

Research Article

Modelling Underload Cascading Failure and Mitigation Strategy of Supply Chain Complex Network in COVID-19

Hong Liu ^{1,2}, Yunyan Han,³ Jinlong Ni ^{1,2} and Anding Zhu ^{2,3}

¹School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

²Contemporary Business and Trade Research Center of Zhejiang Gongshang University,
Key Research Institute of Humanities and Social Sciences of the Ministry of Education, Hangzhou 310018, China

³School of Management and E-Business, Zhejiang Gongshang University, Hangzhou 310018, China

Correspondence should be addressed to Jinlong Ni; nijl@mail.zjgsu.edu.cn

Received 22 September 2021; Revised 27 December 2021; Accepted 5 January 2022; Published 21 February 2022

Academic Editor: A. M. Bastos Pereira

Copyright © 2022 Hong Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The outbreak of COVID-19 has caused problems such as shortage of workforce, cost increase, cash flow tension, and uncertainty of supply chain. It has a specific negative impact on the raw material supply, procurement management, production resumption, logistics, and market of the supply chain, which can trigger cascading failures in supply chain networks. Aiming at the failure of upstream/downstream firms in supply chain networks due to the decreased product demand/material supply under the COVID-19, the present study adopted an underload cascading failure model for the supply chain networks. In this model, the hierarchical supply chain networks were constructed based on the Erdos Renyi (ER) model and Barabasi Albert (BA) model. The validity of the model was verified under random attack and target attack. In the random attack mode, the influences of model parameters were studied, and in the target attack mode, the influence of target protection and random protection measures on enhancing network invulnerability was also studied. Simulation results showed that the initial load and capacity lower bound of nodes impact cascading failure size. The former has a positive correlation with cascading failure size, while the latter negatively correlates with cascading failure size. Furthermore, random protection measures are more practical to prevent cascading failures.

1. Introduction

The ongoing COVID-19 pandemic has posed severe disruptions on global supply chains [1, 2]. After the outbreak of the COVID-19 pandemic, firms faced more challenges such as labor shortage, cost increase, cash flow interruption, and the other uncertain emergencies of the supply chain, which have negative impacts on raw materials supply, procurement management, production resumption, and logistics and market in supply chains [3, 4]. A supply chain network is a functional chain network structure organized by a few various business entities like suppliers, manufacturers, distributors, and retailers, realizing from raw material purchase to finished product production and final sales [5]. As a dynamic network, the fluctuation of any part of the network can spread quickly in the whole network [6].

Cascading failure is one of the fundamental reasons for supply chain disruptions. Supply chains must consistently achieve robustness by trading off efficiency against vulnerability [7]. The international shipping costs have been rising to more than 400 per cent since the outbreak of COVID-19, resulting in port congestions and supply chain postponements all over the world [8]. On the other side, numerous companies went bankrupt due to COVID-19. According to statistics released by the Administrative Office of the U.S. Courts, there were more than one million bankruptcy filings from 2020 to 2021 [9]. Similarly, there were more than ten thousand company bankruptcies related to Japan's pandemic from 2020 to 2021 [10]. Every company bankruptcy may become the vulnerable point causing subsequent bankruptcies and weakening the robustness of the entire supply chain.

Cascading failure is a condition of interconnected systems when failure on one part can lead to a subsequent failure in corresponding parts and finally cause an overall failure at the system level [11]. Cascading failures in supply chain networks have attracted much attention in recent years. Extant studies mainly focus on network vulnerability [12], cascading failure model [11], and emergency recovery mechanism [13]. However, in conventional studies, the failure is always assumed to be temporary, preidentified, overloaded, and recoverable. For example, Lu et al. studied the robust optimization design under the risk of supply chain network interruption, integrated the emergency strategy into the supply chain network design, and established a robust mixed-integer programming model based on a multiscenario, multiperiod, and single product [14]. Gao and Chen established a cascaded failure model of supply chain networks based on the complex network theory, in which the weak link of a network was identified, and the quantitative evaluation method of supply chain vulnerability was proposed [15]. Yan et al. established the cascade effect method of supply chain network system detection and gave the dynamic node importance evaluation method, based on the theory of complex networks [16]. He and Cheng studied the repair mechanism of the supply chain based on the directed weighted complex network, simulated the damaged situation of the supply chain by adjusting the link weight of the supply chain network, allocated limited repair resources, and repaired the supply chain from the global damage and node damage [17]. Recently, Saura et al. proposed an artificial intelligence-based model to capture the dynamic feature of supply chain networks [18].

However, the cascading failure caused by COVID-19 is quite different from the previous ones. Under the influence of COVID-19, firms will fail due to the decreased product demand or raw materials supply, which belongs to underload failure. Meanwhile, it is a sudden attack on the supply chain with a subsequently long-term and continuous disruption. There is a lack of dynamic models for investigating supply chain disruption under COVID-19. First of all, we identify the following:

- (1) In the traditionally cascading failure models, the upper bound of node capacity is considered (i.e., node failure occurs when the node load exceeds the upper bound of capacity). At the same time, the firms under the influence of COVID-19 are faced with the problem of decreasing product demand or insufficient raw materials supply, whose node failure occurs when the node load is lower than the capacity lower bound.
- (2) In the traditionally cascading failure models, when the node load exceeds the upper bound of capacity, the firm cannot consume many supply orders or demand orders. It will consider giving these orders to other firms with a close cooperation relationship. However, the load of firms in the supply chain network caused by the COVID-19 will be lower than the capacity lower bound, and the load of other firms with close cooperation will be reduced.

We adopt Wang's underload cascading failure model in supply chain networks [19]. More specifically, we adapted the model from three aspects: firm underload failure, firm capacity lower bound, and load redistribution according to the business relationship between firms. On the other side, how does COVID-19 attack the supply chain? How can we improve the supply chain to mitigate the disruption caused by COVID-19? To answer these questions, we adopt two attack strategies: random attack and target attack to test the model's performance. By numerical simulating, we find that it is crucial to maintain close cooperation among supply chain firms to survive the epidemic. Besides, target protection and random protection can improve the survivability of supply chain networks.

Moreover, random protection is more effective than target protection. It is more effective to protect small- and medium-sized firms. Our results implicate that enhancing cooperation relationships within a supply chain network is an effective method to fight against COVID-19.

The rest parts of the paper are organized as follows. In Section 2, we have a brief systematic review of cascading failure related to supply chain networks. Furthermore, in Sections 3 and 4, we present the adapted fundamental model of underload cascading failure and the cascading failure process due to the COVID-19 pandemic. Several numerical simulations are conducted in Section 5. Finally, we draw several conclusions and implications specific to the situation of COVID-19 in Sections 6 and 7.

2. The Cascading Failure Phenomena in Supply Chain Network

Each firm has its capacity, inventory, and demand for raw materials in the supply chain network. When the output of a firm is lower than the minimum production requirements of its operation due to the lack of orders or raw materials, considering the cost problem and profit purpose, the firm may consider suspending production or closing in severe cases. Furthermore, other firms with business contacts with this firm will also be affected, resulting in their output reduction. This process is repeated in the supply chain network, spreading failures and subsequent failures. The successive failures in the supply chain network mean that the failures of one or a few firms will cause the failures of other firms through the supply-demand connection between firms and eventually lead to the failures of a considerable part of the failures of the whole supply chain [20–23].

The recent outbreak of the COVID-19 has had a specific impact on the supply of raw materials for firms [24]. This negative effect may be due to shortage or interruption of logistics, especially raw materials or components from high incidence areas of the COVID-19 and even high transportation areas. Taking the automobile supply chain as an example, it is a complex and huge system including various suppliers, manufacturers, logistics providers, distributors, whose general structure is shown in Figure 1, where each node represents a supplier, manufacturer, logistics provider, distributor, and its main body is the material supply system such as parts and components. There are more than 100,000

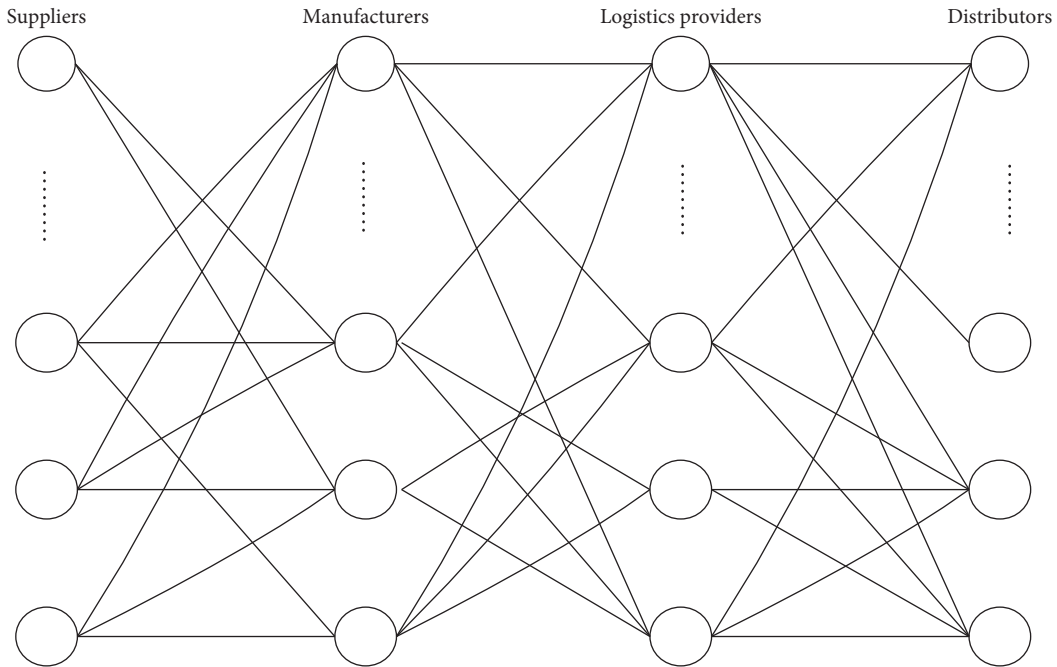


FIGURE 1: A general structure of the automobile supply chain.

Chinese auto parts firms and more than 13,000 firms above the designated size [24]. More than 10,000 foreign-invested auto parts firms have already established production and R & D bases in China. China's essential auto parts manufacturing base is the most seriously affected by the COVID-19, Hubei Province. More than 1,300 auto parts firms are above the designated size, including Bosch, Delphi, Valeo, Lear, Honeywell, and many other multinational auto parts firms. Automobile production involves tens of thousands of parts, thousands to tens of thousands of employees, and global materials procurement. Any abnormality in the supply of automobile parts will affect the production; the suspension of some or some upstream suppliers will lead to the "chain break" crisis in the supply chain and cascade failure [25]. At present, automobile firms are gradually resuming production, but the comprehensive recovery of production capacity needs the efficient operation and synchronous cooperation of the whole supply chain system. As the parts and components firms in Hubei lag the whole country, it has directly affected many domestic mainstream automobile firms and even many international automobile firms, resulting in the closure and suspension of production of some factories or models.

The COVID-19 also has an impact on procurement management. The procurement supply chain is a network system, and the procurement bases are often distributed throughout the country and even around the world. However, due to the prevention degree of COVID-19 and the difference of COVID-19 situation in different regions, the procurement management of firms is faced with significant uncertainty and adjustment risk, which significantly reduces the efficiency of firms. Taking China's auto parts as an example, China is the world's most significant auto production and sales country and one of the most crucial

auto parts manufacturing and supply bases in the world. However, many auto parts, materials, and equipment still need to be imported from abroad: Germany, Japan, South Korea, the United States, etc. At present, most of these countries are high-risk countries. If suppliers in the above countries stop supplying due to the COVID-19, many of the auto parts they supply cannot be replaced. Even if they can be replaced, it will take time. At present, many parts companies and most auto companies in Europe have announced to stop production or partially stop production. Besides, core components and semiconductor products produced by Japan, South Korea, and the United States are also widely used in the automobile industry. Most of the vehicle firms have a large stock of imported spare parts. If the COVID-19 situation worsens, the spare parts firms and material firms in these countries and regions stop production and supply; the domestic firms will be unable to continue production after the stock is used up. The production of Chinese automobiles and spare parts will face a direct impact, which directly affects the regular operation of the whole automotive supply chain network.

The cascading failure literature has many studies. Zhang and Liu studied the vulnerability measurement of the logistics service supply chain, analyzed the interaction law of internal nodes of the logistics service supply chain, and determined the network vulnerability measurement index [12]. Liu et al. constructed a conceptual model for supply chain vulnerability and discussed the impact mechanism of various factors on supply chain vulnerability [26]. Yu et al. studied the complexity and vulnerability of the supply chain network structure under the modern production mode and proposed an analysis method based on the weighted improved node contraction method [27]. Zeng and Zhao proposed a dynamic network load entropy method and

discussed the vulnerability of the cluster supply chain network in the process of cascading failure propagation [28]. Du et al. concluded that moral risk, market risk, and decision-making risk would greatly increase the supply chain's vulnerability, based on the complexity of supply chain integration, operation, and environment [29]. Liu analyzed the supply chain's vulnerability from the perspectives of supply, demand, and environment, established the vulnerability analysis model of the supply chain, and made a statistical analysis of the vulnerability [30]. Tang et al. studied the cascading failure mechanism and the associated supply chain network [31]. Li et al. established a network model with a uniform degree and random distribution and a cascaded failure and invulnerability model, according to the characteristics of the logistics support network [32, 33]. Tang et al. considered the characteristics of nodes such as recovery and repeated failure, constructed a cascaded failure model under the probability propagation mode of fault nodes, and comprehensively analyzed the performance trade-off between edge robustness and node robustness [34]. Tang et al. analyzed the cascading failure characteristics and the robustness of an interdependent supply chain network, which is a typically interdependent network composed of an undirected cyber-layer network and a directed physical-layer network [35]. Geng et al. studied the self-organizing elastic recovery characteristics of the cluster supply chain network [36]. Wang and Xiao studied the cascading failure in the cluster supply network and proposed a resilience method to cascading failures in the cluster supply chain network by leveraging the social resilience of ant colonies [37, 38]. The next sections will employ an underload cascading failure model to investigate the COVID-19 disruption in supply chain networks.

3. The Underload Cascading Failure Model

With the outbreak of the COVID-19, the cascading failure process in the supply chain network is as follows: the upstream firms' products fail due to the decline of demand, and the downstream firms fail due to the lack of material supply. Both the decrease in product demand and the shortage of material supply can be regarded as a load decrease. When the load decreases below the lower bound of capacity, it will cause failure, triggering cascading failure. Therefore, the underload failure model can better describe the level linkage mechanical behavior in the supply chain network. The following definitions are given to describe better the underload cascading failure in the supply chain network.

In the process of modeling, the supply chain network is represented as a directed graph structure in the form of $G = (V, E)$, where $V = \{v_1, v_2, \dots, v_N\}$ is the set of nodes (representing the firms), and the node types include supplier node, manufacturer node, distributor node, and retailer node. $E = \{e_1, e_2, \dots, e_M\}$ is the set of edges (representing the business relations between firms), if the upstream firm node v_i and the downstream firm node v_j has business relations, node v_i and node v_j are connected by a directed edge as $\langle v_i, v_j \rangle$, and the corresponding element in E is $e_{ij} = 1$; otherwise, $e_{ij} = 0$.

3.1. Initial Load. In the cascading failure model, the allocation of the initial load is based on the importance of nodes. Generally, two ways are often used to define a node's initial load as degree approach [39, 40] and the betweenness approach [41–43]. Considering that in the supply chain network, the effective operation of a firm is more and more dependent on other firms, especially its upstream and downstream firms, which are closely connected through business relations. That is to say, a load of a node is naturally closely related to that of its neighbors. So, we consider the way in [44] to define the initial node load as follows:

$$L_i^0 = \left[d_i \sum_{j \in A_i} d_j \right]^\alpha, \quad (1)$$

where L_i^0 is the initial load of node v_i , $d_i = d_{I_i} + d_{O_i}$ is the degree of node v_i , and d_{I_i} is the number of edges from the upstream neighbor nodes to node v_i , d_{O_i} is the number of edges from node v_i to the downstream neighbor nodes. A_i is the neighbour nodes set of node v_i , d_j is the degree of the neighbor node v_j of node v_i . α is an adjustable parameter that governs the initial load strength of nodes.

3.2. Lower Bound of Node Capacity. In the actual network, the ability of nodes to handle the load (i.e., capacity) is usually limited by cost and other factors. The goal of the supply chain network is to provide products for the end-users, and the firms in each link are all for the ultimate purpose of making profits. If the product demand or raw material supply is lower than a certain level, the firm will not operate normally and will eventually suspend production or shut down due to its inability to make profits. Therefore, the load to maintain the regular operation of the firm must be higher than a specific bound. Underload will lead to firm failure. Considering that the failure of the supply chain under the COVID-19 is caused by underload, this paper only considers the capacity lower bound of a firm, which is proportional to its initial node load L_i^0 [37], and is defined as follows:

$$C_i = \beta L_i, \quad i = 1, 2, \dots, N, \quad (2)$$

where C_i is the capacity lower bound of node v_i and $0 \leq \beta \leq 1$ is the lower bound parameter.

3.3. Redistribution of Load. When the supply or demand of firms declines, the firms with a closer business relationship are most affected. In the supply chain network, a load of each node at first is more significant than the capacity lower bound, that is to say, a load of any node satisfies: $C_i \leq L_i$, at this time, the network is in "steady state"; however, in the COVID-19 environment, the supply and demand of nodes in the network are slowly decreasing. When $L_i < C_i$, node failure occurs, that is, due to the cost and other factors, firms will choose to stop production, which shows that this node load will affect the load change of other nodes. This paper defines load redistribution according to the business relationship strength between firms [45], which is expressed as follows:

$$\begin{aligned}\Delta L_{ij} &= L_i \frac{L_j}{\sum_{m \in A_i} L_m}, \\ &= L_i \frac{\left[d_j \sum_{k \in A_j} d_k \right]^\alpha}{\sum_{m \in A_i} \left[d_m \sum_{h \in A_m} d_h \right]^\alpha},\end{aligned}\quad (3)$$

where ΔL_{ij} is the reduced load of the upstream or downstream nearby node v_j of node v_i , A_i is the neighbor nodes set of a failure node v_i .

For the node c in Figure 2, if it fails at time t , its upstream nearby nodes a and b , and downstream nearby nodes d and e will suffer losses. Taking the downstream node d as an example, its reduced load is as follows:

$$\begin{aligned}\Delta L_d &= L_i \frac{L_j}{\sum_{m \in A_i} L_m} \\ &= L_c \frac{L_d}{L_a + L_b + L_d + L_e} \\ &= L_i \frac{\left[d_j \sum_{k \in A_j} d_k \right]^\alpha}{\sum_{m \in A_i} \left[d_m \sum_{h \in A_m} d_h \right]^\alpha} \\ &= L_c \frac{\left[d_d \sum_{k \in A_d} d_k \right]^\alpha}{\left[d_a \sum_{i \in A_a} d_i \right]^\alpha + \left[d_b \sum_{j \in A_b} d_j \right]^\alpha + \left[d_d \sum_{k \in A_d} d_k \right]^\alpha + \left[d_e \sum_{l \in A_e} d_l \right]^\alpha} \\ &= L_c \frac{\left(d_d d_c + d_d d_f + d_d d_g \right)^\alpha}{\left(d_a d_c \right)^\alpha + \left(d_b d_c \right)^\alpha + \left(d_d d_c + d_d d_f + d_d d_g \right)^\alpha + \left(d_e d_c + d_e d_g \right)^\alpha}.\end{aligned}\quad (4)$$

And its load currently is $L_d(t) = L_d(t-1) - \Delta L_d$, if $L_i(t) < C_d$, then node d will fail at time $t+1$. For upstream nodes, the same mode of action occurs in the opposite direction. The cascading failure ends when no new nodes fail due to underload.

3.4. Evaluation Index. With the development of COVID-19, the node load often lies between the initial load and the capacity lower bound; that is, the node state in the model is divided into a normal state, underload, and failure state. In this paper, we consider the way in [46] to define the whole network efficiency based on node efficiency to measure the performance of a supply chain network, and the network efficiency (denoted by EG) is expressed as follows:

$$\begin{aligned}\text{EG} &= \sum_{i=1}^N \frac{\text{eg}_i(t)}{N} \\ &= \sum_{i=1}^N \frac{s_i L_i(t) / L_i}{N},\end{aligned}\quad (5)$$

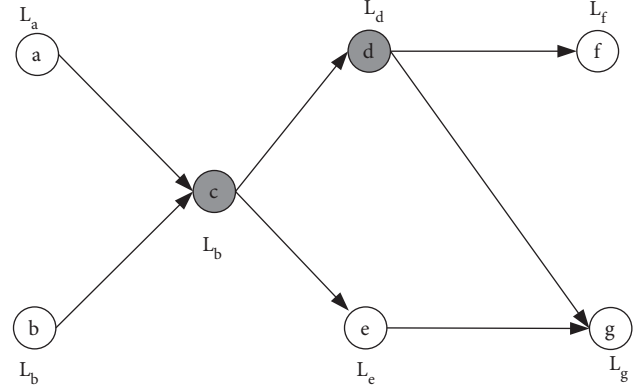


FIGURE 2: Illustration of the load redistribution after a node fails.

where $s_i \in [0, 1]$ indicates the status of each node, of which the value 0 indicates node failure, the value 1 indicates regular node operation, and the other values indicate node efficiency reduction due to underload. In the paper, we assume that all nodes typically work initially, $s_i = 1$. $L_i(t)$ represents the load of the node v_i at time t .

4. The Cascading Failure Process

Based on the above definitions, the process of cascading failure model of supply chain network proposed is as follows:

- (1) Initial condition: network G , with N nodes, M edges, the initial load L_i^0 of node v_i ($i = 1, 2, \dots, N$), capacity lower bound C_i ($i = 1, 2, \dots, N$), node attack ratio p , and adjustable parameters α and β ($0 \leq \beta \leq 1$).
- (2) Node attack mode: when a random attack or target attack is carried out on network nodes, the load of the attacked nodes will be reduced in proportion to p .
- (3) Load redistribution of failure nodes: when a load of a node v_i is less than its capacity lower bound, the node fails, and its load is evenly distributed to its neighbor

nodes. The load redistribution strategy is used. That is, a load of its neighbor node is as follows:

$$\begin{aligned} L_j(t+1) &= L_j(t) - \Delta L_{ij}, e_{ij} \\ &= \langle i, j \rangle. \end{aligned} \quad (6)$$

- (4) For all adjacent nodes v_j ($j = 1, 2, \dots, N$) of node v_i , test their load L_j : if $L_j < C_j$, it causes cascading failure of nodes, and then $v_j \rightarrow v_i$, repeat (3), otherwise keep.
- (5) Simulation termination condition: for all nodes v_k ($k = 1, 2, \dots, N$) of the network, if $L_k \geq C_k$ the simulation is terminated.

5. Simulation and Analysis

Because most supply chain data are confidential or proprietary, building an entire supply chain network is very difficult. From the perspective of the complex network, the research on the supply chain network is mostly based on a typical network model, in which random network (Erdos Renyi, ER) [47] and scale-free network (Barabasi Albert, BA) are primary [48]. In this paper, the ER and BA networks are used to simulate the supply chain network to study its cascading failure dynamics under the COVID-19. Specifically, python 3.6 is used to code the ER and BA networks and the proposed model [49]. The network consists of 6,000 edges and 2,000 nodes. These nodes are divided into four types: supplier, manufacturer, distributor, and retailer. The supplier node is only associated with the manufacturer node, the manufacturer node is associated with the supplier and distributor node, and the distributor node is associated with the manufacturer and retailer node. The retailer is only associated with the distributor. Each experiment runs 20 times independently in the experiment, and the average value is taken as the simulation result [50].

5.1. Effect of Attack Strategies on Cascading Failures. Two attack strategies are generally adopted to trigger the cascading failure in the network: random attack and target attack. Random attack refers to the random selection of a certain proportion of network nodes for an attack. Target attack refers to selecting a certain proportion of important nodes in the network for an attack. In this paper, the random attack strategy adopted is to randomly select a certain proportion of nodes to reduce their load, and the target attack strategy is to select a certain proportion of nodes to reduce their load according to the descending order of node load.

Figure 3 shows the changes in network efficiency when the ER network and BA network face random attacks and target attacks under four kinds of parameter values. We can see from Figure 3 that EG is descending with the increase of attack ratio both in the ER network and in the BA network. Taking Figure 3(c) as an example, when the attack ratio is 20%, the EG of the ER network under random attack and target attack is 0.2825 and 0.0407, while that of the BA network under random attack and target attack is, respectively, 0.5127 and 0.7994. When the attack ratio is 50%, the

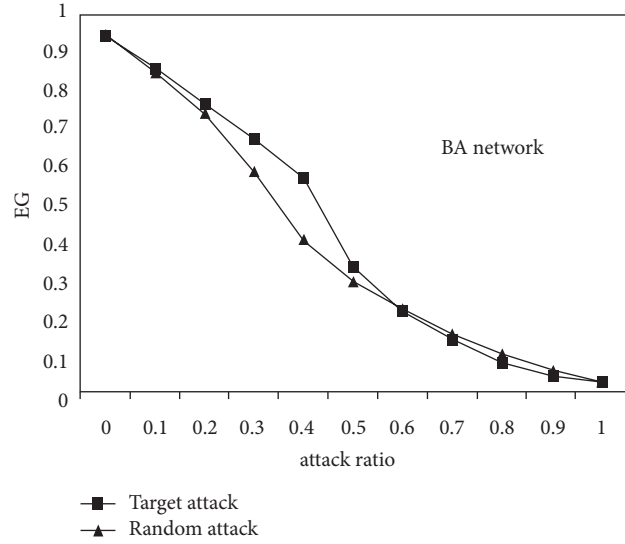
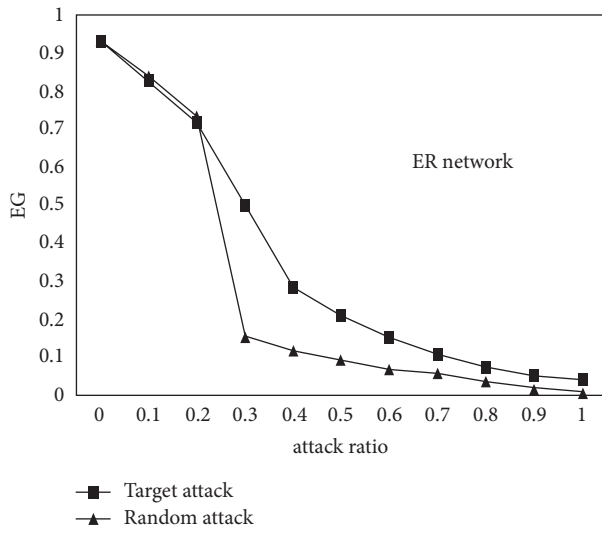
EG of the ER network under random attack and target attack is 0.0658 and 0.0322, while that of the BA network under random attack and target attack is, respectively, 0.1865 and 0.4998. The results of Figure 3 show that the cascading failures of the ER network and the BA network are more easily triggered by random attacks than by target attacks. Similar conclusions can also be found under other parameter combinations.

5.2. Effect of Model Parameters on Cascading Failures. The random attack is more likely to trigger cascading failure than the target attack known from Figure 4, so the following experiments are all carried out under the random attacks.

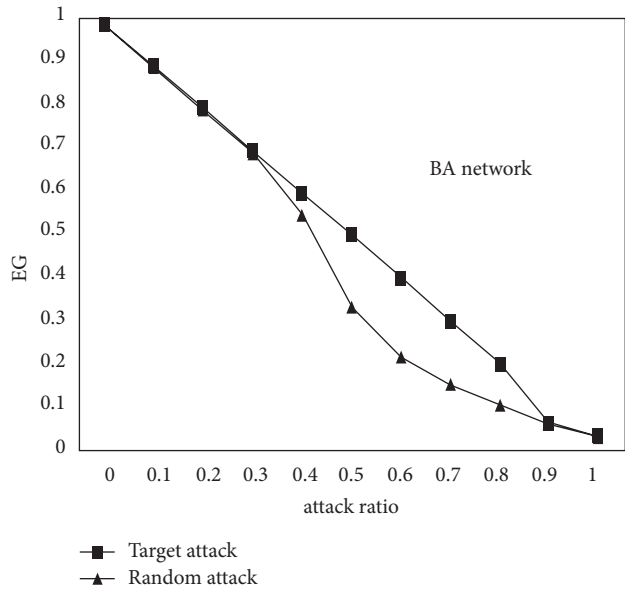
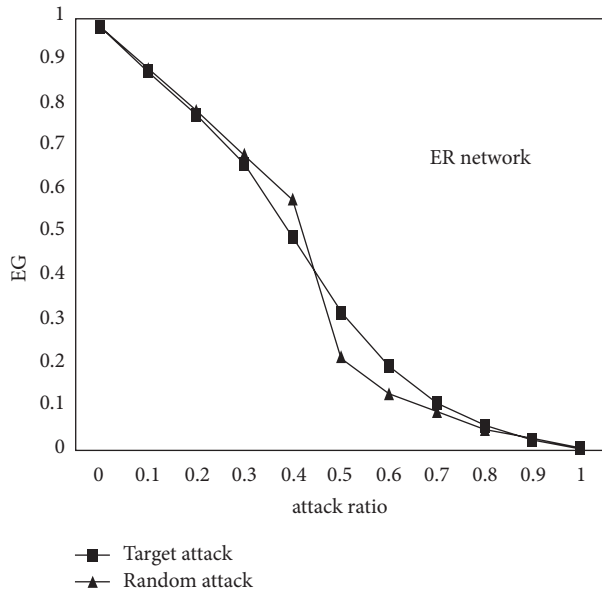
5.2.1. Effect of α on Cascading Failures. In the experiment, the other model parameters are $\beta = 0.5$, $p = 0.4$. Figure 4 shows the EG changes of two network models during cascading failures with different α , where α is used to control the load intensity of nodes. We can see from Figure 4 that EG is ascending with the increase of α both in the ER network and in the BA network. This indicates that the initial load of nodes defined according to the degree of nodes and the degree of neighbor nodes makes the network robust to cascading failure. When $\alpha = 0.8$ and $\alpha = 0.9$, the EG of the ER network changes dramatically after being attacked. It is shown that the robustness of the ER network against cascading failure is relatively weak under the condition of these two kinds of parameters. Furthermore, BA network also has similar performance.

5.2.2. Effect of β on Cascading Failures. In the experiment, the other model parameters are $\alpha = 0.9$, $p = 0.4$. Figure 5 shows the EG changes of two network models during cascading failures with different β , where β is used to control the capacity low bound of nodes. We can see from Figure 5 that EG is descending with the increase of β both in the ER network and in the BA network. It indicates that the higher β value is set (i.e., the minimum production demand of the firm), the more likely underload failure will occur, which is consistent with the actual situation. Furthermore, the lower the β value, the greater the firm's risk tolerance, and the longer the firm can support during the COVID-19. When a node fails, it will cause a loss to its neighbor nodes. If a load of neighbor nodes is close to the capacity lower bound, the loss may cause the further failure of neighbor nodes. The neighbour node can make up for the loss by strengthening the business relationship with other nodes with the same function as the failed node to reduce the possibility of its failure.

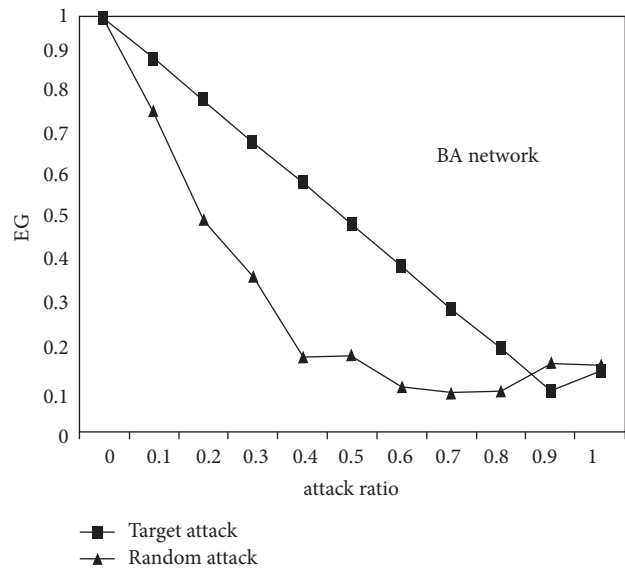
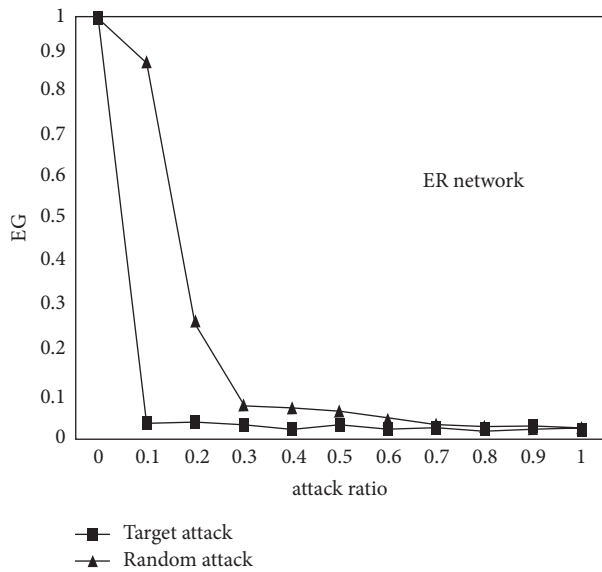
5.2.3. Effect of p on Cascading Failures. In the experiment, the other model parameters are $\alpha = 0.9$, $\beta = 0.6$. Figure 6 shows the EG changes of two network models during cascading failures with different p , where p is used to control the load reduction ratio of the attacked node. We can see from Figure 6 that EG is ascending with the increase of p both in the ER network and in the BA network, and the change of the ER network is more obvious than that of the BA network.



(a)



(b)



(c)

FIGURE 3: Continued.

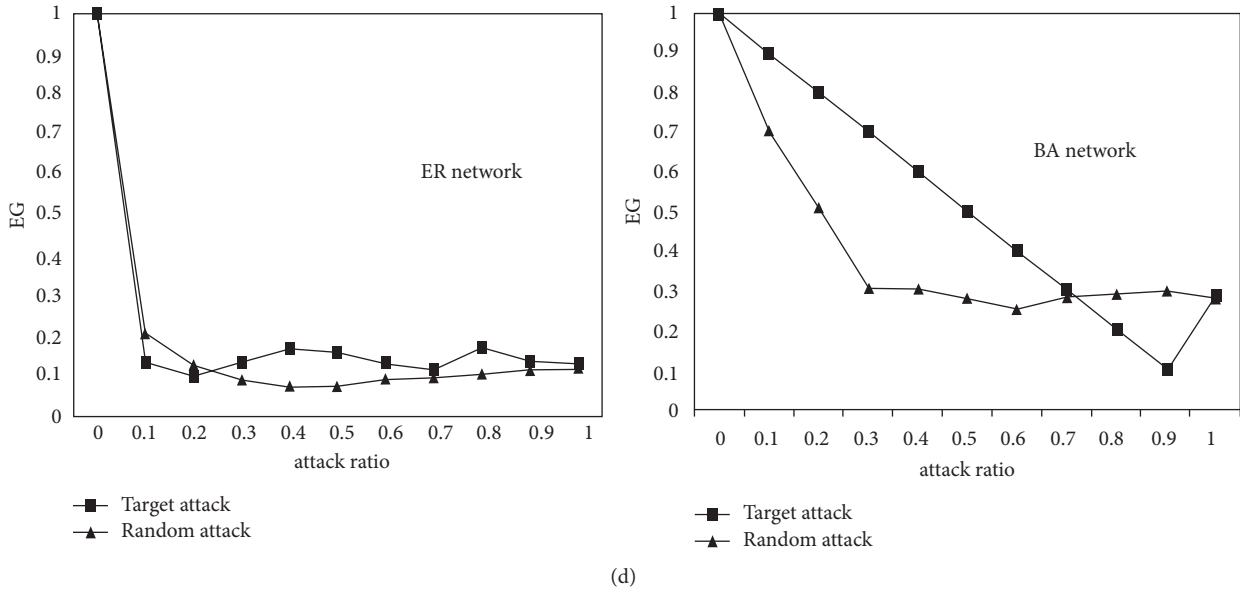


FIGURE 3: Network efficiency under different attack strategies. (a) $\alpha = 0.5, \beta = 0.6, p = 0.5$. (b) $\alpha = 0.8, \beta = 0.5, p = 0.4$. (c) $\alpha = 1.2, \beta = 0.7, p = 0.5$. (d) $\alpha = 1.5, \beta = 0.8, p = 0.6$.

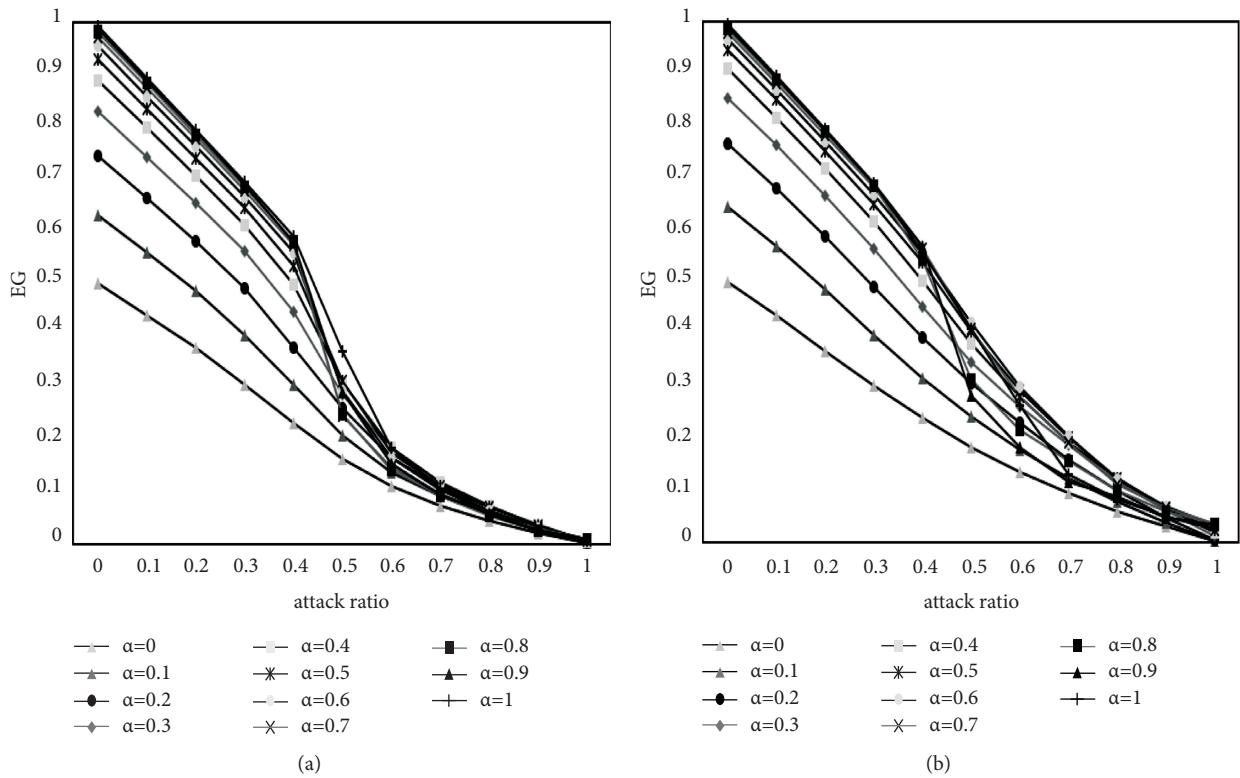


FIGURE 4: Network efficiency under different α . (a) ER. (b) BA.

When $p = 0.4$, that is to say, the attack node's load is reduced to $1 - p = 0.6 \leq \beta$ of the initial load, then there is no cascading failure, and the network efficiency is the largest at this time. When $p = 0.5$, the load of the attacked node is reduced to 50% of the initial load, i.e., $1 - p = 0.5 \leq \beta < 1 - p = 0.5 \leq \beta$; node failure occurs and affects the neighbor nodes,

triggering cascading failure. Currently, network efficiency is the minimum. It shows that the closer the load reduction is to the capacity lower bound, the more likely the nodes are to have cascading failures. At this time, if certain supporting measures are taken for such a firm, the ability of the firm to resist risks can be enhanced.

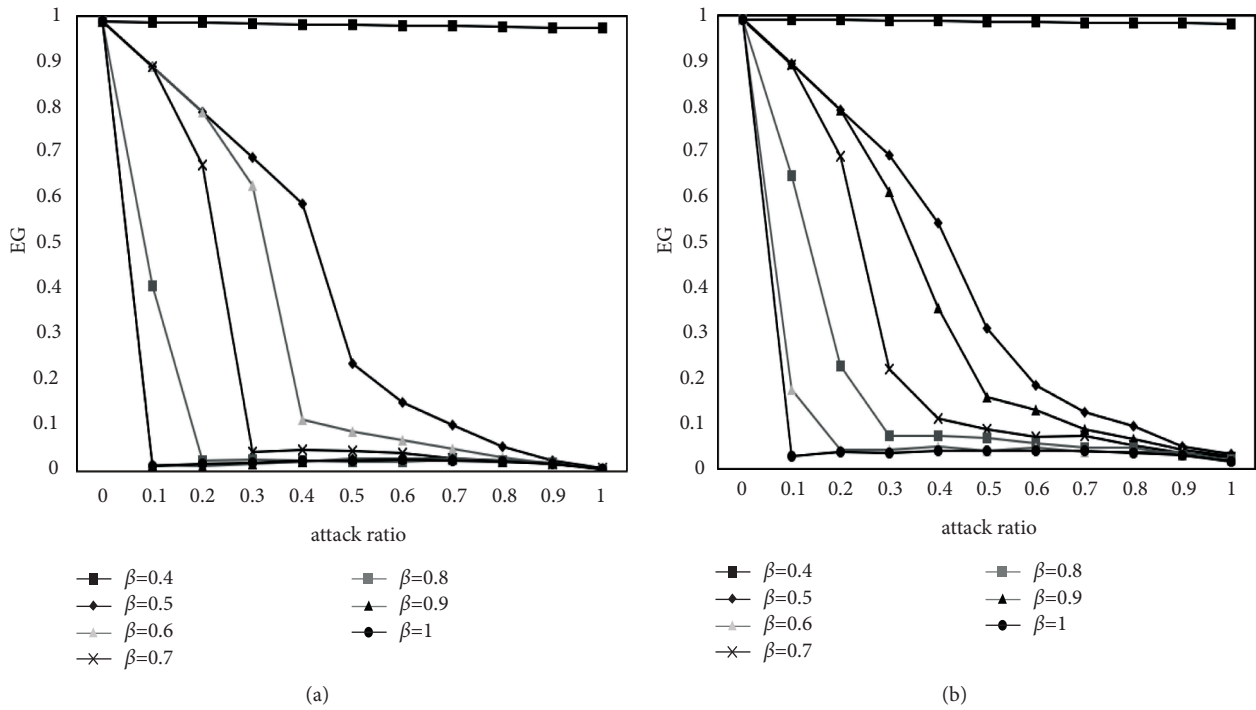


FIGURE 5: Network efficiency under different β . (a) ER. (b) BA.

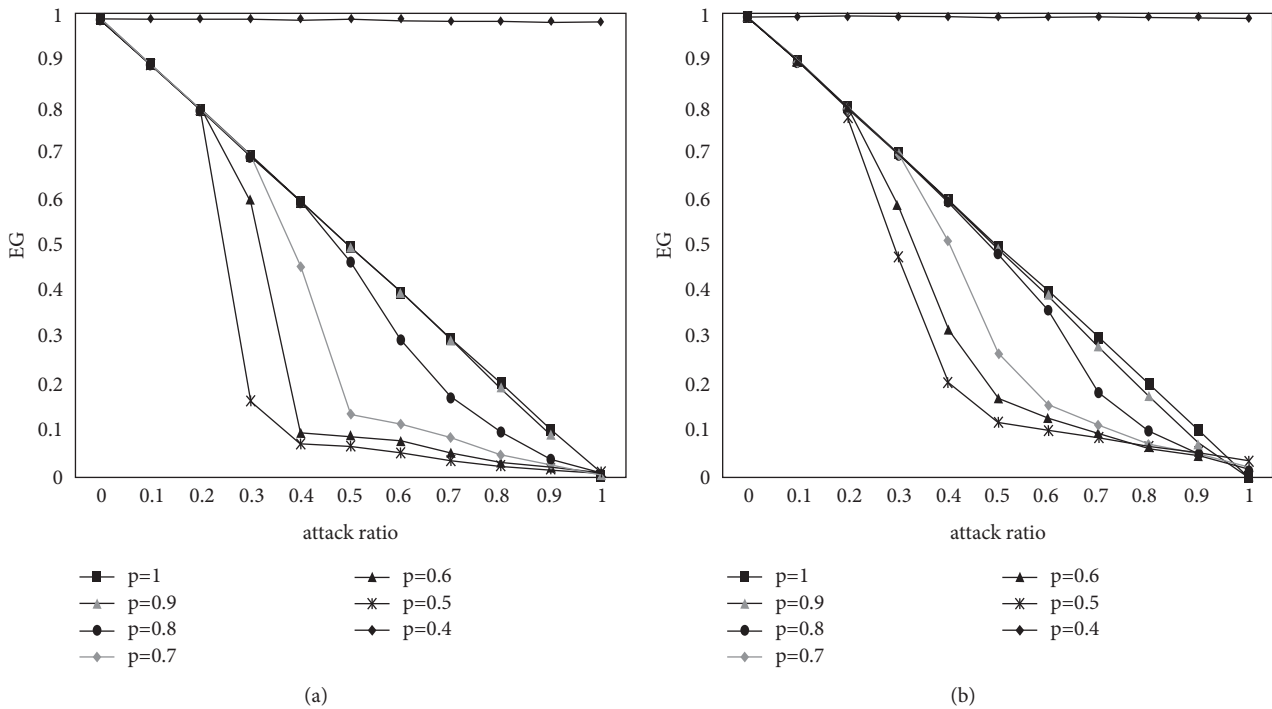


FIGURE 6: Network efficiency under different p . (a) ER (b) BA.

5.3. Effect of Protection Measures on Cascading Failures.

We study the effect of protection measures (such as loans to enterprises and rent reduction) on cascading failure control of the network under the target attacks. Two protection measures are used in the experiment: target protection and random protection. Target protection refers to selecting a

certain proportion of important nodes in the network for protection, while random protection refers to randomly selecting a certain proportion of network nodes for protection. The model parameters are set to $\alpha = 0.8$, $\beta = 0.4$, $p = 0.3$, and the proportion of nodes to be protected is 10% of the proportion of attack nodes, that is to say, select 10% of the

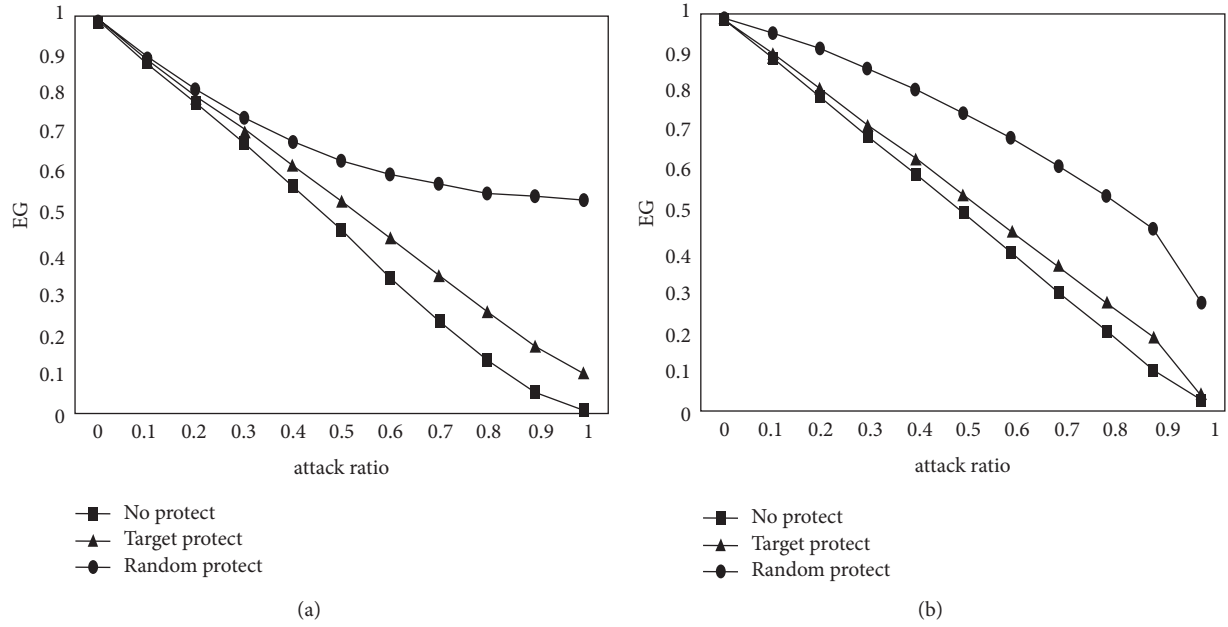


FIGURE 7: Network efficiency under different protection measures. (a) ER. (b) BA.

proportion of attack nodes according to the descending order of node load for target protection, or randomly select 10% of the proportion of attack nodes for random protection. Figure 7 shows the EG changes of two network models during cascading failures with different protection measures. We can see from Figure 7 that two kinds of protection measures can also improve the survivability of the ER network and BA network, and random protection measures are more effective than target protection measures. It shows that the protective measures for small- and medium-sized firms are more effective. Considering the complexity and diversity of business relationships among firms in the real supply chain network, it is difficult to measure it accurately. This conclusion can provide some reference for supply chain risk management during the COVID-19 period.

6. Conclusions and Discussion

In the present study, we propose an underload cascading failure model to investigate the negative outcomes of demand and supply declines caused by the ongoing COVID-19 pandemic. The extant supply chain network models are insufficient to explore the complicated and diverse characteristics among firms in the supply chain network. Our model simulates the actual situations after the outbreak of COVID-19 by redistributing the loads among connected nodes. We try to capture the characteristics of the connections among the upstream and downstream firms. The numerical simulations present that the network efficiency is positively related to the firm loads, while the network efficiency is negatively related to the lower bound of production capacity. The simulation results show that the loads and lower bounds' resilience will enhance the supply chain's robustness when preventing the cascading failures during COVID-19.

In addition, our model emphasises underload failure: upstream firms fail due to the decline of demand, and downstream firms fail due to the decrease of supply. Based on the underload failure, we analyze the effect of model parameters on the cascading failure of the supply chain network. The simulation results show that the adjustable parameters α and β , respectively, represent the firm's strength and the ability to resist risks, which will affect the spread of cascading failures. During the COVID-19, some protection measures for some firms will positively enhance the invulnerability of the entire supply chain network.

Finally, random attack strategies simulate the impact of failure caused by COVID-19 on the entire supply chain network composed of firms of variable sizes. The simulations of attacking the core nodes with large production scales show that the protection measures improve network efficiency. Although the core nodes play an essential role in maintaining the stability of the supply chain network system, providing protective measures for small- and medium-sized enterprises has more obvious effects on preventing network failure and improving network efficiency.

7. Theoretical and Practical Implications

Our study will contribute to the cascading failure literature on supply chain network systems. COVID-19 poses challenges to the extant theories of supply chain management. The negative outcomes of the COVID-19 are unpredictable and uncontrollable. We adapt the underload cascading failure mode to the actual situations of COVID-19, which have never happened before. The proposed model will be valuable for future studies. In addition, our study also has three practical implications. First, for large enterprises, increasing redundant partners in the supply chain network will help to reduce the mutual trust costs for temporary

cooperation purposes. Production capacity exchange with redundant cooperators will help reduce the failure rate of enterprise nodes. In addition, enterprises can appropriately increase the redundancy of raw materials and products, such as increasing inventory and backup products. They can also deal with the changes in demand or supply to maintain the regular production progress.

Second, our study implicates that we must pay attention to the production coordination of various small- and medium-sized enterprises in the supply chain. The problems of difficult and expensive financing of small and medium-sized enterprises have been intensively exposed under the impact of the COVID-19. From the perspective of policy regulation, policy innovation and system design play an essential role in improving the quality and efficiency of the supply system. During the epidemic period, the government took measures such as economic support and tax reduction for a certain number of small- and medium-sized enterprises, which helped the supply chain network coordinate the production cycle and capital flow cycle as a whole and ensure network efficiency.

Finally, our study also implicates that we need to actively adopt new technologies to reduce the cost and risk of supply chain management. The new technology can also involve virus detection and personnel health tracking. Even if there is a sporadic epidemic, it can respond and deal with it quickly to provide better safety protection and psychological protection for enterprise production, contributing to the resumption of production and solving the problem of labor shortages during the epidemic. In the future, we will further study the specific protection measures to enhance the invulnerability of the supply chain network.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the Social Science Planning Foundation of Zhejiang Province, China (Grant no. 21NDJC080YB), Zhejiang Public Welfare Research Project (Grant no. LGF20G010004), General Scientific Research Project of Zhejiang Department of Education China (Grant no. 1300KZ0419912), and Zhejiang Natural Science Foundation Project (Grant no. LY19F020007).

References

- [1] D. Guan, D. Wang, S. Hallegatte, S. Joseph Davis, and au fnm, "Global supply-chain effects of COVID-19 control measures," *Nature Human Behaviour*, vol. 4, no. 6, pp. 577–587, 2020.
- [2] P. Chowdhury, S. Paul, S. Kaisar, and M. D. Abdul Moktadir, "COVID-19 pandemic related supply chain studies: a systematic review," *Transportation Research Part E*, vol. 148, Article ID 102271, 2021.
- [3] A. Kumar, S. K. Mangla, P. Kumar, and M. Song, "Mitigate risks in perishable food supply chains: learning from COVID-19," *Technological Forecasting and Social Change*, vol. 166, Article ID 120643, 2021.
- [4] R. Van Hoek, "Research opportunities for a more resilient post-COVID-19 supply chain – closing the gap between research findings and industry practice," *International Journal of Operations & Production Management*, vol. 40, no. 4, pp. 341–355, 2020.
- [5] W. Klibi, A. Martel, and A. Guitouni, "The design of robust value-creating supply chain networks: a critical review," *European Journal of Operational Research*, vol. 203, pp. 283–293, 2010.
- [6] L. Tang, K. Jing, J. He, and H. E. Stanley, "Robustness of assembly supply chain networks by considering risk propagation and cascading failure," *Physica A*, vol. 459, pp. 129–139, 2016.
- [7] A. Nagurney, "Optimisation of supply chain networks with inclusion of labor: applications to COVID-19 pandemic disruptions," *International Journal of Production Economics*, vol. 235, Article ID 108080, 2021.
- [8] December, 2021 <https://think.ing.com/articles/the-rise-and-rise-of-global-shipping-costs>.
- [9] December, 2021 <https://www.uscourts.gov/news/2021/11/08/bankruptcy-filings-continue-fall-sharply>.
- [10] December, 2021 <https://www.nippon.com/en/japan-data/h01109/>.
- [11] J. Wang, "Robustness of complex networks with the local protection strategy against cascading failures," *Safety Science*, vol. 53, pp. 219–225, 2013.
- [12] G. S. Zhang and W. Liu, "Vulnerability measurement research of complex network of logistics service supply chain," *Computer Engineering and Applications*, vol. 53, no. 19, pp. 224–230, 2017.
- [13] J. Ke, X. Du, L. Shen, and L. Tang, "Robustness of complex networks: cascading failure mechanism by considering the characteristics of time delay and recovery strategy," *Physica A*, vol. 534, Article ID 122061, 2019.
- [14] M. F. Lu, W. J. Chen, and C. J. Liang, "Emergency supply chain network robust optimisation for mitigating disruption risk," *Journal of Hefei University of Technology*, vol. 10, no. 38, pp. 1417–1423, 2015.
- [15] J. Gao and Y. Y. Chen, "Vulnerability analysis of supply chain network in cascading failure," *Logistics Engineering and Management*, vol. 38, no. 10, pp. 80–83, 2016.
- [16] Y. Yan, X. Liu, and X. T. Zhuang, "Cascading failure model and method of supply chain based on complex network," *Journal of Shanghai Jiaotong University*, vol. 44, no. 3, pp. 322–331, 2010.
- [17] H. M. He and Y. L. Cheng, "Research on supply chain repair mechanism based on directed weighted complex network," *Journal of Railway Science and Engineering*, vol. 13, no. 11, pp. 2299–2304, 2016.
- [18] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marques, "Setting B2B digital marketing in artificial intelligence-based CRMs: a review and directions for future research," *Industrial Marketing Management*, vol. 98, no. 10, pp. 161–178, 2021.
- [19] Y. C. Wang and F. P. Zhang, "Modeling and analysis of under-load-based cascading failures in supply chain networks," *Nonlinear Dynamics*, vol. 92, pp. 1403–1417, 2018.

- [20] L. Geng and R. B. Xiaio, "Resilience measure of supply network based on DIIM," *Computer Integrated Manufacturing Systems*, vol. 20, no. 5, pp. 1211–1219, 2014.
- [21] W. Pan, J. Dong, K. Liu, and J. Wang, "Topology and topic-aware service clustering," *International Journal of Web Services Research*, vol. 15, no. 3, pp. 18–37, 2018.
- [22] R. Z. Qiu, Y. Z. Wang, and X. Y. Huang, "Robust supply chain network design based on uncertain disruption probability," *Computer Integrated Manufacturing Systems*, vol. 22, no. 10, pp. 2458–2468, 2016.
- [23] F. P. Fernandes and F. W. S. Lima, "Persistence in the zero-temperature dynamics of the q -states Potts model on undirected Barabasi-Albert networks and Erdos-Renyi random graphs," *International Journal of Modern Physics C*, vol. 19, no. 12, pp. 1777–1785, 2008.
- [24] H. Song, "The implication of the novel coronavirus outbreak to supply chain flexibility management," *China business and market*, vol. 34, no. 3, pp. 11–16, 2020.
- [25] A. Zhu, W. Chen, J. Zhang, X. Zong, W. Zhao, and Y. Xie, "Investor immunisation to Ponzi scheme diffusion in social networks and financial risk analysis," *International Journal of Modern Physics B*, vol. 33, no. 11, 2019.
- [26] J. G. Liu, Y. X. Zhou, B. Lu, and J. L. Zhao, "The reduction mechanism of supply chain vulnerability based on supply chain disruption risk," *Systems Engineering Theory & Practice*, no. 3, pp. 556–566, 2015.
- [27] K. P. Yu, Y. Yang, N. Liu, F. Li, and J. Z. Xie, "Vulnerability of complicated supply chain network based on weighted improved nodes contraction method," *Computer Integrated Manufacturing Systems*, vol. 20, no. 4, pp. 963–970, 2014.
- [28] Y. Zeng and R. Xiao, "Modelling of cluster supply network with cascading failure spread and its vulnerability analysis," *International Journal of Production Research*, vol. 52, no. 23, pp. 6938–6953, 2014.
- [29] Z. P. Du, G. Y. Hu, and Y. S. Liu, "Research on supply chain vulnerability based on complexity," *China Business and Market*, vol. 25, no. 6, pp. 49–53, 2011.
- [30] F. Liu, *Research of the Impact of Supply Chain Risk Management on Supply Chain Vulnerability*, Zhejiang University, Hangzhou, China, 2010.
- [31] L. Tang, J. He, and K. Jing, "Cascading failure mechanism and robustness of interdependent supply chain networks," *Journal of Management Sciences in China*, vol. 19, no. 11, pp. 33–44, 2016.
- [32] Y. Li, J. Wu, and Y. J. Tan, "Critical invulnerability study for cascading failure of tactical logistics networks," *Journal of System Simulation*, vol. 24, no. 5, pp. 1030–1034, 2012.
- [33] Y. Li, J. Wu, and Y. J. Tan, "Invulnerability study for cascading failure of the logistics support networks of capacity evenly distributed," *Journal of Systems Engineering*, vol. 25, no. 6, pp. 853–860, 2010.
- [34] L. Tang, P. Jiao, J. K. Li, K. Jing, and Z. H. Jin, "Cascading failure mechanism and robustness of complex networks with recovery strategy," *Control and Decision*, vol. 10, no. 33, pp. 1841–1850, 2018.
- [35] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: cascading failure and robustness," *Physica A*, vol. 443, pp. 58–69, 2016.
- [36] L. Geng, R. Xiao, and S. Xie, "Research on self-organisation in resilient recovery of cluster supply chains," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 758967, 2013.
- [37] Y. C. Wang and R. B. Xiao, "An ant-colony based resilience approach to cascading failures in cluster supply network," *Physica A*, vol. 462, pp. 150–166, 2016.
- [38] W. Pan, B. Song, K. Li, and K. Zhang, "Identifying key classes in object-oriented software using generalised k -core decomposition," *Future Generation Computer Systems*, vol. 81, pp. 188–202, 2018.
- [39] D. L. Duan, "Cascading failure of complex networks based on load local preferential redistribution rule," *Complex Systems and Complexity Science*, vol. 12, no. 1, pp. 33–39, 2015.
- [40] D. L. Duan, X. D. Ling, X. Y. Wu, D. H. OuYang, and B. Zhong, "Critical thresholds for scale-free networks against cascading failures," *Physica A*, vol. 416, pp. 252–258, 2014.
- [41] A. Motter and Y. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, Article ID 065102, 2002.
- [42] A. Motter, "Cascade control and defense in complex networks," *Physical Review Letters*, vol. 93, no. 9, Article ID 098701, 2004.
- [43] H. Li, T. Wang, W. Pan et al., "Mining key classes in Java projects by examining a very small number of classes: a complex network-based approach," *IEEE Access*, vol. 9, Article ID 28076, 2021.
- [44] J. Wang and L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability," *Physica A*, vol. 388, pp. 1289–1298, 2009.
- [45] R. R. Yin, B. Liu, H. R. Liu, and Y. Q. Li, "Research on invulnerability of the random scale-free network against cascading failure," *Physica A*, vol. 444, pp. 458–465, 2016.
- [46] Z. Li, Y. H. Guo, G. A. Xu, and Z. M. Hu, "Analysis of cascading dynamics in complex networks with an emergency recovery mechanism," *Acta Physica Sinica*, vol. 63, no. 15, p. 158901, 2014.
- [47] P. Erdos and A. Rnyi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.*, vol. 5, pp. 17–61, 1960.
- [48] A. Barabasi and R. Albert, "Emergence of scaling in random network," *Science*, vol. 286, pp. 509–512, 1999.
- [49] J. R. Saura, D. Ribeiro-Soriano, and D. Palacio-Marques, "Using data mining techniques to explore security issues in smart living environments in Twitter," *Computer Communications*, vol. 179, no. 11, pp. 285–295, 2021.
- [50] W. Pan, H. Ming, C. K. Chang, Z. Yang, and D.-K. Kim, "ElementRank: Ranking Java software classes and packages using multilayer complex network-based approach," *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2272–2295, 2019.