Received July 12, 2020, accepted August 4, 2020, date of publication August 12, 2020, date of current version August 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016050

Memetic Algorithm With Local Neighborhood Search for Bottleneck Supplier Identification in Supply Networks

PING LOU, YUTING CHEN, AND JUNWEI YAN
School of Information Engineering, Wuhan University of Technology, Wuhan 430000, China

Corresponding author: Yuting Chen (chenyuting03@whut.edu.cn)

This work was supported in part by the National Natural Science Foundation Committee (NSFC) of China under Grant 51875429 and Grant 51905397.

ABSTRACT With the development of lean manufacturing and economic globalization, supply networks increasingly become complex and large-scale, within which thousands of firms inter-depend with each other. Due to these increasing inter-dependencies, disruption of a quite few critical suppliers, namely bottleneck suppliers, can induce high loss to a supply network and even make the whole network dysfunction. Identification of bottleneck suppliers is significantly important for supply network risk management. Thus, in this article, a method based on a memetic algorithm with local neighborhood search (MALNS) is proposed to identify bottleneck suppliers in a two-stage supply network. Firstly, a model based on multipartite network is designed to describe the product supply-demand relations between multiple manufacturers and suppliers, which considers the different roles of manufacturer and supplier and differentiates the products that suppliers supply. To assess the loss caused by supplier disruptions, two performance metrics of supply networks, average product availability rate and manufacturer functioning rate, are presented. Then, a MALNS-based method is proposed to identify bottleneck suppliers, i.e., suppliers whose disruption will decrease both performance metrics most greatly. Finally, a case study based on a real automobile supply network is presented to validate the applicability and effectiveness of the proposed method.

INDEX TERMS Supply network disruption, complex network theory, bottleneck supplier identification, memetic algorithm.

I. INTRODUCTION

Supply networks are constructed when manufacturers rely on suppliers to purchase products in order to accomplish the final products [1]. Moreover, supply networks become more and more complex and large-scale with the increasing development of lean manufacturing and economic globalization. Thousands of firms reciprocally depend on each other to form a complex system [2].

In the same time, these inter-dependencies also make supply networks vulnerable. Due to these inter-dependencies, disruption of a few critical suppliers can propagate throughout the whole network and finally dysfunction the entire system [3]–[7]. In 2011, Thailand flooding damaged several hard disc suppliers, leading multiple computer manufacturers depending on them unable to continue production [8]. Around the same year, Tohoku earthquake affected almost all major automobile manufacturers globally, because several Japanese suppliers were damaged severely in the earthquake [9]. In 2018, the main plant of an automobile supplier, Meridian Magnesium, caught fire. This incidence also forced multiple automobile manufacturers to stop production including BMW, Mercedes-Benz, General Motors, Fiat Chrysler Automobiles and Ford Motor Co. [10]. In the meanwhile, there were also man-made supply disruptions in supply networks. In 2016, three German plants of Volkswagen halted their production due to supply disruptions [3]. These halts were caused by a legal dispute with a supplier which belongs to the Prevent group. It turned out the Prevent Group as a whole provided multiple critical products, such as gear boxes and car seats textiles. A supply disruption caused by one of these suppliers may be mitigated, but the combined disruption of

The associate editor coordinating the review of this manuscript and approving it for publication was Donghyun Kim.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

these suppliers finally led to production halts. These real cases demonstrate risks exposed to manufacturers. In such a complex supply network with a large number of suppliers and manufacturers, there is a category of critical suppliers, namely bottleneck suppliers. Bottleneck suppliers refer to suppliers whose disruption can inflict great loss to the performance of entire supply network [11]. Due to the structural positions in a supply network, namely how their business relationships are linked with others, bottleneck suppliers act as the ''linchpin'' of the supply network and the removing of them can destroy the entire network [5], [11]–[13]. In order to guarantee the operation of a supply network, it is highly important to identify bottleneck suppliers. Identification of bottleneck suppliers can give an accurate robustness assessing of supply networks. By identifying these critical suppliers, the worst-case supplier disruption scenario can be determined. Since system robustness refers to its ability to maintain the basic operation under disruptions, greater ability to withstand the worst-case disruption certainly indicates greater robustness. Besides, identification of these critical suppliers may allow the redesign of supply networks and development of specific risk mitigation policies in order to enhance the robustness of supply networks. However, because of the structural complexity of supply networks, it is difficult to identify bottleneck suppliers.

Recently, complex network theory which has been applied into many areas, provides a powerful tool to depict the structural complexity of supply networks. To identify bottleneck suppliers, studies based on complex network theory were proposed in the past decades. Most of them use network centrality metrics to identify bottleneck suppliers, since network centrality metrics indicate the position importance of a node in the network [4], [12]–[14]. Based on complex network-based modeling methods, a supply network can be abstracted as a set of nodes (firms) and links connecting nodes (inter-firm relations). Bottleneck suppliers are identified using network centrality metrics. The most commonly used metric is degree centrality, namely the number of edges attached to a node [13], [14]. Such methods assume that disruption of suppliers with higher centrality can inflict greater loss to the entire supply network. In other words, the importance to supply network performance is assigned to a supplier before assessing the impact of its disruption. However, these network centrality metrics can only provide a rough approximation on how vital a supplier is to the performance of a supply network. In many cases, these metrics are found not correlated with the severity of network loss [15]. As Kim *et al.* found in their study, disruption of suppliers with higher value of degree centrality may not inflict greater damage to a supply network [5]. On the contrary, the disruption of a supplier with a small value of degree may dysfunction the whole network. Besides, network centrality metrics only provide the importance of a single supplier, it remains unclear how useful these measures are in detecting which combinations of multiple disrupted suppliers can inflict the greatest loss on the performance of a supply network [16]. Since disruptive events may damage multiple suppliers simultaneously. It is necessary to consider the impact of simultaneous disruption of multiple suppliers, when identifying bottleneck suppliers. Thus, network centrality-based methods fail to provide an accurate identification of bottleneck suppliers.

Based these previous works, this article proposes a MALNS-based bottleneck supplier identification method. Firstly, a supply network model based on multipartite network is developed to describe product supply-demand relations between suppliers and manufacturers. Based on the model, two metrics are proposed to measure the performance decreasing of a supply network caused by supplier disruptions. Then, a MALNS-based method is designed for bottleneck supplier identification. Finally, a case study based on a real large-scale automobile supply network is presented. The effectiveness of proposed performance metrics and bottleneck supplier identification method are validated by comparative experiments.

The remainder of this article is listed as follows. The related works are expounded in Section 2. Section 3 presents multipartite supply network model and performance evaluation. Section 4 shows the MALNS-based method for bottleneck supplier identification. Section 5 presents a case study based on a real automobile supply network. Section 6 gives a brief conclusion.

II. RELATED WORKS

A. SUPPLY NETWORK MODELS AND PERFORMANCE METRICS BASED ON COMPLEX NETWORK

Complex network theory provides a powerful tool to conceptualize supply networks. Using the complex network modeling methods, a supply network can be described as a set of nodes and links connecting nodes to denote firms and inter-firm relations respectively [17], [18]. Such configuration facilitates the analysis of supply network performance facing disruption.

Attempting to investigate the tolerance of supply networks to hypothetical supplier disruptions, various complex network-based supply network models and corresponding performance metrics are also proposed [19]–[22]. Yet, to facilitate the analysis, most of these studies describe supply networks as unipartite networks. These studies assume that a supply network is homogeneous. The different roles of firms and various types of inter-firm relations are neglected, which is extremely unrealistic and limits the analysis of supply networks [23]. Due to the unipartite network modeling, these studies have to adopt standard unipartite network topological metrics to measure the performance of a supply network facing disruptions, like average path length in the largest connected component (LCC) or size of the largest connected component (SLCC) [19], [20], [23]. A few researches consider the different roles of firms when modeling supply networks. Zhao *et al.* propose a supply network model composed by two types of nodes, namely demanders and suppliers [24]–[26]. Based on the model, they also propose a performance metric, supply availability rate, namely the proportion of demanders having access to suppliers. However, Zhao's studies merely consider the different roles of demander and supplier, they still treat suppliers to be equivalent. In a supply network, suppliers can be differentiated by the products they supplying. Some suppliers supply general products, which are provided by many suppliers. Some suppliers provide rare products, which are supplied by a very few suppliers. Compared with disruption of suppliers supplying general products, disruption of suppliers supplying rare products may inflict greater damage to the system [21], [27]. The model without differentiating the products that suppliers supplying will not reflect the importance of suppliers supplying rare products, although disruption of such suppliers would halt the production of manufacturers.

In summary, these previous works proposed a lot of complex network-based supply network models and corresponding performance metrics. However, most studies are limited to model supply networks as unipartite networks, others only consider the different role of firms. These simplifications limit the analysis of supply network. Thus, this study contributes to propose a supply network model, which considers the different roles of manufacturer and supplier and differentiates the products suppliers supplying. Based on the model, two performance metrics are also proposed to measure the loss of whole supply network caused by supplier disruptions.

B. BOTTLENECK SUPPLIER IDENTIFICATION USING NETWORK CENTRALITY METRICS

Recent supplier-caused supply network disruption events, such as Thailand floods and Tohoko earthquake, bring to the forefront the issue of detecting a type of hidden yet critical suppliers that may exist deep in a supply network [28]. Unlike traditional strategic suppliers [29], such critical suppliers may not provide any critical product or technology. The operation of a supply network depends on such critical suppliers because of their structural position in the network, namely how they are linked with other firms by business relations. Such critical suppliers gained a lot of attention in the past decades. Mizgier *et al.* define such critical suppliers as bottleneck suppliers [11]. While Yan *et al.* name such critical suppliers as nexus suppliers [12], [13]. In this study, we adopt the definition of bottleneck supplier proposed by Mizgier *et al.*.

To identify bottleneck suppliers, many researches have been proposed [17], [28], [30]–[33]. Craighead *et al.* describe a supply network as a set of nodes and edges connecting nodes [14]. Based on the network model, they present the proposition that the severity of a supplier disruption is positively related to the suppliers' structural centrality, such as degree centrality. That is to say, an unplanned event disrupting one or more suppliers occupying central positions in a supply network would cause greater loss than the disruption of less central suppliers in the supply network. This proposition attracts a lot of attentions from supply chain managers and researchers. And some researchers also find that disruption of suppliers occupying a more central position may not inflict greater damage to a supply network. Mizgier *et al.* also model a supply network using a weighted directed network, where nodes present firms and edge weight denote purchasing volumes [11]. Then, common used network centrality measures, such as degree centrality and betweenness centrality are discussed in the context of supply networks. Based on these centrality metrics, they propose a methodology for identifying bottleneck suppliers, i.e., suppliers that can induce high losses owing to disruptions in a supply network. However, the effectiveness of their method is verified using a simplistic and stylized supply network model which is composed by only six nodes. Ledwoch *et al.* also introduce network centrality metrics to identify risky suppliers [34]. For example, closeness centrality can be used to identify the suppliers whose disruption will make the cascading failure to progress the quickest. Betweenness centrality can be used to identify the highest risk suppliers among intermediaries. Yan *et al.* conceptualize the definition of nexus supplier [13]. According to the research of Yan *et al.*, nexus suppliers can affect the performance of a supply network because they take central positions in the supply network. Although Yan *et al.* introduce the concept of nexus supplier, their study is mainly from theoretic point of view. Based on the research of Yan *et al.*, Shao *et al.* propose a data-analytics framework for identifying nexus suppliers through a comprehensive use of multiple centrality measures [12]. However, the issues of how nexus suppliers may impact the performance of a supply network is still not explored in their study. They fail to explore questions like whether the identified nexus suppliers are more vital to the performance of a supply network.

Indeed, these previous works contribute a lot to identify bottleneck suppliers using standard network centrality metrics or a comprehension of these metrics. However, these network centrality metrics can only provide an approximation on how vital a supplier is to the performance of a supply network. Besides, most of these studies are from theoretic point of view or are limited by using simple and theoretical supply network model to validate their methods. There lacks studies using real industrial cases to validate the effectiveness of proposed bottleneck supplier identification methods. In the meanwhile, some scholars doubt whether these network centrality metrics can effectively identify bottleneck suppliers [5], [33]. Thus, this study proposes a novel method to identify bottleneck suppliers. Unlike traditional network centrality-based methods, our method does not use metrics to approximate the importance of suppliers. In the proposed method, a MALNS is designed to identify bottleneck suppliers in a two-stage supply network. In addition, based on an empirical automobile supply network, the effectiveness of proposed bottleneck suppliers identification method is validated.

III. MULTIPARTITE SUPPLY NETWORK MODEL AND PERFORMANCE METRICS

A. MULTIPARTITE SUPPLY NETWORK MODEL

Fig. 1(a) presents a two-stage supply network, where manufacturers purchase products from suppliers in order to

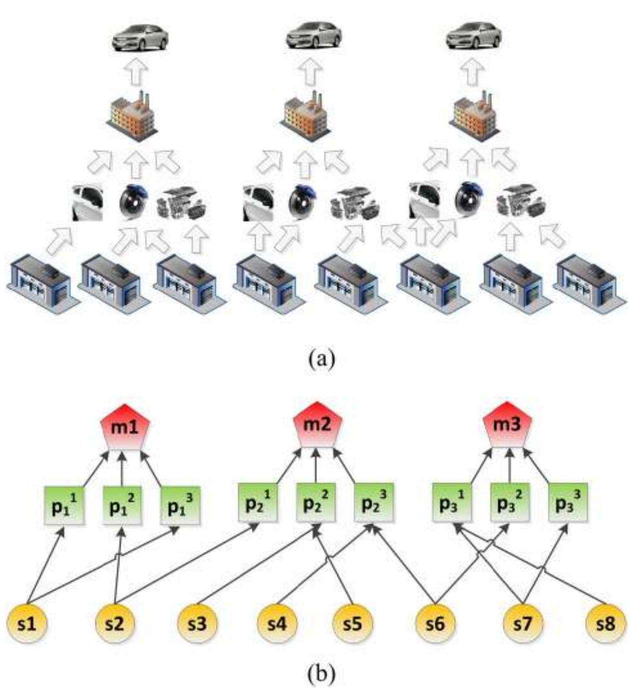

FIGURE 1. Illustration of multipartite supply network modeling. (a) Product supply-demand relations between manufacturers and suppliers. (b) Multipartite supply network model.

produce their own products. This is a general topology concerned in many previous researches [27], [35]. To describe the product supply-demand relations between manufacturers and suppliers, multipartite network is used to model this supply network. Multipartite network or multipartite graph is an important part of complex networks, which is characterized by the existing of different types of nodes and edges only exist between different types of nodes [36].

As shown in Fig. 1(b), these product supply-demand relations between manufacturers and suppliers are modeled as a directed multipartite network $G = \{M, P, S, E^{PM}, E^{SP}\}$, where the M, P and S are three disjoint and independent node sets, E^{PM} and E^{SP} are edge sets, representing directed edges between nodes in P and M and directed edges between nodes in S and P respectively.

$M = \{m_1, m_2, \ldots, m_{NM}\}$ represents manufacturers, where N_M refers to the number of manufacturer nodes in the network. $P = P(m_1) \cup P(m_2) \cup P(m_3), \ldots, \cup P(m_{NM})$ denotes products, where $P(m_j) = \{p_j^i | i = 1, 2, \ldots, |P(m_j)|\}$ represents products demanded by manufacturer m_j, $|P(m_j)|$ denotes the total number of products demand by manufacturer m_j. $S = \{s_1, s_2, \ldots, s_{NS}\}$ represents suppliers, where N_S is the number of supplier nodes in the network.

E^{PM} and E^{SP} are edge sets. $E^{PM} = \{(p_j^i, m_j) | i = 1, 2, \ldots, |P(m_j)|; j = 1, 2, \ldots, N_M\}$ represents the demanding relations between products and manufacturers, where (p_j^i, m_j) refers to a directed edge from p_j^i to m_j, representing that manufacturer m_j demands product p_j^i. $E^{SP} = \{(s_k, p_j^i) | k = 1, 2, \ldots, N_S; j = 1, 2, \ldots, N_M; i = 1, 2, \ldots, |P(m_j)|\}$ represents the supplying relations between products and suppliers, where (s_k, p_j^i) refers to a directed edge from s_k to p_j^i, representing that supplier s_k supplies product p_j^i to manufacturer m_j. In this study, only product supply-demand relations between manufacturers and suppliers are concerned. Thus, edges only exist between nodes in M and P and between nodes in P and S.

B. PERFORMANCE METRICS

Bottleneck supplier identification refers to identifying suppliers whose disruption will cause the greatest loss of the supply network performance. Thus, it is necessary to propose proper supply network performance metrics for evaluating the loss caused by supplier disruptions. In a supply network, the performance metrics should be able to show whether entities in the network can get necessary supplies to maintain normal operations. The inability to deliver products or materials to those who need them is a failure, which will decrease the performance of the supply network [37]. Based on this consideration, Zhao *et al.* propose supply availability rate which is the percentage of demanders that have access to suppliers in the network [24]–[26]. The expression of supply availability rate is presented as (1).

$$A = \frac{|A_M|}{N_M} \tag{1}$$

$$A_M = \{s_k \in S | \exists m_j : \exists p_{mj,sk}\} \tag{2}$$

where A_M represents the set of manufacturer nodes that have access to supplier nodes in the network, where $p_{mj,sk}$ denotes a path between nodes m_j and s_k. Consequently, the supply availability for a supply network network is defined as the ratio between the cardinalities of sets A_M and M.

As shown in (1), supply availability rate treats all suppliers to be equivalent, neglecting that suppliers can supply different types of products. Such simplification is unrealistic. In many real cases, the reason why manufacturers halt their production is the product supply shortage. For example, in 2011 Thailand flooding, the production of computer manufacturer was halted due to supply shortage of hard disc. Using supply availability rate to measure the performance of supply networks will not reflect such point. Thus, based on the definition of supply availability rate, two performance metrics, average product availability rate and manufacturer functioning rate are proposed.

Firstly, the definition of product availability rate R_j is introduced. In a supply network represented by $G = \{M, P, S, E^{PM}, E^{SP}\}$, manufacturers and suppliers play quite different roles. A manufacturer cannot perform its production duty for long without the supply of all necessary product from its suppliers. Thus, the product availability rate R_j of a given manufacturer m_j is defined as the proportion of its necessary products having access to suppliers, shown in (3).

$$R_j = \frac{\sum_{i=1}^{|P(m_j)|} \varepsilon(|\varphi(p_j^i)|)}{|P(m_j)|} \tag{3}$$

where $|P(m_j)|$ is the number of product nodes connected with m_j, representing the total number of necessary products for it. p_j^i is the ith product node connected to m_j. $|\varphi(p_j^i)|$ represents the number of supplier nodes connected with p_j^i. ε is unit step function, when $|\varphi(p_j^i)| > 0$, $\varepsilon(|\varphi(p_j^i)|) = 1$, otherwise, $\varepsilon(|\varphi(p_j^i)|) = 0$.

Then, according to product availability rate R_j, the following two performance metrics are introduced.

Average product availability rate R_A. When some suppliers are disrupted in a supply network, part manufacturers will lose supplies of necessary products, others may not be affected. To evaluate the damage to the entire network caused by the supplier disruptions, it necessary to consider the average level of manufacturers' availability of their necessary products. Thus, based on product availability rate R_j, average product availability rate of network G is defined by (4).

$$R_A(G) = \frac{1}{N_M}\sum_{j}^{N_M} R_j \tag{4}$$

where N_M is the total number of manufacturers in the network G, R_j is the product availability rate of manufacturer $m_{j,}$.

Then, manufacturers functioning rate R_F is also introduced. The average product availability rate R_A can reflect the system performance, but it still has some limitations. Fig. 2 describes two supplier disruption scenarios of the same supply network. In Fig. 2(a), supplier s_1 is disrupted. In Fig. 2(b), supplier s_2 is disrupted. In this study, the disruption of a supplier is considered to loss all production ability and the recovery of it is neglected. Thus, the disruption of a supplier node is modeled as removing it from the network. In addition, the adaptive behaviors of manufacturers, such as purchasing product from alternative suppliers, are also neglected. Such modeling method is used in many previous studies [20], [24], [25]. As presented in Fig. 2(a) and (b), the network after disrupting s_1 and after disrupting s_2 have the same average product availability rate. However, the proportions of manufacturers having access to all necessary products to produce their own products are quite different. In Fig. 2(a), the disruption of s_1 only leads to manufacturer m_1 losing product supply. While in Fig. 2(b), the disruption of s_2 leads both m_1 and m_2 losing product supply. Thus, compared with s_1, disruption of supplier s_2 inflicts greater damage to the entire supply network. Because disruption of s_1 only affects one manufacturer, while disruption of s_2 can affect two manufacturers. Only considering the average product availability rate, such difference will not be reflected. Therefore, to evaluate the supply network performance more comprehensively, the definition of manufacturer functioning rate is also proposed. Manufacturer functioning rate refers to the proportion of manufacturers having access to all necessary products to perform production duty in a supply network. Thus, the manufacturer functioning rate of network G is presented by (5).

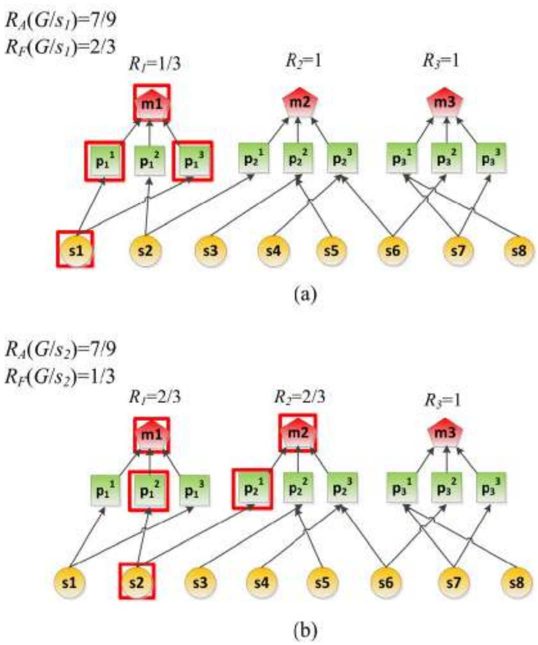

FIGURE 2. Performance evaluation of a multipartite supply network facing supplier disruptions. (a) Supplier disruption scenario 1. (b) Supplier disruption scenario 2.

$$R_F(G) = \frac{1}{N_M}\sum_{j}^{N_M} \delta(1 - R_j) \tag{5}$$

where N_M is the total number of manufacturers in the network G, R_j is the product availability rate of manufacturer $m_{j,}\delta(.)$ is unit impulse function, when 1-R_j = 0, $\delta(1 - R_j) = 1$, otherwise, $\delta(1 - R_j) = 0$.

IV. MEMETIC ALGORITHM WITH LOCAL NEIGHBORHOOD SEARCH FOR BOTTLENECK SUPPLIER IDENTIFICATION

In this section, MALNS-based bottleneck supplier identification method is presented. Firstly, the problem of bottleneck supplier identification is described. Then, MALNS is proposed.

A. PROBLEM DESCRIPTION

Bottleneck supplier identification refers to finding a single supplier or a group of suppliers whose disruption will cause the maximum deterioration of the network performances [11]. In this study, a multipartite network model $G = \{M, P, S, E^{PM}, E^{SP}\}$ is used to describe a two-stage supply network. Based on the model, two performance metrics, average product availability rate R_A and manufacturer functioning rate R_F are proposed. Thus, bottleneck supplier identification in the two-stage supply network presented in this study refers to finding a limited subset of supplier nodes I whose disruption will decrease both R_A and R_F most greatly. This is a typical optimization problem. In this study, the disruption of a supplier is modeled as the removing of it. Thus, the bottleneck supplier identification problem is described as below:

$$\max_I H(I) \tag{6}$$

$$s.t.\ |I| = K \tag{7}$$

$$H(I) = \alpha[R_A(G) - R_A(G/I)] + (1-\alpha)[R_F(G) - R_F(G/I)] \tag{8}$$

where $I \subseteq S$ represents any subset suppliers. $|I|$ represents the number of suppliers in I. K is a predefined integer. Constrain (7) denotes the number of identified bottleneck suppliers should be equal to the predefined integer K. G/I refers to the residual part of G after removing supplier subset I. $R_A(G/I)$ represents the average product availability rate of G/I.$R_F(G/I)$ denotes manufacturer functioning rate of G/I.$\alpha \in [0, 1]$ is a weighting parameter. If $0 \leq \alpha < 0.5$, the average product availability rate R_A is treated to be more important. If $0.5 < \alpha \leq 1$, the manufacturer functioning rate R_F is treated to be more important. In this study, the two performance metrics are treated to be equally important. Thus, the value of α is set to be 0.5.

B. MEMETIC ALGORITHM WITH LOCAL NEIGHBORHOOD SEARCH

Generally speaking, to solve the bottleneck supplier identification problem, these are two categories of methods: exact algorithms and evolutionary algorithms. Theoretically, exact algorithms can guarantee the optimality of solutions. However, the exact algorithm is time consuming, it may not suitable for large-scale networks. Meanwhile, evolutionary algorithms provide an alternative, since it can find approximate solutions of high-quality within a acceptable time. For example, when identifying K bottleneck suppliers in a supply network composed by N_S suppliers, there will be $C^{K_{NS}}$ possible solutions. Modern supply networks can be large-scale, which can contain thousands of suppliers. Thus, we adopt evolutionary algorithm to solve the bottleneck identification problem.

Memetic algorithm (MA) represents a type of evolutionary algorithms, which is optimized using a neighborhood search-based improvement procedure within a classical genetic algorithm framework [38]–[41]. Considering the out performance of MA in many other fields, this study proposes a MA improved by a local neighborhood searching procedure, which is named as MALNS, to identify the bottleneck suppliers. The proposed MALNS is composed of five main procedures: Initialization, parent individual selection, offspring individual generation, local neighborhood search and population update. The flowchart of algorithm is presented in Fig. 3.

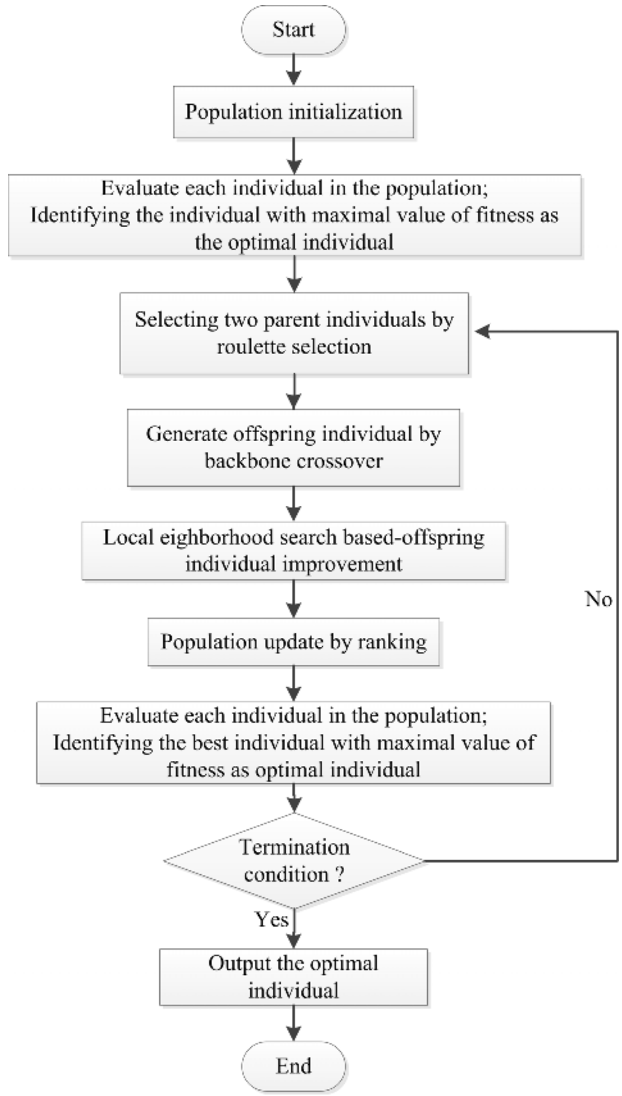

FIGURE 3. Flowchart of the proposed MALNS.

1) INDIVIDUAL CODING AND EVALUATION

In the proposed MALNS, each possible bottleneck supplier subset is represented by an individual. And a set of individuals is defined as a population. The population is represented by $POP = \{I_1, I_2, .., I_{pop\_size}\}$, where I_i is the ith individual in POP and pop_size is the number of individuals in the population. Classical individual coding methods include binary and string coding *et al.*. This article adopts string coding method. Thus, the ith individual in the population can be presented by $I_i = [I_i(1), I_i(2), \ldots, I_i(K)]$, where $I_i(j)$ is the jth gene of individual I_i, representing the number of a supplier node in G, K is the predefined number of identified bottleneck suppliers. Fig. 4 illustrates the string-based individual coding method.

In terms of bottleneck supplier identification, each individual represents a subset of bottleneck suppliers. Operations are performed to search for the optimal bottleneck supplier subset whose disruption will decrease both performance evaluation metrics R_A and R_F most greatly. Thus, each individual will be evaluated using a fitness value, those individuals with bigger fitness values are considered to be better ones. The fitness value of individual I_i is defined using (8).

2) INITIALIZATION

The initialization of a population is greatly significant, since it will affect not only the accuracy but also the convergence

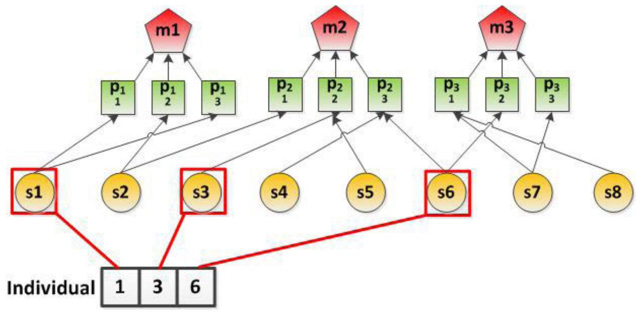

FIGURE 4. Illustration of string-based individual coding.

speed of algorithms. To start with a high-quality population, a local neighborhood search-based individual generation procedure is introduced. First, an individual is generated randomly. Then, it is improved by the local neighborhood search procedure described in Section 4.2.5. The improved individual will be put into the population, if it is different from individuals already existing in the population. Otherwise, it will be modified by a random swapping procedure until it is different from all existing individuals. Then, the modified individual will be inserted into the population. The individual generation procedure will be repeated by *pop_size* times to get the initial population. The procedure is shown in Algorithm 1.

Algorithm 1 Population Initialization

Input: $G = \{M, P, S, E^{PM}, E^{SP}\}$, K, $N\_{improvement}$ and *pop_size*
Output; $POP = \{I_1, I_2, \ldots, I_{POP\_size}\}$
$POP = \emptyset$;
while size *(POP)* < *pop_size* ***do***
  I = selecting K suppliers form S randomly;
  // improve individual I using local neighborhood search
  $I \leftarrow$ *Local neighborhood search(I, G,* $N_{improvement}$,*)*;
  If $I \cap POP == \emptyset$ ***do***
    $POP = POP \cup I$;
  else
    while $I \cap POP \neq \emptyset$ ***do***
      Modify / by swapping $u \in I$ with $v \in S/I$ randomly;
  endwhile
      $POP = POP \cup I$;
  endif
endwhile
Return *POP*;

3) ROULETTE-BASED PARENT INDIVIDUAL SELECTION

Traditional parent individuals selection methods include random selection method, tournament selection method, roulette selection method and so on. To keep the good properties from elite individuals, roulette selection method is adopted in this study.

4) BACKBONE CROSSOVER-BASED OFFSPRING INDIVIDUAL GENERATION

Crossover is a critically important procedure, it defines the way that parent individuals transmit properties to the offspring individuals. An effective crossover operation should be capable to transmit good properties from parent individuals to offspring individuals. Thus, to preserve the good properties of parent individuals, the backbone crossover is adopted in this study to generate high-quality offspring individuals [42]. The procedure is shown is Fig. 5.

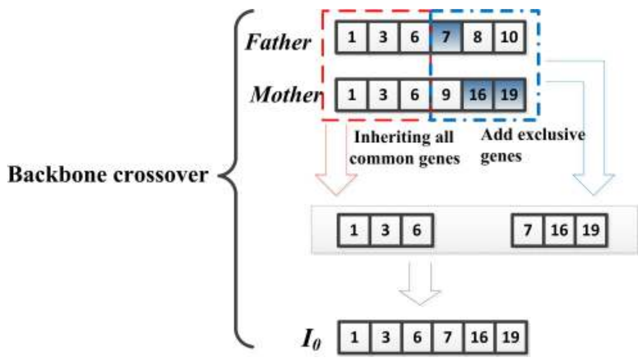

FIGURE 5. Backbone crossover-based offspring individual generation.

Assuming *Father* and *Mother* are two parent individuals selected from the population *POP*, the generation of offspring individual I_0 is listed as below:

Firstly, a partial individual I_0' is generated by inheriting all common genes of *Father* and *Mother*, $I_0' = Father \cup Mother$. The size of I_0' is defined as $|I_0$'$|$.

Then, randomly select K - $|I_0$'$|$ genes form the set $(Father \cup Mother) \setminus (Father \cap Mother)$, and add these selected genes into the I_0' to generate an offspring individual I_0.

5) LOCAL NEIGHBORHOOD SEARCH

Neighborhood search is an operation to improve the quality of an offspring individual by modifying part of it. To ensure a fast and effective improvement of an offspring individual, a local neighborhood search is proposed. The local neighborhood search is presented in Algorithm 2, which contains two parts: vulnerability-based local neighborhood determination and a two-stage exchanging procedure. Fig. 6 presents an example to illustrate the proposed local neighborhood search.

a: VULNERABILITY-BASED LOCAL NEIGHBORHOOD DETERMINATION

When a product node losing all supply links, the manufacturer connected with it will not be able to perform its production duty and product availability rate of it will also decrease. So it is reasonable to assume product nodes with less supply links are more vulnerable and the disruption of supplier nodes intensively connected with vulnerable product nodes may

Algorithm 2 Local Neighborhood Search

Input; $G = \{M, P, S, E^{PM}, E^{SP}\}$, I_0 and $N_{\_improvement}$
Output: I_0
for $i = 0, 1, 2, 3 \ldots, N_{\_improvement}$ ***do***
  //Vulnerability-based local neighborhood determination
  Determine the vulnerable product nodes in G/I_0;
  Search for the supplier node $S_{\_add}$;
 // two-stage exchanging procedure
  $I_0^* \leftarrow I_0 \cup \{S_{\_add}\}$;
  $S_{\_remove} \leftarrow \arg\min_{w \in I0}\{f(I_0^*) - f(I_0^* \backslash \{w\})\}$;
  $I_0 \leftarrow I_0^* \backslash \{S_{\_remove}\}$;
endfor
Return I_0;

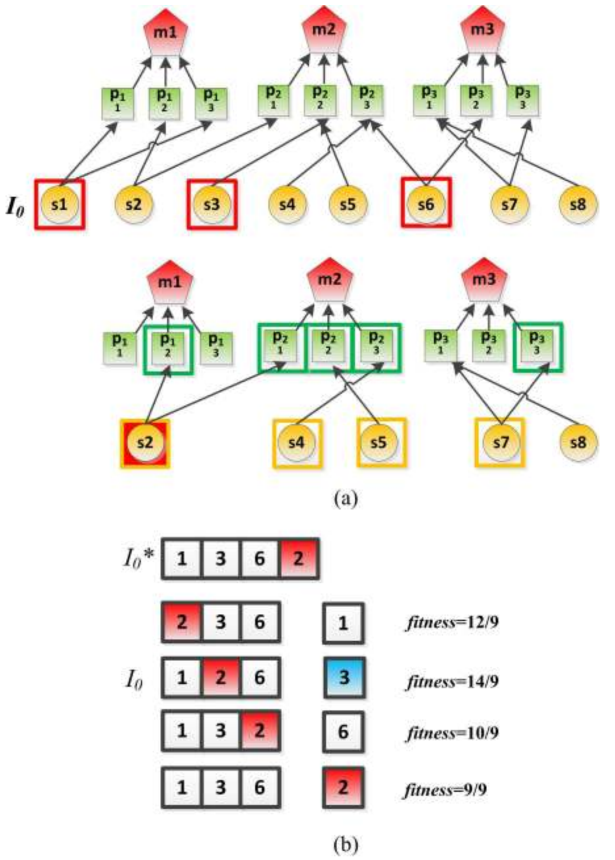

FIGURE 6. Illustration of local neighbor search-based offspring individual improvement. (a) Vulnerability-based local neighborhood determination. (b) Two phase nodes exchange method.

inflict a larger damage. Thus, when exchanging a supplier node $u \in I_0$ with a supplier node $v \in S\backslash I_0$ to improve the quality of I_0, it is preferable to select v having more connections with vulnerable product nodes, namely less connected product nodes. Based on this consideration, a vulnerability-based local neighborhood determination method is designed.

(a) Calculate the in-degree of all product nodes in $G(S/I_0)$, namely the number of supply connections. Then, determine the vulnerability threshold of product nodes using roulette selection. The procedures are listed as below: Firstly, summarize all possible values of the in-degree of product nodes and remove 0 value to get all possible value of vulnerability threshold. Second, since the product nodes with a smaller value of in-degree tend to be vulnerable, the priority weight of these possible value is defined as the reciprocal of it. Based on the priority weight, a roulette selection is used to determine the vulnerability threshold L.

(b) Search for product nodes in $G(S/I_0)$ of which the in-degrees are smaller than vulnerability threshold L but bigger than 0 as vulnerable product nodes.

(c) Determine the supplier node having most connections with the vulnerable product nodes in $G(S/I_0)$ to be the candidate supplier node $s_{\_add}$.

b: TWO PHASE NODES EXCHANGE METHOD

(a) Add the candidate supplier node $s_{\_add}$ into I_0 to generate I_0*.

(b) Search for the supplier node $s_{\_remove}$, of which the removing that causes the minimum decrease of fitness.

6) RANKING-BASED POPULATION UPDATE

After the local neighborhood search-based offspring individual improvement, a population updating strategy will be performed. As shown in Algorithm 3, firstly, the improved offspring individual I_0 is added into the population POP to generate POP^*. Then, evaluate all the individuals in POP^* according to the scoring function and identify the worst individual. Finally, the worst individual is removed from POP^* to generate the updated population. The scoring function is presented using (9).

$$Score(i) = \gamma^* Score_F(i) + (1-\gamma)^* Score_D(i) \quad (9)$$

$$Score_F(i) = \frac{fitness(i)}{\sum_{j=0}^{pop\_size} fitness(j)} \quad (10)$$

$$Score_D(i) = \frac{diversity(i)}{\sum_{j=0}^{pop\_size} diversity(j)} \quad (11)$$

$$diversity(i) = \sum_{j \in POP*, j \neq i} 1 - \frac{|I_i \cap I_j|}{|I_i \cup I_j|} \quad (12)$$

Algorithm 3 Ranking-Based Population Update

Input: POP, I_0
Output: POP
$POP^* = POP \cup \{I_0\}$;
for $i = 0, 1, 2, \ldots, pop_{\_size}$ ***do***
  Evaluate individual according to the score function;
endfor
Identifying I_w with the lowest score in POP^* ;
$POP = POP^* \backslash \{I_w\}$;
Return POP;

where $Score_F(i)$ and $Score_D(i)$ represent the fitness score and the diversity score of individual I_i in population $POP*$ respectively. $Score_F(i)$ refers to the comparative quality of I_i in POP, while $Score_D(i)$ refers to the comparative diversity contribution of it. $\gamma \in [0, 1]$ is the weighting coefficient between fitness score and diversity score, which is empirically set to 0.7. $fitness(i)$ is the fitness value of individual I_i, denoting the quality of I_i. $diversity(i)$ represents the diversity contribution of I_i to POP^*, which is measured by the dissimilarity between it and the remaining individuals in POP^*.

V. CASE STUDY

To illustrate the applicability and effectiveness of the proposed bottleneck supplier identification method, a case study is presented in this section. Firstly, a large-size of data is collected to construct an empirical automobile multipartite supply network. Then, based on the empirical network, experiments are conducted to evaluate the proposed supply network performance metrics and MALNS-based bottleneck supplier identification method. All of the simulations were taken on a PC equipped with an Intel core i7 processor with 3.2 GHz and 16 GB RAM based on Matlab 2014a.

A. EMPIRICAL MULTIPARTITE SUPPLY NETWORK

The online automobile supplier database provided by one of the biggest automobile product e-commerce procurement platforms in China, Gasgoo (www.gasgoo.com), is used as the data source. This database provides information of more than 20000 automobile suppliers in China, such as company names, the lists of supplied products and clients. The database allows users to search for suppliers by client names and supplied products. Based on the database, supply-demand information of 27 types of automobile products between 5574 suppliers and 47 manufacturers in China was collected.

An empirical automobile multipartite supply network **is** modeled with the collected data. The 47 automobile manufacturers are abstracted as 47 manufacturer nodes. Each manufacturer node is connected with 27 product nodes, representing the 27 types of automobile products demanded by it. Then, according to the supplying relations between products and suppliers, links are also built between product nodes and supplier nodes. In summary, the network contains 6890 nodes and 28705 edges. Nodes contain 47 manufacturer nodes, 1269 product nodes and 5574 supplier nodes. Edges include 27576 supply edges from supplier nodes to product nodes and 1269 demand edges from product nodes to manufacturer nodes.

To explore structural character of the empirical network, degree distributions of the network are investigated, including the out-degree of supplier nodes and the in-degree of product nodes. According to previous works, it has been found that the degree distributions of most real-life networks can be approximated by five distributions: power law, truncated-power law, exponential, stretched exponential and log-normal distributions [43]. Thus, the degree distributions are fitted using the five distributions and good of fitness R^2 is used for evaluation. It is found the most approximate of both degree distributions is the stretched exponential distribution. The observed degree distributions and the best fitting curves are presented in Fig. 7. This indicates that the automobile supply network is neither a random network nor a scale-free network, but between them [44].

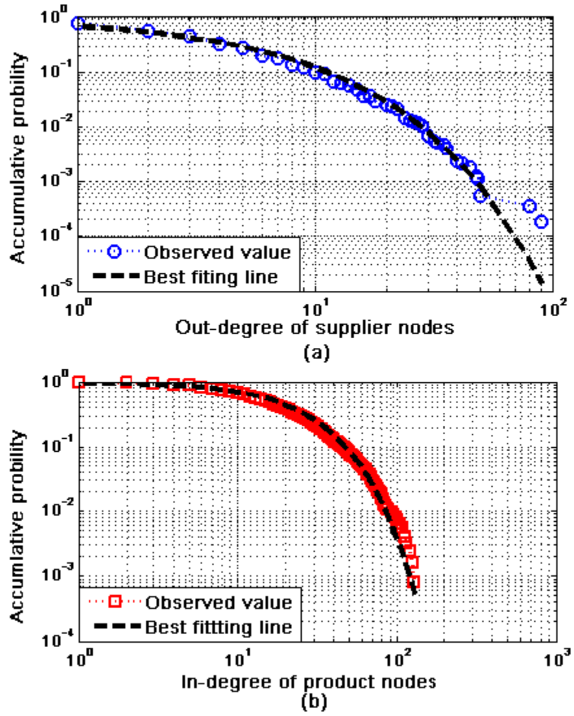

FIGURE 7. Degree distributions of the empirical multipartite automobile supply network. (a) Out-degree of supplier nodes. (b) In-degree of product nodes.

B. EVALUATION OF PROPOSED PERFORMANCE METRICS

To evaluate the proposed supply network performance metrics, comparison between the proposed performance metrics and a common used supply network performance metric, SLCC [22] are made. According to the research of Kim *et al.*, performance metrics of supply networks should be able to distinguish the robustness of different supply networks facing supplier disruptions [5]. Thus, performance metrics variation of both the original empirical multipartite supply network and the structurally modified ones facing random supplier disruption are compared. Adding edges is a commonly used robustness enhancing method. Thus, low-degree edge addition strategy [45] is used to add edges between product nodes and supplier nodes for network structural modification.

As presented in Fig. 8(a), (b) and (c), performance metrics comparison between the original network and structural modified ones are presented. As shown in Fig. 8(a), the three curves of SLCC almost overlap with each others. It is evident that SLCC can not distinguish the robustness of different supply networks clearly. As shown in Fig. 8(b) and (c),

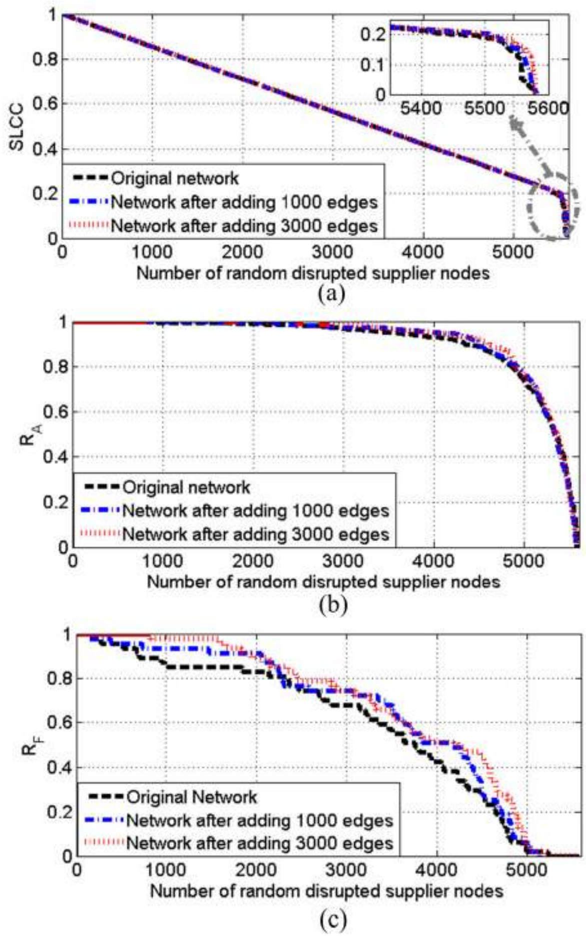

FIGURE 8. Comparison of supply network performance metrics. (a) SLCC. (b) Average product availability rate. (c) Manufacturer functioning rate.

compared with SLCC, average product availability rate and manufacturer functioning rate can reflect the difference between original network and network after adding edges more evidently. It is also found that structural modification using low-degree edge addition strategy can increase supply network robustness. In both Fig. 8(a), (b) and (c), with the number of added edge increasing, curves of performance metrics decline slower. That is to say, with the number of added edge increasing, supply network presents stronger tolerance of supplier disruptions.

C. EVALUATION OF MALNS-BASED BOTTLENECK SUPPLIER IDENTIFICATION

Based on the empirical multipartite supply network, experiments are also performed to evaluate the performance of proposed MALNS-based bottleneck supplier identification method. Firstly, a preparation experiment is performed to set parameters. Then, to verify the effectiveness of the proposed MALNS-based bottleneck supplier identification method, comparative experiment is also conducted.

1) PARAMETER SETTING

Like most evolutionary algorithms, the proposed MALNS also has to set parameters and the value of parameters may affect the performance of algorithm. As presented in Section 4.2, the parameters of the proposed MALNS includes population size *pop_size* and times of offspring individual local improvement $N\_{improvement}$. The *pop_size* is set to 20 according to previous works [39]. Then, performance of the proposed MALNS-based bottleneck supplier identification method under different value of $N\_{improvement}$ is analyzed to define a proper value of it. Firstly, K is settled to be 10, namely use 10 bottleneck supplier identification as an instance for parameter setting. Then, the termination condition is defined to be 100 generation. Quality of optimal individuals $I_{optimal}$ and running time are analyzed under different $N\_{improvement}(0.1^*K, 0.2^*K, \ldots, 0.5^*K)$. The optimal individual represents the identified bottleneck suppliers. Thus, the quality of optimal individual is measured using $R_A(G/I_{optimal})$ and $R_F(G/I_{optimal})$, which represents the network performance after disrupting the identified bottleneck suppliers. Each simulation is repeated 10 times.

The experiment result is presented in Fig. 9. As shown in Fig. 9(a), the running time increases linearly as the increasing of $N\_{improvement}$. As presented in Fig. 9(b) and (c), both $R_A(G/I_{optimal})$ and $R_F(G/I_{optimal})$ decrease with the increasing of $N\_{improvement}$. It also has been noticed that decrement of both $R_A(G/I_{optimal})$ and $R_F(G/I_{optimal})$ is most obvious between 0.1^*K and 0.2^*K. To get a balance of time efficiency and solution quality, $N\_{improvement}$ is settled to be 0.2^*K in the following works.

2) COMPARATIVE EXPERIMENT

To evaluate the performance of the proposed MALNS-based bottleneck supplier identification method, experiment is also made to compare it with other methods. Comparison with traditional network centrality-based approach including degree centrality-based (DC) [14] and betweenness centrality-based (BC) [11] bottleneck supplier identification method is made. In these approaches, supplier nodes with the largest value of centrality in the network are selected as bottleneck suppliers. Besides, comparison with evolutionary algorithm-based method is also made. Two universal critical nodes identification methods, GA [46] and Greedy2 [47], are also used to identify the bottleneck suppliers in the supply network. To make a fair comparison, GA-based bottleneck supplier identification method and the proposed MALNS-based bottleneck supplier identification method were running on our platform with the same time limit $T_{max} = 16000$ seconds [48]. Except for T_{max}, the default parameter values of GA settled in the work of Boginski and Commander are adopted [46]. In addition, we also use random selection-based method (RAND) to validate the effectiveness of bottleneck supplier identification methods mentioned above.

Performance comparison of the six bottleneck supplier identification methods is presented by Fig. 10 and Table 1.

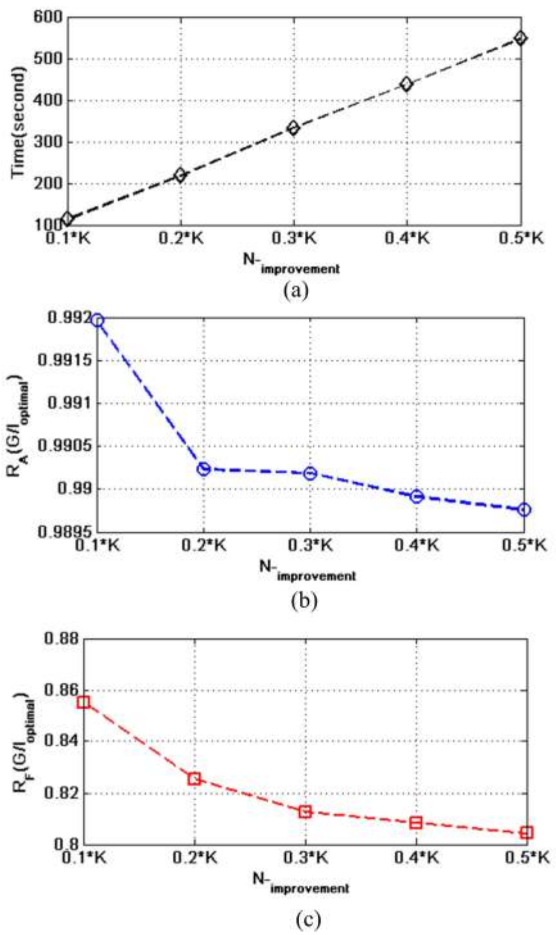

FIGURE 9. The performance of MALNS-based bottleneck supplier identification under different value of $N_{\_improvement}$. (a) Running time. (b) $R_A(G/I_{optimal})$. (c) $R_F(G/I_{optimal})$.

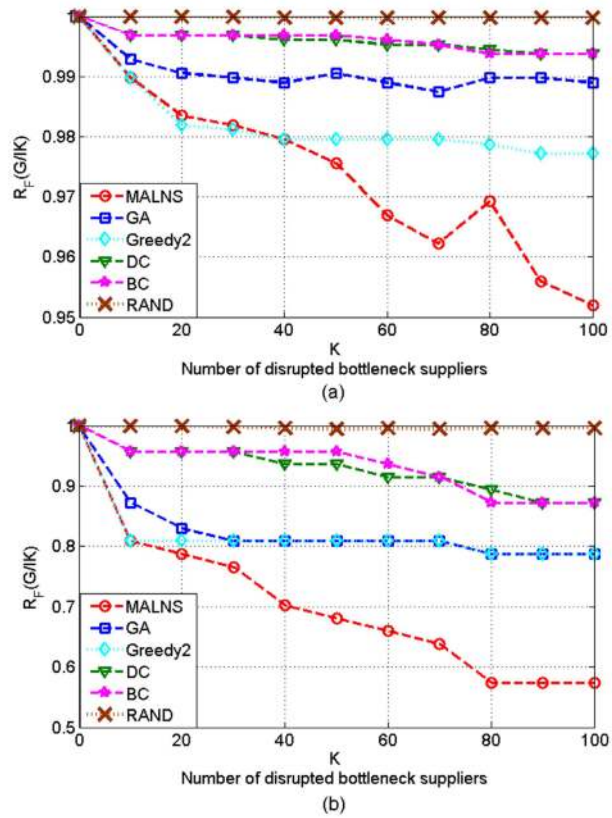

FIGURE 10. Performance comparison between MALNS-based bottleneck supplier identification method and other methods. (a) Average product availability rate after disrupting K bottleneck suppliers. (b) Manufacturer functioning rate after disrupting K bottleneck suppliers.

TABLE 1. Average value comparison for R_A (G/I_K) and R_F (G/I_K).

Method	Mean($R_A(G/I_K)$)	Mean($R_F(G/I_K)$)
MALNS	**0.9740**	**0.6978**
GA	0.9903	0.8212
Greedy2	0.9815	0.8127
DC	0.9958	0.9276
BC	0.9961	0.9323
RAND	0.9999	0.9967

Fig. 10(a) and (b) present the curves of the average product availability rate $R_A(G/I_K)$ and manufacturer functioning rate $R_F(G/I_K)$ of the empirical mutipartite supply network after disrupting K bottleneck supplier nodes respectively. To quantify the comparison, average value of $R_A(G/I_K)$ and $R_F(G/I_K)$ are also presented in Table 1. In Table 1, $Mean(R_A(G/I_K))$ and $Mean(R_F(G/I_K))$ represent the average value of $R_A(G/I_K)$ and $R_F(G/I_K)$ respectively. The smaller average values of $Mean(R_A(G/I_K))$ and $Mean(R_F(G/I_K))$ refer to greater damage to the network by disrupting the identified bottleneck supplier nodes, namely better performance of the bottleneck supplier identification method.

In Fig. 10(a), along with increasing of disrupted bottleneck suppliers, all the average product availability rate curves decrease evidently except for RAND-based method. By comparing RAND-based bottleneck supplier identification method with other methods, it is found that both centrality-based and evolutionary algorithm-based methods perform much better than RAND-based method. Such results validates the rationality of centrality metrics and the effectiveness of evolutionary algorithms. In addition, DC-based and BC-based bottleneck supplier identification methods perform far more worse than other three evolutionary algorithm-based methods. Such result indicates that traditional network centrality metrics fail to identify bottleneck suppliers accurately. Besides, when the number of disrupted bottleneck suppliers is smaller than 40, greedy2-based bottleneck supplier identification method performs slightly better than MALNS-based method. When the number of disrupted bottleneck suppliers is bigger than 40, MALNS-based bottleneck supplier identification method performs much better than greedy2-based method. Fig. 10(b) shows a similar trend shown in Fig. 10(a). In the Table. 1, MALNS-based bottleneck supplier identification method obtains the minimal average value of both

$R_A(G/I_K)$ and $R_F(G/I_K)$. Overall, MALNS-based bottleneck supplier identification method achieves the best performance to minimize both performance metrics. Such results prove that the proposed MALNS-based bottleneck supplier identification method can detect bottleneck suppliers effectively.

3) EVALUATION OF PROPOSED LOCAL NEIGHBORHOOD SEARCH

To further explore the effectiveness of proposed local neighborhood search procedure, a comparative experiment is also performed to compare the proposed MALNS with an alternative version MARES where the local neighborhood search procedure is replaced by the conventional random exchange strategy [49]. That is to say, at each neighborhood search iteration of MARES, a random supplier node $u \in I_0$ is exchanged by a random supplier node $v \in S \setminus I_0$ to generated a new individual. If the new individual is better than I_0, the original individual I_0 will be replaced by the new individual. Otherwise, it will not be accepted.

The experimental results are shown in Fig. 11. Fig. 11(a) and (b) present the fitness curves of MALNS and MARES under $K = 10$ and $K = 30$ respectively. It can be observed that MALNS can find better individuals in a shorter time in the both two instances. Thus, the proposed local neighborhood search procedure can effectively increase the performance of MA, suggesting that MALNS is a suitable method for detecting bottleneck suppliers.

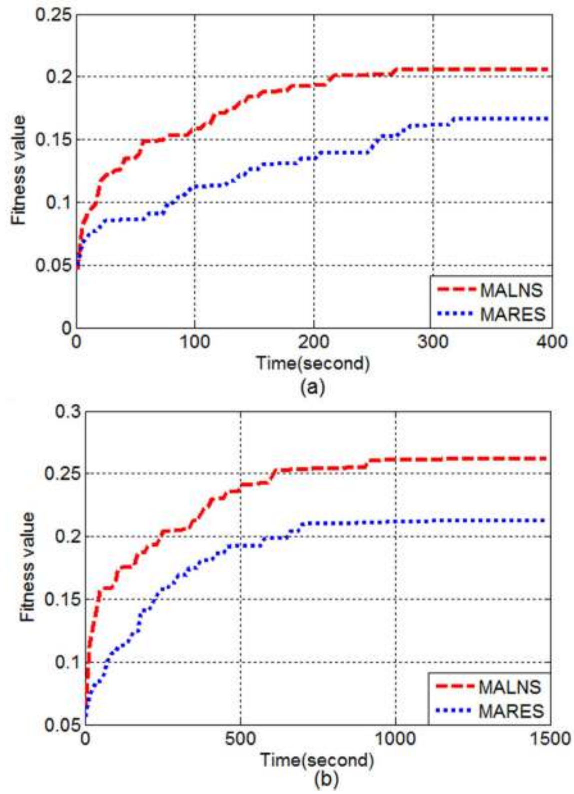

FIGURE 11. Fitness curve comparison between MALNS and MARES. (a) K = 10.(b) K = 30.

D. EXPERIMENTAL RESULTS DISCUSSION

The structural character of empirical automobile supply network is analyzed. As a result, it is found that degree distribution of automobile supply network exhibits stretched exponential distribution. Such finding indicates the automobile supply network is not homogeneous. A few hub firms occupy major market.

The comparison between proposed supply network performance metrics and the standard network metric SLCC is made. It is found that SLCC does not reliably distinguish among different supply networks on robustness. Therefore, researchers need to define performance metrics carefully when evaluating supply network performance facing supplier disruptions. In addition, it is also found that low degree-based edge addition strategy can improve the robustness of supply network. Such findings can also provide some insights for supply network risk mitigation.

The effectiveness of proposed MALNS-based bottleneck supplier identification method is validated using comparative experiments. First, comparing with random selection-based bottleneck supplier identification method with centrality-based and evolutionary algorithm-based methods, it is verified the rationality of centrality metrics and the effectiveness of evolutionary algorithms. By comparing evolutionary algorithm-based with network centrality-based bottleneck supplier identification methods, it is also found that network centrality-based methods fail to provide an accurate detection of bottleneck suppliers. Such result presents the difficulty to identify bottleneck suppliers. The main reason behind this is that these centrality metrics can only reflect the local importance of a supplier. However, from a network perspective, bottleneck supplier identification needs considering the overall network structure. Besides, it is also observed that the empirical automobile supply network is vulnerable. In a supply network including more than 5000 suppliers, disruption of 10 bottleneck suppliers can lead 20% manufacturers fail to obtain all necessary products to continue their production. By disrupting less than 100 bottleneck suppliers, nearly half manufacturers will not achieve all necessary products to perform their production duties. Thus, identification of these bottleneck suppliers is highly important, since the disruption of them will induce extremely high loss.

VI. CONCLUSION

Recent supplier-caused supply network disruption events bring to the forefront the issue of detecting bottleneck suppliers, namely suppliers whose disruption will induce high loss to the entire supply network. Identification of bottleneck supplier is significantly important for supply network risk management. Thus, this article proposes a MALNS-based method to identify bottleneck suppliers. This article can be concluded as below:

Firstly, a multipartite supply network model has been developed to reflect the fact that nodes play heterogeneous roles in a supply network, which is not the case for many other networks. Based on the network model, two performance metrics describing the product availability of manufacturers are proposed: average product availability rate and manufacturer functioning rate. Compared with conventional network metric SLCC, the proposed performance metrics can distinguish the robustness of different supply networks more effectively.

Secondly, a MALNS-based bottleneck supplier method is proposed. Instead of using metrics to approximate how vital a supplier is to the performance of a supply network, the proposed method uses a MA improved by a local neighborhood search procedure, namely MALNS, to identify bottleneck suppliers.

Third, this study also has implications for empirical researches. A large size of data was collected to construct an empirical automobile supply network. Structural character of the empirical network is analyzed. It is found that supply networks in real life are neither scale-free nor random networks, but between them. Such finding implies that the real supply networks are not homogeneous. A few hub firms occupy major market.

Finally, based on the empirical network, the effectiveness of proposed MALNS-based bottleneck supplier identification method is validated. Therefore, the proposed method provides supply network managers and researchers with an effective tool to quantify the losses of a supply network due to disruptions from single or multiple suppliers. Using the bottleneck identification method proposed in this study, supply network managers and researchers can easily discover which suppliers are most critical for supply network performance and pose the greatest threat. They can both identify the bottleneck suppliers and estimate the potential impact of disruptions.

However, this study still has some limitations. The proposed model in this study only considers a two-stage supply network. Besides, the purchasing volume of each product between suppliers and manufacturers is also neglected. Thus, the work presented in this article will be extended into a context of multistage supply networks and will take the purchasing volume into consideration in the future.

REFERENCES

[1] A. Brintrup and A. Ledwoch, "Supply network science: Emergence of a new perspective on a classical field," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 28, no. 3, Mar. 2018, Art. no. 033120.

[2] H. El Raoui, M. Oudani, and A. El Hilali Alaoui, "Coupling soft computing, simulation and optimization in supply chain applications: Review and taxonomy," *IEEE Access*, vol. 8, pp. 31710–31732, 2020.

[3] 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.

[4] A. Käki, A. Salo, and S. Talluri, "Disruptions in supply networks: A probabilistic risk assessment approach," *J. Bus. Logistics*, vol. 36, no. 3, pp. 273–287, Sep. 2015.

[5] Y. Kim, Y.-S. Chen, and K. Linderman, "Supply network disruption and resilience: A network structural perspective," *J. Oper. Manage.*, vols. 33–34, no. 1, pp. 43–59, Jan. 2015.

[6] A. R. Singh, P. K. Mishra, R. Jain, and M. K. Khurana, "Design of global supply chain network with operational risks," *Int. J. Adv. Manuf. Technol.*, vol. 60, nos. 1–4, pp. 273–290, Apr. 2012.

[7] A. Salamai, O. K. Hussain, M. Saberi, E. Chang, and F. K. Hussain, "Highlighting the importance of considering the impacts of both external and internal risk factors on operational parameters to improve supply chain risk management," *IEEE Access*, vol. 7, pp. 49297–49315, 2019.

[8] M. Kamalahmadi and M. M. Parast, "An assessment of supply chain disruption mitigation strategies," *Int. J. Prod. Econ.*, vol. 184, pp. 210–230, Feb. 2017.

[9] C. A. MacKenzie, J. R. Santos, and K. Barker, "Measuring changes in international production from a disruption: Case study of the Japanese earthquake and tsunami," *Int. J. Prod. Econ.*, vol. 138, no. 2, pp. 293–302, Aug. 2012.

[10] M. Martinez, "Supplier fire ripples across the industry," *Automot. News*, vol. 92, no. 6829, p. 0001, 2018.

[11] K. J. Mizgier, M. P. Jüttner, and S. M. Wagner, "Bottleneck identification in supply chain networks," *Int. J. Prod. Res.*, vol. 51, no. 5, pp. 1477–1490, Mar. 2013.

[12] B. B. M. Shao, Z. Shi, T. Y. Choi, and S. Chae, "A data-analytics approach to identifying hidden critical suppliers in supply networks: Development of nexus supplier index," *Decis. Support Syst.*, vol. 114, pp. 37–48, Oct. 2018.

[13] T. Yan, T. Y. Choi, Y. Kim, and Y. Yang, "A theory of the nexus supplier: A critical supplier from a network perspective," *J. Supply Chain Manage.*, vol. 51, no. 1, pp. 52–66, Jan. 2015.

[14] 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.

[15] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. R. S. Tanaka, and W. Willinger, "The 'robust yet fragile' nature of the Internet," *Proc. Nat. Acad. Sci. USA*, vol. 102, no. 41, pp. 14497–14502, Oct. 2005.

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

[17] Y. Kim, T. Y. Choi, T. Yan, and K. Dooley, "Structural investigation of supply networks: A social network analysis approach," *J. Oper. Manage.*, vol. 29, no. 3, pp. 194–211, Mar. 2011.

[18] T. Kito, S. New, and K. Ueda, "How automobile parts supply network structures may reflect the diversity of product characteristics and suppliers' production strategies," *CIRP Ann.*, vol. 64, no. 1, pp. 423–426, 2015.

[19] F. Ma, H. Xue, K. F. Yuen, Q. Sun, S. Zhao, Y. Zhang, and K. Huang, "Assessing the vulnerability of logistics service supply chain based on complex network," *Sustainability*, vol. 12, no. 5, p. 1991, Mar. 2020.

[20] 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.

[21] J. Nakatani, K. Tahara, K. Nakajima, I. Daigo, H. Kurishima, Y. Kudoh, K. Matsubae, Y. Fukushima, T. Ihara, Y. Kikuchi, A. Nishijima, and Y. Moriguchi, "A graph theory-based methodology for vulnerability assessment of supply chains using the life cycle inventory database," *Omega*, vol. 75, pp. 165–181, Mar. 2018.

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

[23] S. Perera, M. G. H. Bell, and M. C. J. Bliemer, "Network science approach to modelling the topology and robustness of supply chain networks: A review and perspective," *Appl. Netw. Sci.*, vol. 2, no. 1, p. 33, Oct. 2017.

[24] 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.

[25] 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.

[26] 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.

[27] A. Brintrup, J. Barros, and A. Tiwari, "The nested structure of emergent supply networks," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1803–1812, Jun. 2018.

[28] S. P. Borgatti and X. Li, "On social network analysis in A supply chain context," *J. Supply Chain Manage.*, vol. 45, no. 2, pp. 5–22, Apr. 2009.

[29] S. M. Wagner and J. L. Johnson, "Configuring and managing strategic supplier portfolios," *Ind. Marketing Manage.*, vol. 33, no. 8, pp. 717–730, Nov. 2004.

[30] R. C. Basole, S. Ghosh, and M. S. Hora, "Supply network structure and firm performance: Evidence from the electronics industry," *IEEE Trans. Eng. Manag.*, vol. 65, no. 1, pp. 141–154, Feb. 2018.
[31] E. Delbufalo, "The influence of supply network structure on firm's multiple innovation capabilities: A longitudinal study in the fashion industry," *Manage. Decis.*, vol. 53, no. 10, pp. 2457–2476, Nov. 2015.
[32] M. C. Dong, Z. Liu, Y. Yu, and J.-H. Zheng, "Opportunism in distribution networks: The role of network embeddedness and dependence," *Prod. Oper. Manage.*, vol. 24, no. 10, pp. 1657–1670, Oct. 2015.
[33] J. F. B. Valenzuela, X. Fu, G. Xiao, and R. S. M. Goh, "A network-based impact measure for propagated losses in a supply chain network consisting of resilient components," *Complexity*, vol. 2018, Feb. 2018, Art. no. 1724125.
[34] A. Ledwoch, A. Brintrup, J. Mehnen, and A. Tiwari, "Systemic risk assessment in complex supply networks," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1826–1837, Jun. 2018.
[35] M. Xu, S. Radhakrishnan, S. Kamarthi, and X. Jin, "Resiliency of mutualistic supplier-manufacturer networks," *Sci. Rep.*, vol. 9, no. 1, p. 13559, Sep. 2019.
[36] Q. Cai, M. Pratama, S. Alam, C. Ma, and J. Liu, "Breakup of directed multipartite networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Jan. 21, 2019, doi: 10.1109/TNSE.2019.2894142.
[37] A. Neely, M. Gregory, and K. Platts, "Performance measurement system design: A literature review and research agenda," *Int. J. Oper. Prod. Manage.*, vol. 25, no. 12, pp. 1228–1263, Dec. 2005.
[38] F. Baesler and C. Palma, "Multiobjective parallel machine scheduling in the sawmill industry using memetic algorithms," *Int. J. Adv. Manuf. Technol.*, vol. 74, nos. 5–8, pp. 757–768, Sep. 2014.
[39] Z. Lü and J.-K. Hao, "A memetic algorithm for graph coloring," *Eur. J. Oper. Res.*, vol. 203, no. 1, pp. 241–250, May 2010.
[40] F. Neri and C. Cotta, "Memetic algorithms and memetic computing optimization: A literature review," *Swarm Evol. Comput.*, vol. 2, pp. 1–14, Feb. 2012.
[41] W. Sun, J.-K. Hao, W. Wang, and Q. Wu, "Memetic search for the equitable coloring problem," *Knowl.-Based Syst.*, vol. 188, Jan. 2020, Art. no. 105000.
[42] Y. Zhou, J.-K. Hao, and B. Duval, "Opposition-based memetic search for the maximum diversity problem," *IEEE Trans. Evol. Comput.*, vol. 21, no. 5, pp. 731–745, Oct. 2017.
[43] B. Vandermarliere, A. Karas, J. Ryckebusch, and K. Schoors, "Beyond the power law: Uncovering stylized facts in interbank networks," *Phys. A, Stat. Mech. Appl.*, vol. 428, pp. 443–457, Jun. 2015.
[44] P.-P. Zhang, K. Chen, Y. He, T. Zhou, B.-B. Su, Y. Jin, H. Chang, Y.-P. Zhou, L.-C. Sun, B.-H. Wang, and D.-R. He, "Model and empirical study on some collaboration networks," *Phys. A, Stat. Mech. Appl.*, vol. 360, no. 2, pp. 599–616, Feb. 2006.
[45] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Phys. A, Stat. Mech. Appl.*, vol. 357, nos. 3–4, pp. 593–612, Nov. 2005.
[46] V. Boginski and C. W. Commander, "Identifying critical nodes in protein-protein interaction networks," *Clustering Challenges Biol. Netw.*, pp. 153–167, Feb. 2009.
[47] B. Addis, R. Aringhieri, A. Grosso, and P. Hosteins, "Hybrid constructive heuristics for the critical node problem," *Ann. Oper. Res.*, vol. 238, nos. 1–2, pp. 637–649, Mar. 2016.
[48] R. Aringhieri, A. Grosso, P. Hosteins, and R. Scatamacchia, "A general evolutionary framework for different classes of critical node problems," *Eng. Appl. Artif. Intell.*, vol. 55, pp. 128–145, Oct. 2016.
[49] Y. Zhou, J.-K. Hao, and F. Glover, "Memetic search for identifying critical nodes in sparse graphs," *IEEE Trans. Cybern.*, vol. 49, no. 10, pp. 3699–3712, Oct. 2019.

PING LOU received the M.S. and Ph.D. degrees in mechanical engineering from the Huazhong University of Science and Technology of China, Wuhan, in 1997 and 2004, respectively. She is currently a Professor with the School of Information Engineering, Wuhan University of Technology. Her research interests include network manufacturing, digital manufacturing, intelligent manufacturing, and supply chain.

YUTING CHEN received the master's degree from the Wuhan University of Technology, China, in 2014, where she is currently pursuing the Ph.D. degree. Her research interests include intelligent manufacturing, supply chain, and complex networks.

JUNWEI YAN received the M.S. degree in communication and information system from the Wuhan University of Technology, China, in 2009, the joint Ph.D. degree from the School of Mechanical Engineering, University of Birmingham, U.K., in 2016, and the Ph.D. degree from the Wuhan University of Technology, in 2018. His research interests include cloud manufacturing, digital twin, FBG sensors applications, and machine learning.