Physica A 459 (2016) 129–139

Contents lists available at ScienceDirect

Physica A

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

Robustness of assembly supply chain networks by considering risk propagation and cascading failure

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

[a] School of Transportation, Southeast University, Nanjing, Jiangsu, 210096, PR China
[b] Industrial Engineering Department, Shenyang Aerospace University, Shenyang, Liaoning 110136, 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 risk model of assembly supply chain network.
- A cascading failure model based on production capability loss is developed.
- We consider different disruption scenarios and their probability.
- We assess network robustness at different node threshold and linking intensity.
- The simulation results show that 30% nodes removal cause network collapse.

ARTICLE INFO

Article history:
Received 22 December 2015
Received in revised form 17 March 2016
Available online 27 April 2016

Keywords:
ASCN
Cascading failure
Risk propagation
Network robustness

ABSTRACT

An assembly supply chain network (ASCN) is composed of manufacturers located in different geographical regions. To analyze the robustness of this ASCN when it suffers from catastrophe disruption events, we construct a cascading failure model of risk propagation. In our model, different disruption scenarios *s* are considered and the probability equation of all disruption scenarios is developed. Using production capability loss as the robustness index (RI) of an ASCN, we conduct a numerical simulation to assess its robustness. Through simulation, we compare the network robustness at different values of linking intensity and node threshold and find that weak linking intensity or high node threshold increases the robustness of the ASCN. We also compare network robustness levels under different disruption scenarios.

1. Introduction

In recent years we have begun to understand the behavior of phenomena such 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 influence of this production loss spread to other countries and sent shockwaves through the worldwide motor industry. The main cause was the disruption of the supply chain supporting the manufacturing subsystem. If companies transfer their

* Corresponding author. Tel.: +86 13555771799.
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.2016.04.030
0378-4371/

internal risks to their supply chain partners, directly or indirectly they affect those partners [1]. The negative effects of risk are transferred to other companies because most real-world supply chain networks are geographically dispersed [2–4]. Although strong interdependencies increase supply chain efficiency, they also decrease system robustness—and when disruption occurs the negative effects are more severe. Since supply chain system becomes more and more important in current global production mode, it is necessary to do the study of supply chain robustness by considering the disruption propagation. More importantly, assembly supply chain is one of the most popular one because it is important and fundamental in manufacturing industry. Consequently, we aim to assess the robustness of ASCN.

Because all supply chains networks are vulnerable to disruption, supply chain risk management has been the subject of much recent study. The goal is to secure the uninterrupted flow of directed materials and undirected information [5]. When a firm is able to manage the risk of disruption they can better serve their customers, and thus increasing the robustness of supply chain networks is an important competitive factor in any free market [6–8]. 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, increasing chain agility, and mitigating risk [9–15]. Wu et al. [16] proposed a disruption analysis network methodology for modeling how the effects of disruptions propagate through a supply chain. Oke and Gopalakrishnan [17] investigated how to classify and manage the risks in the supply chain of a large US retailer and classified risks as either inherent and of high frequency or disruptive and of low frequency. They developed risk mitigation techniques that included generic strategies for handling most types of risk and specialized strategies for handling particular risks. Marucheck et al. [18] examined how the global supply chain creates or exacerbates vulnerabilities, and they focused on how operations management science can provide fresh insights into product safety concerns and security in the global supply chain. Świerczek found that dependence relationships can cause the transmission of disruptions to "Snowball" through a supply chain network or through a portion of it. He modeled this effect by linking the disruption intensity and extent of supply chain integration to the amplification of transmitted disruptions [19].

Our goal here is to construct a cascading failure model of risk propagation that can quantify the robustness of ASCN under different disruption scenarios. Most current studies of cascading failures in complex networks have focused on single networks [20–23]. Holme and Kim [20] studied evolving networks based on the Barabási–Albert scale-free network model with vertices sensitive to overload breakdown. They considered two cases of load limitation, i.e., when the average number of connections per vertex increases with the network size and when it remains constant. They found avalanche-like breakdowns for both load limitations in their work and, to avoid these avalanches, the authors argue that the capacity of the vertices has to grow with the size of the system. The irregular dynamics of the formation of a giant component has also been studied. Moreno et al. [21] studied the tolerance to congestion failures in communication networks with a scale-free topology. They proposed that the traffic load carried by each damaged element in the network must be partially or totally redistributed among the remaining elements. Overloaded elements might fail in turn and trigger a failure cascade that isolates large portions of the network. They also found a critical traffic load above which the probability of massive traffic congestions destroying the network communication capabilities is finite. Motter and Lai showed that, for complex networks, the loads can be redistributed among the nodes, and intentional attacks can lead to a cascade of overload failures. They also demonstrated that the heterogeneity of complex networks makes them particularly vulnerable to attacks, because disabling a single key node can trigger a large-scale cascade [22]. Wang and Xu [23] investigated cascading failures in coupled map lattices with different topologies. They found that cascading failures occur much more frequently in small-world and scale-free coupled map lattices than in globally coupled map lattices. There have also been some recent studies of failure cascades in interdependent networks. Buldyrev et al. [24] recently used a one-to-one correspondence model to study the ramifications of interdependence between two networks. Their analytical framework used a generating-function formalism widely applied in studies of percolation and structure within single networks [25]. This framework for interdependent networks enables us to follow the dynamics of the failure cascades and derive analytic solutions for the final steady state. Researchers have used this work of Buldyrev in a variety of ways to study interdependent networks [26–31].

In summary, our goal is to quantify the robustness of ASCN against disruption in order to provide a scientific basis for the development of network protection. Our innovations of studying the cascading failure of ASCN are in two aspects: the risk propagation mode and the RI of ASCN. Applying cascading failure theory, we will (i) describe the concept of risk propagation in an ASCN, (ii) construct a cascading failure model to depict the dynamic process of risk propagation, and (iii) use different disruption scenarios to assess the robustness of ASCN.

2. Theoretical risk model of supply chain network

2.1. Conceptual framework for risk propagation

Every entity in a supply chain network faces risk. When a natural disaster, criminal act, or terrorist act disrupts a supply chain network, we need to be able to quantify the risk that it will propagate and to analyze its mode of propagation. Fig. 1 shows a traditional supply chain operation model.

There are four types of entity that form a single supply chain network: suppliers, production centers, distribution centers, and customers. Here we assume all entities to be network nodes [32]. The links between those nodes in the supply chain network are called connectivity links, and can transfer risk. Whenever any of the nodes in a directed supply chain network is disrupted and fails, there is a risk that they will propagate.

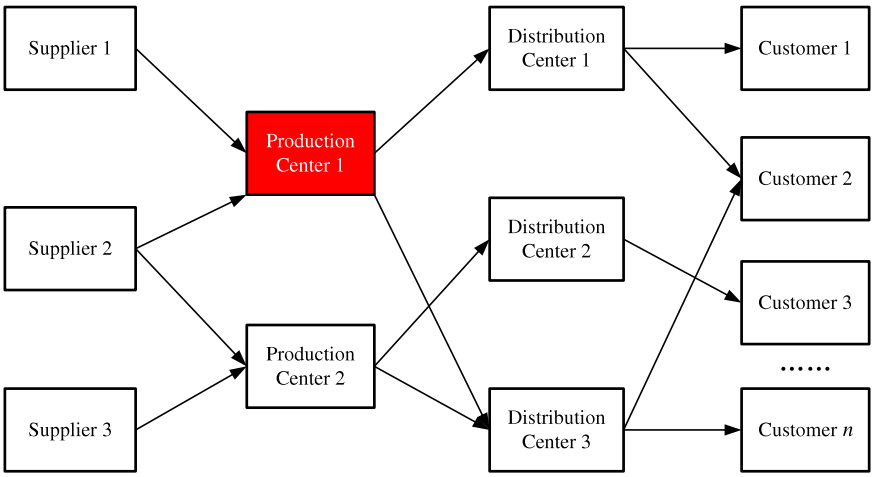

Fig. 1. A traditional supply chain operation model.

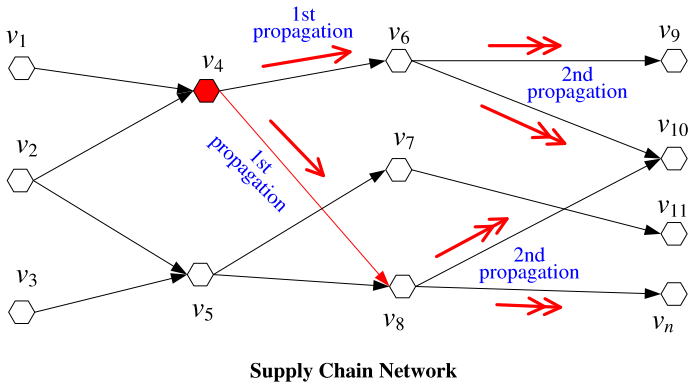

Fig. 2. Risk propagation through supply chain networks.

Fig. 2 shows the process of risk propagation. When disruption causes one or more nodes to fail, because of their connectivity links there is a risk that failure will propagate to other nodes.

Fig. 2 shows that the risk propagation process has a ripple effect. When a node v_4 fails at time t_0 the failure can propagate to neighbor nodes v_6^P and v_8^P ("first risk propagation") through connectivity links. Then failed nodes v_6^P and v_8^P can transfer the failure to their downstream neighbor nodes accordingly ("second risk propagation"). This process continues through to the final customers. It is thus important to be able to quantify the risk that failure will propagate and to assess the robustness of the entire assembly supply chain.

2.2. Cascading failure model of risk propagation in assembly supply chain

In this study we consider one type of supply chain network, i.e., an ASCN. As discussed above, the assembly supply chain is one of the most popular supply chain types. From network perspective, ASCN is directed network, and upstream nodes in assembly network provide components to downstream nodes. So, the directed links between nodes denote the supply and demand relationship. Examples of ASCN include the automobile manufacturing, computer fabrication, and airplane production industries. To assess the maximum risk a supply chain network can encounter, we evaluate network robustness when the disruption events are catastrophic, i.e., when the duration of the disruption event greatly exceeds the length of time required for product delivery. In an ASCN for final product A many upstream manufacturers produce parts for the downstream manufacturers. Let $i \in M = \{1, 2, \ldots, m\}$ be the index of all manufacturers. Fig. 3 shows an ASCN, but focuses on the process from the part manufacturers to the final assembled products, i.e., it is only one portion of the traditional supply chain network shown in Fig. 1. Each node is a particular part k, but the pattern differs from the traditional supply chain network [32] because each manufacturer has the ability to produce a variety of parts. The demand quantity of final product A from customers, denoted by q_A, is known in advance. The quantity of part k required at manufacturer i is q_{ki}, thus the total quantity demand q_k of part k is $\sum_i q_{ki}$, and $r_{kk'}$ denotes the number of upstream parts k required for each downstream part k'.

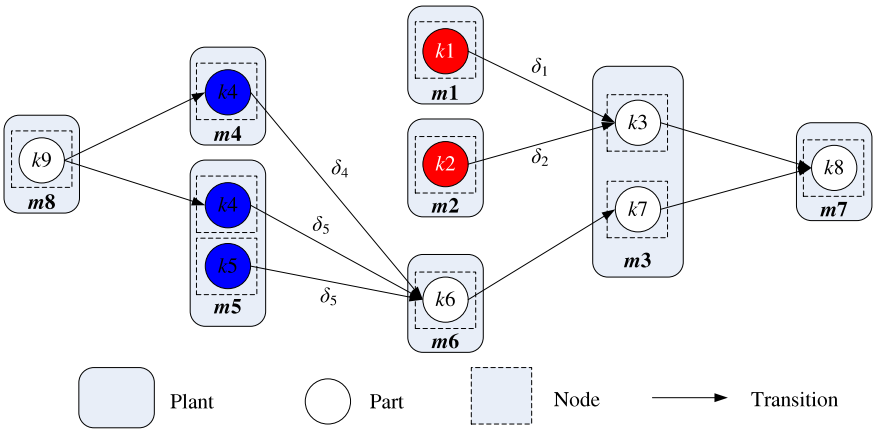

Fig. 3. A sample sketch of assembly supply chain.

We use our model to measure the production capability loss of an entire supply chain during a catastrophic disruption, one that causes the production capability of a manufacturer to fail completely. Downstream manufacturers are affected through connectivity links, and we define "linking intensity" $\delta_{ii'}$ to quantify how much manufacturer i influences manufacturer i', $0 \leq \delta_{ii'} \leq 1$. When manufacturer i is disrupted and fails, the produced risks (production capability loss) to its downstream part k' at manufacturer i' is $q_{ki}\delta_{ii'}/r_{kk'}$. Each manufacturer usually employs countermeasures to lower risk, e.g., by improving inventory level in order to reduce $\delta_{ii'}$. We also define a threshold $\Phi_{k'i'}$ for part k' at manufacturer i' when the risks are being propagated. When the remaining production capability $q'_{k'i'}$ drops below $\Phi_{k'i'}$ due to the lack of upstream parts at manufacturer i, the node part k' at manufacturer i' also fails, and the risk propagates and causes a failure cascade. In particular, when there are two or more disrupted upstream manufacturers, the risk to the connected downstream nodes will be at a maximum.

Note that part manufacturers for complex products are commonly located in different geographical regions, both domestic $l = 1$ and foreign $l = 2$. Let M_1 ($M_1 \subseteq M$) be the set of domestic manufacturers, and M_2 ($M_2 \subseteq M$) be the set of foreign manufacturers, $M_1 \cup M_2 = M$. Because foreign manufacturers are more susceptible to material flow breakdown due to disruptions in long distance shipping, domestic manufacturers tend to be more reliable. The local disruption probability for manufacturer i is α_i and thus the probability that manufacturer i will not be disrupted is $1-\alpha_i$. In addition, manufacturers located in the same region constitute a group risk and can collapse simultaneously when disrupted by earthquake, flooding, hurricane, and general strikes. The probability that there will be a simultaneous disruption of all manufacturers in region l is α_l^*. If p_s is the probability that disruption scenario s will occur, and if there are a total of q disruption scenarios, $q = 2^m$., probability p_s can be represented

$$p_s = \begin{cases} \alpha_1^*\alpha_2^* + \alpha_1^*(1-\alpha_2^*)\prod_{i\in M_2}\alpha_i + \alpha_2^*(1-\alpha_1^*)\prod_{i\in M_1}\alpha_i + (1-\alpha_1^*)(1-\alpha_2^*)\prod_{i\in M}\alpha_i & \text{if } M_s = \phi \\ (1-\alpha_1^*)\alpha_2^*\prod_{i\in M_s}(1-\alpha_i)\prod_{i\in M_1\setminus M_s}\alpha_i + (1-\alpha_1^*)(1-\alpha_2^*)\prod_{i\in M_s}(1-\alpha_i)\prod_{i\notin M_s}\alpha_i & \text{if } M_s \subseteq M_1 \\ (1-\alpha_2^*)\alpha_1^*\prod_{i\in M_s}(1-\alpha_i)\prod_{i\in M_2\setminus M_s}\alpha_i + (1-\alpha_1^*)(1-\alpha_2^*)\prod_{i\in M_s}(1-\alpha_i)\prod_{i\notin M_s}\alpha_i & \text{if } M_s \subseteq M_2 \\ (1-\alpha_1^*)(1-\alpha_2^*)\prod_{i\in M_s}(1-\alpha_i)\prod_{i\notin M_s}\alpha_i & \text{if } M_s \cap M_1 \neq \phi \quad \text{and} \quad M_s \cap M_2 \neq \phi \end{cases} \tag{1}$$

where M_s is the set of manufacturers that are still functional under the disruption scenario s.

2.3. Robustness index (RI) of an ASCN

The robustness index (RI) quantifies the robustness of an ASCN. Traditional assessment method of network robustness is based on the number of ultimate failed nodes. However, it is not suitable for measuring the robustness of ASCN since the node will not fail completely while disruption occurs. Commonly, it will lead to production capability loss when some enterprises (nodes) are affected by initial disruptions. Consequently, we use production capability loss as RI. Another reason that we employ production capability loss as RI in assembly supply chain is that we usually evaluate the disruption affection based on the number of products that can finally be provided to customers. Here we measure the RI in two ways: (1) RI $= \sum_{i=1}^{m} U_{i,\infty}/m$, where $U_{i,\infty}$ is the final number of product units that can be delivered, i.e., the final production capability when a single manufacturer i is removed, and (2) RI $= \sum_s P_s U_{s,\infty}$, where $U_{s,\infty}$ is the final number of product units that can be delivered when there is a disruption s. Note that the second RI measurement takes into account all disruption scenarios.

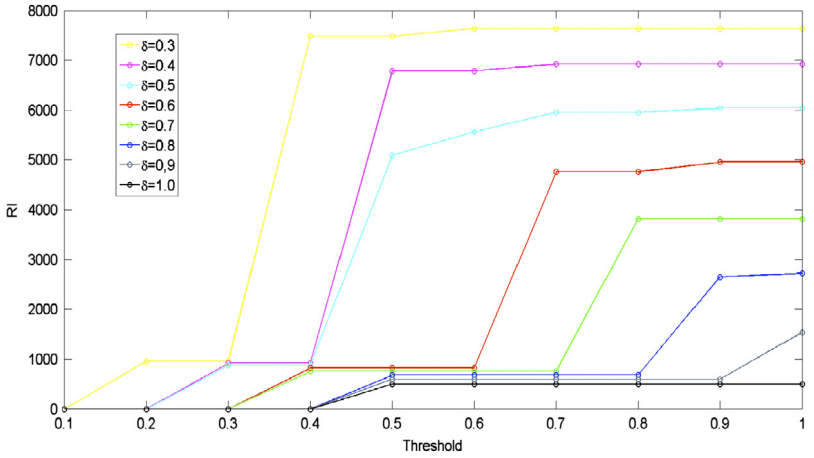

Fig. 4a. *RI* of ASCN at different threshold Φ.

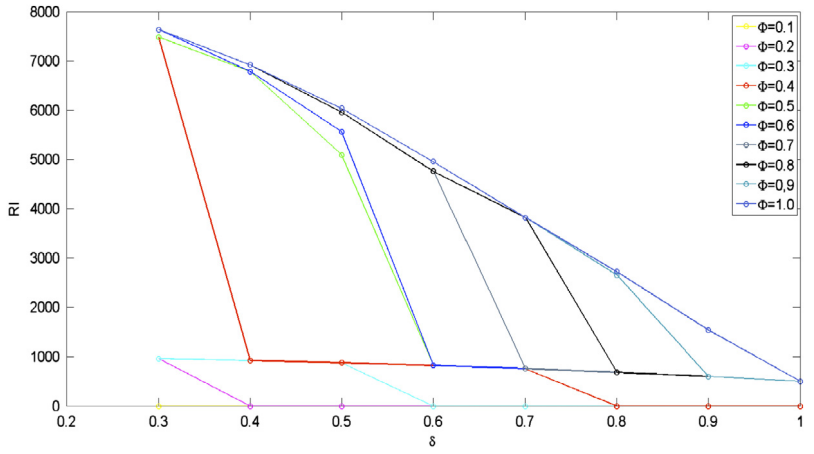

Fig. 4b. *RI* of ASCN at different linking intensity δ.

3. Computational examples

We next implement a numerical simulation of a randomly generated ASCN with fixed q_{ki} and $r_{kk'}$ and use these computational examples to demonstrate how the risk propagation model can be used to quantify the robustness of an assembly supply chain at risk of disruption. Here $q_A = 10\,000$, $\delta_{ii'}$ changes from 0.3 to 1 with a step size of 0.1, and $\Phi_{k'i'}$ changes from 0.1 to 1 with a step size of 0.1. There are 500 manufacturers located in different geographical regions, and we simulate the RI using different disruption scenarios.

3.1. $\mathrm{RI} = \sum_{i=1}^{m} U_{i,\infty}/m$

Figs. 4a and 4b show the results using this formulation. When we fix the threshold $\Phi_{k'i'}$, the RI decreases as the linking intensity increases, indicating a higher probability that risks will be propagated to the nodes that are downstream of a failed node and that production capability will decrease. When we fix the linking intensity, the RI increases as the threshold increases because this threshold increase improves the defensive capability of the downstream nodes. Thus fewer nodes fail and the RI value increases. In particular, when threshold $\Phi_{k'i'}$ is at 10% all the robustness indices are 0 irrespective of linking intensity, i.e., there is minimum robustness. When $\Phi_{k'i'}$ is 20%, the RI is 955 only when the linking intensity is 30%. At all other linking intensity values RI is 0.

Similarly, when the linking intensities are 80%, 90%, and 100%, the RI value remains at 0, even when threshold $\Phi_{k'i'}$ does not exceed 40%.

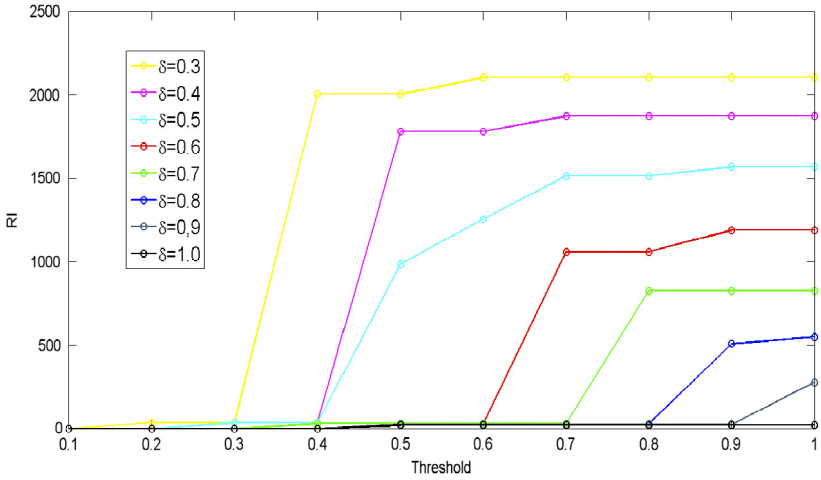

Fig. 5a. *RI* at 10% manufacturers disruption with different threshold Φ.

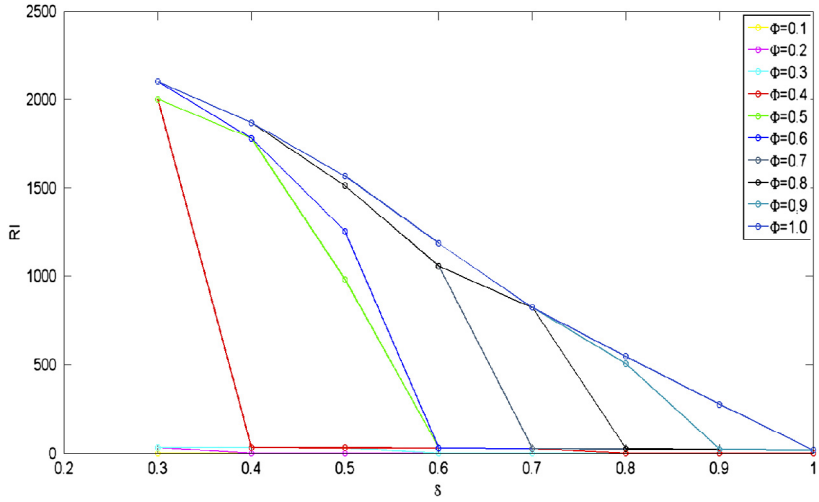

Fig. 5b. *RI* at 10% manufacturers disruption with different linking intensity δ.

3.2. RI $= \sum_s P_s U_{s,\infty}$

Using this RI formulation requires that we take the disruption probability into consideration. Here the disruption probability is uniformly distributed over [0.005, 0.01] for domestic manufacturers $i \in M_1$ and over [0.05, 0.1] for foreign manufacturers $i \in M_2$, i.e., the disruption probabilities are drawn independently from U [0.005, 0.01] and from U [0.05, 0.1], respectively, for domestic and foreign manufacturers. The simultaneous global disruption probability is $\alpha_1^* = 0.00001$ for domestic region 1 and $\alpha_2^* = 0.0001$ for foreign region 2.

(1) 10% manufacturers disruption scenario

Figs. 5a and 5b show that, when 10% manufacturers are disrupted, the simulation results from the RI $= \sum_s P_s U_{s,\infty}$ formulation indicate a decrease RI comparing with the simulation results from the $\sum_{i=1}^{m} U_{i,\infty}/m$ formulation. This difference is due to the fact that the disruption probability has been taken into consideration.

(2) 20% manufacturers disruption scenario

Figs. 6a and 6b show the simulation results when 20% manufacturers are disrupted.

Here the RI values sharply decrease, indicating that removing 20% manufacturers seriously influences the ASCN. It also indicates that the robustness drops because the 500 manufacturers must now rely on a simple assembly network structure, in which case the dependence between each node is tightened. Figs. 7a and 7b show that when 30% manufacturers are removed virtually all RI values fall to 0.

To determine whether changing the robustness affects network structure, we conduct a numerical simulation for 1000 manufacturers. Figs. 8a, 8b, 9a, and 9b show that when we remove 10% or 20% manufacturers the robustness is greater than when the network only encompasses 500 manufacturers. This larger-scale network structure also has increased

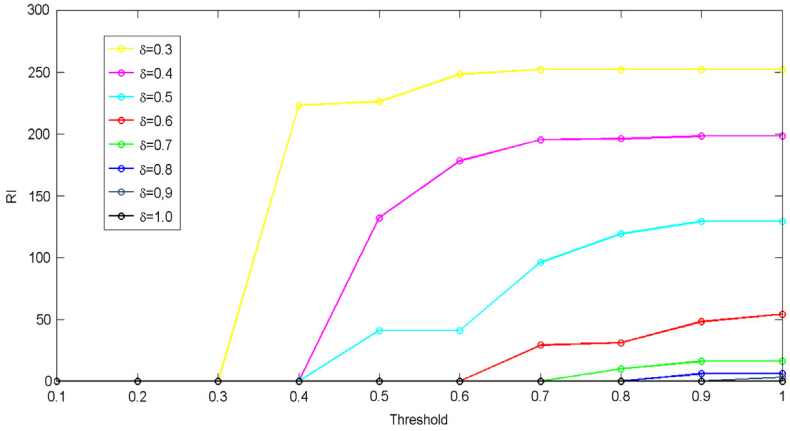

Fig. 6a. *RI* at 20% manufacturers disruption with different threshold Φ.

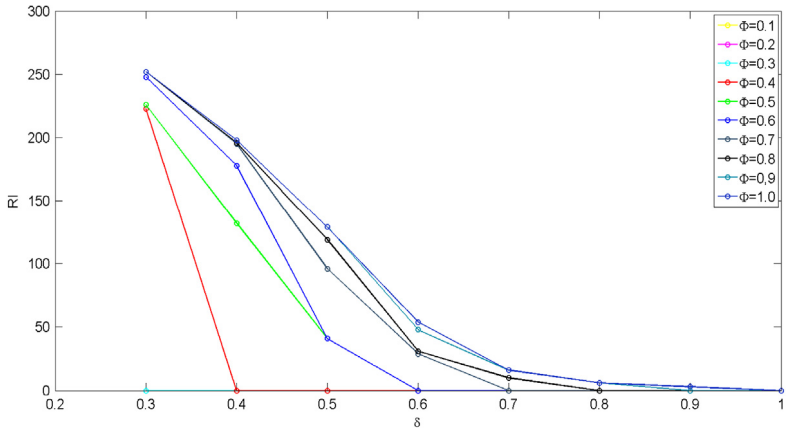

Fig. 6b. *RI* at 20% manufacturers disruption with different linking intensity δ.

redundancies, i.e., multiple suppliers can provide the identical part for downstream manufacturers, and this increases the robustness of the supply chain. These figures clearly indicate that as the network structure becomes more complex and increases in size the robustness of the ASCN will also increase. A large-scale network requires more parts for the final product, but more suppliers provide identical parts for the downstream manufacturers and this makes the network more reliable.

(3) All disruption scenarios

The RI value when all disruption scenarios are taken into account is the simple summation of RI when 10% manufacturers are disrupted, when 20% manufacturers are disrupted, when 30% manufacturers are disrupted, and so on. Figs. 7a and 7b show that the RI will be almost always be 0 when 40% or more node removals occur, and thus the simulation results for all disruption scenarios show results similar to those of the sum of RI at 10% manufacturers disruption, 20% manufacturers disruption, and 30% manufacturers disruptions (see Figs. 10a and 10b).

(4) Random removal of manufacturers

In order to measure the RI value while the manufacturers are removed randomly, we also do the simulation based on different manufacturer removal fraction, $1 - p$. Here, the RI is average value based on 20 times simulation. The simulation results are shown in Fig. 11.

While threshold Φ and linking intensity δ are both 50%, the RI is 981 correspondingly at 10% nodes removal, 41 at 20% nodes removal, and 1 at 30% nodes removal. While threshold Φ and linking intensity δ are 60% and 30% respectively, the RI is 2102 at 10% nodes removal, 248 at 20% nodes removal, 15 at 30% nodes removal. While threshold Φ and linking intensity δ are 80% and 60% respectively, the RI is 1056 at 10% nodes removal, 31 at 20% nodes removal, 1 at 30% nodes removal. While threshold Φ and linking intensity δ are both 100%, the RI is 18 at 10% nodes removal, 0 at 20% and 30% nodes removal. Note that while nodes are removed at approximately 30%, almost all values of RI become 0.

4. Conclusions

In this paper we have described the ASCN and analyzed the risk propagation process. By considering different disruption scenarios, we have constructed a cascading failure model of risk propagation. The goal has been to measure the robustness of

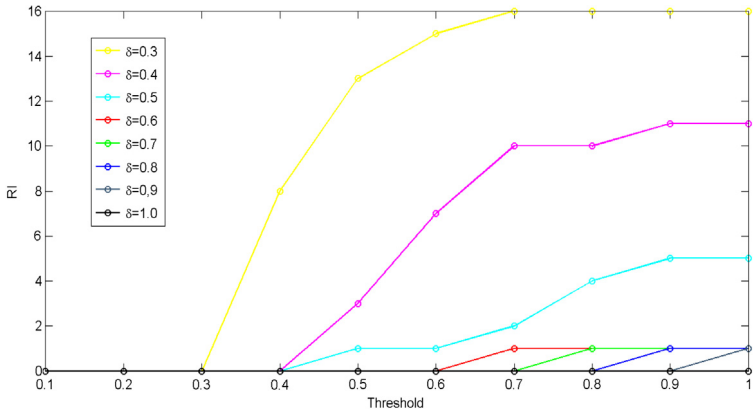

Fig. 7a. *RI* at 30% manufacturers disruption with different threshold Φ.

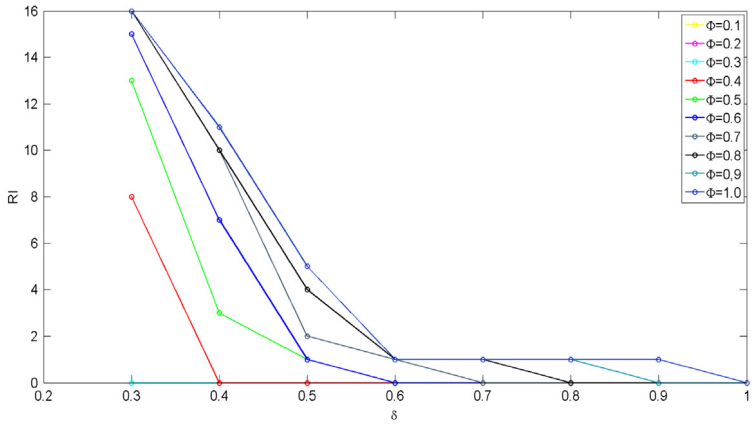

Fig. 7b. *RI* at 30% manufacturers disruption with different linking intensity δ.

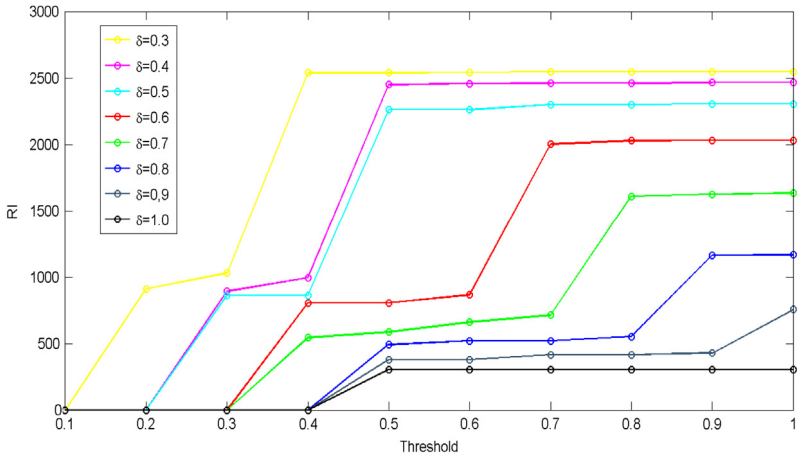

Fig. 8a. *RI* at 10% manufacturers disruption with different threshold Φ (1000 manufacturers).

an ASCN. In our model, the measurement of network robustness is based on production capacity loss, i.e., the final quantity of product that can be delivered to customers after risk propagation. To analyze the effect of ASCN robustness at different parameters of linking intensity $\delta = 0.3$–1, and $\Phi = 0.1$–1, we have simulated the RI of an ASCN. The simulation results show that the value of RI increases with increase in the threshold, and decreases with increase in the linking intensity. We have also carried out simulations at different disruption scenarios and taken disruption probability into account. We have found that almost all values of RI drop to 0 when there is 30% or more nodes disruptions. We have also compared the

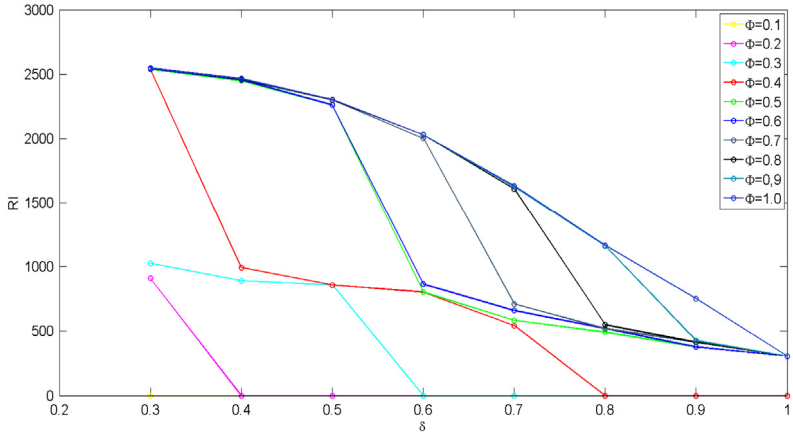

Fig. 8b. *RI* at 10% manufacturers disruption with different linking intensity δ (1000 manufacturers).

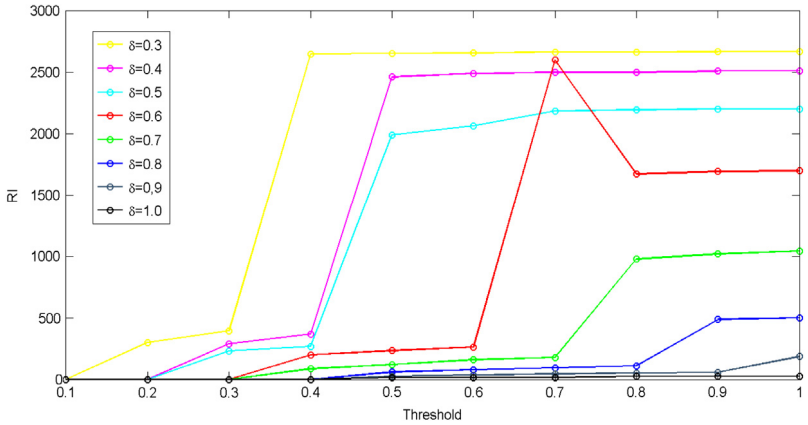

Fig. 9a. *RI* at 20% manufacturers disruption with different threshold Φ (1000 manufacturers).

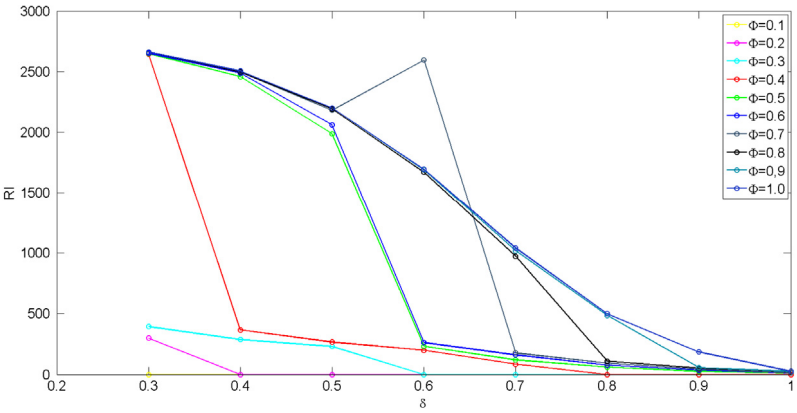

Fig. 9b. *RI* at 20% manufacturers disruption with different linking intensity δ (1000 manufacturers).

simulation results on 500 manufacturers with a larger complex ASCN of 1000 manufactures and found that more complex network structure and the redundancies in the upstream suppliers improve the robustness of the ASCN.

In summary, our research could provide a valuable analysis tool for the robustness of an interdependent supply chain network as it experiences attack. Our research may also provide the scientific basis for network structure optimization and cascading failure control.

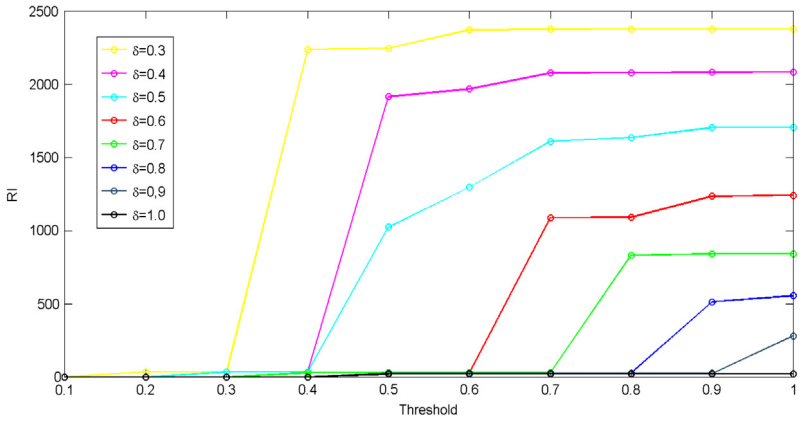

Fig. 10a. *RI* at all disruption scenarios with different threshold Φ.

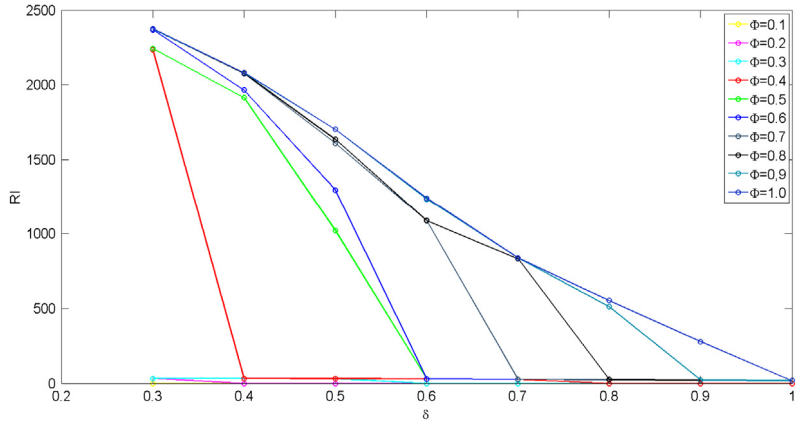

Fig. 10b. *RI* at all disruption scenarios with different linking intensity δ.

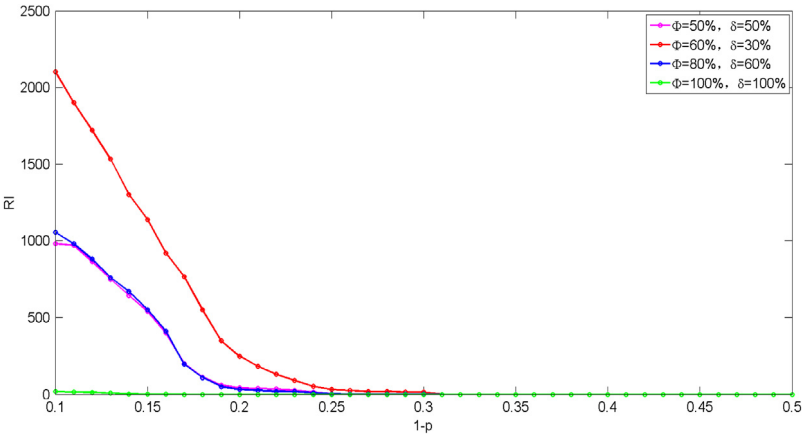

Fig. 11. *RI* at random removal of manufacturers.

Acknowledgments

This work was partially supported by grant 71201106, 71371044 and 71472034 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] W. Klibi, A. Martel, Scenario-based supply chain network risk modeling, European J. Oper. Res. 223 (2012) 644–658.
[2] P.R. Kleindorfer, G.H. Saad, Managing disruption risks in supply chains, Prod. Oper. Manage. 14 (2005) 53–68.
[3] Y. Sheffi, The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, The MIT Press, Cambridge, MA, 2005.
[4] 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.
[5] P. Kraljic, Purchasing must become supply management, Harv. Bus. Rev. 61 (1983) 109–117.
[6] A. Tsay, N. Agrawal, Channel dynamics under price and service competition, Manuf. Serv. Oper. Manage. 2 (2000) 372–391.
[7] T. Boyaci, G. Gallego, Supply chain coordination in a market with customer service competition, Prod. Oper. Manage. 13 (2005) 3–22.
[8] T. Xiao, D. Yang, Price and service competition of supply chains with riskaverse retailers under demand uncertainty, Int. J. Prod. Econ. 114 (1) (2008) 187–200.
[9] R. Narasimhan, S. Talluri, Perspectives on risk management in supply chains, J. Oper. Manage. 27 (2009) 114–118.
[10] S. Chopra, M.S. Sodhi, Managing risk to avoid supply-chain breakdown, MIT Sloan Manage. Rev. 46 (2004) 52–61.
[11] C.S. Tang, Perspectives in supply chain risk management, Int. J. Prod. Econ. 103 (2006) 451–488.
[12] B. Tomlin, On the value of mitigation and contingency strategies for managing supply chain disruption risks, Manage. Sci. 52 (2006) 639–657.
[13] R. Sarathy, Security and the global supply chain, Transp. J. 45 (2006) 28–51.
[14] S.M. Wagner, C. Bode, An empirical examination of supply chain performance along several dimensions of risk, J. Bus. Logist. 29 (2008) 307–325.
[15] S. Rao, T.J. Goldsby, Supply chain risks: a review and typology, Int. J. Logist. Manage. 20 (2009) 97–123.
[16] T. Wu, J. Blackhurst, P. O'Grady, Methodology for supply chain disruption analysis, Int. J. Prod. Res. 45 (2007) 1665–1682.
[17] A. Oke, M. Gopalakrishnan, Managing disruptions in supply chains: A case study of a retail supply chain, Int. J. Prod. Econ. 118 (2009) 168–174.
[18] A. Marucheck, N. Greis, C. Mena, L. Cai, Product safety and security in the global supply chain: Issues, challenges and research opportunities, J. Oper. Manage. 29 (2011) 707–720.
[19] 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.
[20] P. Holme, B.J. Kim, Vertex overload breakdown in evolving networks, Phys. Rev. E 65 (2002) 066109.
[21] Y. Moreno, R. Pastor-Satorras, A. Vázquez, A. Vespignani, Critical load and congestion instabilities in scale-free networks, Europhys. Lett. 62 (2003) 292–298.
[22] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (2002) 065102.
[23] X.F. Wang, J. Xu, Cascading failures in coupled map lattices, Phys. Rev. E 70 (2004) 056113.
[24] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[25] 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.
[26] S.V. Buldyrev, N.W. Shere, G.A. Cwilich, Interdependent networks with identical degrees of mutually dependent nodes, Phys. Rev. E 83 (2011) 016112.
[27] X.Q. Huang, J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of interdependent networks under targeted attack, Phys. Rev. E 83 (2011) 065101(R).
[28] 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.
[29] 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.
[30] 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.
[31] J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (2012) 40–48.
[32] L. Tang, K. Jing, J. He, H.E. Stanley, Complex interdependent supply chain networks: Cascading failure and robustness, Physica A 443 (2016) 58–69.