Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5550837, 11 pages
https://doi.org/10.1155/2021/5550837

Research Article

Rewiring Strategy Based on Directed Betweenness to Mitigate Disruptions of Large-Scale Supply Chain Networks

Hui Xia

Hunan Open University, Changsha 410004, China

Correspondence should be addressed to Hui Xia; xiahy111@163.com

Received 16 January 2021; Revised 8 April 2021; Accepted 6 May 2021; Published 15 May 2021

Academic Editor: Mahmoud Mesbah

In current large-scale supply chain networks, unexpected disruptions degrade the supply availability and network connectivity for modern enterprises. How to improve the robustness of supply chain networks is very important for modern enterprises. In this paper, we explore how to improve the robustness of supply chain networks from a topological perspective. Firstly, through the empirical data-driven study, we show that the directed betweenness metric is more suitable than the other topological metrics in evaluating the robustness of supply chain networks. Then, we propose a rewiring algorithm based on directed betweenness to improve network robustness under the impact of disruptions. The experimental results in the large-scale supply chain network show that the rewiring algorithm based on directed betweenness effectively improves the network robustness.

1. Introduction

In recent years, the global supply chain networks have witnessed tremendous growth in scale. However, the complex and competitive business environment also increases uncertainty and risk. Supplier bankruptcies, natural calamities, and even large pandemic will lead to the disruptions of supply chain network. Moreover, the impacts of disruption are spread and amplified to a larger scale with the global interconnected supply chain network [1, 2]. For example, since 2020, the efficiency of the supply chain management model is seriously hit by unprecedented disease outbreaks, namely, COVID-19. In this pandemic, many important transportation routes around the world are disrupted after the drivers become sick. In Asia, the labor shortages lead to the shutdown of some manufacturers that rely on labor-intensive processes. Therefore, how to effectively control the risk of supply chain network of "transport and production" and "worker movement" becomes one of the key concerns of modern firms and organizations [3–5].

Fundamentally, the supply chain network is a graph consisting of nodes and edges, which transfer goods from suppliers to customers through multiple paths. In recent years, many researchers have explored improving the robustness of the supply chain network from the perspective of network topology [6]. Based on the graph theory and metrics, considerable works have already been conducted to mitigate disruption problems by protecting the central nodes. Unfortunately, despite much progress in improving the robustness of supply chain network according to the node centrality, how to better identify and quantify the node centrality in the complex, dynamic, and large-scale supply chain network has remained elusive.

To identify and assess the importance of nodes, the researchers have designed a wide range of network metrics, such as degree centrality [7], semilocal centrality [8], and closeness centrality [9]. However, these metrics focus on the local or neighbor information of nodes, without considering the global information of end-to-end paths [10]. To address this problem, the betweenness centrality is proposed. Specifically, for a given connected graph, there exists at least one shortest path between each pair of nodes. The betweenness centrality for each node is the number of the shortest paths that pass through the node. Compared with the metrics only considering the local information, the betweenness centrality indicates the importance of nodes from the global view.

Though the betweenness centrality provides a more comprehensive indicator of node centrality, it cannot present the transfer direction of the supply chain network. In fact, all goods in the supply chain network are transferred from the suppliers to customers. Even if one node is the intersection of lots of paths from the customers to suppliers, it should not be selected as the forwarding node in the supply chain network. The betweenness centrality cannot reflect this direction feature, resulting in a loss of accuracy in qualifying the node centrality under the highly complex and dynamic networking scenarios.

In this paper, we explore how to mitigate disruptions of large-scale supply chain networks according to the directed betweenness. Specifically, we propose to use the directed betweenness as the metric to indicate the importance of nodes. Based on the directed betweenness, we propose a new rewiring algorithm to improve the network robustness. The contributions of this paper are as follows (Table 1).

(1) We firstly study and analyze the robustness of the supply chain network and evaluate the performances of existing metrics of node centrality. We conduct the data-driven test to analyze the impact of directed betweenness on the largest connected component, average path length, and average clustering coefficient.

(2) Then, we propose a rewiring strategy based on directed betweenness to improve the network robustness under the impact of network disruptions. Our proposed rewiring strategy removes the node with the largest directed betweenness in the paths from the suppliers to customers to add randomness into the supply chain network with a controlled way.

(3) Finally, we use a data-driven test to show that the rewiring strategy based on directed betweenness greatly improves the network robustness on supply availability and network connectivity in presence of both random and targeted disruptions. For example, in the data-driven test, the connectivity improvement of the rewiring algorithm is up to about 45%.

The remainder of the paper is organized as follows: We first present the related works on improving network robustness of supply chain network in Section 2. In Section 3, we conduct an extensive study to evaluate the existing metrics of node centrality in large-scale supply chain network. In Section 4, we propose the rewiring algorithm to improve the network robustness of the supply chain network under the disruption risks. In Section 5 and Section 6, we show the test results of metrics of node centrality and the rewiring algorithm under typical supply chain networks, respectively. Finally, we give the conclusion remarks and future research in Section 7.

2. Related Work

A robust supply chain network can tolerate the failure of some nodes and maintain connectedness under random or target disruptions [11, 18]. Due to the features of dynamics, complexity, and uncertainty in a large-scale supply chain network, it is vitally important to ensure robustness to cope with potential disruptions.

To alleviate the impact of disruptions, some preventative strategies are proposed to introduce redundancy into the supply chain networks such as contingent dual sourcing strategy (CDSS) [19]. The backup suppliers, relayers, and transfer paths are employed in advance to handle the disruptions [12, 20]. If the disruptions cannot be avoided, the ripple effect is also needed to be controlled quickly and effectively [13]. The above proactive strategies can effectively mitigate the impact of known and predictable disruptions in advance. For unknown or unpredictable disruptions, however, these strategies may be less useful or even totally useless.

The research of [10] firstly introduces the topological perspective into the robustness research of the supply chain network. To improve the network robustness, some works disconnect and reconnect edges to transform the random or hierarchical network topology into the scale-free topology with high resilience. Hierarchy+ [14] connects the edges between nodes with the same type to improve scalability. Compared with Hierarchy+, degree, and locality-based attachment (DLA), [15] considers the heterogeneous roles of nodes and adds new edges according to both degree and locality. To improve network robustness, a localized rewiring approach RLR is proposed to probabilistically disconnect the edge from the node with a high degree and randomly reconnect to the other node [16]. Three heuristic solutions based on the delivery delay and fractional quantity loss are proposed to recover sudden disruption [17]. However, it is hard to obtain an optimal solution with heuristic schemes.

Compared with the above works on the supply chain network, we quantify the node importance through a new metric: we use the directed betweenness to indicate the node centrality for transfer direction from the suppliers to customers. Since we introduce the direction into the betweenness metric, the directed betweenness can give higher accuracy in evaluating the importance of nodes in the supply chain network than the widely used metrics such as degree centrality, semilocal centrality, closeness centrality, and betweenness centrality. Moreover, based on the directed betweenness, we propose a rewiring algorithm to recover the network from disruptions. To improve the network robustness under disruptions, the rewiring algorithm removes the node with the largest directed betweenness from the shortest paths. By considering the transfer direction from the global view, our design gives a more accurate indication of node centrality and therefore effectively improves the network robustness in terms of supply availability and network connectivity.

3. Directed Betweenness

To indicate the importance of nodes in a complex network, many topological metrics are proposed in recent decades. In this section, we compare and evaluate these topological metrics by using a data-driven test. Then, we show why the

Table 1: Related works.

Scheme	Advantages	Disadvantages
CDSS [11]	Contingent dual sourcing strategy effectively mitigates the negative effects of the supply disruption on buyer	The reliability level of dual sourcing limits the advantages
Reference [12]	A stochastic mixed-integer programming approach to integrated supplier selection and customer order scheduling in the presence of supply chain disruption risks	Computing overhead becomes high in complex cases
Reference [13]	Facility protection for major employers mitigates the ripple effect and enhances sustainability	The backup distribution center could only slightly improve the service level in the short term
Reference [10]	The topological perspective is introduced into the robustness research of supply chain network	Only give the possible solutions to improve network robustness
Hierarchy+ [14]	Extends the hierarchical model by allowing edges between nodes of the same type	Arbitrarily creates many edges, resulting in large overhead
DLA [15]	New nodes make connections based on both degree and locality to provide balanced resilience	Does not consider the path direction
RLR [16]	Randomized local rewiring improves the network robustness on the supply availability and network connectivity metrics	Random rewiring may lead to suboptimal performance
Reference [17]	A model to generate a recovery plan after a sudden disruption occurrence and propose three heuristic solutions based on the delivery delay and fractional quantity loss	The heuristic schemes hardly obtain the optimal solutions

directed betweenness can better indicate the node centrality in a large-scale supply chain network.

3.1. Comparison of Topological Metrics. As the simplest centrality, the degree centrality of one node is the number of edges it has. If one node has a high degree, it has large centrality. Figure 1 shows one example of the connected graph, in which nodes D, E, F, H, and I have the degree centralities of 3. However, the degree centrality only considers the local conditions, while ignoring the impact of node failure on the connectedness of the whole graph. Take Figure 1 as an example. The graph consists of two dense groups of nodes that are connected by a few nodes (i.e., F, G, and H). If any node of F, G, and H does not work, the whole network is divided into two parts. Based on this observation, nodes F, G, and H are more important than D and I, though they have the same degree of centralities.

In the supply chain network, the goods are transferred from suppliers to customs. Compared with the degree centrality, the betweenness centrality focuses on the influence of a node on the good flows in a graph. The betweenness centrality is the number of the shortest paths that pass through the node. In Figure 1, the betweenness centralities of nodes F, G, and H are 35, 36, and 35, while that of nodes D and I are 11 and 20, respectively. Since providing a more comprehensive indicator of node centrality from the global view, the betweenness centrality is more suitable for the supply chain network.

Unfortunately, the betweenness centrality does not reflect the path direction from the suppliers to customs in the supply chain network. As shown in Figure 2, if the edge direction is not considered, the betweenness centralities of nodes B and C are equal. However, if the edges have directions, the number of the shortest paths from nodes A to J through nodes B and C becomes 1 and 2, respectively. Therefore, in order to indicate the node centrality in supply chain networks, we put forward the directed betweenness to present the number of the shortest directed paths from the suppliers to the customs.

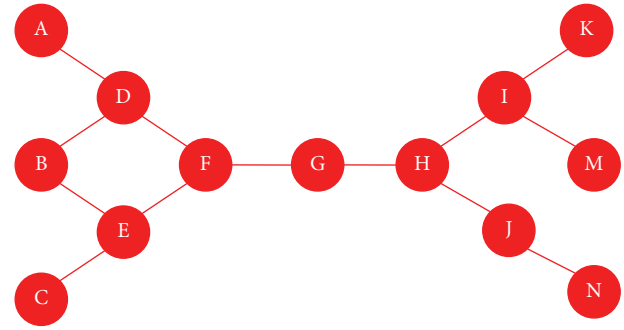


Figure 1: An example to compare different topological metrics.

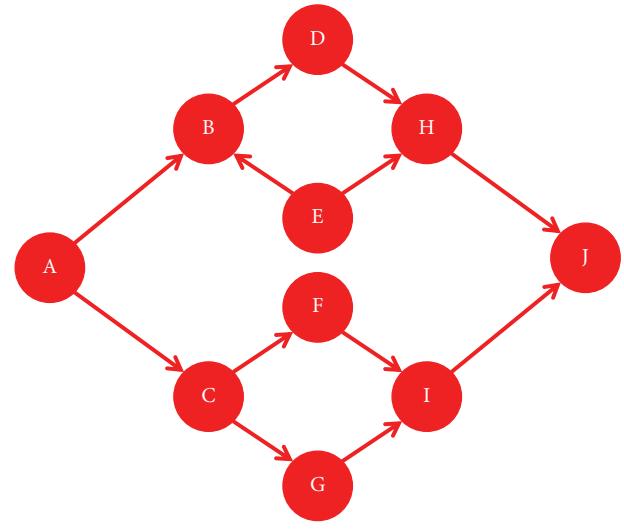


Figure 2: An example to compare nondirected and directed betweenness.

Next, we conduct the data-driven test to investigate how these topological metrics indicate the node importance in real supply chain networks. The data traces are from the supply chain network of transportation of freight and cargo [21]. There are 626 nodes and 1112 edges in this supply chain network. The source, intermediate, and destination locations of freight and cargo transportation are presented as nodes in the data traces.

In the following, we, firstly, sort all nodes according to different metrics of node centrality including the degree, in-degree, out-degree, nondirected betweenness, and directed betweenness. The degree, in-degree, and out-degree are the numbers of edges, in-edges, and out-edges, respectively. Then, we measure the network connectedness after TopK nodes are removed from the network. Here, we use the following three metrics to indicate network connectedness:

Largest connected component (LCC): LCC is the fraction of nodes in the largest connected component to all nodes after the nodes are removed. LLC can reflect the network connectedness after disruptions.

Average path length (APL): APL is the average number of edges in the shortest path between all pairs of nodes in the graph.

Average clustering coefficient (ACP): given a node that has k neighbor nodes, then, at most $(k(k-1))/2$ edges exist between the k neighbor nodes. The clustering coefficient is defined as the fraction of the actually existing edges over $(k(k-1))/2$ edges. Then, ACP is the average value of the clustering coefficient of all nodes in the graph. It shows the degree to which nodes in a graph tend to cluster together.

Figure 3 shows the size of the largest connected component after TopK nodes are removed from the network. We compare the effects when the removed TopK nodes are selected according to different metrics of node centrality. As shown in Figure 3, after the nodes are removed from the graph, the size of the largest connected component decreases as the graph is divided into multiple parts. However, if the TopK removed nodes are sorted based on the directed betweenness, the size of the largest connected component decreases sharply, much faster than the other metrics. This result shows that the directed betweenness can indicate the node importance more accurately.

Next, we measure the average path length under different ratios of removed TopK nodes, which are selected according to different metrics of node centrality. Figure 4 shows that since considering the global network connectedness, the nondirected betweenness and directed betweenness metrics have a larger impact on the average path length than the metrics of degree, in-degree, and out-degree. Compared with the other metrics, the directed betweenness metric can select more important nodes in connecting network. Thus, the average path length under the directed betweenness metric is the lowest.

Figure 5 shows the average clustering coefficient with different metrics of node centrality. If the directed betweenness metric is used to sort the TopK nodes, the average

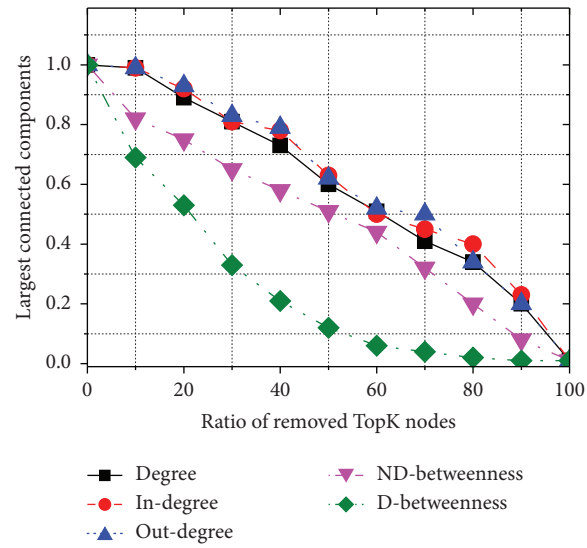


Figure 3: Largest connected component with increasing ratio of removed TopK nodes. ND-betweenness and D-betweenness stand for nondirected betweenness and directed betweenness, respectively.

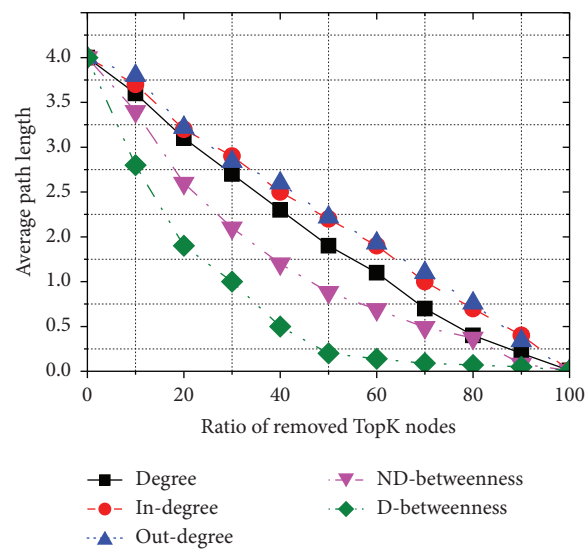


Figure 4: Average path length with increasing ratio of removed TopK nodes.

clustering coefficient decreases faster than the other metrics. This result shows that when the removed nodes are chosen based on the average clustering coefficient, the density of ties between nodes is greatly reduced.

Based on the above analysis, we make the following conclusion: according to the measurement results of the largest connected component, average path length, and average clustering coefficient, the directed betweenness can indicate the node importance more accurately in the large-scale supply chain network compared with the undirected betweenness. This unique observation result motivates us to propose a new rewiring algorithm based on directed betweenness.

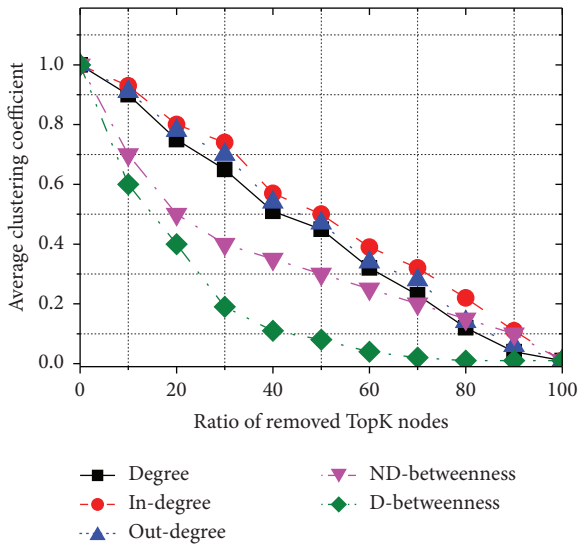


Figure 5: Average clustering coefficient with increasing ratio of removed TopK nodes.

4. Directed Betweenness-Based Rewiring

Based on the connectedness analysis, we observe that the directed betweenness is more accurate in indicating the node centrality in the typical large-scale supply chain network. Therefore, in this section, we introduce the rewiring approach, which improves the network robustness according to the directed betweenness.

Algorithm 1 shows the pseudocode of directed betweenness based rewiring for a given network.

To rewire a supply chain network, we iterate through all the shortest paths from the suppliers to the customs with the following four steps:

(1) With a predetermined rewiring probability p, one node with the largest directed betweenness is selected

(2) The selected node and its edges to its neighbor nodes are temporarily removed from the graph

(3) The supplier node finds the shortest path from the remaining graph to each custom node

(4) The removed node and its edges to its neighbor nodes are added back into the graph

The rewiring probability p fundamentally determines how much rewiring is triggered. If p is 1, all the shortest paths from the suppliers to customs will be rewired. On the contrary, if p is 0, no rewiring will occur and the whole network is not changed. In general, the target of the rewiring process is to add randomness into the supply chain network with a controlled way. A larger p will lead to more rewiring and bring more randomness into the network.

For the enterprise managers, the rewiring algorithm based on directed betweenness provides a guide to improve the robustness of the supply chain. Specifically, according to the transfer paths from suppliers to customers, the graph of the supply chain network is constructed. Then, with the rewiring algorithm, the nodes with the largest directed betweenness are removed from the shortest paths to improve network robustness.

5. Evaluation of Node Centrality Metrics under Disruptions

In this section, we analyze the impact of disruptions on the supply chain network. Firstly, we describe the evaluation metrics including supply availability and network connectivity. Then, we test the network robustness under both random and targeted disruptions.

5.1. Evaluation Metric. In a large-scale supply chain network, a single disruption may initially disable only one or a few nodes. However, the impact of a single disruption may propagate to a large scale along interconnected edges. Therefore, disruptions in a small portion of the supply chain network may cause the catastrophic failure of the whole network. Thus, it is very important for the supply chain network to still maintain function and connectedness under unexpected disruptions. Here, we describe the evaluation metrics of the network robustness and network efficiency under disruption.

5.1.1. Network Connectivity. To assess the network connectivity, we use the normalized size of the largest connected component, which is defined as the fraction of the size of the largest connected component N_{after} after disruption over the number of nodes N_{before} in the network before the disruption. That is,

$$\text{NLCC} = \frac{N_{\text{after}}}{N_{\text{before}}}. \quad (1)$$

NLCC is between 0 and 1. If the supply chain network is well-connected and robust, it has a larger value of NLCC.

Input:
a graph $G(V, E)$;
a rewiring probability p;
For each supplier node $v_i \in V$:
begin
  For each shortest path p_{ij} from v_i to custom node $v_j \in V$:
  begin
    r = Random $(0, 1)$;
    if $(r < p)$
    begin
      v_{toRemove} = the node which has the largest directed betweenness on p_{ij};
      delete v_{toRemove} and its edges to its neighbor nodes from G;
      p_{ij} = search the shortest path from v_i to v_j;
      add v_{toRemove} and its edges to its neighbor nodes into G;

Algorithm 1: Rewiring algorithm.

5.1.2. Network Efficiency. Though the normalized size of the largest connected component can indicate the network connectivity, it cannot show the network efficiency. In a supply chain network with high efficiency, the path from the supplier to customs should be as short as possible. Here, we define network efficiency E as

$$E = \frac{2}{N(N-1)} \sum_{i \neq j \in V} \frac{1}{d_{ij}}, \tag{2}$$

where N is the number of nodes and d_{ij} is the length of the shortest path from node v_i to node v_j. If no path from node v_i to node v_j exists, d_{ij} is infinity and then $1/d_{ij}$ equals 0.

We use E and E^* to denote the network efficiency after and before disruption, respectively. Thus, the normalized network efficiency NE is

$$\text{NE} = \frac{E}{E^*}. \tag{3}$$

5.1.3. Variation of Connectivity and Efficiency. Due to the different roles of nodes in the supply chain network, different nodes have various impacts on network connectivity and efficiency. To evaluate these impacts of disruptions, we define the variation ratio of network connectivity as

$$\Delta S = \frac{\text{NLCC}_1 - \text{NLCC}_2}{\Delta N}, \tag{4}$$

where NLCC_1 and NLCC_2 are the normalized sizes of the largest connected component after two different disruptions, respectively. ΔN is the varying number of failure nodes in two disruptions.

Similarly, the variation ratio of network efficiency is

$$\Delta E = \frac{\text{NE}_1 - \text{NE}_2}{\Delta N}, \tag{5}$$

where NE_1 and NE_2 are the normalized network efficiency after two different disruptions.

5.2. Test Setting. We conduct the data-driven test to evaluate the robustness of the supply chain under random disruptions and targeted disruptions. The data is collected from the transportation network of freight and cargo [21]. To simulate the random disruptions and targeted disruptions, we remove nodes from the network. Specifically, in order to simulate random disruptions, we remove the randomly selected nodes one by one from the supply chain network. For the targeted disruptions, we progressively removed the TopK nodes, which are sorted based on the directed betweenness of node centrality.

5.3. Result Analysis. To evaluate and compare the network connectivity and efficiency, we adopt the robustness metrics including network connectivity, network efficiency, and variation ratio of robustness after disruptions.

5.3.1. Impact of Random Disruption. Firstly, we measure the network performances in terms of normalized connectivity and efficiency under the impact of random disruption. We randomly remove the nodes and add the ratio of removed nodes from 0 to 100%.

In Figure 6, the normalized network connectivity and efficiency decrease with increasing the ratio of removed nodes. Compared with the normalized network connectivity, the decreasing speed of normalized network efficiency is faster. These results indicate that, after the random disruption occurs, the nodes reselect the shortest path to the destination to maintain keep good network connectivity. However, the reselected paths are suboptimal in having a larger length than the failure path. Therefore, when good network connectivity is kept, the network efficiency is unavoidably lost.

5.3.2. Impact of Targeted Disruption. We measure the normalized size of the largest connected component under the impact of targeted disruption. Specifically, we sort the nodes according to the directed betweenness of node centrality. Then, we remove a portion of TopK nodes from

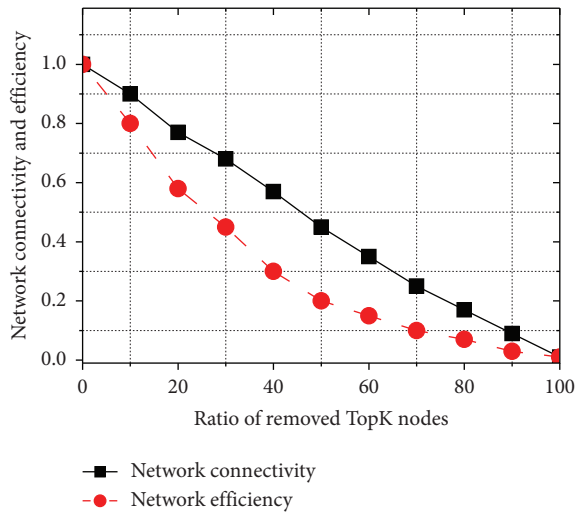


Figure 6: Network connectivity and efficiency under random disruptions.

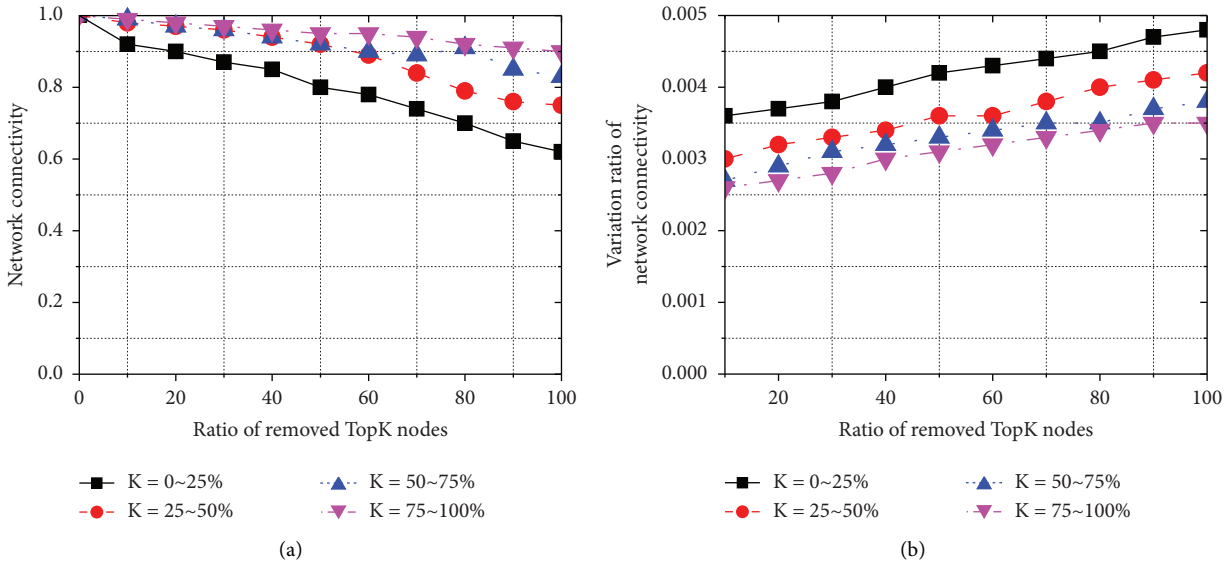


Figure 7: Network connectivity under targeted disruption. (a) Network efficiency. (b) Variation ratio of network efficiency.

the network to simulate the targeted disruption. To investigate the impacts of nodes with different directed betweenness, we increase the ratio of removed nodes in the top 0–25%, 25–50%, 50–75%, and 75–100% nodes of the whole network.

Figure 7 shows the network connectivity with varying ratios of removed TopK nodes. Figure 7(a) shows that if the removed nodes are in the top 0–25% of all nodes, the network connectivity decreases faster than the other cases. For example, if all top 25% nodes are lost, the size of the largest connected component in the remaining network drops to only 61%. Figure 7(b) shows the variation ratio of network connectivity with different ratios of removed nodes. The top 25% nodes have the largest variation ratio of network connectivity. This result indicates that the top 25% nodes in directed betweenness play the most important roles in ensuring network connectivity.

5.3.3. Network Efficiency under Targeted Disruption. Under the targeted disruptions, the network efficiency is also degraded. Figure 8 shows the network efficiency when the nodes are removed.

Figure 8(a) shows that if the removed nodes are in the top 25% nodes, the network efficiency is the lowest. Since the nodes of the shortest paths are removed, the paths other than the shortest one are employed to keep connections from the suppliers to customs, leading to suboptimal network efficiency. The results shown in Figure 8(b) also verify this observation. The top 25% nodes have the largest variation ratio of network efficiency.

6. Evaluation on Rewiring Algorithm

In this section, we evaluate the performance of the rewiring algorithm in a data-driven test. We use the data from a

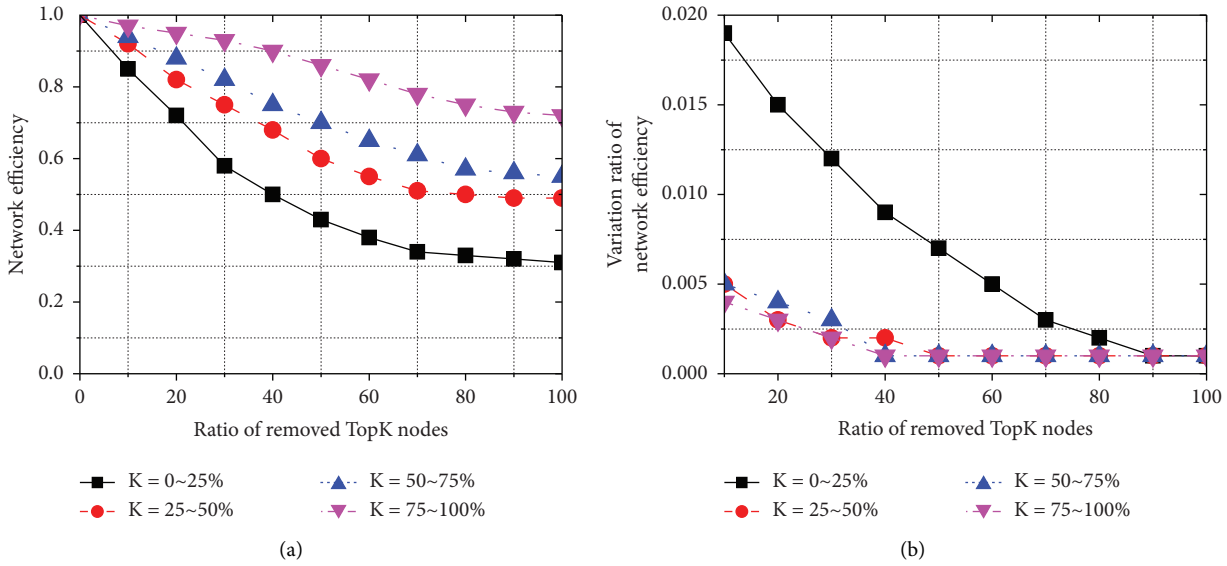


Figure 8: Network efficiency under targeted disruption. (a) Network efficiency. (b) Variation ratio of network efficiency.

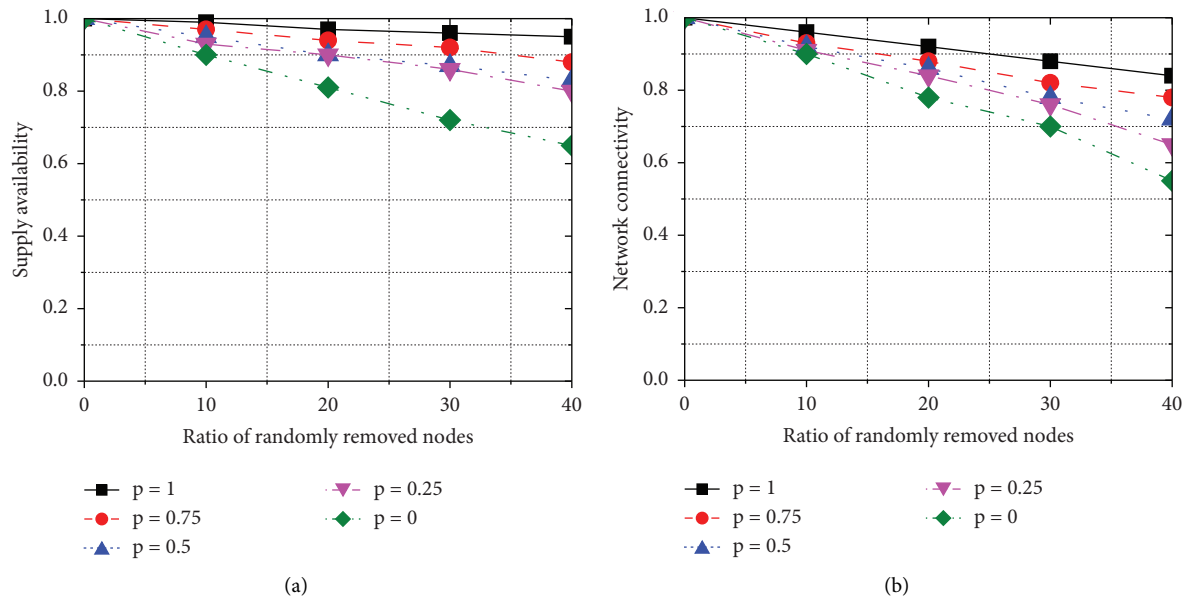
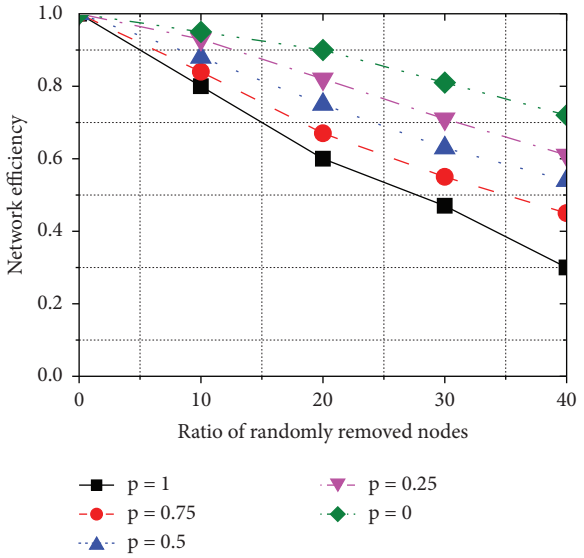
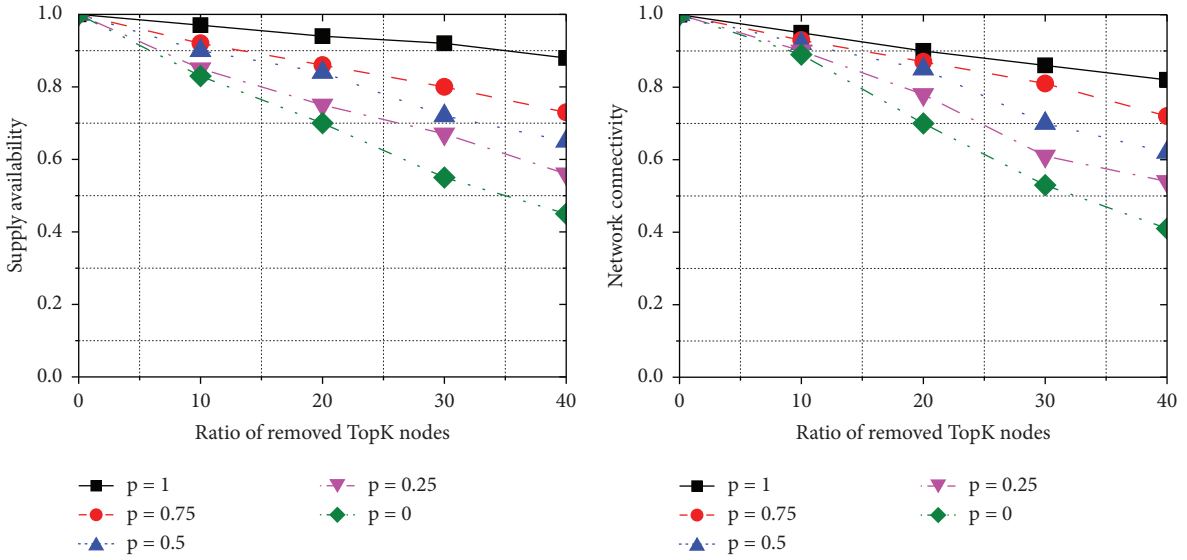


Figure 9: Continued.



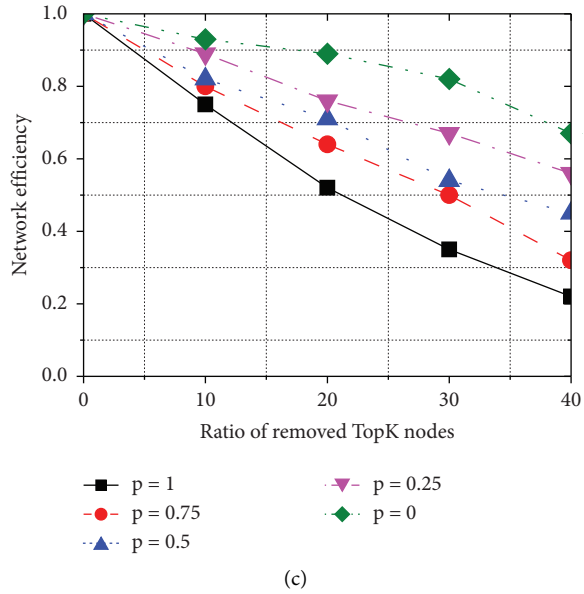
(c)

Figure 9: Military logistic network under random disruption. (a) Supply availability. (b) Network connectivity. (c) Network efficiency.



(a) (b)

Figure 10: Continued.



(c)

Figure 10: Military logistic network under targeted disruption. (a) Supply availability. (b) Network connectivity. (c) Network efficiency.

typical military logistic network [10], which has 1000 nodes, including 150 supply, 550 demand, and 300 relay nodes. To conduct a comprehensive performance evaluation, we change the rewiring probability p after disruptions.

In the test, we use the supply availability as the metric to test if the supplier can successfully deliver supplies to customers. Specifically, consider a supply chain network with the supplier, customer, and relay nodes. We use V_C and V_S to denote the two nonoverlapping subsets of customer and supply nodes, respectively. Meanwhile, we use V_C^* to denote the set of customer nodes that can connect to supply nodes through delivery paths. That is,

$$V_C^* = v_i \in V_C | \exists v_j \in V_S : \exists p_{ij}. \tag{6}$$

The supply availability SV is the ratio between the cardinalities of sets V_C^* and V_C as

$$\text{SV} = \frac{|V_C^*|}{|V_C|}. \tag{7}$$

In the test, we measure the supply availability, network connectivity, and network efficiency under the random and targeted disruptions.

Figure 9 shows the network performance when the nodes are randomly removed. If p equals 0, the rewiring operation is not triggered. Figure 9(a) shows the higher rewiring probabilities p lead to larger supply availability. Figure 9(b) shows that the rewiring approach greatly increases network connectivity. When the ratio of randomly removed nodes is 40%, the connectivity improvement is up to about 45%. However, through the rewiring operation achieving better performances of availability and connectivity, Figure 9(c) shows that the rewiring operation degrades the delivery efficiency. When the rewiring probability p increases, the nodes have more chances to reselect suboptimal paths, resulting in lower network efficiency.

To simulate the targeted disruption, we remove nodes by the order of directed betweenness. Compared with the case of random disruption, Figure 10(a) shows that the supply availability decreases faster under targeted disruptions since the conjunction nodes are removed by purpose. Figure 10(b) shows that the rewiring algorithm greatly improves network connectivity. Figure 10(c) shows the rewiring leads to loss of network efficiency. Fortunately, the efficiency loss is acceptable, since the supply availability and network connectivity are greatly improved.

7. Conclusion

In this paper, we explore how to improve the robustness of large-scale supply chain networks from the topological perspective. We analyze the topological metrics such as the largest connected component, average path length, and average clustering coefficient in the supply chain network. Based on the measurement results of real data trace, we reveal that the directed betweenness can indicate the node importance more accurately in the large-scale supply chain network compared with the undirected betweenness. Then, we propose a rewiring algorithm based on directed betweenness to improve network robustness under disruptions. The results of the data-driven test in the real supply chain network show that our design greatly improves the network robustness in terms of supply availability and network connectivity in presence of random and targeted disruptions.

There are some issues that will be addressed in the future. Firstly, the rewiring algorithm only considers one metric in searching the shortest path, while there may exist multiple targets in the supply chain. We will investigate how to combine the metrics which could reflect different objects in delivering goods, such as minimizing delay, cost, and risk. Meanwhile, the probability of rewiring operation needs to be

further optimized. We would like to propose a self-adjustment scheme to tune the probability of rewiring operation according to different requirements from users.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] J. Wang, R. R. Muddada, H. Wang et al., "Toward a resilient holistic supply chain network system: concept, review and future direction," *IEEE Systems Journal*, vol. 10, no. 2, pp. 410–421, 2016.

[2] T. Wu, J. Blackhurst, and P. O'grady, "Methodology for supply chain disruption analysis," *International Journal of Production Research*, vol. 45, no. 7, pp. 1665–1682, 2007.

[3] M. M. Queiroz, D. Ivanov, A. Dolgui, and S. Fosso Wamba, "Impacts of epidemic outbreaks on supply chains: mapping a research agenda amid the COVID-19 pandemic through a structured literature review," *Annals of Operations Research*, vol. 289, pp. 1–38, 2020.

[4] D. Ivanov and A. Dolgui, "OR-methods for coping with the ripple effect in supply chains during COVID-19 pandemic: managerial insights and research implications," *International Journal of Production Economics*, vol. 232, Article ID 107921, 2021.

[5] C. W. Craighead, D. J. Ketchen, and J. L. Darby, "Pandemics and supply chain management research: toward a theoretical toolbox," *Decision Sciences*, vol. 51, no. 4, pp. 838–866, 2020.

[6] H. Elleuch, E. Dafaoui, A. Elmhamedi, and H. Chabchoub, "Resilience and vulnerability in supply chain: literature review," *IFAC-Papers Online*, vol. 49, no. 12, pp. 1448–1453, 2016.

[7] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215–239, 1978.

[8] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 391, no. 4, pp. 1777–1787, 2012.

[9] G. Sabidussi, "The centrality index of a graph," *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.

[10] H. P. Thadakamalla, U. N. Raghavan, S. Kumara, and A. Albert, "Survivability of multiagent-based supply networks: a topological perspective," *IEEE Intelligent Systems*, vol. 19, no. 5, pp. 24–31, 2004.

[11] D. Ivanov, "Disruption tails and revival policies: a simulation analysis of supply chain design and production-ordering systems in the recovery and post-disruption periods," *Computers & Industrial Engineering*, vol. 127, pp. 558–570, 2019.

[12] T. Sawik, "Integrated selection of suppliers and scheduling of customer orders in the presence of supply chain disruption risks," *International Journal of Production Research*, vol. 51, no. 23-24, pp. 7006–7022, 2013.

[13] D. Ivanov, "Revealing interfaces of supply chain resilience and sustainability: a simulation study," *International Journal of Production Research*, vol. 56, no. 10, pp. 3507–3523, 2018.

[14] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted disruptions," *IEEE Systems Journal*, vol. 5, no. 1, pp. 28–39, 2011.

[15] L. Geng, R. Xiao, and S. Xie, "Research on self-organization in resilient recovery of cluster supply chains," *Discrete Dynamics in Nature and Society*, vol. 2013, no. 11, Article ID 758967, 2013.

[16] K. Zhao, A. Kumar, and J. Yen, "Achieving high robustness in supply distribution networks by rewiring," *IEEE Transactions on Engineering Management*, vol. 58, no. 2, pp. 347–362, 2011.

[17] S. K. Paul, S. Asian, M. Goh, and S. A. Torabi, "Managing sudden transportation disruptions in supply chains under delivery delay and quantity loss," *Annals of Operations Research*, vol. 273, no. 1-2, pp. 783–814, 2019.

[18] S. M. Ali, S. K. Paul, P. Chowdhury et al., "Modelling of supply chain disruption analytics using an integrated approach: an emerging economy example," *Expert Systems with Applications*, vol. 173, Article ID 114690, 2021.

[19] V. Gupta, B. He, and S. P. Sethi, "Contingent sourcing under supply disruption and competition," *International Journal of Production Research*, vol. 53, no. 10, pp. 3006–3027, 2015.

[20] P. Singhal, G. Agarwal, and M. Mittal, "Supply chain risk management: review, classification and future research directions," *International Journal of Business Science and Applied Management*, vol. 3, pp. 15–42, 2011.

[21] S. P. Willems, "Real-world multi-echelon supply chains used for inventory optimization: online appendix," *Manufacturing and Service Operations Management*, vol. 1, pp. 19–23, 2006.