RAIRO-Oper. Res. 58 (2024) 5403–5419
https://doi.org/10.1051/ro/2024207

RAIRO Operations Research
www.rairo-ro.org

OVERLOAD CASCADING FAILURE DETECTION ALGORITHM FOR MULTI-LAYER SUPPLY CHAIN NETWORK CONSIDERING DELAY PROBABILITY FACTOR

Bingfang Lu* and Ranran Li

Abstract. At present, the supply chain is multi-layered and complicated, and its failure detection is based solely on the characteristic threshold, which does not lack the ability to describe the complex supply chain. An overload cascading failure detection algorithm for multi-layer supply chain network considering delay probability is proposed. Based on the multi-layer supply chain network including raw material suppliers, manufacturers, distributors and retailers, the overload cascading failure model of the multi-layer supply chain network is constructed through networking, and the overload cascading failure process of the multi-layer supply chain network is described through three aspects: initial load, node capacity and overload node load distribution. By monitoring and analyzing the status update messages of each node in the supply chain network, and considering the delay probability factor, the node and path that may lead to cascading failure are identified by predicting the delay probability of the next message through the historical message delay probability, and the overload cascading failure detection of the multi-layer supply chain network is realized. The experimental results show that the algorithm can effectively detect the failure of each overloaded enterprise node in the multi-layer supply chain network, which is helpful to enhance the early warning and response ability of the cascade failure of the supply chain network. The algorithm can realize the failure detection of supply chain network under different attack conditions and initial failure ratio of nodes, and measure the anti-risk ability of supply chain network. Under deliberate attack and when the initial attack node is a supplier network layer node, it has a greater impact on the multi-layer supply chain network.

Received December 28, 2023. Accepted October 23, 2024.

1. Introduction

Supply chain network is composed of member organizations connected with core enterprises [1], which are directly or indirectly connected with their suppliers or customers, from the beginning to the consumer. It is not only a logistics chain, an information chain and a capital chain connecting suppliers to users, but also a value-added chain. Materials in the supply chain increase their value due to the processes of processing, packaging and transportation, which brings benefits to related enterprises. The core position of supply chain network in global trade is more and more prominent, and the economic development of countries around the world and people's food, clothing, housing and transportation are inseparable from the normal operation of supply chain network. At present, the perfection of supply chain network has created a more convenient and efficient living

Keywords. Delay probability, supply chain network, node load, node capacity, cascade failure.

Southern Power Grid Supply Chain Group Co., Ltd, Guangzhou, Guangdong 510620, P.R. China.
*Corresponding author: huilu1638026509@163.com

platform for people [2], promoted the stable development of China's economy, accelerated the optimization of industrial structure, made digitalization and networking the main way of economic development, and at the same time made the national economic competitiveness step up to a higher level. It can be seen that the supply chain network is closely related to our life [3] and plays an irreplaceable role in the development of China's economy. However, the supply chain network often faces various uncertainties and risks [4], such as delay, failure and overload. These factors may lead to the cascading failure of supply chain network and bring huge losses to enterprises. The problem of overload cascade failure has always been a hot research topic in supply chain network. In daily life, once the overload cascade failure occurs in supply chain network, it will have a serious impact on personal life, enterprise operation and even national economic development. How to reduce the damage caused by the failure of supply chain network is a key problem to be solved urgently. Therefore, it is of great significance to detect the overload cascading failure of supply chain network [5] for ensuring the stability and reliability of supply chain network.

In order to analyze the overload cascading failure problem of the supply chain network from a scientific perspective, many experts start with the real supply chain network and extract useful data for in-depth analysis. For example, Sapna *et al.* continuously collects and monitors historical data values and location information by deploying sensor nodes at key locations in the supply chain network [6], identify network boundary nodes, coverage hole boundary nodes and event boundary nodes based on monitoring historical data values and location information, These nodes are used as the detection of the boundaries of sub regions to find the nodes that will fail in time and send data to the base station for final decision. However, this method ignores the uncertainty of message transmission in the supply chain network and cannot better find the potential failure risk. Anuradha *et al.* relied on the gateway nodes to first identify the possible faulty nodes in the network and communicate with the Mobile Robot Network (MRN) [7]. Subsequently, the algorithm identifies the faulty node by analyzing the residual energy of each node. In practice, each node needs to update its residual energy information periodically so that other nodes can accurately determine its status. In addition, if a node does not update its residual energy information in time before it runs out of energy, it may cause other nodes in the network to mistakenly believe that the node has failed. Janakiraman *et al.* proposed an improved algorithm for detecting failed nodes based on rank criterion [8], which is used to effectively locate failed nodes during dynamic exchange of emergency messages in critical situations. This algorithm affects the location of failed nodes under the dynamic exchange of emergency messages through the IRC-NOS-DM model, which helps to send warning messages to enterprise nodes facing the impact of channel competition. It is developed to improve the transmission rate of warning packets while minimizing overhead, delay and channel utilization. Through the reliable warning message transmission, the accurate positioning of the failed nodes in the network can create a reliable environment and realize the detection of the failed nodes in the network. However, this method needs some changes or adjustments to adapt to the network with many nodes, and dynamic exchange of emergency messages may lead to additional overhead and delay.

Considering the delay probability factor can better reflect the uncertainty of message transmission in the supply chain network [9], so as to predict the potential failure risk more accurately, find the failure risk in time, and take corresponding measures to intervene and deal with it, thus enhancing the robustness and stability of the supply chain network; It can optimize the resource allocation in the supply chain network and improve the overall operational efficiency; It can better evaluate the risks and benefits between layers, thus promoting the cooperation between layers and jointly realizing the stable operation of the network. Therefore, applying the delay probability factor to the cascading failure detection algorithm of multi-layer supply chain network overload can improve the prediction accuracy, find risks in advance, optimize resource allocation, enhance robustness and promote cooperation.

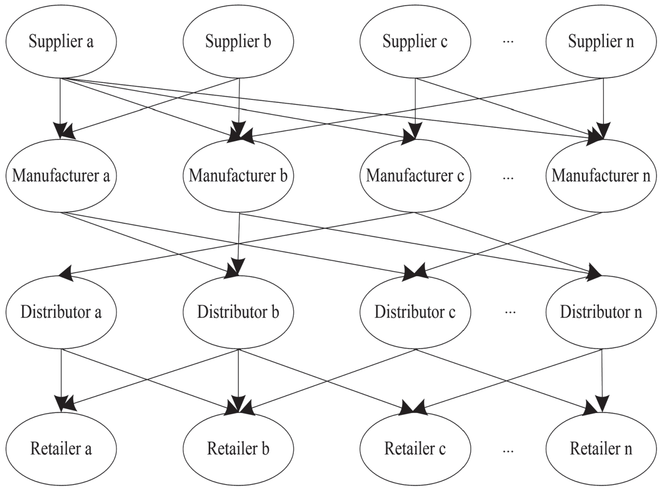


FIGURE 1. Schematic diagram of multi-layer supply chain network.

2. Multi-layer supply chain network overload cascade failure detection algorithm

2.1. Multi-tier supply chain network model construction

Supply chain network is a hierarchical network [10], including supplier network, manufacturer network, distributor network, retailer network and other entities. Enterprises will establish cooperative relations according to supply and demand, thus constructing a multi-layer supply chain network model of raw material suppliers–manufacturers–distributors–retailers. Based on the complex network analysis method, this paper maps enterprises into nodes, the cooperative relationship between enterprises is characterized by edges, and the scale of transactions between enterprises is represented by edge weights, as shown in Figure 1.

The supply chain network is divided into four levels, which are raw material suppliers, manufacturers, distributors and retailers from top to bottom. Assuming that the business scope of an enterprise will not expand, the cooperative relationship between enterprises will only occur at the upper and lower levels, but there is no cooperative relationship between different levels, and an enterprise can establish contacts with many enterprises. Because the supply chain network is difficult to obtain empirical data support, the strength of interaction between upstream and downstream levels of the supply chain is taken as the basis for whether there is a connection between enterprises, the attraction strength between enterprises is established through the law of gravity. In response to your question, I have provided the following explanation and answer in the article: If the network has a more general structure, with supplier nodes at the top and retailer nodes at the bottom, but without assuming the “middle” of the network, then discuss the following situation:

(1) Diversity of node types and functions.
   - In complex scenarios such as chemical engineering supply chains, there are multiple types of nodes in between. For example, in addition to common manufacturers and distributors, there may also be nodes dedicated to providing specific chemical raw material processing services, whose function is to preliminarily process raw materials to meet the requirements of subsequent production steps. The existence of these nodes will change the path of logistics and information flow, making the load distribution and propagation rules based on a simple four layer structure more complex.

   There are some auxiliary nodes, such as quality inspection nodes, research and development nodes, etc. The quality inspection node will inspect the products that have passed through, and unqualified products may be intercepted, which will affect the load situation of subsequent nodes. Research and development nodes may improve products based on market demand and technological development, thereby changing production processes and the demand for raw materials, which in turn affects the load balancing and stability of the entire supply chain.

(2) Complexity of connection relationships.
- The connection relationship is no longer a simple hierarchical connection. In the chemical engineering supply chain, there may be situations where suppliers have specific business connections directly with retailers, such as some special chemical reagent suppliers providing products directly to specific large retailers, bypassing the intermediate manufacturer and distributor links. This cross layer connection will disrupt the original load propagation and distribution pattern.
- The connections between intermediate nodes are more complex and diverse. For example, different manufacturers may form tight connections due to collaborative research and development or shared resources, which may result in a different redistribution of load between these nodes compared to a simple hierarchical structure. Moreover, the connections between nodes may be dynamically changing, and the cooperative relationships between nodes may change with market demand, technological advancements, or corporate strategic adjustments, thereby affecting the stability of the supply chain and the mode of fault propagation.

(3) Impact on fault detection algorithms.
For the detection of node faults, due to the complexity of node types and connection relationships, the propagation path of faults becomes difficult to predict. In a simple four layer structure, faults may propagate from upper to lower layers in a relatively fixed pattern, but in more complex structures, faults may rapidly spread throughout the network through various cross layer connections and complex intermediate node relationships, making it difficult for fixed rule-based fault detection algorithms to accurately identify fault nodes and predict fault propagation paths.

The definition of node capacity and load will also become more complex. Different types of nodes may have different capacity measurement standards, for example, the capacity of quality inspection nodes may be related to detection capability and processing speed, while the capacity of research and development nodes may be related to research and development resources and innovation capabilities. The calculation of load also needs to consider more factors, such as the requirements of different nodes for product quality, technical content, etc. This makes the load calculation method based on simple supply and demand relationship definition no longer applicable, thereby affecting the accuracy of determining whether nodes are overloaded in fault detection algorithms.

The cooperative relationship between enterprises is screened and established through the threshold method. Among them, the strength of attraction between enterprises is directly proportional to the scale of the two enterprises and inversely proportional to the spatial distance between enterprises, and the gravity model between enterprises is established:

$$\begin{cases} A_{ij} = \frac{W_i W_j}{d_{ij}^2} \\ W_i = \frac{(\mathrm{RC}_i - \mathrm{RC}_{\min})}{(\mathrm{RC}_{\max} - \mathrm{RC}_{\min})} \\ d_{ij} = \begin{cases} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, & i \neq j \\ 1, & i = j. \end{cases} \end{cases} \tag{1}$$

Among them, A_{ij} represents the strength of attraction between enterprise i and enterprise j; W_i represents the node strength of enterprise i; W_j represents the node strength of enterprise j; d_{ij} represents the spatial distance between enterprise i and enterprise j. Considering that the distribution deviation of registered capital data of enterprises is large, the registered capital data of enterprises is standardized by extreme range, and the node strength of enterprises is characterized by the processed data. Among them, RC_i represents paid-in capital scale of enterprise i; $\mathrm{RC}_{\max}$ represents the largest paid-in capital scale in the enterprise's hierarchy; $\mathrm{RC}_{\min}$ represents the smallest paid-in capital scale in the enterprise's hierarchy. The spatial distance between enterprises is described by the spatial distance between provincial capitals where enterprises are located, among which,x indicates the longitude of the provincial capital where the enterprise is located; y indicates the latitude of the provincial capital where the enterprise is located, and the distance between enterprises in the same province is the minimum value of 1.

By collecting the information of many raw material suppliers, manufacturers, distributors and retailers, a multi-layer supply chain network model is constructed [11]. The specific construction steps are as follows:

(1) Initialize the number of enterprise nodes, select the adjacent upstream and downstream levels, and take raw material suppliers and manufacturers as examples to calculate the inter-enterprise attraction of different levels A_{ij}, i is a raw material supplier level enterprise, j is a manufacturer-level enterprise.
(2) According to the threshold method, only when the attraction A_{ij} between two enterprises exceeding the set threshold ξ, upstream enterprise i establishes a cooperative relationship between downstream enterprise j.
(3) Select different levels of enterprise nodes and repeat the previous two steps to establish a multi-layer supply chain network of raw material suppliers–manufacturers, manufacturers–distributors and distributors–retailers.

Because of the reciprocity between enterprises in the supply chain network, the supply chain network is represented by a network diagram $G = (P, L, Q, A)$ through networking, among them, $P = \{p_1, \ldots, p_N\}$ express a collection of N enterprise nodes, and classified according to the level in the supply chain, including suppliers, manufacturers, distributors and retailers; $L = \{l_1, \ldots, l_M\}$ express a collection of M links (business relationships between enterprises); $Q = \{q_1, \ldots, q_M\}$ express a set of M link weights; $A = \{a_1, \ldots, a_N\}$ express adjacency matrix of N enterprise nodes, in which, a_{ij} is a $(0, 1)$ variable, representing an enterprise whether node i and j are connected. G can be represented by $N \times N$ weight matrix of G^w, among them, q_{ij} represents link weights between enterprise node i and enterprise node j, such as volume of business, chain length, etc., if $q_{ij} = 0$, it means that two enterprise nodes are not connected. The supply chain network is constructed by the way of similar weight. The greater the link weight, the smaller the distance between enterprise nodes in the supply chain network and the closer the relationship. Network efficiency refers to the degree of effectiveness that the network can exert during operation, and the shortest path length of the supply chain network is used to describe the transmission performance and efficiency of the network.

$$E(G) = \frac{1}{N(N+1)} \sum_{i \neq j \in G} e_{ij} = \frac{1}{N(N+1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}. \tag{2}$$

Set $E_0(G)$ represent the efficiency of the supply chain network in normal operation; $E_e(G)$ represents the network efficiency of the supply chain network after cascading failure. The shortest path d_{ij} from enterprise node i to enterprise node j is calculated by the Floyd shortest path algorithm. The algorithm process of Floyd shortest path is to take the distance matrix of enterprise node as the initial matrix, using this algorithm to assume that the shortest path from an enterprise node i to an enterprise node j is dis_{ij}, for each node in the supply chain network k, check whether it exists $dis_{ij} > dis_{ik} + dis_{kj}$. If it exists, update the shortest path $dis_{ij} = dis_{ik} + dis_{kj}$. Traverse all nodes in the supply chain network to get the shortest distance matrix of the supply chain network.

2.2. Supply chain network overload cascade failure modeling

Suppose that in the supply chain network, each enterprise node starts to run normally at a certain time, as shown in Figure 2a. After a period of time, due to the failure of enterprise node i, the business relationship between i and enterprise nodes j_1, j_2, j_3, j_4 is affected, which cause supply interruption, as shown in Figure 2b. Because it cannot meet the requirements of the enterprise node j_1, j_2, j_3, j_4, leading failure of enterprise node j_1, j_2, j_3, j_4, and further affects its business cooperation, as shown in Figure 2c, ultimately leading to the complete

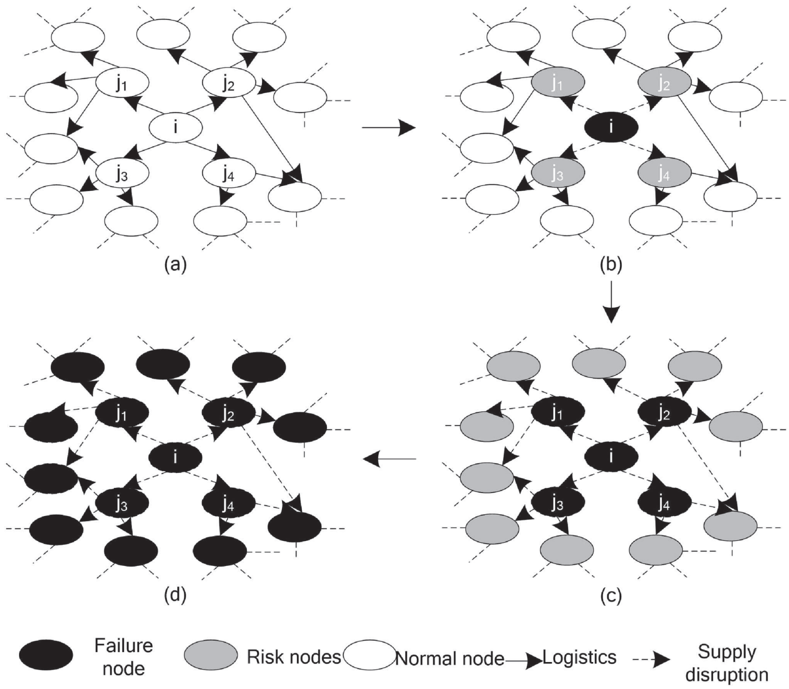


FIGURE 2. Overload cascading failure process of supply chain network.

failure of the supply chain network, as shown in Figure 2d. The failure of a single node in the supply chain network will have two impacts: load propagation and load redistribution [12]. Load propagation will lead to the overload failure of new nodes, and the load redistribution and the link weight value of nodes will affect each other. This cycle will eventually lead to the cascade failure of the entire supply chain network.

2.2.1. Initial load

An enterprise node of an upper-layer network suffers from external interference, which leads to the failure of the load exceeding the upper limit. The same type of upper-layer supplier node may cause the subsequent upper-layer node overload cascade failure because of the load redistribution of the failed node [13], and the load is distributed according to the size of the upper-layer node degree. At the same time, because of the connection between the upper and lower networks, the failure of the upper network node will lead to the failure of the lower network node, and the upper supplier enterprise will fail due to the overload, and the goods originally supplied by the upper node to the lower node will be reduced to zero, resulting in the failure of the lower node due to the lack of goods. In the supply chain network, logistics is the load, and the initial load is the initial logistics volume of each enterprise node. In order to ensure the balance between supply and demand, the demand load or supply load of enterprise nodes is often related to the supply load or demand load of neighboring enterprises [14]. Considering that each node in the supply chain network has the characteristics of supply and demand, the load of these two points is determined separately. The initial load can be defined as:

$$L_i^S(0) = \left(z_i^{\text{out}} \sum_{r\in\Gamma_i} z_r^{\text{out}}\right)^{\theta} \tag{3}$$

$$L_i^D(0) = \left(z_i^{\text{in}} \sum_{r\in\Gamma_i} z_r^{\text{in}}\right)^{\theta}. \tag{4}$$

Among them, $L_i^S(0)$ represents supply load of the initial enterprise node i, that is, supply; $L_i^D(0)$ represents demand load of the initial enterprise node i, that is, demand; Γ_i represents a set of enterprise nodes connected with enterprise nodes i, z_i and z_r respectively represent the degree of enterprise nodes i and enterprise nodes r, that is, the number of enterprises connected with enterprise nodes i and enterprise nodes r; z_i^{in} and z_i^{out} respectively represent the in-degree and out-degree of enterprise nodes i; z_r^{in} and z_r^{out} respectively represent the in-degree and out-degree of enterprise nodes r; θ represents an adjustable parameter, the greater the θ, the greater the difference in initial load between enterprise nodes.

According to formulas (3) and (4), the supply and demand of each enterprise node in the supply chain network can be balanced.

2.2.2. Node capacity

There are connections between the upper and lower levels of the supply chain network, such as information transmission, material transportation and money transaction. The upper network node has an upper limit and the lower network node has a lower limit. Once the upper network node's capacity exceeds its own upper limit or the lower network node's capacity is lower than its lower limit, the node will have the risk of failure [15]. In the actual operation process, enterprises in the supply chain network usually formulate corresponding measures to prevent risks. For example, the failure of upstream enterprises will lead to the production risk of downstream enterprises, while the failure of downstream enterprises will lead to the inventory risk of upstream enterprises, so there is a certain capacity range in the supply and demand of enterprises, indicating the early warning ability of enterprises to deal with risks. When the supply or demand exceeds the capacity range, enterprises will be disturbed by risks. The upper load limit indicates the enterprise's ability to cope with excessive inventory or excessive demand. Generally, the upper load limit is directly proportional to the initial load, so the upper supply load limit and the upper demand load limit can be defined as:

$$C_i^S = (1+\beta)L_i^S(0) \tag{5}$$

$$C_i^D = (1+\beta)L_i^D(0). \tag{6}$$

When a business i, that in the event of a cessation of business by a downstream enterprise, the products produced by the enterprise i will not be marketable, making excess stockpiles of enterprise i exist, at which point C_i^S represents storage space set aside for enterprise i to cope with excess inventory, etc.; when a business i, that in the event of the termination of the business of an upstream enterprise, the enterprise i has insufficient raw materials for production, resulting in enterprises i unable to meet the needs of downstream enterprises, so that the stockpile of enterprises i is insufficient, at which point the C_i^D represents the finished goods reserved for enterprise i in advance, etc.; and β indicates the overload factor.

Correspondingly, the set load floor is proportional to the initial load, and the supply load floor and demand load floor can be defined as follows.

$$U_i^S = (1-\beta)L_i^S(0) \tag{7}$$

$$U_i^D = (1-\beta)L_i^D(0). \tag{8}$$

For ease of description, use L_i referring to L_i^S and L_i^D, C_i referring to C_i^S and C_i^D, U_i referring to U_i^S and U_i^D, then C_i and U_i represent the upper load limit and lower load limit of enterprise i, when load $L_i \in [U_i, C_i]$, the business i maintain normal business operations. β is determined by the risk early warning investment of enterprise i, the greater the β, the greater the ability to warn of risk for i, when $\beta = 0$, indicating that the enterprise i has no risk warning capability.

2.2.3. Overloaded node load distribution

In the supply chain network [16], the failure of enterprise node will make the node connected to the upstream enterprise poor supply, downstream enterprise demand dissatisfaction, and then make the supply chain network to redistribute the flow of upstream and downstream nodes. In the completion of the load distribution of enterprise nodes, if the enterprise's inflow load or outflow load and its corresponding inflow and outflow capacity ratio is less than the range of the enterprise can withstand, the enterprise node due to supply and demand problems caused by poor operation, thus leading to the failure, which in turn triggered a new round of risk transfer.

Considering the reality of node failure [17], the load will be preferentially allocated to high-capacity nodes, so when the node failure occurs in the cascade failure model, the load of the failed node is allocated to the neighboring node enterprises in a way that is proportional to the initial load, *i.e.*, the load is preferentially allocated to the high-capacity node allocation strategy. In the supply chain network, the closer the enterprise relationship the greater the loss suffered, the load allocation is proportional to the link weight. Assuming that failure occurs for the enterprise node i at time of t, the load and associated link weight of this node is 0. The load distribution process is as follows.

(1) Distribute load to neighboring nodes according to the following equation.

$$\Delta L_{ij}(t-1) = L_i(t-1)\frac{w_{ij}(0)}{\sum_{m\in\Gamma_i} w_{im}(0)}. \tag{9}$$

Among them, $\Delta L_{ij}(t-1)$ represents the amount of failure load caused by enterprise node i failure to enterprise node j. $L_i(t-1)$ represents failure load for enterprise when node i failure. $w_{ij}(0)$ represents the initial weights link weights of the enterprise nodes i; Γ_i represents the set of neighboring nodes of enterprise node i; m represents the number of neighboring nodes of enterprise node i.

(2) Updating the load of enterprise node j and calculate the link weights with its neighboring nodes:

$$L_j(t) = L_j(t-1) + \Delta L_{ij}(t-1) \tag{10}$$

$$w_{jl}(t) = w_{jl}(0)\frac{L_j(t)L_l(t)}{L_j(0)L_l(0)}. \tag{11}$$

(3) If the enterprise nodes load $L_j(t)$ is greater than the capacity of the enterprise node C_j and then, at the next moment, the further failures of enterprise node j will occur, cascading failures continue to propagate, and enterprise node j transit from a normal state to an overloaded state, which is defined here as a risky state.

2.3. Overload cascade failure detection for multi-layer supply chain networks considering delay probability factors

Each node in the supply chain may send status update messages periodically to inform other nodes of their status and availability. These messages can include information such as inventory level, production progress, and transportation status, so that other nodes can understand the overall status of the supply chain. Therefore, status update messages can be used to detect and confirm the connection and availability of the supply chain. In the actual supply chain network environment, the traditional failure detection algorithm with a fixed timeout value is obviously not flexible enough because of the large changes in message delay [18]. If the fixed value is too small, it is easy to cause too many false alarms; If the fixed value is set too large, the detection time will become longer. Therefore, ideally, this timeout value can change with the actual supply chain network status. When the load of the enterprise nodes in the supply chain network is small, this value is smaller; On the contrary, it is larger. For this reason, an adaptive failure detection algorithm based on delay probability is designed for the multi-layer supply chain network. This algorithm obtains a timeout value after analyzing and calculating the history of the node status update message delay in the supply chain network. This timeout value changes with the actual message delay, and has strong adaptability. During the operation of the supply chain network, the frequency that a correct process is incorrectly judged as invalid by other correct processes is called error rate, which is a common indicator to measure the accuracy of failure detection [19]. The error rate is caused by the delay of the status update message exceeding the preset timeout value and the loss of the status update message. The two events are independent. A message lost cannot be timeout. The same message will be received eventually if it just fails to arrive after the timeout. The status update message delay timeout and status update message loss are related to the supply chain network status, and the status update message delay timeout is also affected by the supply chain node's QoS requirements for failure detection. The query accuracy PA is used to represent the QoS requirements of supply chain nodes, where, PA $\in (0, 1)$. PA can be flexibly set according to the requirements of different supply chain nodes to meet the QoS requirements of different supply chain nodes. When the supply chain nodes have high requirements on the accuracy of overload cascading failure detection of the supply chain network. The value of PA should be set larger; when the speed of overload cascade failure detection of the supply chain network is required to be high, PA can be turned down slightly.

The basic algorithm for overload cascade failure detection in supply chain networks is described as follows.

Set $\sup\{x : p(t \le x) = 1\}$ is the upper bound of the random variable in the supply chain network, *i.e.*, $\sup(t)$: $\mathrm{low}\{x : p(t \ge x) = 1\}$ is the lower bound of the random variable in the supply chain network, *i.e.*, $\mathrm{low}(t)$, then $\sup(t)$ and $\mathrm{low}(t)$ is the only finite number.

If t is a bounded random variable in the supply chain network, then $F(t) = \frac{\sup(t)+\mathrm{low}(t)}{2}$ is the average of the random variable t in the supply chain network; if $\mathrm{low}(t) \ge 0$, then $B(t) = \sqrt{\sup(t) \times \mathrm{low}(t)}$ is the geometric mean of the random variable t in the supply chain network.

Set t is a bounded random variable in the supply chain network, the mathematical expectation and variance of t are $H(t)$ and $V(t)$, and $\mathrm{low}(t) \ge 0$, then there is:

$$V(t) \le 2H(t) \times [F(t) - B(t)]. \tag{12}$$

Set the mathematical expectation of the delay interval between the arrival of state update messages for the supply chain network D is $H(D)$, then for any $t > 0$, there is:

$$P(D > t) \le \frac{2H(D) \times [F(t) - B(t)]}{[t - H(D)]^2}, (t > H(D)). \tag{13}$$

Because in overload cascade failure detection in multi-layer supply chain networks [20], the delay interval between the arrival of state update messages is a random probability event. For this reason, set D is the delay probability of the arrival of the state update message, whose variance is $V(D)$, then by Chebyshev's inequality, we have:

$$P(D > t) \le \frac{V(D)}{[t - H(D)]^2}, (t > H(D)). \tag{14}$$

Thus, from equations (12) and (14), it follows that:

$$P(D > t) \le \frac{2H(D) \times [F(D) - B(D)]}{[t - H(D)]^2}. \tag{15}$$

This algorithm does not consider the packet loss rate, and can be divided into two parts: message sending and receiving and prediction of message delay time. The server of failure detection service and the enterprises in the supply chain network do not need to establish a permanent connection. At this time, electronic data interchange (EDI) system can be used to achieve communication.

(1) Each enterprise node in the supply chain network regularly sends status update messages to its failure detector in the form of EDI system data packets. The status update message includes order status, inventory information, transportation information, production progress, exceptions, and the serial number of the status update message, which is incremental.
(2) Statistic recent supply chain networks q individual from the node of the inspected enterprise q of its delay probability factor that computed for the status update message sent, calculate $Hq(D)$, $F(D)$ and $B(D)$, and obtained on the basis of calculation for $Hq(D)$, $F(D)$ and $B(D)$ that yields the time interval ND at which the next state update message in the supply chain network is likely to arrive. Among them, $Hq(D)$ is

the mathematical expectation of the delay probability D of the state update message sent by the enterprise node q in the supply chain network. The mathematical expectation of the $F(D)$ is the average value of D; $B(D)$ is the geometric mean of D. On this basis, the historical prediction delay probability of the supply chain network is weighted. Let the time of the current prediction be T_1, whose corresponding weights is P_1, the time of the previous prediction is T_2, corresponding weights is P_2, the time of the previous prediction is T_i, corresponding weights is P_i, the time of the previous prediction is T_w, corresponding weights is P_w, of which, w is the size of the history window of this supply chain network, and $\sum_{i=1}^{w} P_i = 1$. According to Zipf's first law, $P_i = \frac{K}{i}$, of which, K is a parameter, the value of K can be calculated by normalizing:

$$\sum_{i=1}^{w} P_i = \sum_{i=1}^{w} \frac{K}{i} = K \sum_{i=1}^{w} \frac{1}{i} \approx K * (\ln w + r) = 1. \tag{16}$$

Among them, r is Euler's constant. Therefore, it can be defined as follows:

$$K \approx \frac{1}{\ln w + r}. \tag{17}$$

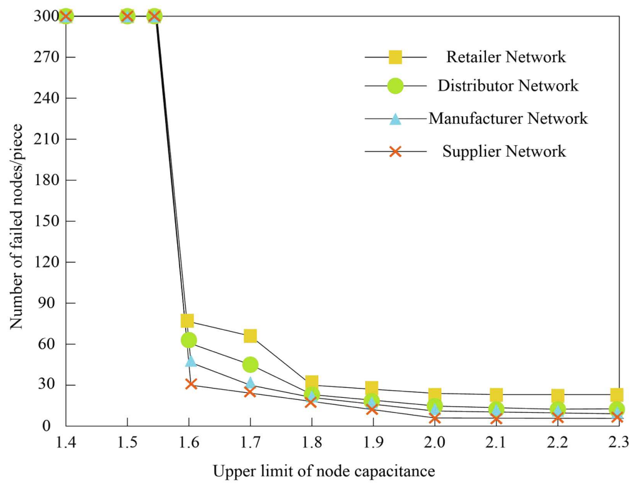
Obtaining the predicted value ND of the delay probability for the arrival of the next state update message in the supply chain network. Based on the delay probability of the arrival of the historical state update message of the supply chain network and the predicted delay probability of the arrival of the next state update message of the supply chain network, the timeout value of the timer at the moment of the arrival of the next state update message of the supply chain network is set.

(3) If the delay probability obtained by updating the message history delay record based on the state of the supply chain network within $\mathrm{ND}p_i(q)$, the enterprise node in the supply chain network is considered to be running normally if it receives the corresponding status update message; On the other hand, if no status update message is received from the enterprise node in the supply chain network within $\mathrm{ND}p_i(q)$, it indicates that the node has failed, realizing the overload cascade failure detection of the multi-layer supply chain network.

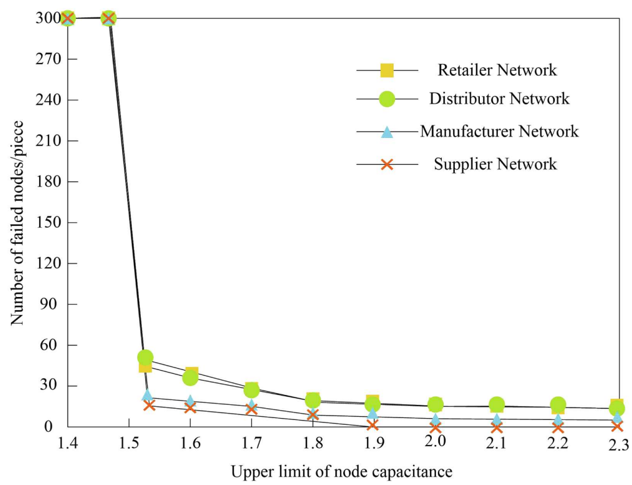
3. Experimental analysis

Since the supply chain network in life has scale-free characteristics, in order to test the effectiveness of the fault detection algorithm, the Barabasi Albert (BA) scale-free multi-level supply chain network model shown in Figure 1 will be constructed for simulation. The model includes multiple nodes of suppliers, manufacturers, distributors, retailers and the edges of the supply chain network, such as orders and transportation. The initial status of the supply chain network is set to m_0 enterprise nodes, each iteration introduces a new node, the $m(m \leq m_0)$ nodes are connected based on the probability obtained from the node degree calculation. Construct an unscaled supply chain network model with the number of nodes 500–1500, set $m_0 = 5$, $m = 5$, set the adjusted load parameters $\beta = 2$, the experiments were run independently for 30 times and averaged.

Because in the normal state of multi-layer supply chain network, the load of each enterprise node is within the capacity, when the load exceeds the upper limit of the capacity, the node will be transformed from the normal state to the overload state, and there is the risk of cascade failure, if the node exceeds the maximum risk control capacity of the enterprise, the normal business of the enterprise will be interrupted, and it will be transformed directly to the failure state, while the nodes in the risky state will take emergency recovery measures, and if recovery fails, it will be transformed to the failure state, resulting in the overload cascade failure in the multi-layer supply chain network. Therefore, different node capacity upper limit is set, different layers in the supply chain network are deliberately attacked, and the attack ratio is set to 0.6%, the algorithm in this paper detects the state of each node and edge in the supply chain network in real time and records the number of failed nodes, and the state change of each node and edge at each time is used to calculate the delay probability of each node and edge to complete the overloaded cascade failure detection in the multi-layer supply chain network, and the validation results are shown in Figure 3.



(a)



(b)

FIGURE 3. Overload cascading failure detection results in a multi-layer supply chain network using the method proposed in this article. (a) Intentionally attacking supplier networks. (b) Deliberate attack on retailer networks.

As can be seen in Figure 3a, in the process of detecting cascading failures of overload in the multi-layer supply chain network through the algorithm in this paper, the supplier network nodes are deliberately attacked. When the upper limit of node capacity is increased to 1.6, the number of failed nodes in the multi-layer supply chain network decreases significantly, and when the upper limit of node capacity is 2.0, the algorithm in this paper detects 5 failed nodes in the supplier network, There are 9 failed nodes in the manufacturer's network, 16 failed nodes in the distributor's network, and 30 failed nodes in the retailer's network. There are no other new failed nodes. This indicates that the increase in the upper limit parameter of node capacity reduces the number of new failed nodes or does not add new failed nodes; It can be seen from Figure 3b that under the same attack proportion, the retailer network nodes are deliberately attacked. When the node capacity ceiling parameter is

1.54, the number of failed nodes in the multi-layer supply chain network decreases significantly. When the node capacity ceiling is 1.9, the algorithm in this paper detects that there are 0 failed nodes in the supplier network and 8 failed nodes in the manufacturer network, There are 18 failed nodes in both the distributor network and the retailer network, and there are no new failed nodes in the network. It shows that the algorithm in this paper can effectively detect the failure of each overloaded enterprise node in the multi-layer supply chain network, help to enhance the early warning and response ability to cascading failure of the supply chain network, improve the stability and reliability of the supply chain network, reduce operational risk, and ensure the normal operation of the supply chain network and business continuity.

The cascading failure process of a multi-layer supply chain network stops when the network does not generate new failed nodes, or ends when the entire network collapses. Therefore, the number (and proportion) of failed nodes is used to describe the result of the overloaded cascade failure process of the multi-layer supply chain network. The higher the number of failed nodes (and the higher the proportion of failed nodes), the more vulnerable the multi-layer supply chain network is. Set Ψ' as the number of all failed nodes in the supply chain network after an overload cascade failure in the supply chain network. Ψ is the number of all initial nodes in the supply chain network. Then, the proportion ζ of failed nodes is:

$$\zeta = \frac{\Psi'}{\Psi}. \tag{18}$$

Among them, the larger the ζ, the larger the scale of cascade failure in the multi-layer supply chain network, the larger the number of failed nodes in the multi-layer supply chain network, and the more vulnerable the multi-layer supply chain network.

The attack method of the initial failure node in the multi-layer supply chain network adopts intentional attack or random attack, intentional attack refers to select a part of the node in the network with large degree value to attack, that is to say, the degree value of the node is ranked from large to small, and a certain proportion of the nodes from the front to the back of the ranked nodes are selected for attacking, so as to make it invalid. Random attack refers to randomly select a certain percentage of nodes in the network to attack to make it fail. After selecting a certain percentage of initial failure nodes, the cascade failure process of multi-layer supply chain network starts until there are no new failure nodes or the whole network collapses. When the size of multi-layer supply chain network is set to 500, 1000 and 1500 nodes, intentional and random attacks are carried out on supplier and retailer network layers respectively, and the algorithm of this paper is applied to detect the overload cascade failure of multi-layer supply chain network, and analyze the risk-resistant ability of multi-layer supply chain network. The proportion of total failed nodes in the multi-layer supply chain network is used to measure the vulnerability of the network, and the larger the proportion, the more vulnerable the multi-layer supply chain network is, and the validation results are shown in Figure 4.

As can be seen from Figure 4, regardless of the size of the multi-layer supply chain network, whether it is a deliberate attack or a random attack, the algorithm in this paper detects that the curve of the supplier network layer arrives first ξ point with a value of 1 indicate that the supply chain collapse threshold is smaller when initially attacking the nodes in the supplier network layer, *i.e.*, the multi-layer supply chain network collapses faster. Under the premise that the multi-layer supply chain network has not collapsed completely, with the same initial failure ratio, the supplier network layer curve is smaller than the retailer network layer curve, high value ξ means that the vulnerability of the multi-layer supply chain network when attacking the supplier network layer is greater than that when attacking the retailer network layer, which proves that the multi-layer supply chain network is more vulnerable and easier to collapse when attacking the supplier network layer. Comparing Figures 4c and 4d, it can be found that when the initial attack proportion is 7%, the multi-layer supply chain network will all collapse whether attacking the supplier network layer or the retailer network layer, while the multi-layer supply chain network will show stronger robustness when attacking randomly, and only when the initial attack proportion is not less than 30% can the multi-layer supply chain network collapse completely. It can be seen that this algorithm can effectively detect the failure of the supply chain network under different attack conditions and different initial failure ratios of nodes, and measure the anti risk ability of the supply chain

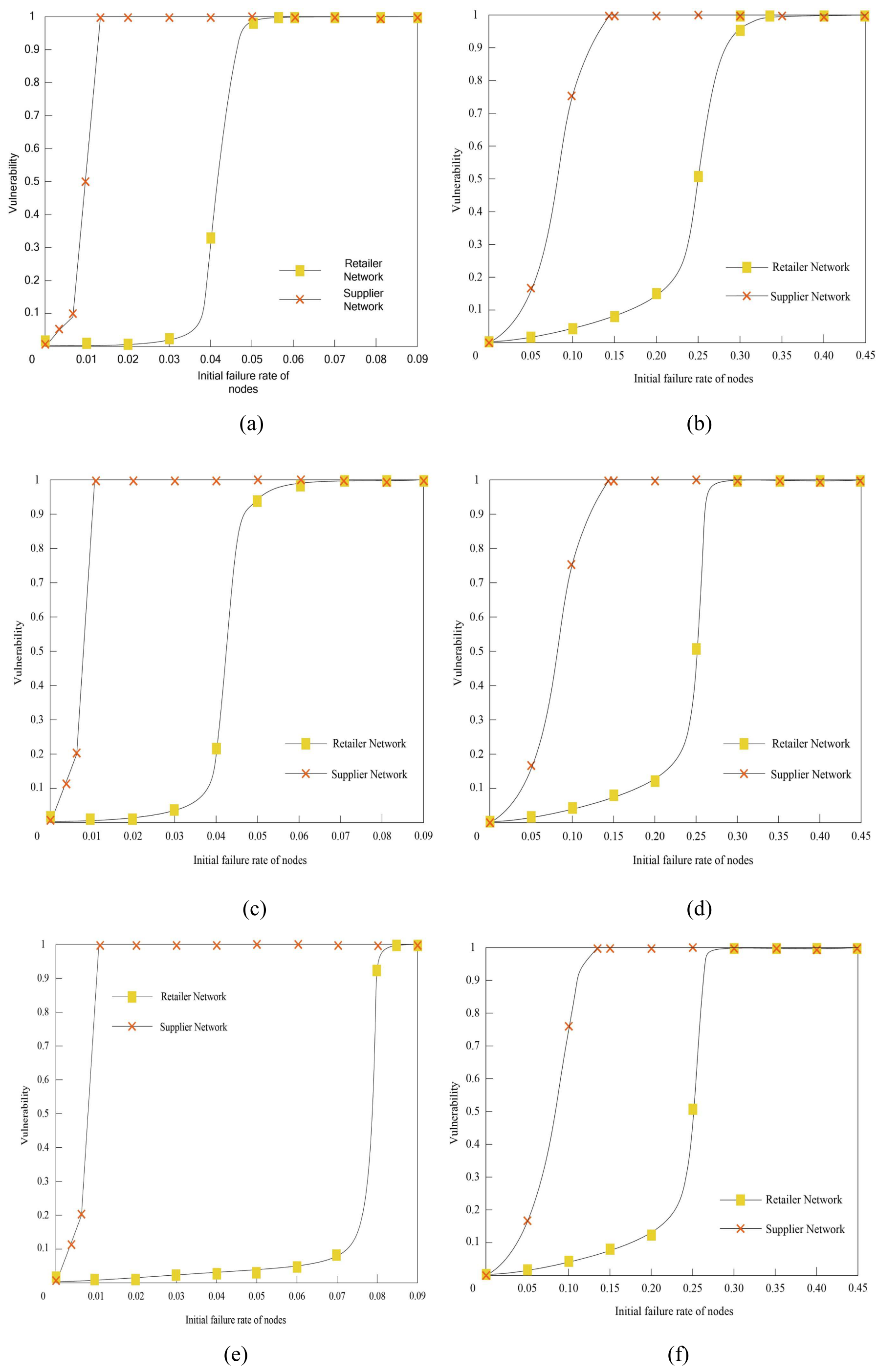


FIGURE 4. Vulnerability of multilayer supply chain networks under different node initial failure ratios. (a) Intentional attack with 500 nodes. (b) Random attack with 500 nodes. (c) Intentional attack with 1000 nodes. (d) Random attack with 1000 nodes. (e) Intentional attack with 1500 nodes. (f) Random attack with 1500 nodes.

network. A purposeful and artificial attack on an important enterprise in a multi-layer supply chain network can easily lead to the paralysis of the entire multi-layer supply chain network. In the face of a small range of natural damage, the multi-layer supply chain network has a certain ability to resist risks.

When the nodes in the multi-layer supply chain network fail, the failed nodes in the network will be disconnected from other nodes, therefore, the connectivity of the multi-layer supply chain network will change with the cascade failure process in the network. In order to further verify the effectiveness of this paper's algorithm for overloaded cascade failure detection in multi-layer supply chain network, set the size of multi-layer supply chain network as the number of nodes is 1000, and carry out deliberate and random attacks on the supplier network layer and the retailer network layer, respectively, and the maximum connectivity slice index ε for measuring the impact of failed nodes on the efficiency of a multi-layer supply chain network, the formula is expressed as:

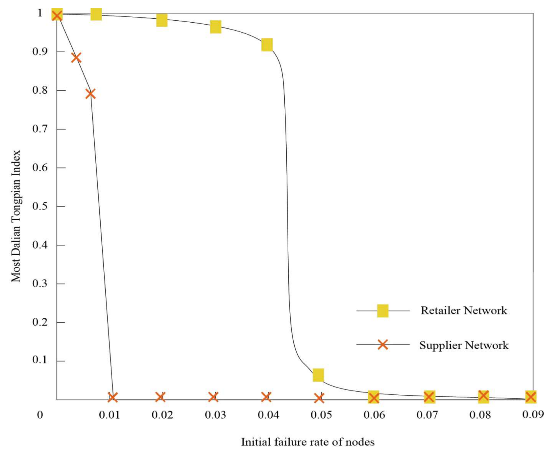
$$\varepsilon = \frac{\iota'}{\Psi}. \tag{19}$$

Among them, ι' is the number of nodes in the maximally connected subgraph in the multilayer supply chain network; the ε is an indicator of the maximum number of connected slices, the larger ε, the better the multi-layer supply chain network connectivity, then the efficiency of the multi-layer supply chain network is increased, and the cascade failure process has less impact on the multi-layer supply chain network structure. The validation results are shown in Figure 5.

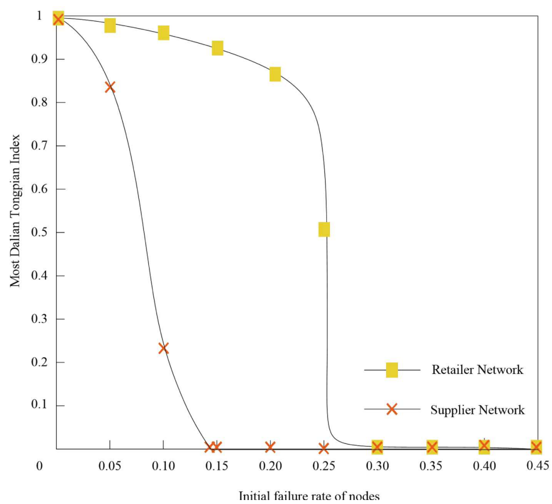
Figure 5 illustrates the maximum connectivity slice metrics of the multi-layer supply chain network obtained by applying the algorithm of this paper through detection, when ε is 1, it means that the multi-layer supply chain network is all connected, and the efficiency of the multi-layer supply chain network is the highest in this case. When ε is 0, all the nodes in the multi-layer supply chain network are isolated nodes and are not connected, so the efficiency is the lowest. As can be seen in Figure 5, regardless of the initial attack on the supplier network layer or retailer network layer, the maximum connectivity slice index ε reaches 0 point faster when deliberately attacked. In addition, whether it is intentional attack or random attack, the initial attack node is the supplier network layer node, the impact on the efficiency of the multi-layer supply chain network is greater, so that the maximum connectivity index will fall to the point of 0 more quickly. The experimental results show that the application of this paper's algorithm can effectively detect the network connectivity changes caused by overload cascade failure of supply chain network under different types of attacks with different initial failure ratios of nodes, among which, the deliberate attack has a greater impact on the supply chain network, and the impact of the attack on the supplier network layer is greater than that on the retailer network layer.

Realistic supply chain network scenarios are simulated, including multiple suppliers, producers, distributors, and final consumers as key links. To simulate different failure scenarios, we set up multiple initial failure rates, including random attack scenarios of 5% and 10%, as well as scenarios where nodes at a specific supplier network layer are intentionally attacked. These settings aim to simulate various failure scenarios that may occur in the supply chain network, and thus verify the performance of the failure detection algorithms in real-world applications. In order to evaluate the performance of the algorithms, key metrics such as failure detection accuracy and testing time under different failure scenarios are recorded and comprehensively analyzed and compared. The specific results are shown in Table 1. The experimental results are shown in Table 1.

Analyzing Table 1, it can be seen that from the perspective of failure detection accuracy, the method in this paper shows high accuracy in a variety of scenarios. In the random attack scenarios with initial failure rates of 5% and 10%, the failure detection accuracy reaches 92% and 89%, respectively, which indicates that the method has strong failure identification capability under random attacks. When the initial failure node is a provider network layer node and is intentionally attacked, although the accuracy rate decreases to 78%, this value is still at a high level, which shows the stability and reliability of the method under complex attack scenarios. Second, in terms of testing time, the method in this paper also performs well. In random attack scenarios with an initial failure rate of 5% and 10%, the test time is 4.2 min and 4.8 min, respectively, and this test speed ensures rapid diagnosis and response after failures occur. Even in the case of intentional attacks on the provider network layer nodes, the test time is only 5.5 min, which is still an acceptable time range to meet the needs of practical



(a)



(b)

FIGURE 5. Maximum connectivity of multi-layer supply chain networks under different initial failure ratios of nodes. (a) Intentional attack. (b) Random attack.

applications. In terms of risk resistance assessment, this paper's methodology has a high overall evaluation value of 8.5/10 by comprehensively evaluating the performance of the supply chain network under different attack conditions and the proportion of initially failed nodes, which indicates that the methodology has a significant effect in enhancing the risk resistance of the supply chain network, and is able to provide a strong support for enterprise's risk management. In addition, the method in this paper also shows excellent performance in terms of resource optimization effect. By optimizing the resource allocation efficiency through the algorithm, an increase of 15% is achieved, which means that enterprises can utilize the existing resources more effectively, improve productivity and reduce costs. Finally, in terms of enhancing network robustness, the application of the methods in this paper makes the supply chain network more resistant to failures. Specifically, the network robustness is increased by 20%, and this significant improvement means that the supply chain network can maintain stable operation and efficient collaboration even in the face of complex and changing failure scenarios.

TABLE 1. Results of the applicability of the algorithm in this paper.

Experimental indicators	Situation description	Numerical performance	Applicability
Failure detection accuracy	Initial failure rate of 5%, random attack	92%	High
	Initial failure rate of 10%, random attack	89%	Higher
	The initial failed node is a supplier network layer node, intentionally attacked	78%	Secondary
Testing time	Initial failure rate of 5%, random attack	4.2 min	Faster
	Initial failure rate of 10%, random attack	4.8 min	Faster
	The initial failed node is a supplier network layer node, intentionally attacked	5.5 min	Acceptable
Risk resistance assessment	Performance of supply chain networks under different attack conditions and initial failure node ratios	Comprehensive evaluation value 8.5/10	Good
Resource optimization effect	Resource allocation efficiency optimized through algorithms	Increase by 15%	Remarkable
Enhancement of network robustness	After the application of algorithms, the supply chain network has the ability to resist failures	Increase by 20%	Obvious

4. Conclusion

Considering the complexity of multi-layer supply chain network, this paper establishes a multi-layer supply chain network overload cascade failure model and combines the delay probability to complete the multi-layer supply chain network overload cascade failure detection, and analyzes the detection effect of this paper's algorithm and the vulnerability of the network under different attack modes, as well as the influence of the supplier network layer and the retailer network layer on the collapse of the whole network through simulation experiments. The results show that the algorithm can effectively detect the failure of each overloaded enterprise node in the multi-layer supply chain network under the same attack ratio, and the larger the node capacity, the fewer the failure nodes exist; At the same time, no matter the initial attack is on the supplier network layer or the retailer network layer, with the same initial failure ratio, the network does not collapse under the same attack ratio, but it does not collapse under the same attack ratio. When the initial failure ratio is the same, the number of failed nodes in the retailer network layer is obviously more than that in the supplier network layer, and the retailer network layer is more fragile under the premise that the network has not collapsed. When the initial attack node is a node in the supplier network layer, the threshold value of network collapse is smaller, *i.e.*, the initial attack node in the supplier network layer, the supply chain network is more prone to collapse. The algorithm proposed in this paper can better reflect the real-life supply chain network failure through failure detection, which provides a reference for controlling the collapse of multi-layer supply chain network in order to improve the robustness of multi-layer supply chain network and reduce the loss of multi-layer supply chain network.

References

[1] B. Ruskey and E. Rosenberg, Minimizing risk in Bayesian supply chain networks. *Comput. Ind. Eng.* **169** (2022) 108134.1–108134.12.

[2] S. Laari, P. Wetzel, J. Toyli and T. Solakivi, Leveraging supply chain networks for sustainability beyond corporate boundaries: explorative structural network analysis. *J. Clean. Prod.* **377** (2022) 1–17.

[3] Y. Li and C.W. Zobel, Exploring supply chain network resilience in the presence of the ripple effect. *Int. J. Prod. Econ.* **228** (2020) 107693.1–107693.13.

[4] F.J. Nezhad, M. Taghizadeh-Yazdi, J.H. Dahooie, A.Z. Babgohari and S.M. Sajadi, Designing a new mathematical model for optimising a multi-product RFID-based closed-loop food supply chain with a green entrepreneurial orientation. *Br. Food J.* **124** (2022) 2114–2148.

[5] S. Lian, X. Han, H. Li, *et al.*, Simulation of detection method of anomalous node mining in a distributed network. *Comput. Simul.* **40** (2023) 409–413.

[6] K.K. Pattanaik and A. Trivedi, A dynamic distributed boundary node detection algorithm for management zone delineation in precision agriculture. *J. Netw. Comput. App.* **167** (2020) 102712.1–102712.19.

[7] M.P. Anuradha, A.M. Swetha and M. Doraipandian, Fault node detection and connectivity restoration with mobile relay node in wireless sensor networks. *J. Comput. Sci.* **16** (2020) 551–558.

[8] S. Janakiraman, An improved rank criterion-based NLOS node detection mechanism in VANETs. *Int. J. Intell. Unmanned Syst.* **9** (2020) 1–15.

[9] M. Raeispour, H. Atrianfar, H.R. Baghaee and G.B. Gharehpetian, Resilient distributed control of BESSs and VSC-based microgrids considering switching topologies and nonuniform time-varying delays. *IET Gener. Transm. Distrib.* **14** (2020) 5060–5071.

[10] S.D. Tsolas and M.M.F. Hasan, Resilience-aware design of interconnected supply chain networks with application to water-energy nexus. *AIChE J.* **67** (2021) 17386.1–17386.11.

[11] Y. Jabarzadeh, H. Reyhani Yamchi, V. Kumar and N. Ghaffarinasab, A multi-objective mixed-integer linear model for sustainable fruit closed-loop supply chain network. *Manage. Environ. Qual. Int. J.* **31** (2020) 1351–1373.

[12] R.S. Gaykar, V. Khanaa and S.D. Joshi, Mapping of virtual machines using machine learning algorithms for detection of faulty nodes. *Int. J. Saf. Secur. Eng. Interdiscipl. J. Res. App.* **12** (2022) 681–690.

[13] D. Chen, D. Sun, Y. Yin, L. Dhamotharan, A. Kumar and Y. Guo, The resilience of logistics network against node failures. *Int. J. Prod. Econ.* **244** (2022) 108373.1–108373.15.

[14] F. Paulis, S. Scafati, C. Olivieri and A. Orlandi, Single-step algorithm for the cascade assembly of multiple S-parameters based multiports networks. *Int. J. RF Microwave Comput.-Aided Eng.* **32** (2022) 23070–23082.

[15] R. Rathore, J.J. Thakkar and J.K. Jha, Evaluation of risks in foodgrains supply chain using failure mode effect analysis and fuzzy VIKOR. *Int. J. Qual. Reliab. Manage.* **38** (2020) 551–580.

[16] P. Verma, Assessment of pre and post-disaster supply chain resilience based on network structural parameters with CVAR as a risk measure. *Int. J. Prod. Econ.* **227** (2020) 107655.1–107655.17.

[17] R.N. Jadoon, A.A. Awan, M.A. Khan, W.Y. Zhou and A. Shahzad, An efficient nodes failure recovery management algorithm for mobile sensor networks. *Math. Probl. Eng.* **2020** (2020) 1749467.1–1749467.14.

[18] G.U. Alozie, A. Arulselvan, K. Akartunal and E.L. Pasiliao, A heuristic approach for the distance-based critical node detection problem in complex networks. *J. Oper. Res. Soc.* **73** (2022) 1347–1361.

[19] I.H. Abdulqadder, S. Zhou, D. Zou, I.T. Aziz and S.M.A. Akber, Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Comput. Netw.* **179** (2020) 107364.1–107364.19.

[20] R.R. Priyadarshini and N. Sivakumar, Failure prediction, detection & recovery algorithms using MCMC in tree-based network topology to improve coverage and connectivity in 3D-UW environment. *Appl. Acoust.* **158** (2020) 107053.1–107053.9.