This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3090332, IEEE Access

IEEE Access
Multidisciplinary ⁞ Rapid Review ⁞ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Research on Supply Chain Network Resilience Considering the Exit and Reselection of Enterprises

YONGZHENG TIAN, YUQIANG SHI, XIAOQIU SHI, MINGHUI LI, AND MIN ZHANG
School of Manufacturing Science and Engineering, Southwest University of Science and Technology, Mianyang 621000, China

Corresponding author: Min Zhang (904502317@qq.com).

This work was supported in part by the Natural Science Foundation of Southwest University of Science and Technology under Grant 20zx7117.

ABSTRACT In a complex environment, how to construct a resilient supply chain network (SCN) that can resist disruptions is a problem of great concern in supply chain management. In order to provide some insights for constructing a resilient SCN, this paper studies the influence of network structures on SCN resilience from the perspective of complex networks. Considering the exit and reselection of enterprises that have been ignored in previous studies, we propose a new SCN model in which nodes are connected with each other based on degree, fitness, and distance. Subsequently, different disruption scenarios are simulated and the resilience of the SCN generated by the proposed model is compared with that of previous models. The simulation results show that the SCN generated by the proposed model is resilient to random disruptions, but vulnerable to targeted disruptions. In particular, the resilience of the SCN will be seriously affected when the strong-strong alliance is broken. Through the research on the influence of the parameters (e.g., α, β, and f) of the proposed model on SCN resilience, we find that α has a significant impact on SCN resilience. The larger the value of α, the worse the resilience of the corresponding SCN. The parameter β has a slight effect on SCN resilience, and the more uniform the distribution of f in the network, the better the resilience of the corresponding SCN. This study may contribute to the design and resilience optimization of SCNs.

INDEX TERMS Complex networks, disruptions, network structures, supply chain network resilience.

I. INTRODUCTION

With the development of globalization, a supply chain system has gradually evolved into a huge and complex system, in which the cooperation between enterprises has formed a complex supply chain network (SCN) [1]–[2]. In an increasingly turbulent and complex environment, SCNs are exposed to various disruptions, such as earthquakes, floods, and terrorist attacks, which will affect the normal operation of SCNs and even cause serious economic losses [3]–[6]. For example, the tsunami and earthquake in Japan in 2011 disrupted the SCN of Toyota Motor Corporation and resulted in the production losses of 140,000 vehicles [7]. Similarly, the outbreak of Corona Virus Disease 2019 has seriously affected the logistics and production activities of many industries, such as automobile industry, aviation industry, and tourism industry [8]–[11]. Facing a complex and changeable environment, how to design a resilient SCN that can withstand various disruptions has attracted the attention of many scholars [12]–[18].

A resilient SCN means that it can operate stably or quickly return to a normal state despite disruptions [1], [19]–[20]. The guarantee of SCN resilience is usually related to preventive measures, reaction behaviors, and recovery strategies against disruptions [3], [21]–[25]. Intuitively, supply chain network disruptions (SCNDs) are defined as unexpected events that interrupt the normal operation (e.g., the flow of goods and services) of SCNs [26]–[27]. They may be caused by natural disasters or man-made events.

In order to design a resilient SCN, many scholars have conducted studies from multiple perspectives, such as risk management [28]–[32], control theory [33]–[37], and mathematical modeling and simulation [38]–[42]. In addition, many researchers have studied SCN resilience from the perspective of complex networks [43]–[50], because it is a simple and effective method that can capture the structural characteristics of an SCN, thus contributing to the construction of a resilient SCN. This paper also studies from the perspective of complex networks, regarding enterprises as nodes and cooperative relationships as edges. As demonstrated in [51], the structure of an SCN has a significant impact on SCN resilience. Different network structures show different resilience in the face of disruptions. For example, the scale-free network [52] is vulnerable to targeted disruptions, while the random network [53] is resilient. Meanwhile, a local failure of an SCN may cause the failure of the whole supply chain system due to the interaction between enterprises in an SCN. It is called cascading failures [54] or ripple effects [55]. Generally, there are static and dynamic methods can be used to study SCN resilience from the perspective of complex networks. The dynamic method considers cascading failures, while the static method does not. According to [5], the static method can simply and intuitively analyze the influence of network structures on SCN resilience. Thus, the static method is also used in this paper. In most cases, the failure of an enterprise to manage SCNDs is usually due to the lack of understanding of SCN structures [6]. Thus, the exploration of SCN structures can help supply chain managers design a resilient SCN or respond to SCNDs.

Network models are very important for the study of SCN resilience from the perspective of complex networks, because they can generate SCNs with specific structures [5]. After extensive classification, Perera *et al.* [56] found that SCN models mainly focus on BA [52], ER [53] and WS [57] models. In particular, BA model has attracted wide attention because it reflects the growth and priority connection characteristics of a real network. The degree-based priority connection of BA model reflects the enterprise's attention to the business scale of its partners. The enterprise (node) with larger business scale (larger degree) can establish cooperative relationships (edges) with more enterprises. This also reflects the reality that the rich are getting richer. As time goes on, older enterprises will get more cooperation, i.e., older nodes will have larger degrees. However, the growth rate of a node's degree is not only related to the age of the node. In reality, enterprises with high-quality products can obtain a lot of cooperative business in a short time. This property is called the fitness of a node [58]. In addition, enterprises will give priority to closer enterprises when looking for partners [1], [5]. Therefore, in addition to the degree of a node, the fitness of a node and the distance between nodes need to be considered when setting the connection rules of an SCN model.

Moreover, most existing studies only consider the situation of new nodes entering the network. In reality, the structure of an SCN is not immutable. There will be enterprises entering an SCN because of the need of cooperation, and there will also be enterprises leaving an SCN because of the end of cooperation or market transfer. For example, an enterprise in an SCN will withdraw from the SCN when it ends its cooperative relationships with other enterprises. Meanwhile, in order to ensure the continuous operation of business, the enterprises that originally cooperated with it will seek for cooperation with other enterprises (i.e., reselection). Therefore, we propose a new SCN model based on the above considerations. In addition, most studies only consider random or targeted disruptions, whose objects are only nodes or edges. In fact, an SCN may face random and targeted disruptions at the same time (mixed disruptions [5]), and nodes and edges may also be damaged simultaneously [6]. Therefore, this paper will fully consider different disruption scenarios and study the influence of network structures on SCN resilience, so as to provide some insights for building a resilient SCN.

In summary, this study contributes to the existing literature by filling in the following research gaps: (i) the exit and reselection of enterprises that have been neglected in previous studies are considered in this study when modeling an SCN; (ii) node degree, fitness and distance are considered simultaneously in the connection rules of the SCN model; and (iii) different from previous studies, different disruption scenarios are fully considered in this study, including different disruption types and objects.

The rest of this paper is organized as follows. Section II reviews the related research, and Section III describes the proposed SCN model and the resilience metrics used. In Section IV, different disruption scenarios are simulated, and the results are analyzed in Section V. Section VI summarizes the results and discusses the future work.

II. RELATED WORK

This paper mainly studies the impact of network structures on SCN resilience under different disruption scenarios. Thus, the literature review mainly focuses on SCN models, SCNDs, and resilience metrics.

A. SUPPLY CHAIN NETWORK MODELS AND RESILIENCE METRICS

Different SCN models generate SCNs with different structures. In previous studies, researchers have proposed many SCN models. For instance, Xuan *et al.* [59] introduced different supplier-customer connection rules in their model to construct SCNs, and compared with BA and ER models. The connection rule of BA model is the degree-based priority connection, i.e., the larger the degree (the number of neighbour nodes) of an old node, the larger the probability of a new node connecting with it, while the connection rule of ER model is random connection. Kim *et al.* [6] used the models mentioned in [60] to generate SCNs with scale-free, block-diagonal, centralized, and diagonal structures. Zhao *et al.* [43] proposed a random local

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3090332, IEEE Access

TABLE 1. Some existing SCN models and their resilience metrics

Studies	Connection rules	Resilience metrics
Zhao *et al*. [1]	● Degree-based priority connection. ● Distance-based rule: a new node is more likely to connect with a closer old node.	● Supply availability rate. ● Size of LFS. ● Average supply path length in LFS. ● Maximum supply path length in LFS.
Shi *et al*. [5]	● Degree-based priority connection. ● Random connection. ● Distance-based rule.	● Size of LFCS. ● Average path length in LFCS. ● Maximum path length in LFCS.
Nair and Vidal [44]	● Degree-based priority connection. ● Random connection.	● Average path length. ● Clustering coefficient. ● Size of LCS. ● Maximum path length in LCS.
Sun *et al*. [45]	● Priority connection based on node degree and competition coefficient: a new node is more likely to connect with an old node with larger degree and larger competition coefficient.	● The ratio of the size of LCS to the size of the network after disruptions. ● The rate of change of the size of LCS. ● The ratio of the average degree of LCS to the average degree of the original network. ● The ratio of the average path length in LCS to the average path length in the original network.
Ledwoch *et al*. [46]	● Degree-based priority connection. ● Random connection.	● Total cost incurred by all agents. ● Costs incurred by the original equipment manufacturer. ● Average unit fill-rate of agents. ● Unit fill-rate of the original equipment manufacturer.
Thadakamalla *et al*. [51]	● Degree-based priority connection. ● Random local connection: a new node is randomly connected to an old node in a local area.	● Size of LCS. ● Average path length in LCS. ● Maximum path length in LCS.
Xu *et al*. [62]	● Priority connection based on node strength and distance: a new node is more likely to connect with an old node with higher strength and closer distance.	/
Wang *et al*. [63]	● Degree-based priority connection. ● Random connection. ● Supply-specific.	● Supply availability rate. ● Size of LFS. ● Average supply path length in LFS. ● Maximum supply path length in LFS. ● Network resilience score.
Xia [64]	/	● Size of LCS . ● The reciprocal of average path length in LCS.
Li and Zobel [65]	● Degree-based priority connection. ● Random connection. ● Random reconnection.	● Number of healthy nodes. ● Size of LCS. ● The ratio of the size of LCS to the average path length in LCS.

rewiring rule to simulate the situation that an SCN will adjust after a period of time. Sun *et al*. [45] introduced a competition coefficient and established an SCN model based on BA model. Ledwoch *et al*. [46] used BA and ER models to generate SCNs and studied the influence of network structures on the effectiveness of risk management. Wang *et al*. [48] used BA and KE [61] models to generate SCNs and studied their under-load cascade failures. Xiong *et al*. [50] and Thadakamalla *et al*. [51] established corresponding SCN models based on the characteristics of military SCNs. Xu *et al*. [62] established an agile SCN model based on node strength and distance to analyze its evolution mechanism. These SCN models correspond to different connection rules. Table 1 lists some existing SCN models and their resilience metrics.

As shown in Table 1, the existing SCN models rarely consider the situation of nodes exiting the SCN. Although Shi *et al*. [5] considered the exit of nodes, they did not consider the situation that other nodes will choose nodes again after some nodes exit. This is also a very common phenomenon in reality. Therefore, this paper also considers the exit and reselection of nodes besides the entry of nodes. Moreover, most of the models in Table 1 consider the degree-based priority connection. However, as aforementioned, the degree-based priority connection does not reflect the fact that young enterprises with high-quality products can also get a lot of cooperative business. Therefore, the fitness of a node also needs to be considered [58]. Following [1] and [5], the distance-based rule is also considered in this paper.

Generally, most existing studies use the largest connected sub-network (LCS) to measure SCN resilience. As shown in [44], the size of LCS and the maximum path length in LCS were used by them to measure SCN resilience. The size of LCS, the average path length, and the maximum path length in LCS were used by Thadakamalla et al. [51] to measure SCN resilience. The size of LCS and the reciprocal of average path length in LCS were used by Xia [64] to measure SCN resilience. The size of LCS and the ratio of the size of LCS to the average path length in LCS were used by Li and Zobel [65] to measure SCN resilience. Moreover, considering the different roles of nodes, Zhao et al. [1] and Shi et al. [5] proposed metrics based on the largest functional sub-network (LFS) and the largest full-role connected sub-network (LFCS) respectively to measure SCN resilience. Essentially, LFS and LFCS can be regarded as LCSs with consideration of nodes' heterogeneity, so they are more suitable for SCN resilience evaluation. LFS is more suitable for military SCNs, and LFCS is more suitable for SCNs in the context of manufacturing. This paper measures SCN resilience based on LFCS.

B. SUPPLY CHAIN NETWORK DISRUPTIONS

SCNDs can be divided into random and targeted disruptions [1]. The objects of disruptions include nodes and edges. Random disruptions are mainly caused by natural disasters, such as floods, earthquakes, and tsunamis. The probability of this kind of event occurring is small, but once it happens, it will bring serious consequences. For example, the flood in Thailand in 2011 and the tsunami and earthquake in Japan in 2011 all brought heavy losses to the corresponding industry [6]–[7]. In the case of random disruptions, the probability of each node or edge being attacked is equal. By contrast, targeted disruptions are mainly caused by man-made disasters, such as terrorist attacks, military strikes, and economic sanctions. Examples of this category include terrorism and piracy in Somalia in 2008, political crises in Nepal in 2015, and the legal dispute between Volkswagen and its suppliers in 2016 [66]–[67]. In targeted disruptions, the more important parts are more likely to be attacked. Once the important nodes in an SCN are attacked, the whole network will collapse quickly [1].

In a word, it is very important to design a resilient SCN that can resist various disruptions. Meanwhile, it is necessary to understand the resilience of an SCN under different disruptions. In previous studies, Ledwoch *et al.* [46] and Li and Zobel [65] studied the situation where nodes were randomly disrupted. Zhao *et al.* [1] and Thadakamalla *et al.* [51] studied the impact of node disruptions on SCN resilience against random and targeted disruptions. Azad *et al.* [68] studied the situation where nodes or edges were randomly disrupted. Adenso-Díaz *et al.* [69] studied the situation of edge disruptions in random and targeted disruptions. According to [6], Disrupting only nodes or edges may not cause network-level disruptions, thus they proposed the concept of network-level disruptions and simulated random disruptions. Shi *et al.* [5] proposed the concept of mixed disruptions in consideration of the situation that random and targeted disruptions may occur simultaneously, and conducted research on node disruptions. Table 2 lists some of the disruptions simulated in existing studies.

TABLE 2. SCND scenarios of some existing studies

Studies	Disruption types	Disruption objects
Zhao *et al.* [1]	● Random disruptions ● Targeted disruptions	● Nodes
Shi *et al.* [5]	● Random disruptions ● Targeted disruptions ● Mixed disruptions	● Nodes
Nair and Vidal [44]	● Random disruptions ● Targeted disruptions	● Nodes
Ledwoch et al. [46]	● Random disruptions	● Nodes
Thadakamalla *et al.* [51]	● Random disruptions ● Targeted disruptions	● Nodes
Li and Zobel [65]	● Random disruptions	● Nodes
Bier *et al.* [67]	● Random disruptions ● Targeted disruptions	● Nodes
Azad *et al.* [68]	● Random disruptions	● Nodes ● Edges
Adenso-Díaz *et al.* [69]	● Random disruptions ● Targeted disruptions	● Edges
Reyes Levalle and Nof [70]	● Random disruptions ● Targeted disruptions	● Nodes

In general, most studies only consider random or targeted disruptions, and only nodes or edges are disrupted. Actually, the type of disruption is usually unknown. In addition to random and targeted disruptions, an SCN may also face mixed disruptions [5]. In any disruption type, the disruption object may be only nodes or edges, or both nodes and edges may be disrupted at the same time. Thus, different disruption scenarios are fully considered in this paper.

III. METHODS

A. COMPLEXITY ANALYSIS OF SUPPLY CHAIN NETWORKS

An SCN is a complex network composed of a large number of interacting individuals. It shows the characteristics of node complexity, structural complexity, and dynamic complexity of network topology.

The node complexity is mainly reflected in the diversity of nodes. There are a large number of nodes in a complex network, and each node represents an independent individual with its own unique functions. For example, there are many enterprises such as suppliers, manufacturers, distributors, and retailers in an SCN. Nodes represent these enterprises, and the establishment of connections between nodes reflects their functionality.

The structural complexity is mainly reflected in the complex links between nodes. In a complex network, due to the large number of nodes, the connections between different nodes eventually form different network structures, thus presenting different structural characteristics. In an SCN, the relationship between enterprises is very complex. Usually, one enterprise has partnerships with multiple enterprises. If the industrial chain of an enterprise is regarded as one chain, an SCN is the integration of multiple chains.

The dynamic complexity of network topology mainly means that the network structure is constantly changing, which is mainly affected by two aspects. First, it is the impact of the environment. An SCN is in a complex and changeable environment. Politics, culture, economy, and other factors all affect its composition and development. Second, an SCN is a self-organizing network, and it has a collaborative evolution process with the dynamically changing environment. In the network, nodes are constantly entering and exiting, and new cooperative relationships are constantly being produced. Nodes with strong adaptability continue to grow and develop.

In addition, the core enterprises in an SCN have high aggregation. In an SCN, a core enterprise has a great market advantage, and it is often relied on by many enterprises, thus it plays an important role in the SCN. Therefore, enterprises with greater market advantages in market competition tend to have stronger competitiveness.

B. SUPPLY CHAIN NETWORK MODEL

Following [1], [5] and [51], an SCN is represented as an undirected graph $G(V, E)$, where V is the set of nodes, representing enterprises. V is composed of subsets V_s (suppliers), V_m (manufacturers), V_d (distributors), and V_r (retailers), as in (1) [5]. E is the set of edges, representing cooperative relationships. If there is a cooperative relationship between enterprises V_i and V_j, then nodes V_i and V_j are interconnected with each other to form an edge e_{ij}.

$$V = V_s \cup V_m \cup V_d \cup V_r \text{, where } V_x \cap V_y = \varnothing, \\ \text{when } x \neq y, x, y \in \{s, m, d, r\} \qquad (1)$$

Figure 1 illustrates an SCN with 20 nodes, including six suppliers, three manufacturers, four distributors, and seven retailers. There will be connections not only between upstream and downstream enterprises, but also between enterprises at the same level.

As aforementioned, there are both entry and exit of enterprises in a real SCN. When an enterprise exits, the enterprise that originally cooperated with it will reselect an enterprise to cooperate. Moreover, according to [5], an SCN will experience three stages of growth, maturity, and decline from the perspective of life cycle. In the growth stage, more enterprises enter than exit. In the maturity stage, there is a balance between entry and exit, and more enterprises exit during the decline stage. Therefore, considering the above phenomena, we propose a new SCN model, which is called the growth-maturity-decline and reselection (GMDR) model.

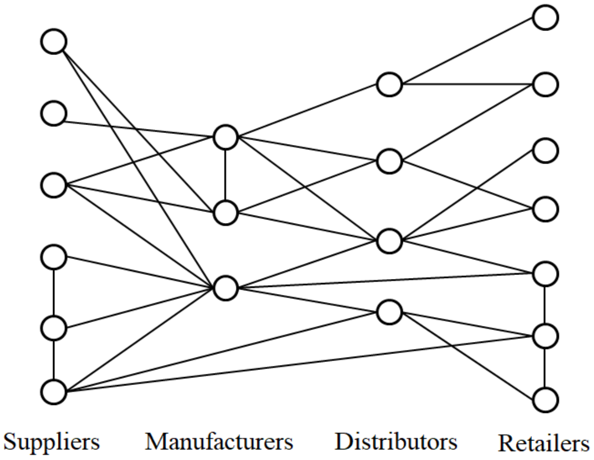


FIGURE 1. An example of an SCN.

The connection rules of GMDR model consider node degree, fitness and distance, which are proposed on the basis of [1], [5], [52] and [58]. At present, most SCN models are based on BA model [45]. The degree-based priority connection rule of BA model means that a new enterprise is more willing to cooperate with enterprises with more partners. Thus, the new enterprise is more likely to obtain greater benefits. However, the degree-based priority connection will cause the degree of an old node to accumulate over time. Actually, if an old enterprise cannot adapt to the development of society, it will eventually be eliminated. Similarly, if a young enterprise has good development potential and can provide high-quality products (i.e., large fitness), it also has the opportunity to establish partnerships with a large number of enterprises. Therefore, it is necessary to consider not only degree, but also fitness. The node fitness follows a certain probability distribution [58]. Meanwhile, the distance between nodes is considered because a new node is more likely to connect to a closer old node, which means less costs [1], [5]. The distance between two nodes refers to the shortest path length between two nodes, i.e., the number of edges in the shortest path from one node to another. Nodes representing suppliers (s), manufacturers (m), distributors (d), and retailers (r) enter successively according to a certain ratio (s: m: d: r). The GMDR model can be described as follows:

Step 1: This model starts with N_0 fully connected nodes.

Step 2: Growth stage (GMDR-G). G new nodes enter the network and each of them is connected with W old nodes in the network. After that, G/2 nodes are randomly selected to exit the network. The connection rules are as follows:

- Rule 1: The first edge is connected to an old node V_i with probability P_i, which is determined by the node's degree k_i and fitness f_i, defined as

$$P_i = \frac{(k_i f_i)^{\alpha}}{\sum_j (k_j f_j)^{\alpha}}, \alpha > 0 \tag{2}$$

- Rule 2: The second edge is connected to an old node V_j ($V_j \neq V_i$) with probability P_j, which is determined by the distance d_j between the new node and the old node V_j, defined as

$$P_j = \frac{{d_j}^{-\beta}}{\sum_l {d_l}^{-\beta}}, \beta > 0 \tag{3}$$

- Rule 3: When a node V_b exits the network, each neighbor node of node V_b is connected to a node V_c with probability P_c, which is jointly determined by the degree k_c and fitness f_c of node V_c, as well as the distance d_c between the neighbor node of V_b and node V_c, defined as

$$P_c = \frac{(k_c f_c)^{\alpha} * {d_c}^{-\beta}}{\sum_u (k_u f_u)^{\alpha} * {d_u}^{-\beta}} \tag{4}$$

Step 3: If the number of nodes does not reach the total number of nodes (N), return to Step 2, otherwise, go to Step 4.

Step 4: Maturity stage (GMDR-M). G new nodes enter the network, and then G nodes are randomly selected to exit the network. This process is repeated Z times. The connection rules are the same as Step 2.

Step 5: Decline stage (GMDR-D). G new nodes enter the network, and then G/2 nodes are randomly selected to exit the network. This process is repeated Z times. After that, G/2 new nodes enter the network, and G nodes are randomly selected to exit. This process is repeated Z times. The connection rules are the same as Step 2.

Equation (2) is a connection rule based on degree and fitness. The larger the degree and fitness of an old node, the larger the probability that a new node will connect to it. In (2), α is a priority parameter of degree and fitness. The larger the value of α, the more likely a new node is to connect to a node with larger degree and fitness. Equation (3) is a connection rule based on distance. It means that the probability of connecting with local nodes is large. In (3), β is a distance priority parameter. The larger the value of β, the more likely a new node is to connect to a closer node. Equation (4) is a connection rule based on degree, fitness, and distance. It means that the nodes with large degree, large fitness, and close distance will be selected preferentially.

C. RESILIENCE METRICS

As aforementioned, most studies are based on LCS (i.e., the largest sub-network in which any two nodes can be connected) to measure SCN resilience, such as the size of LCS and the average path length in LCS. The size of LCS refers to the number of nodes in LCS, and the average path length in LCS refers to the average of the shortest path lengths of all node pairs in LCS. However, the use of LCS usually ignores the heterogeneity of nodes. In a real SCN, different types of enterprises play different roles. Upstream enterprises provide products for downstream enterprises, and downstream enterprises pay funds to upstream enterprises. As demonstrated in [1] and [71], only by maintaining the supply-demand relationship between upstream and downstream enterprises can the normal operation of an SCN be maintained. According to [5], an SCN can operate stably for a long time only when suppliers, manufacturers, distributors, and retailers exist. Therefore, following [5], the LFCS is used to measure SCN resilience in this paper. The LFCS refers to an LCS that includes each type of node (V_s, V_m, V_d, and V_r), as shown in (5) ~ (7).

$$G_A(V,E) = \{G(V,E) \mid \forall V_i \in V, \forall V_j \in V, \exists e_{ij} \in E\} \tag{5}$$

$$\begin{aligned} G_B(V,E) = \{G_A(V,E) \mid \exists i, V_i \in V_s \wedge \exists j, V_j \in V_m \wedge \exists l, \\ V_l \in V_d \wedge \exists h, V_h \in V_r\} \end{aligned} \tag{6}$$

$$\begin{aligned} G_{LFCS}(V,E) = \{G_B(V,E) \mid \forall G(V,E) \in G_B(V,E), \\ |G(V,E)| \leq |G_B(V,E)|\} \end{aligned} \tag{7}$$

$G_A(V, E)$ is the connected network set, $G_B(V, E)$ is the full-role connected network set, and $G_{LFCS}(V, E)$ is the LFCS set. This paper uses the size of LFCS (SLFCS) and the average path length in LFCS (as shown in (8)) to measure SCN resilience.

$$L_{LFCS} = \frac{1}{N_{LFCS}(N_{LFCS} - 1)} \sum_{i \neq j} d_{ij} \tag{8}$$

Equation (8) is the calculation of the average path length in LFCS (L_{LFCS}), where N_{LFCS} is the total number of nodes in LFCS, and d_{ij} is the shortest path length from node V_i to node V_j.

The SLFCS reflects the connectivity of an SCN. When an SCN is attacked, it may be divided into several sub-networks, and the cooperation between enterprises will be limited to a smaller network. Therefore, the larger the SLFCS, the better the SCN resilience. Moreover, the average path length in LFCS reflects the efficiency of an SCN. The shorter the distance between two enterprises, the more convenient the cooperation between them. Therefore, the shorter the average path length in LFCS, the better the SCN resilience.

IV. NUMERICAL SIMULATION

A. SIMULATION SETUP

Since it is very difficult to experiment with SCNDs in reality, we use computer simulations for experiments. First, BA, ER, ASCN [62], and GMDR models are used to generate SCNs (in the absence of specific instructions, the corresponding SCN is represented by the corresponding model, e.g., the SCN generated by ER model can also be represented by ER model), then disruptions are simulated. After that, their resilience is compared. The disruption schemes are shown in Table 3. Assuming that N = 600, node fitness follows a normal distribution, $f \sim N(50, 10)$. This means that the average value of fitness in a network is 50, and variance is 10. Here, the value of fitness is large, making it possible for young nodes to get a lot of connections as well. Corresponding to the connection rules of new nodes entering the network, W = 2 is set. Accordingly, N_0 = 2. Following [5], G = 2, s: m: d: r = 5: 4: 1: 10, and Z = 200. Furthermore, α = 1, and β = 1. Every situation runs 20 times independently and takes the average value.

TABLE 3. Disruption schemes

Disruption types	Disruption objects
Random disruptions	● Nodes ● Edges ● Nodes and edges
Targeted disruptions	● Nodes ● Edges ● Nodes and edges
Mixed disruptions	● Nodes ● Edges ● Nodes and edges

Figure 2 illustrates the degree distribution of an SCN generated by GMDR model. As shown in Figure 2, the degree distribution of this SCN shows the characteristic of a power-law distribution, which is the significant feature of a scale-free network.

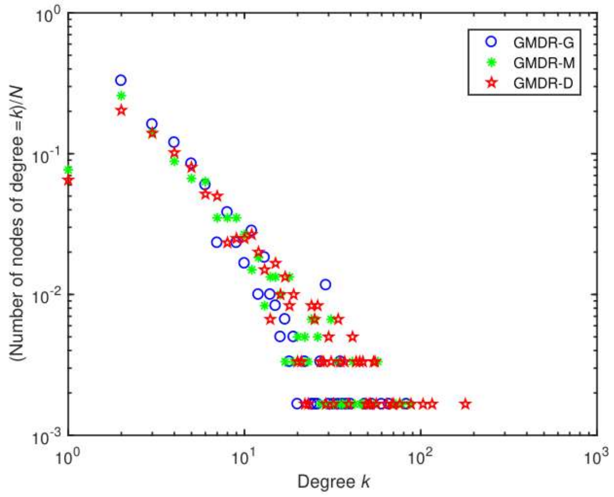


FIGURE 2. The degree distribution of GMDR model with 600 nodes.

As shown in Table 3, different disruption scenarios are simulated. In any disruption type, the edge connected to a node will also fail when the node is disrupted. Therefore, when only nodes are disrupted, edges connected to the removed nodes are removed together. In order to simulate the situation that nodes and edges are disrupted at the same time, a node and its edges are removed first, and then an edge is removed from the remaining edges. In random disruptions, nodes/edges are randomly removed from a network, while the important nodes/edges are preferentially removed from a network in targeted disruptions. There are many ways to measure the importance of nodes/edges, such as degree centrality and betweenness centrality [1], [5], [72]. This paper chooses the widely used degree centrality to measure the importance of nodes. The larger the degree of a node is, the more important the node is. Since there is no clear definition of the degrees of edges, following [72], betweenness centrality is chosen to measure the importance of edges. The edge betweenness of an edge is defined as the proportion of the number of shortest paths passing through the edge in the total number of shortest paths in a network. Therefore, the edge betweenness ($B(e)$) for an edge $e \in E$ is defined as

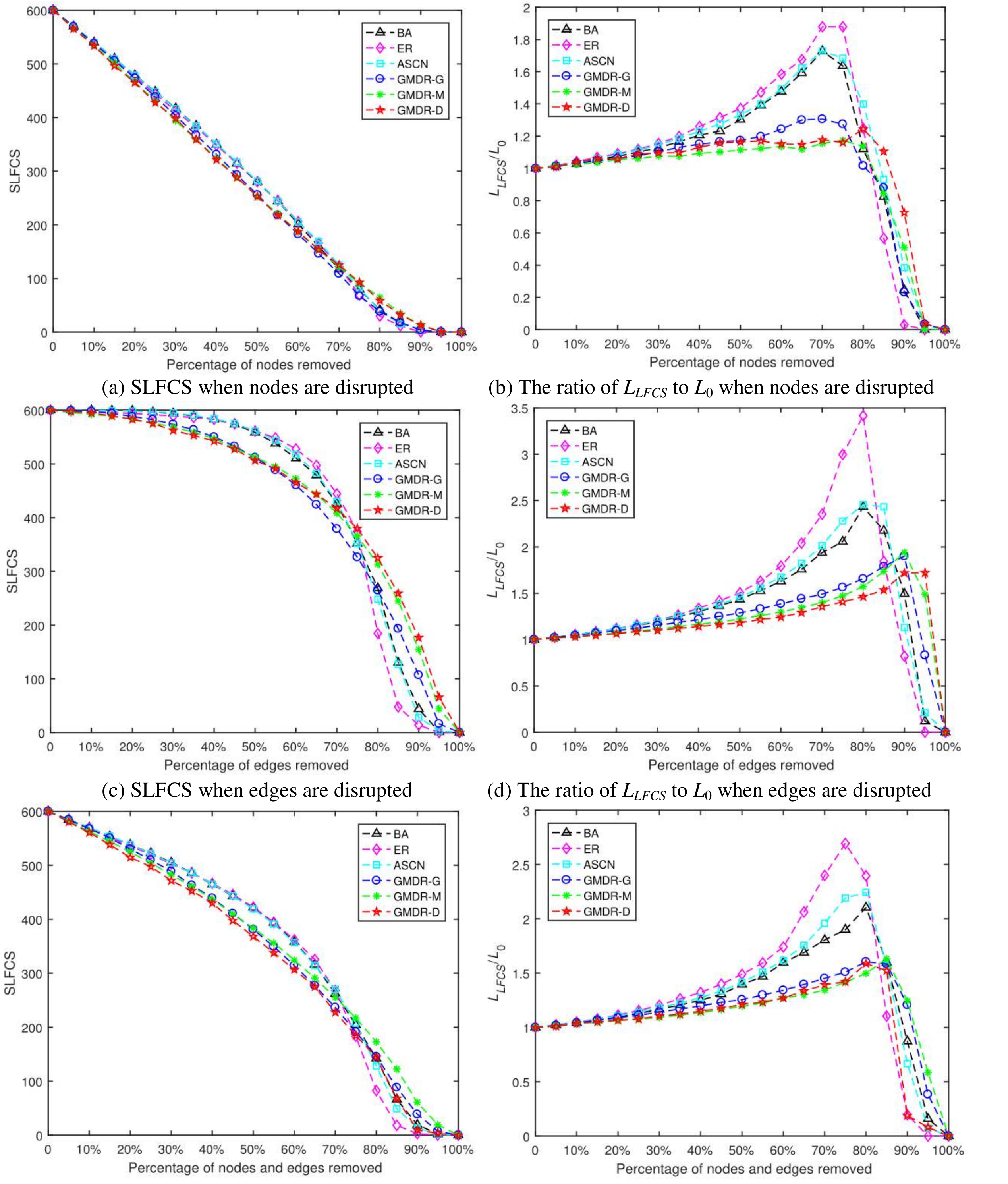
$$B(e) = \sum\nolimits_{a \neq b} \frac{Q_{ab}(e)}{Q_{ab}} \tag{9}$$

where $Q_{ab}(e)$ is the number of paths passing through edge e among all the shortest paths from node V_a to node V_b, and Q_{ab} is the number of the shortest paths from node V_a to node V_b. The larger the edge betweenness is, the more important the edge is. As mentioned in [5], in order to simulate the mixed disruptions, the targeted disruptions are performed first, and then the random disruptions are performed.

In our simulation, 5% of nodes and/or edges of a network are removed at each step, which is the same as [1]. In order to ensure fairness, an SCN generated by each model has the same number of nodes. With the occurrence of disruptions, SLFCSs of different models will change differently due to the different network structures they generate. L_{LFCS} will also change with the SLFCS, but it is unreasonable to compare it in different SLFCSs [1], [5]. Therefore, divide L_{LFCS} by the initial average path length (L_0) in the network to ensure reasonableness and fairness.

B. SIMULATION RESULTS OF RANDOM DISRUPTIONS

Figure 3 reveals the responses of BA, ER, ASCN, and GMDR models to random disruptions. As can be seen from Figure 3(a), SLFCSs of these models decrease almost linearly with the removal of nodes, and their performances are very similar. For example, when 50% of nodes are removed, about 47% of nodes in BA, ER, and ASCN models remain connected, and about 42% of nodes in GMDR model remain connected. This shows that they are resilient to random disruptions of nodes. In Figure 3(b),



(a) SLFCS when nodes are disrupted

(b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

(c) SLFCS when edges are disrupted

(d) The ratio of L_{LFCS} to L_0 when edges are disrupted

(e) SLFCS when nodes and edges are disrupted

(f) The ratio of L_{LFCS} to L_0 when nodes and edges are disrupted

FIGURE 3. Responses of BA, ER, ASCN, and GMDR models to random disruptions. (a) is the SLFCS when nodes are disrupted, (b) is the ratio of L_{LFCS} to L_0 when nodes are disrupted, (c) is the SLFCS when edges are disrupted, (d) is the ratio of L_{LFCS} to L_0 when edges are disrupted, (e) is the SLFCS when nodes and edges are disrupted, and (f) is the ratio of L_{LFCS} to L_0 when nodes and edges are disrupted.

their average path lengths first increase and then decrease. Generally, the network connectivity will be affected after removing some nodes, so the average path length will increase, indicating that the supply accessibility between enterprises will deteriorate [1]. When a certain number of nodes are removed, the average path length in a network begins to decrease, because the network has been decomposed into several small sub-networks with relatively

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3090332, IEEE Access

close nodes' distances. At this time, the SCN has become very fragmented and cannot provide normal functions. Thus, the slower the average path length increases and the later the inflection point of a curve appears, indicating that the better the resilience of an SCN. Figure 3(b) shows that the average path length of GMDR model increases more slowly than that of BA, ER, and ASCN models, indicating that GMDR model is more resilient than BA, ER, and ASCN models when only nodes are disrupted in random disruptions. Similarly, BA and ASCN models perform similarly, and they are both better than ER model.

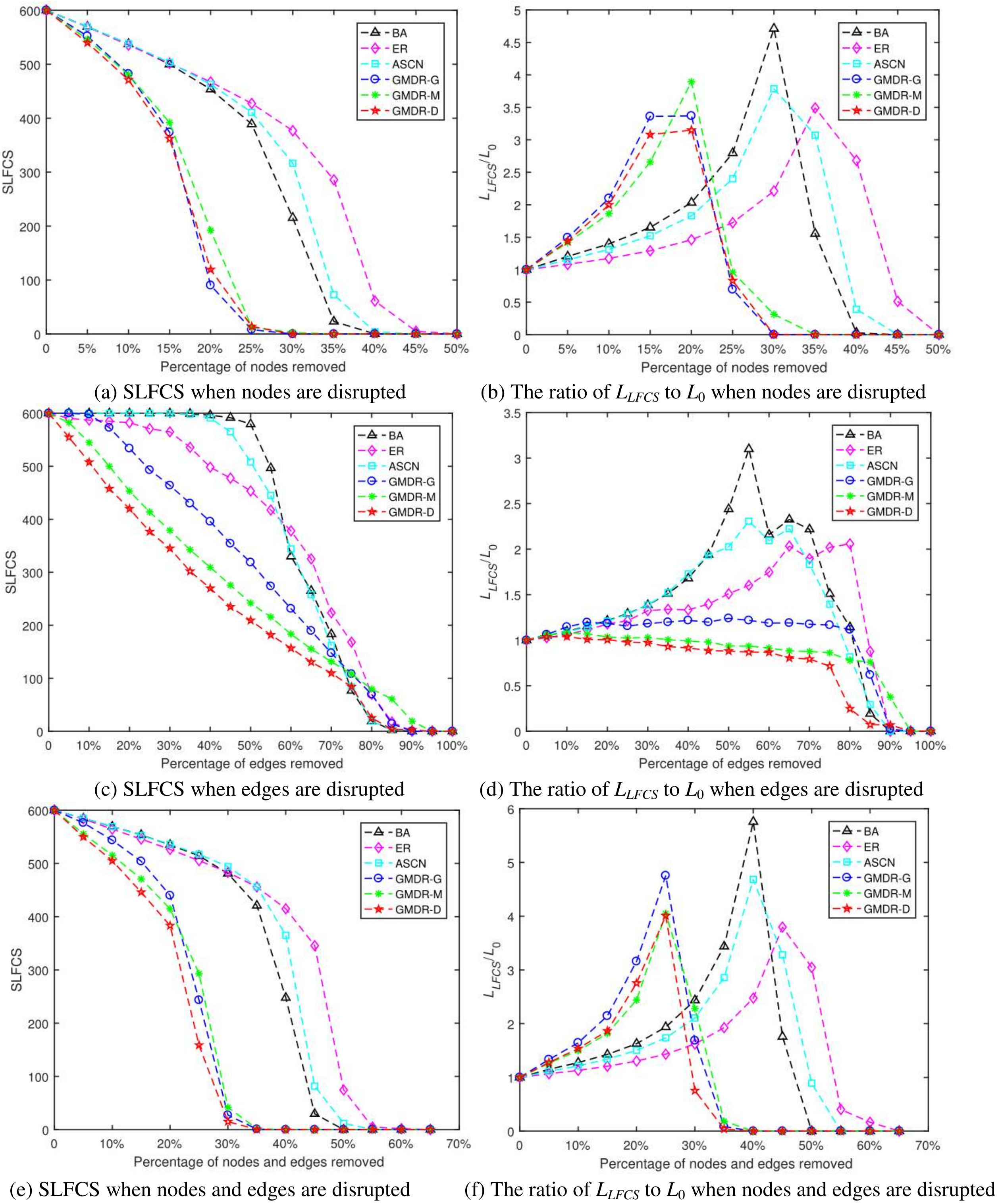
Figures 3(c) and 3(d) reflect the resilience of BA, ER, ASCN, and GMDR models when only edges are disrupted in random disruptions. As shown in Figure 3(c), SLFCSs of these models first decrease slowly with the removal of edges, and then drop rapidly when 70% of edges are removed. It means that they are very resilient in this case. In Figure 3(d), the average path length of GMDR model increases more slowly than that of BA model, while that of BA model increases more slowly than that of ASCN and ER models. The average path length of ER model increases the fastest. Moreover, according to the order of inflection points, we can see that ER model first appears an inflection point, then ASCN and BA models, and finally GMDR model. Therefore, GMDR model is the most resilient when edges are disrupted randomly, BA model is better than ASCN model, and ER model is the worst. Similarly, according to Figures 3(e) and 3(f), similar results can be obtained as shown in Figures 3(c) and 3(d) when nodes and edges are disrupted simultaneously in random disruptions. In a word, BA, ER, ASCN, and GMDR models are resilient to random disruptions. GMDR model performs best, BA model is better than ASCN model, and ER model performs worst.

C. SIMULATION RESULTS OF TARGETED DISRUPTIONS

Figure 4 shows the responses of BA, ER, ASCN, and GMDR models to targeted disruptions. Figure 4(a) shows that the SLFCS of GMDR model drops rapidly as nodes are removed. For example, when 30% of nodes are removed, GMDR model has collapsed. This means that GMDR model is very vulnerable when nodes are disrupted in targeted disruptions. BA model is slightly better than GMDR model, but it is also vulnerable. When 35% of nodes are removed, BA model almost collapses, while about half of the nodes in ER model remain connected. Similarly, ASCN model is slightly better than BA model, but worse than ER model. Therefore, ER model is more resilient than ASCN, BA, and GMDR models when only nodes are disrupted in targeted disruptions. According to the change of the average path length of each model in Figure 4(b), the same result can be obtained as Figure 4(a). Figures 4(c) and 4(d) reflect the resilience of these models when only edges are disrupted in targeted disruptions. As shown in Figure 4(c), SLFCS of GMDR model shows an obvious downward trend after a few edges are removed. The curves of BA, ER, and ASCN models decline more slowly than that of GMDR model. Obviously, SLFCSs of BA and ASCN models drop very slowly in the early stage, but rapidly in the later stage. Figure 4(d) shows that the average path length of GMDR model starts to decline after a transient rise. BA and ASCN models appear inflection points when 55% of edges are removed, and ER model appears an inflection point when 80% of edges are removed. The average path length of ASCN model increases more slowly than that of BA model. Thus, GMDR model is very vulnerable, ASCN model performs better than BA model, and ER model performs best in this case. Figures 4(e) and 4(f) show the responses of these models when nodes and edges are disrupted simultaneously in targeted disruptions. The curve shapes in Figures 4(e) and 4(f) are similar to those in Figures 4(a) and 4(b), respectively. Therefore, the same results can be obtained as shown in Figures 4(a) and 4(b). In general, GMDR model is very vulnerable to targeted disruptions. BA model is better than GMDR model, ASCN model is slightly better than BA model, and ER model is the best.

D. SIMULATION RESULTS OF MIXED DISRUPTIONS

Figure 5 shows the responses of BA, ER, ASCN, and GMDR models to mixed disruptions. Figures 5(a) and 5(b) show the results that only nodes are disrupted. As shown in Figure 5(a), the SLFCS of GMDR model drops the fastest. The SLFCS of BA model drops slightly faster than that of ASCN model, and the SLFCS of ER model drops the slowest. For example, when 40% of nodes are removed, GMDR model almost collapses while there are 41% of nodes remain connected in BA model, 53% in ER model, and 48% in ASCN model. Moreover, Figure 5(b) shows that GMDR model first appears an inflection point, then BA model, and finally ASCN and ER models. Therefore, we can know that GMDR model is vulnerable to mixed disruptions of nodes. ASCN model performs better than BA model, and ER model performs best. Figures 5(c) and 5(d) show the results that only edges are disrupted. According to Figure 5(c), the SLFCS of GMDR decreases the fastest in the early stage, but it is opposite in the later stage. According to Figure 5(d), the average path length of GMDR model grows the slowest, and the inflection point of GMDR model appears the latest. Therefore, GMDR model performs best in this case. Similarly, we can know that ER model is better than ASCN model, and ASCN model is better than BA model. Figures 5(e) and 5(f) show the results that nodes and edges are disrupted simultaneously. Their curve shapes are similar to those in Figures 5(a) and 5(b), respectively. Thus, the same results can be obtained as shown in Figures 5(a) and 5(b). In general, GMDR model performs best when only edges are disrupted in mixed disruptions, ER model performs better



(a) SLFCS when nodes are disrupted

(b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

(c) SLFCS when edges are disrupted

(d) The ratio of L_{LFCS} to L_0 when edges are disrupted

(e) SLFCS when nodes and edges are disrupted

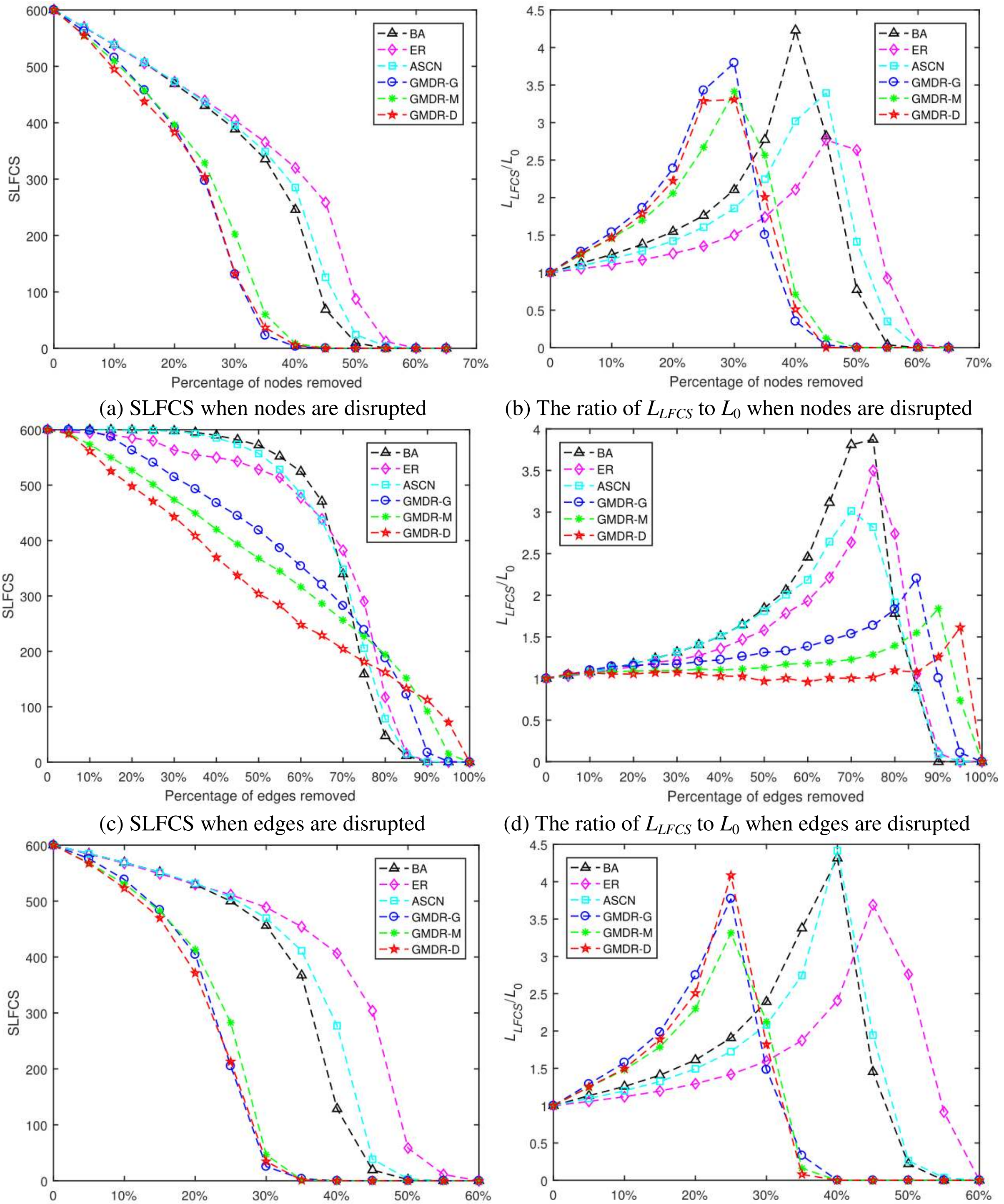
(f) The ratio of L_{LFCS} to L_0 when nodes and edges are disrupted

FIGURE 4. Responses of BA, ER, ASCN, and GMDR models to targeted disruptions. (a) is the SLFCS when nodes are disrupted, (b) is the ratio of L_{LFCS} to L_0 when nodes are disrupted, (c) is the SLFCS when edges are disrupted, (d) is the ratio of L_{LFCS} to L_0 when edges are disrupted, (e) is the SLFCS when nodes and edges are disrupted, and (f) is the ratio of L_{LFCS} to L_0 when nodes and edges are disrupted.

than ASCN model, and ASCN model performs better than BA model. In the other two cases, GMDR model is the worst while ER model is the best, and ASCN model is better than BA model.

E. INFLUENCE OF PARAMETERS OF GMDR ON SUPPLY CHAIN NETWORK RESILIENCE

The parameters of GMDR model are shown in Table 4. As demonstrated in [5], the more even the distribution of



(a) SLFCS when nodes are disrupted

(b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

(c) SLFCS when edges are disrupted

(d) The ratio of L_{LFCS} to L_0 when edges are disrupted

(e) SLFCS when nodes and edges are disrupted

(f) The ratio of L_{LFCS} to L_0 when nodes and edges are disrupted

FIGURE 5. Responses of BA, ER, ASCN, and GMDR models to mixed disruptions. (a) is the SLFCS when nodes are disrupted, (b) is the ratio of L_{LFCS} to L_0 when nodes are disrupted, (c) is the SLFCS when edges are disrupted, (d) is the ratio of L_{LFCS} to L_0 when edges are disrupted, (e) is the SLFCS when nodes and edges are disrupted, and (f) is the ratio of L_{LFCS} to L_0 when nodes and edges are disrupted.

enterprises with different roles, the better the resilience of an SCN, i.e., an SCN performs well when *s*: *m*: *d*: *r* = 1: 1: 1: 1. In addition, the influence of parameters *N*, *G*, and *W* on SCN resilience can be ignored [5]. As described in GMDR model, the parameter *Z* acts on the maturity and decline stages of an SCN. In the maturity stage, the number of nodes entering and exiting is equal, an SCN will keep a certain balance. Thus, the influence of parameter *Z* is slight

TABLE 4. Parameters of GMDR model

Parameters	Description
s: m: d: r	Proportion of suppliers, manufacturers, distributors and retailers in an SCN.
N	The total number of nodes in an SCN.
N_0	The initial number of nodes.
G	The number of new nodes per entry.
W	The number of old nodes connected to a new node.
Z	Number of repetitions.
α	An adjustable priority parameter of degree and fitness.
β	An adjustable priority parameter of distance.
f	Node fitness.

and can be ignored. In the decline stage, there are more nodes exiting an SCN, so the performance of an SCN will decrease with the increase of Z [5]. Zhao *et al.* [1] pointed out that the parameter N_0 has a slight impact on SCN resilience. Therefore, this paper mainly studies the influence of parameters α, β, and f on SCN resilience. According to the results of front experiments, GMDR model is very sensitive to targeted disruptions, especially when nodes are disrupted. Moreover, the GMDR-G, GMDR-M, and GMDR-D models have similar resilience. Therefore, we use GMDR-G model to generate an SCN and study the influence of parameters α, β, and f on SCN resilience when nodes are disrupted in targeted disruptions. The settings of other parameters remain unchanged. Every situation runs 20 times independently and takes the average value.

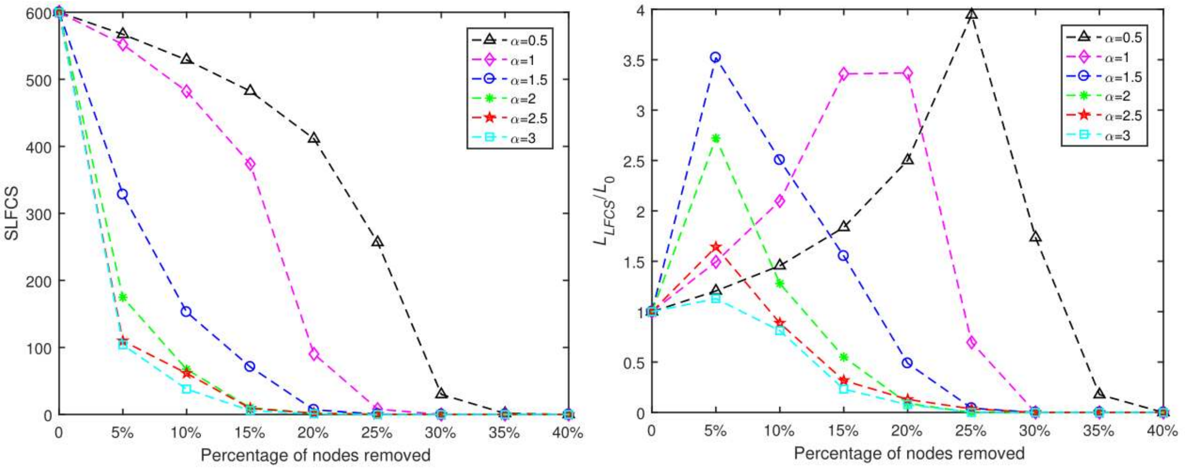
First, we study the influence of parameters α and β on SCN resilience. Keep $\beta = 1$, and α changes from 0.5 to 3 with a step size of 0.5; then keep $\alpha = 1$, and β changes from 0.5 to 3 with a step size of 0.5. Figures 6 and 7 show the results. Figure 6(a) shows that the larger the value of α, the faster the SLFCS drops. For example, when 5% of nodes are removed, about 95% of nodes remain connected when $\alpha = 0.5$, and about 17% of nodes remain connected when $\alpha = 3$. Therefore, we can know that α has a significant effect on SCN resilience. The larger the value of α, the worse the SCN resilience. Figure 6(b) shows that the larger the value of α, the earlier the inflection point appears. Thus, the same result can be obtained as in Figure 6(a). As can be seen from Figure 7, with the increase of β, the SLFCS decreases slightly, the average path length of the network increases slightly, and the inflection point appears earlier. This means that β has a slight impact on SCN resilience. As the value of β increases, the resilience of the SCN will slightly decline.

As mentioned in [58] and [73]–[74], node fitness obeys a certain probability distribution. In this section, we study the influence of fitness on SCN resilience in different probability distribution functions. In addition to the normal distribution used in front experiments, the classical Poisson distribution, discrete uniform distribution, and exponential distribution are also used. The mean value of fitness is the same in different distribution functions. The results are shown in Figure 8. Figure 8(a) shows that SLFCS decreases the fastest under exponential distribution and the slowest under normal and Poisson distributions. Figure 8(b) shows that the inflection points appear in the order of exponential distribution, discrete uniform distribution, normal distribution, and Poisson distribution. This means that node fitness obeys different probability distribution functions will have a significant impact on SCN resilience. Among the distribution functions used, the resilience of the SCN is the best when node fitness follows normal distribution and Poisson distribution, followed by discrete uniform distribution, and the worst is exponential distribution.

V. RESULT ANALYSIS AND DISCUSSION

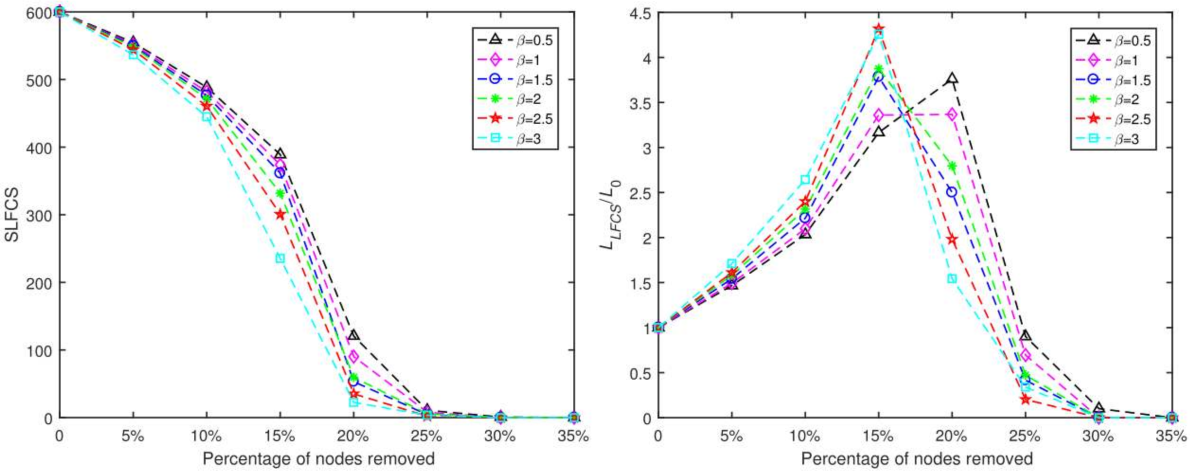
According to the above simulation results, ER model is resilient to both targeted and random disruptions, which also verifies the results of previous studies [1] and [5]. Because the degree distribution of nodes in ER model follows a Poisson distribution, i.e., the distribution of degrees is quite uniform. Node disruptions, whether random or targeted, usually have an impact on a local scope. Thus, it is also not surprising that ER model can also perform well in mixed disruptions. Moreover, the impact of a node being disrupted is greater than that of an edge being disrupted. This is because a node may have multiple edges, and the failure of a node will cause the failures of the edges connected with the node. On the contrary, the failure of one edge does not necessarily lead to the failure of one node. ER model corresponds to the random connection rule, but in a real SCN, enterprises do not select partners completely at random [5]. Previous studies have found that most SCNs are scale-free networks [47], [75].

Different from ER model, BA model corresponds to the degree-based priority connection rule, and the degree distribution of its nodes follows a power-law distribution, which is exactly the structural feature of a scale-free network. This means that a small number of nodes are connected with most nodes in the SCN generated by BA model, so most nodes have very small degrees. Therefore, even if the nodes with small degrees are disrupted, the impact on the whole SCN is not great, but once the nodes with large degrees are disrupted, the whole SCN will collapse rapidly. Because of this characteristic, BA model is resilient to random disruptions, but vulnerable to targeted disruptions. In addition, we observe that removing a few important edges does not have a great impact on SCN resilience. This is because a node with large degree has many edges, which are considered to be important. Even if



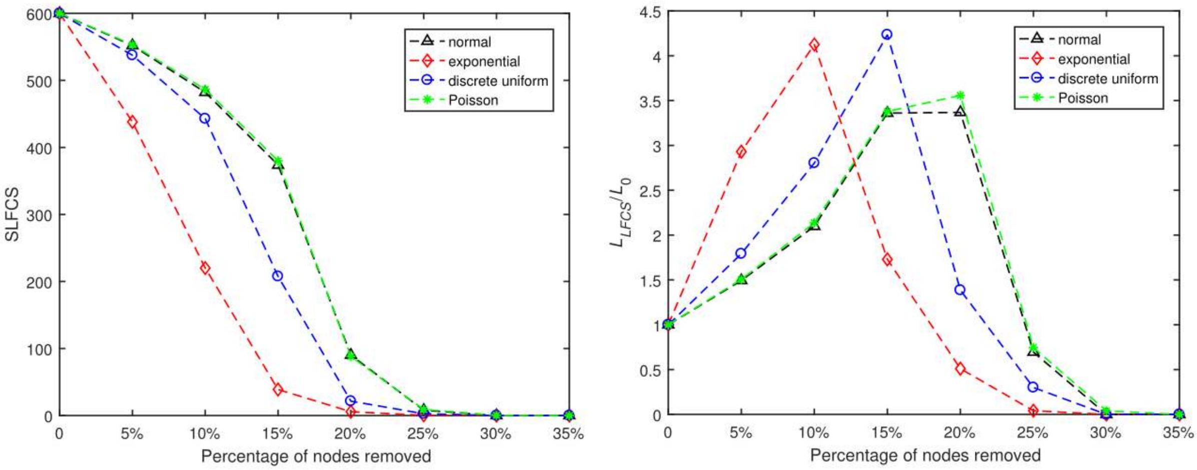
(a) SLFCS when nodes are disrupted (b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

FIGURE 6. **The influence of parameter *α* on SCN resilience when nodes are disrupted in targeted disruptions. (a) is the SLFCS and (b) is the ratio of L_{LFCS} to L_0.**



(a) SLFCS when nodes are disrupted (b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

FIGURE 7. **The influence of parameter *β* on SCN resilience when nodes are disrupted in targeted disruptions. (a) is the SLFCS and (b) is the ratio of L_{LFCS} to L_0.**



(a) SLFCS when nodes are disrupted (b) The ratio of L_{LFCS} to L_0 when nodes are disrupted

FIGURE 8. **The influence of parameter *f* on SCN resilience when nodes are disrupted in targeted disruptions. (a) is the SLFCS and (b) is the ratio of L_{LFCS} to L_0.**

some of these edges are removed, a network can still maintain good connectivity. However, the function of the whole SCN will suffer a great loss when most of these edges are removed. In BA model, the node with larger degree is more likely to connect with more new nodes. This reflects the phenomenon that the rich are getting richer in reality. However, as aforementioned, the degree of an old node increases over time. If an old enterprise cannot adapt to the development of society, it will eventually be eliminated. On the contrary, if a young enterprise has good development potential and can provide good products, it may also develop very well. Therefore, not only degree but also fitness should be considered in the model of generating an SCN.

ASCN model is an agile SCN model, which is similar to BA model. The connection rule of ASCN model is the priority connection based on node strength and distance. This means that enterprises will give priority to enterprises with high strength and close distance when choosing partners. Compared with BA model, the connections of nodes in an SCN generated by ASCN model are relatively more uniform. Even if important nodes with a large number of connections are disrupted, the number of nodes that remain connected is relatively large. Therefore, the SCN generated by ASCN model is slightly more resilient to targeted disruptions and slightly more vulnerable to random disruptions than the SCN generated by BA model. However, ASCN model also does not consider the exit and reselection of enterprises.

The SCN generated by GMDR model is also a scale-free network. Therefore, GMDR model is also resilient to random disruptions, but vulnerable to targeted disruptions. Unlike BA model, GMDR model takes into account both degree and fitness, so even a young node may get a lot of connections. The priority connection rule based on degree and fitness corresponds to the phenomenon that high-quality enterprises with more partners can obtain more cooperation in reality. The distance-based connection rule of GMDR model corresponds to the localization of enterprise cooperation, which means the convenience of cooperation. In addition, GMDR model considers the exit and reselection of enterprises, and in the reselection, enterprises are more inclined to cooperate with local high-quality enterprises with more partners. This will lead to the emergence of a strong-strong alliance, which is also a very important phenomenon in an SCN. Once the alliance is destroyed, the resilience of an SCN will be seriously affected. Therefore, the resilience of GMDR model will rapidly degrade when the important nodes and/or edges are disrupted in targeted disruptions. The priority connection rule based on degree corresponds to the concern of an enterprise on the cost and efficiency of cooperation [1], [5]. Then the priority connection rule based on degree and fitness corresponds to the concerns of cost, efficiency, and quality. Cooperating with high-quality enterprises with more partners will help enterprises to expand cooperative business and obtain greater benefits. However, if only paying attention to these factors, the final result may be the vulnerability to targeted disruptions [1]. Therefore, an enterprise should not only focus on the enterprise with large degree, large fitness and close distance when choosing a partner. Meanwhile, if we want to design a SCN that is resilient to mixed disruptions, we should not only consider the priority connection, but also consider other strategies to make up for the shortcomings of priority connection, such as the random connection of ER model. In particular, we should identify and protect the important nodes and the cooperation between them in an SCN.

Through the study of the influence of parameters α, β, and f on SCN resilience, we find that α has a significant impact on SCN resilience. The larger the value of α, the worse the SCN resilience. This is because the larger the value of α, the more enterprises tend to cooperate with the enterprise with large degree and fitness. When $\alpha > 1$, there will be a hub connected to almost all nodes in the network. Once the hub is removed, the entire network will quickly collapse. When $\alpha > 2$, the resilience of the corresponding SCN changes slightly as α increases, because a hub is fully connected to other nodes in the network. Even if α increases, the structure of corresponding SCN will not change much. Compared with α, β has a slight impact on SCN resilience. As β increases, the resilience of the corresponding SCN decreases slightly. This is because when a node is connected with a node with large degree and fitness, the node can access other nodes more conveniently. Although the probability of choosing a closer enterprise will increase when the value of β becomes larger, it will not change greatly. In addition, an SCN is very vulnerable when the fitness f follows the exponential distribution. In contrast, it performs well when f follows the Poisson distribution. In the exponential distribution, the distribution of f in the network is very uneven, while it is the opposite in the Poisson distribution. The node with large f is connected to most nodes in the network. If the difference of f in a network is particularly large, there will be a winner-takes-all phenomenon [58], [74]. Once the node with large f is removed, the whole network will be greatly affected. Therefore, the more uniform the distribution of f in an SCN, the better the SCN resilience.

In our model, we consider the exit and reselection processes of enterprises. When enterprises make reselection, they will be attracted by dominant enterprises again, so that dominant enterprises can accumulate lager degrees. This will lead to the increasing importance of dominant enterprises in an SCN. Once these enterprises are at risk, the resilience of the entire network will be severely affected. Moreover, the reselection of enterprises may form an alliance between dominant enterprises, which can bring great benefits to the enterprises within the alliance. Similarly, once this relationship is destroyed, the resilience of the network will also be affected. Therefore, the SCN generated by our model is very vulnerable to targeted disruptions. Compared with other models, it better reflects the impact of the enterprise's reselection process on SCN resilience.

In summary, the following important inspirations for managers can be obtained through the research of this paper. First, managers should understand the supply chain system from a macro perspective. In an SCN, the micro behaviors of enterprises will bring about changes in the network structure, thus affecting the performance of the network. Therefore, in order to better respond to disruptions and implement management, managers should have an understanding of SCN structures. Second, it is necessary to discover and protect the important enterprises in an SCN. Generally, the enterprise that plays a pivotal role in an SCN is very important. It usually has cooperative relationships with most enterprises in the network. Once it is attacked, the entire SCN will be greatly affected. Therefore, it often becomes the primary target of malicious attacks. Third, it is necessary to protect the alliance relationship between important enterprises. An important enterprise is often attached by many other enterprises, thus these enterprises will form a group. Therefore, the alliance between two important enterprises often brings huge benefits to these two groups. Once this alliance is destroyed, it will have a huge impact on the entire SCN. Fourth, it is necessary to reduce the centrality of an SCN. Although the high centrality of the network helps to improve the operational efficiency of the network, it also increases the vulnerability of the network. Therefore, in order to prevent the serious impact of the disruption of important enterprises, managers can reduce the centrality of the network by cooperating with more other enterprises. Meanwhile, reducing the centrality of an SCN can also promote the diversification of cooperation and prevent monopoly.

VI. CONCLUSION

This paper studied the influence of the structure of an SCN on SCN resilience from the perspective of complex networks, so as to provide insights for the design of a resilient SCN. First, we propose a new SCN model called GMDR, which takes into account the exit and reselection of enterprises. Compared with the previous models, the connection rules of this model consider degree, fitness and distance, which can better reflect a real SCN. Then, different disruption scenarios are simulated, and the resilience of SCNs generated by BA, ER, ASCN, and GMDR models is compared. Finally, the influence of the parameters of GMDR model on SCN resilience is studied.

The simulation results show that GMDR model is resilient to random disruptions, but very vulnerable to targeted disruptions, especially when the strong-strong alliance is destroyed, it will have a great impact on the whole SCN. In addition, the effect of α on SCN resilience is significant. The larger the value of α, the worse the SCN resilience. The parameter β has a slight effect on SCN resilience. As the value of β increases, the SCN resilience will decrease slightly. Meanwhile, the more uniform the distribution of f in an SCN, the better the SCN resilience.

The main contributions of this study are as follows. In terms of theory, this study considers the exit and reselection of enterprises that have been overlooked in previous studies, and constructs an SCN model based on node degree, fitness, and distance. Moreover, this study fully considers different disruption types and objects, and uses computer simulations to measure the resilience of SCN under different disruption scenarios. Therefore, this study enriches the SCN theory and expands the research on SCN resilience. In terms of practice, this study provides some insights for the construction of SCNs and disruption management. Managers should have an understanding of SCN structures, and strengthen the protection of important enterprises and their alliance relationships in an SCN. Meanwhile, enterprises should enhance the diversification of cooperation and avoid excessive dependence on important enterprises, so as to prevent the SCN resilience from being seriously affected when important enterprises have risks.

There are also some limitations that can be resolved to extend this research. First, this study does not consider the risk propagation in an SCN. In fact, due to the interaction between enterprises, the disruption of any enterprise will have an impact on the enterprises associated with it, thus the whole SCN will be affected. Therefore, capturing the risk propagation can help enterprises better deal with disruptions. In particular, understanding how risks are spread in SCNs will facilitate the construction of resilient SCNs. Second, some important factors are not considered, such as the capacity of a node and the weight of an edge. In reality, the capacity of an enterprise is limited and cannot expand indefinitely. Moreover, the strength of cooperation between enterprises is different. Some partnerships are strong, while others are not. Considering these factors can help us to depict SCNs more realistically. In addition, the exploration of the relationship between the resilience of individual enterprises and that of the whole network will also be beneficial to supply chain management. Future research can also try to study the collaboration and competition [76]–[78] between enterprises in SCNs from the perspective of cost and resilience. Usually, the pursuit of resilience often leads to increased costs. Therefore, how to ensure the SCN resilience at a relatively low cost is also an interesting direction.

REFERENCES

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

[2] M. Piraveenan, H. Jing, P. Matous, and Y. Todo, "Topology of international supply chain networks: A case study using factset revere datasets," *IEEE Access*, vol. 8, pp. 154540–154559, Aug. 2020.

[3] S. Hosseini, D. Ivanov, and A. Dolgui, "Review of quantitative methods for supply chain resilience analysis," *Transp. Res. Part E Logist. Transp. Rev*., vol. 125, pp. 285–307, May. 2019.

[4] V. Dixit, P. Verma, and M. K. Tiwari, "Assessment of pre and post-disaster supply chain resilience based on network structural parameters with CVaR as a risk measure," *Int. J. Prod. Econ.*, vol. 227, Sep. 2020, Art. no. 107655.

[5] X. Q. Shi, W. Long, Y. Y. Li, D. S. Deng, Y. L. Wei, and H. G. Liu, "Research on supply network resilience considering random and targeted disruptions simultaneously," *Int. J. Prod. Res.*, vol. 58, no. 21, pp. 6670–6688, Nov. 2019.

[6] Y. Kim, Y. S. Chen, and K. Linderman, "Supply network disruption and resilience: A network structural perspective," *J. Oper. Manag.*, vol. 33–34, pp. 43–59, Jan. 2015.

[7] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: Cascading failure and robustness," *Phys. A Stat. Mech. its Appl.*, vol. 443, no. 2, pp. 58–69, Feb. 2016.

[8] A. Dolgui, D. Ivanov, and B. Sokolov, "Reconfigurable supply chain: the X-network," *Int. J. Prod. Res.*, vol. 58, no. 13, pp. 4138–4163, Jul. 2020.

[9] D. Ivanov and A. Dolgui, "Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak," *Int. J. Prod. Res.*, vol. 58, no. 10, pp. 2904–2915, May. 2020.

[10] N. J. Rowan and J. G. Laffey, "Challenges and solutions for addressing critical shortage of supply chain for personal and protective equipment (PPE) arising from Coronavirus disease (COVID19) pandemic – Case study from the Republic of Ireland," *Sci. Total Environ.*, vol. 725, Jul. 2020, Art. no. 138532.

[11] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, Drones, AI, Blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, May. 2020.

[12] N. Shin and S. Park, "Supply chain leadership driven strategic resilience capabilities management: A leader-member exchange perspective," *J. Bus. Res.*, vol. 122, pp. 1–13, Jan. 2021.

[13] B. R. Tukamuhabwa, M. Stevenson, J. Busby, and M. Zorzini, "Supply chain resilience: Definition, review and theoretical foundations for further study," *Int. J. Prod. Res.*, vol. 53, no. 18, pp. 5592–5623, Sep. 2015.

[14] J. T. Margolis, K. M. Sullivan, S. J. Mason, and M. Magagnotti, "A multi-objective optimization model for designing resilient supply chain networks," *Int. J. Prod. Econ.*, vol. 204, pp. 174–185, Oct. 2018.

[15] W. J. Tan, A. N. Zhang, and W. Cai, "A graph-based model to measure structural redundancy for supply chain resilience," *Int. J. Prod. Res.*, vol. 57, no. 20, pp. 6385–6404, Oct. 2019.

[16] S. Hosseini and D. Ivanov, "A new resilience measure for supply networks with the ripple effect considerations: a Bayesian network approach," *Ann. Oper. Res.*, early access, Dec 9, 2020. doi: 10.1007/s10479-019-03350-8.

[17] K. Zhao, Z. Zuo, and J. V. Blackhurst, "Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach," *J. Oper. Manag.*, vol. 65, no. 2, pp. 190–212, Mar. 2019.

[18] F. Sabouhi, M. S. Jabalameli, A. Jabbarzadeh, and B. Fahimnia, "A multi-cut L-shaped method for resilient and responsive supply chain network design," *Int. J. Prod. Res.*, vol. 58, no. 24, pp. 7353–7381, Dec. 2020.

[19] M. Kamalahmadi and M. M. Parast, "A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research," *Int. J. Prod. Econ.*, vol. 171, pp. 116–133, Jan. 2016.

[20] J. Pires Ribeiro and A. Barbosa-Povoa, "Supply chain resilience: Definitions and quantitative modelling approaches – A literature review," *Comput. Ind. Eng.*, vol. 115, pp. 109–122, Jan. 2018.

[21] F. Lücker, R. W. Seifert, and I. Biçer, "Roles of inventory and reserve capacity in mitigating supply chain disruption risk," *Int. J. Prod. Res.*, vol. 57, no. 4, pp. 1238–1249, Feb. 2019.

[22] S. Hosseini and K. Barker, "A Bayesian network model for resilience-based supplier selection," *Int. J. Prod. Econ.*, vol. 180, pp. 68–87, Oct. 2016.

[23] J. Namdar, X. P. Li, R. Sawhney, and N. Pradhan, "Supply chain resilience for single and multiple sourcing in the presence of disruption risks," *Int. J. Prod. Res.*, vol. 56, no. 6, pp. 2339–2360, Sep. 2017.

[24] X. Wang, M. Herty, and L. Zhao, "Contingent rerouting for enhancing supply chain resilience from supplier behavior perspective," *Int. Trans. Oper. Res.*, vol. 23, no. 4, pp. 775–796, Jul. 2016.

[25] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, "Building organizational resilience in the face of multiple disruptions," *Int. J. Prod. Econ.*, vol. 197, pp. 63–83, Mar. 2018.

[26] C. W. Craighead, J. Blackhurst, M. J. Rungtusanatham, and R. B. Handfield, "The severity of supply chain disruptions: Design characteristics and mitigation capabilities," *Decis. Sci.*, vol. 38, no. 1, pp. 131–156, Feb. 2007.

[27] M. Baghersad and C. W. Zobel, "Assessing the extended impacts of supply chain disruptions on firms: An empirical study," *Int. J. Prod. Econ.*, vol. 23, Jan. 2021, Art. no. 107862.

[28] U. R. de Oliveira, F. A. S. Marins, H. M. Rocha, and V. A. P. Salomon, "The ISO 31000 standard in supply chain risk management," *J. Clean. Prod.*, vol. 151, pp. 616–633, May. 2017.

[29] R. Sreedevi and H. Saranga, "Uncertainty and supply chain risk: The moderating role of supply chain flexibility in risk mitigation," *Int. J. Prod. Econ.*, vol. 193, pp. 332–342, Nov. 2017.

[30] D. Ivanov and A. Dolgui, "Low-certainty-need (LCN) supply chains: A new perspective in managing disruption risks and resilience," *Int. J. Prod. Res.*, vol. 57, no. 15–16, pp. 5119–5136, Aug. 2019.

[31] S. DuHadway, S. Carnovale, and B. Hazen, "Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery," *Ann. Oper. Res.*, vol. 283, no. 1–2, pp. 179–198, Dec. 2019.

[32] Y. C. Saglam, S. Y. Çankaya, and B. Sezen, "Proactive risk mitigation strategies and supply chain risk management performance: An empirical analysis for manufacturing firms in Turkey," *J. Manuf. Technol. Manag.*, early access, Dec 10, 2020. doi: 10.1108/JMTM-08-2019-0299.

[33] V. L. M. Spiegler, M. M. Naim, and J. Wikner, "A control engineering approach to the assessment of supply chain resilience," *Int. J. Prod. Res.*, vol. 50, no. 21, pp. 6162–6187, Aug. 2012.

[34] D. Ivanov, A. Dolgui, and B. Sokolov, "Applicability of optimal control theory to adaptive supply chain planning and scheduling," *Annu. Rev. Control*, vol. 36, no. 1, pp. 73–84, Apr. 2012.

[35] T. J. Yang and W. G. Fan, "Information management strategies and supply chain performance under demand disruptions," *Int. J. Prod. Res.*, vol. 54, no. 1, pp. 8–27, Jan. 2016.

[36] V. L. M. Spiegler, A. T. Potter, M. M. Naim, and D. R. Towill, "The value of nonlinear control theory in investigating the underlying dynamics and resilience of a grocery supply chain," *Int. J. Prod. Res.*, vol. 54, no. 1, pp. 265–286, Jan. 2016.

[37] D. Ivanov, S. Sethi, A. Dolgui, and B. Sokolov, "A survey on control theory applications to operational systems, supply chain management, and Industry 4.0," *Annu. Rev. Control*, vol. 46, pp. 134–147, Oct. 2018.

[38] S. R. Yadav, N. Mishra, V. Kumar, and M. K. Tiwari, "A framework for designing robust supply chains considering product development issues," *Int. J. Prod. Res.*, vol. 49, no. 20, pp. 6065–6088, Oct. 2011.

[39] X. W. Qin, X. Liu, and L. X. Tang, "A two-stage stochastic mixed-integer program for the capacitated logistics fortification planning under accidental disruptions," *Comput. Ind. Eng.*, vol. 65, no. 4, pp. 614–623, Aug. 2013.

[40] Y. Kristianto, A. Gunasekaran, P. Helo, and Y. Hao, "A model of resilient supply chain network design: A two-stage programming with fuzzy shortest path," *Expert Syst. Appl.*, vol. 41, no. 1, pp. 39–49, Jan. 2014.

[41] M. J. Ramezankhani, S. A. Torabi, and F. Vahidi, "Supply chain performance measurement and evaluation: A mixed sustainability and resilience approach," *Comput. Ind. Eng.*, vol. 126, pp. 531–548, Dec. 2018.

[42] A. Pavlov, D. Ivanov, A. Dolgui, and B. Sokolov, "Hybrid fuzzy-probabilistic approach to supply chain resilience assessment," *IEEE Trans. Eng. Manag.*, vol. 65, no. 2, pp. 303–315, Apr. 2018.

[43] K. Zhao, A. Kumar, and J. Yen, "Achieving high robustness in supply distribution networks by rewiring," *IEEE Trans. Eng. Manag.*,

vol. 58, no. 2, pp. 347–362, May. 2011.

[44] A. Nair and J. M. Vidal, “Supply network topology and robustness against disruptions – An investigation using multi-agent model,” *Int. J. Prod. Res.*, vol. 49, no. 5, pp. 1391–1404, Mar. 2011.

[45] J. Y. Sun, J. M. Tang, W. P. Fu, Z. R. Chen, and Y. R. Niu, “Construction of a multi-echelon supply chain complex network evolution model and robustness analysis of cascading failure,” *Comput. Ind. Eng*., vol. 144, Jun. 2020, Art. no. 106457.

[46] A. Ledwoch, H. Yasarcan, and A. Brintrup, “The moderating impact of supply network topology on the effectiveness of risk management,” *Int. J. Prod. Econ.*, vol. 197, pp. 13–26, Mar. 2018.

[47] S. S. Perera, M. G. H. Bell, M. Piraveenan, D. Kasthurirathna, and M. Parhi, “Topological structure of manufacturing industry supply chain networks,” *Complexity*, vol. 2018, Oct. 2018, Art. no. 3924361.

[48] Y. C. Wang and F. P. Zhang, “Modeling and analysis of under-load-based cascading failures in supply chain networks,” *Nonlinear Dyn.*, vol. 92, no. 3, pp. 1403–1417, May. 2018.

[49] K. Zhao, K. Scheibe, J. Blackhurst, and A. Kumar, “Supply chain network robustness against disruptions: Topological analysis, measurement, and optimization,” *IEEE Trans. Eng. Manag.*, vol. 66, no. 1, pp. 127–139, Feb. 2019.

[50] B. Xiong, R. Fan, S. Wang, B. X. Li, and C. Wang, “Performance evaluation and disruption recovery for military supply chain network,” *Complexity*, vol. 2020, May. 2020, Art. no. 9760604.

[51] H. P. Thadakamalla, U. N. Raghavan, S. Kumara, and R. Albert, “Survivability of multiagent-based supply networks: A topological perspective,” *IEEE Intell. Syst.*, vol. 19, no. 5, pp. 24–31, Sep. 2004.

[52] A. L. Barabási and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, no. 5439, pp. 509–512, Nov. 1999.

[53] P. Erdos and A. Renyi, “On random graphs,” *Publ. Math*., vol. 6, pp. 290–297, Jan. 1959.

[54] L. Tang, K. Jing, J. He, and H. E. Stanley, “Robustness of assembly supply chain networks by considering risk propagation and cascading failure,” *Phys. A Stat. Mech. its Appl.*, vol. 459, pp. 129–139, Oct. 2016.

[55] A. Dolgui and D. Ivanov, “Ripple effect and supply chain disruption management: new trends and research directions,” *Int. J. Prod. Res.*, vol. 59, no. 1, pp. 102–109, Jan. 2021.

[56] S. Perera, D. Kasthurirathna, M. Bell, and M. Bliemer, “Topological rationality of supply chain networks,” *Int. J. Prod. Res.*, vol. 58, no. 10, pp. 3126–3149, May. 2020.

[57] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks,” *Nature*, vol. 393, no. 6684, pp. 440–442, Jun. 1998.

[58] G. Bianconi and A. L. Barabási, “Bose-Einstein condensation in complex networks,” *Phys. Rev. Lett.*, vol. 86, no. 24, pp. 5632–5635, Jun. 2001.

[59] Q. Xuan, F. Du, Y. J. Li, and T. J.Wu, “A framework to model the topological structure of supply networks,” *IEEE Trans. Autom. Sci. Eng.,* vol. 8, no. 2, pp. 442–446, Apr. 2011.

[60] J. W. Rivkin and N. Siggelkow, “Patterned interactions in complex systems: Implications for exploration,” *Manage. Sci.*, vol. 53, no. 7, pp. 1068–1085, Jul. 2007.

[61] K. Klemm and V. M. Eguíluz, “Growing scale-free networks with small-world behavior,” *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, vol. 65, no. 5, May. 2002, Art. no. 057102.

[62] N. R. Xu, J. B. Liu, D. X. Li, and J. Wang, “Research on evolutionary mechanism of agile supply chain network via complex network theory,” *Math. Probl. Eng.*, vol. 2016, Jan. 2016, Art. no. 4346580.

[63] W. Wang, W. N. Street, and R. E. DeMatta, “Topological resilience analysis of supply networks under random disruptions and targeted attacks,” in *Proc. 2015 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2015*, Aug. 2015, pp. 250–257.

[64] H. Xia, “Improve the resilience of multilayer supply chain networks,” *Complexity*, vol. 2020, Jan. 2020, Art. no. 6596483.

[65] Y. Li and C. W. Zobel, “Exploring supply chain network resilience in the presence of the ripple effect,” *Int. J. Prod. Econ.*, vol. 228, Oct. 2020, Art. no. 107693.

[66] R. Dubey, A. Gunasekaran, S. J. Childe, S. Fosso Wamba, D. Roubaud, and C. Foropon, “Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience,” *Int. J. Prod. Res.*, vol. 59, no. 1, pp. 110–128, Feb. 2019.

[67] T. Bier, A. Lange, and C. H. Glock, “Methods for mitigating disruptions in complex supply chain structures: A systematic literature review,” *Int. J. Prod. Res.*, vol. 58, no. 6, pp. 1835–1856, Mar. 2020.

[68] N. Azad, G. K. D. Saharidis, H. Davoudpour, H. Malekly, and S. A. Yektamaram, “Strategies for protecting supply chain networks against facility and transportation disruptions: An improved benders decomposition approach,” *Ann. Oper. Res.*, vol. 210, no. 1, pp. 125–163, Nov. 2013.

[69] B. Adenso-Díaz, J. Mar-Ortiz, and S. Lozano, “Assessing supply chain robustness to links failure,” *Int. J. Prod. Res.*, vol. 56, no. 15, pp. 5104–5117, Aug. 2018.

[70] R. Reyes Levalle and S. Y. Nof, “Resilience by teaming in supply network formation and re-configuration,” *Int. J. Prod. Econ.*, vol. 160, pp. 80–93, Feb. 2015.

[71] T. H. Grubesic, T. C. Matisziw, A. T. Murray, and D. Snediker, “Comparative approaches for assessing network vulnerability,” *Int. Reg. Sci. Rev.*, vol. 31, no. 1, pp. 88–112, Jan. 2008.

[72] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, “Attack vulnerability of complex networks,” *Phys. Rev. E - Stat. Physics, Plasmas, Fluids, Relat. Interdiscip. Top.*, vol. 65, no. 5, May. 2002, Art. no. 056109.

[73] G. Caldarelli, A. Capocci, P. De Los Rios, and M. A. Muñoz, “Scale-free networks from varying vertex intrinsic fitness,” *Phys. Rev. Lett.*, vol. 89, no. 25, Dec. 2002, Art. no. 258702.

[74] S. Ghadge, T. Killingback, B. Sundaram, and D. A. Tran, “A statistical construction of power-law networks,” *Int. J. Parallel, Emergent Distrib. Syst.*, vol. 25, no. 3, pp. 223–235, Jun. 2010.

[75] A. Brintrup, Y. Wang, and A. Tiwari, “Supply networks as complex systems: A network-science-based characterization,” *IEEE Syst. J.*, vol. 11, no. 4, pp. 2170–2181, Dec. 2017.

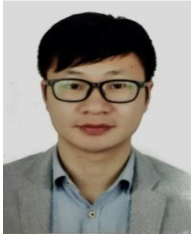
[76] Y. Liu, D. D. Wang, and Q. Xu, “A supply chain coordination mechanism with suppliers’ effort performance level and fairness concern,” *J. Retail. Consum. Serv.*, vol. 53, Mar. 2020, Art. no. 101950.

[77] A. Hendalianpour, M. Hamzehlou, M. R. Feylizadeh, N. Xie, and M. H. Shakerizadeh, “Coordination and competition in two-echelon supply chain using grey revenue-sharing contracts,” *Grey Syst. Theory Appl.*, early access, Jan 31, 2021. doi: 10.1108/GS-04-2020-0056.

[78] X. Qian, F. T. S. Chan, J. Zhang, M. Yin, and Q. Zhang, “Channel coordination of a two-echelon sustainable supply chain with a fair-minded retailer under cap-and-trade regulation,” *J. Clean. Prod.*, vol. 244, Jan. 2020, Art. no. 118715.

YONGZHENG TIAN received the B.E. degrees in industrial engineering from the Southwest University of Science and Technology, Mianyang, China, in 2015. He is currently pursuing the master’s degree with Southwest University of Science and Technology. His current research interest includes supply chain network resilience.

YUQIANG SHI received the M.S. degree from Sichuan University, Chengdu, China, in 2003. He is currently a professor with Southwest University of Science and Technology, Mianyang, China. His research interests include industrial engineering, intelligent manufacturing, and medical service system.



XIAOQIU SHI received the Ph.D. degree from Sichuan University, Chengdu, China, in 2019. He is currently an assistant professor with Southwest University of Science and Technology, Mianyang, China. His research interests include evolutionary algorithms, complex networks, and machine learning.

MINGHUI LI received the M.S. degree from Southwest University of Science and Technology, Mianyang, China, in 2016. He is currently an assistant professor with Southwest University of Science and Technology, Mianyang, China. His research interests include operational research, system simulations, complex networks, and machine learning.

MIN ZHANG received the M.S. degree from Southwest University of Science and Technology, Mianyang, China, in 2014. He is currently a teaching assistant with Southwest University of Science and Technology, Mianyang, China. His research interests include logistics system optimization and complex networks.