (2012) 1708–1720.
[25] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, S. Havlin, Inter-similarity between coupled networks, Europhys. Lett. 92 (2010) 68002–68006.
[26] R. Parshani, S.V. Buldyrev, S. Havlin, Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition, Phys. Rev. Lett. 105 (2010) 048701.
[27] P. Crucitti, V. Latora, M. Marchiori, Model for cascading failures in complex networks, Phys. Rev. E 69 (2004) 045104(R).