Hindawi
Complexity
Volume 2020, Article ID 1292938, 21 pages
https://doi.org/10.1155/2020/1292938

Research Article

Adaptive Variable Neighborhood Search-Based Supply Network Reconfiguration for Robustness Enhancement

Ping Lou, Yuting Chen, and Song Gao

School of Information Engineering, Wuhan University of Technology, Wuhan 430000, China

Correspondence should be addressed to Yuting Chen; chenyuting03@whut.edu.cn

Received 4 August 2020; Revised 19 November 2020; Accepted 25 November 2020; Published 8 December 2020

Academic Editor: Danilo Comminiello

Robustness of a supply network highly depends on its structure. Although structural design methods have been proposed to create supply networks with optimal robustness, a real-life supply network can be quite different from these optimal structural designs. Meanwhile, real cases such as Thailand floods and Tohoku earthquake demonstrate the vulnerability of supply networks in real life. Obviously, it is urgent to enhance the robustness of existing real-life supply networks. Thus, in this paper, a supply network reconfiguration method based on adaptive variable neighborhood search (AVNS) is proposed to enhance the structural robustness of supply networks facing both random and target disruptions. Firstly, a supply network model considering the heterogeneous roles of entities is introduced. Based on the model, two robustness metrics, R_r and R_t, are proposed to describe the tolerance of supply networks facing random and target disruptions, respectively. Then, the problem of reconfiguration-based supply network robustness enhancement is described. To solve the problem effectively and efficiently, a new heuristic based on general variable neighborhood search, namely, AVNS, is proposed. Finally, a case study based on three real-life supply networks is presented to verify the applicability and effectiveness of the proposed robustness enhancing method.

1. Introduction

A supply network is created when two or more entities are connected by resource flows, such as product flows, material flows, or information flows, to fulfill the demands of downstream customers [1]. With the development of international trade and lean manufacture, a modern supply network can be large-scale and extremely complex [2]. Thousands of entities such as suppliers, manufacturers, and retailers are interconnected to form a complex system.

At the same time, disruptions often descend upon supply networks, especially for the global and large-scale ones [3–5]. A related survey indicates that nearly 75% of companies experience at least one supply network disruption a year [6]. These supply network disruptions can mainly be classified into two categories: random disruptions and target disruptions [7–9]. Usually, random disruptions refer to disruptions caused by unintentional destruction, such as natural disasters or accidental events. Target disruptions denote disruptions caused by intentional attacks, like terrorist or military attacks. In a supply network, a disruption may damage only one or a very few number of entities at first, but its impact may propagate through the interconnected entities and even cause massive loss to the entire network [10]. In 2011, Thailand floods damaged several hard disc suppliers, leading multiple computer manufacturers depending on them unable to continue the production [7]. Around the same year, Tohoku earthquake affected almost all major automobile manufacturers globally, because several Japanese suppliers were damaged severely in the earthquake [11]. In 2018, the main plant of an automobile supplier, Meridian Magnesium, caught fire. This incident also forced multiple automobile manufacturers to stop production including BMW, Mercedes-Benz, General Motors, Fiat Chrysler Automobiles, and Ford Motor Co. [12]. There are also real cases of man-made supply network disruptions. In 2016, the production of three plants of Volkswagen in German was halted due to supply disruptions [5]. These production halts were caused by a legal dispute with a supplier which belonged to a prevent group.

Therefore, the robustness of a supply network against disruptions is critically important, and it has gained much attention from supply network managers and researchers in the past decades.

Traditionally, supply network disruptions are investigated from the perspective of risk management. These studies mainly focus on identifying, assessing, and mitigating of risks [13, 14]. Recently, the investigation of supply network disruptions has been expanded to network level [15–18]. From the perspective of network, a supply network can be described as a complex network composed by entities (e.g., manufacturers and suppliers) and inter-entity relations (e.g., product transmitting relations). Using the complex network modeling and analysis methods, it has been revealed that the structural characters of a supply network, such as random and scale-free, affect its robustness greatly [19–23]. To find an optimal structure of supply networks which can withstand both random and target disruptions, supply network structural designs based on various complex network models have been proposed in the past decades [8, 9, 24, 25]. In spite of these proposed optimal structural designs, efforts on structural robustness optimization for existing real-life supply networks are very limited. In reality, the construction of a supply network is the result of various processes, which may be not correlated with the robustness against disruptions. Thus, a real-life supply network can be quite different from these optimal designs. For example, according to the research of Shi et al., supply networks whose degree distribution obeys Poisson distribution are robust to both random and targeted disruptions [25]. However, empirical studies found that degree of many real-life supply networks exhibits power-law distribution [26, 27]. In addition, real cases also reveal the vulnerability of real-life supply networks. One possible method to deal with such a problem is designing an entirely new supply network, which can be costly and time-consuming. It seems more realistic to take the existing structure into consideration and reconfigure the existing supply network. For example, after the great loss in 2011 Tohoku earthquake, Toyota realized the fragility of its supply network [28]. Then, Toyota decided to exam and redesign the current supply network, rather than designing an entirely new supply network to replace the existing one.

Based on these previous works, this study adopts the complex-network view of supply networks and proposes a supply network reconfiguration method based on adaptive variable neighborhood search (AVNS) for robustness enhancement. Firstly, a supply network model considering different roles of entities like manufacturers, suppliers, and retailers is introduced. Based on the model, two metrics are proposed to evaluate the robustness of a supply network facing random and target disruptions, respectively. Then, an AVSN-based supply network reconfiguration method is presented for robustness enhancement. Finally, a case study based on real-life supply networks is presented. The outperformance of the AVSN-based reconfiguration method is validated by comparative experiments.

The remainder of this paper is listed as following. The related works are expounded in Section 2. Section 3 presents the supply network model and robustness evaluation. Section 4 shows the AVNS-based supply network reconfiguration method. Section 5 presents the case study. Section 6 gives a brief conclusion.

2. Related Works

2.1. Supply Network Disruptions and Robustness. Supply network disruptions are unpredictable, unavoidable, and varied, which can be caused by both natural and man-made disasters [29–31]. It has been observed that supply network disruptions occur more frequently and incur more severe damages in the past decades. According to a report of the Centre for Research on the Epidemiology of Disasters, it has been observed that disasters including both natural and man-made disasters have increased exponentially all over the world in the past decades [32]. Considering the varied nature and the severe impacts of supply network disruptions, it is critically important to analyze and enhance the robustness of supply networks facing disruptions.

In the context of supply networks, robustness refers to the ability to maintain the basic function under various situations, including disruptions [33, 34]. A robust supply network should be capable of absorbing disruptions to minimize the negative impact on its performance. In the past years, robustness and several other similar concepts, like resilience and reliability, have been defined broadly [22, 23, 33, 35, 36]. The definitions are varied from author to author. For example, resilience has been defined as the capacity of a supply network to recover from disruptions [37]. A supply network is reliable when it can maintain its basic operation under a minimum service level [35].

To analyze supply network robustness from the view of complex network structure, the robustness of a supply network is defined as its ability to keep the basic function and connectivity under the loss of some structures or functions due to natural and man-made disasters, as it is indicated by Zhao et al. [8, 9, 24].

2.2. Robustness Analysis of Supply Networks from the Perspective of Complex Network. Due to the capability to reveal the inherent laws of complex systems, complex network theory provides an effective tool to analyze complex systems in real life. Along with the wide application of complex network theory in many areas like ecological system [38], communication network [39], and vehicle routing [40], supply network managers and researchers also consider to apply complex network theory into supply network researches.

From the perspective of complex network, a supply network can be described as a set of nodes and edges, which represent entities such as manufacturers and suppliers and inter-entity relations like product transmitting relations, respectively. Using complex network modeling and analysis methods, researchers try to analyze the correlation between supply network structure and robustness so as to find an optimal structure of supply networks, which can withstand both random and target disruptions [22, 23, 25, 41]. As a pioneer, Thadakamalla et al. firstly introduced complex network theory into supply network robustness analysis [36]. Based on the growth models of complex network, they proposed a supply network model based on a hybrid growth mechanism of preferential attachment [42] and random attachment [43]. In addition, they also introduced standard network connectivity measurements, average length in the largest connected component (LCC), and the size of LCC (SLCC) to analyze the tolerance of supply networks facing both random and target disruptions. To analyze the impact of structural characters on supply network robustness, Nair and Vidal constructed twenty supply networks based on agent-based modeling, which includes ten supply networks generated using preferential attachment and ten networks generated using random attachment [22]. SLCC was also adopted to evaluate supply network robustness. They found that the average length of paths connecting nodes in a supply network is negatively correlated with its robustness. Kim et al. also analyzed the robustness of four basic supply network structures to find the optimal supply network structure [20]. They found that scale-free supply network is most robust facing random disruptions. Most of these previous researches describe a supply network as a unipartite network, neglecting the heterogeneous roles of entities in a supply network. Such simplification is extremely unrealistic and also limits the analysis of supply network robustness [23]. Due to the unipartite modeling method, robustness evaluation of supply networks has to use standard network connectivity measurements, such as SLCC. Several researchers have begun to consider the role differences of entities in a supply network, when describing supply networks using complex network models [8, 25, 44, 45]. Zhao et al. proposed a supply network model considering the roles of demanding and supplying nodes [8, 9, 24]. Based on the model, largest functional subnetwork (LFSN) is defined as the largest connected component containing at least one node of supplying nodes and demanding nodes. Then, LFSN-based measurements were used as performance metrics to verify the effectiveness of proposed supply network modeling method. However, in the supply network model proposed by Zhao et al., only two types of nodes are taken into consideration. In reality, a supply network can include multiple types of entities. Based on the study by Shi et al., we proposed a supply network model considering multiple types of entities [25]. Based on the model, they gave the definition of largest all-role connected component (LACC). LACC is defined as a LCC in which all role types of nodes exist. Based on the definition of LACC, size of LACC (SLACC) was introduced as a performance metric to verify the effectiveness of proposed grow-mature-decline (GMD) supply network model.

In spite of these proposed optimal structural designs, efforts on structural robustness optimization for existing real-life supply networks are very limited. Recently, with the emergent of third-party supply network information platforms, empirical studies of supply network structures have been proposed. It is revealed that supply networks in real life can be quite different from these optimal designs [46, 47]. In addition, real cases also present the vulnerability of supply networks in real life. Clearly, it is urgent to develop methods for enhancing the robustness of supply networks in real life. Thus, this study contributes to propose a supply network reconfiguration method based on AVNS for robustness enhancement and the effectiveness of it is validated using supply networks in real life.

3. Supply Network Model and Robustness Evaluation

3.1. Supply Network Model. In this study, a supply network is modeled as a network $G = (V, E)$, where $V = \{v_1, v_2, \ldots v_{|v|}\}$ is the node set, representing the entities in the supply network. $|V|$ represents the total number of nodes. E is the edge set, representing product transmitting relations. $E = (\{v_i, v_j\})$, where $(v_i, v_j \in E)$, if there is a product transmitting relation between node v_i and v_j.

Since entities in a supply network can play various roles like manufacturers, suppliers, and retailers, node type is introduced as a node attribute to describe the specific roles nodes playing. Node type is presented as $\text{Role} = \{\text{role}(v_i)\}$, where $\text{role}(v_i) \in \{\text{type}_1, \text{type}_2, \ldots, \text{type}_M\}$ denotes the specific role of node v_i in the supply network G and M is the total number of node types in the network.

Figure 1 presents an example to illustrate the modeling method. The supply network presented in Figure 1 is composed of 3 different types of entities, namely, retailers, manufacturers, and suppliers. The three types of entities are represented by green, red, and yellow nodes, respectively. Edges connecting these entities represent product transmitting relations between them. It is observed that edges exist not only between different types of nodes but also same types of nodes in the network. The main reason is that, with technological developments, the inter-entity relations can be various and complex in a supply network. Product transmitting relation can exist between different types of entities as well as same types of entities [8, 25].

3.2. Robustness Evaluation. The robustness of a supply network is defined as its ability to keep the basic function and connectivity under the loss of some structures or functions due to natural and man-made disasters [8, 9, 24]. When evaluating the robustness of a supply network, two aspects need to be considered: disruption models for simulating the risk scenarios and evaluation metrics to measure the network's ability to withstand disruptions. Thus, in this section, two commonly used disruption models, random and target disruption models, are introduced. Then, the robustness evaluation metrics corresponding to the two disruption models are also proposed.

3.2.1. Disruption Models. When evaluating the robustness of a supply network, most current studies consider two typical disruption models: random disruption model and target disruption model. They are corresponding to two risk scenarios: unintentional destruction and intentional attack [8, 36, 37]. Based on these previous works, the two types of disruption model are adopted in this study.

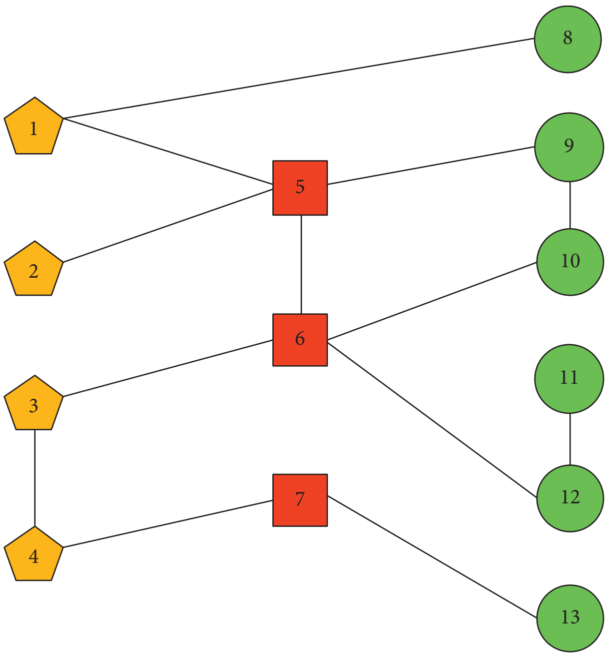


Figure 1: Illustration of the supply network model.

Before introducing the disruption models, the following assumptions are made.

Assumption 1. The disruption of a node in a supply network is treated as the complete damage of it. That is to say, once a node is disrupted, it will lose all the functions of it and it will not recover anymore. Thus, the disruption of a node is modeled as the removal of it.

Assumption 2. The adaptive behaviour of nodes, such as making temporary connections with alternative nodes and so on, is not considered in this study.

(1) Random disruption model. Random disruptions refer to unintentional destruction, such as natural disasters (e.g., earthquakes and floods), unexpected economic events (e.g., recessions and bankruptcy), and accidents (e.g., power blackout and fire). For such disruptions, the places where disruptions descend upon are usually unpredictable. In general, random disruptions are modeled using random node removals, where each node has an equal probability to be disrupted. The procedure of simulating random disruptions can be described as follows:

(a) Ranking nodes randomly.

(b) Nodes are removed from the network progressively following the random ranking calculated in step a. When a node is removed, all of its links in the network are also removed.

(c) The process is iterated until all nodes in the network have been removed.

(2) Target Disruption Model. On the other hand, target disruptions refer to intentional attacks, like terrorist and military attacks, which are aimed at maximizing the damage to the entire supply network by targeting nodes in the network believed to be "important." Usually, the node "importance" is measured by degree, namely, the number of edges attached to it [48]. The procedure of simulating target disruptions is listed as follows:

(a) Ranking nodes according to degree centrality in the descending order. The degree of a given node v_i is presented using the following equation:

$$k_i = |\varphi_i|, \tag{1}$$

where φ_i represents the node set connected to node v_i and $|\varphi_i|$ represents the number of nodes in φ_i.

(b) Nodes are removed progressively following the degree-based ranking. When a node is removed, all of its links in the network are also removed.

(c) The process is iterated until all the nodes in the network have been removed.

3.2.2. Evaluation Metrics. Based on the two disruption models used in this study, two robustness metrics are proposed to evaluate supply networks' tolerance of random and target disruptions, respectively.

Traditionally, network robustness evaluations are mainly based on LCC. Since nodes can play heterogeneous roles in a supply network, the definition of LCC has been extended into the context of supply networks by many previous works. In this study, we will use the definition of LACC and SLACC proposed by Shi et al. to measure the performance of a supply network facing disruptions [25].

Definition 1. LCC is defined as the largest subnetwork in which any pair of nodes can be connected. The expression of LCC is presented using the following equation:

$$G_{cc}(V,E) = \left\{G(V,E) \mid \forall v_i \in V, \quad \forall v_j \in V, \exists \,\text{path connecting } v_i \text{ and } v_j\right\}, \tag{2}$$

$$G_{LCC}(V,E) = \left\{G_{CC}(V,E) \mid \forall G(V,E) \in G_{cc}(V,E), |G(V,E)| <= \left|G_{CC}(V,E)\right|\right\}, \tag{3}$$

where equation (2) denotes the connected component set, which is composed of subnetworks in which any pair of nodes can be connected and equation (3) denotes the set of LCC.

Definition 2. LACC is defined as a LCC that includes at least one node of each role type. The expression of LACC is presented using the following equation:

$$G_A(V,E)=\{G_{\mathrm{cc}}(V,E)|\exists v_{i1}\in V,\mathrm{role}(v_{i1})=\mathrm{type}_1\wedge\cdots\wedge\exists v_{iM}\in V,\mathrm{role}(v_{iM})=\mathrm{type}_M\},\tag{4}$$

$$G_{\mathrm{LACC}}(V,E)=\left\{G_A(V,E)|\forall G(V,E)\in G_A(V,E),|G(V,E)|<=\left|G_A(V,E)\right|\right\},\tag{5}$$

where equation (4) denotes the all role connected component set, which is composed of subnetworks, in which any pair of nodes can be connected and contain all role types and equation (5) denotes the set of LACC.

Based on the definition of LACC, SLACC of a given supply network G is defined as the number of nodes in LACC. The expression is presented using the following equation:

$$\mathrm{SLACC}(G)=\left|G_{\mathrm{LACC}}(V,E)\right|,\tag{6}$$

where $|G_{\mathrm{LACC}}\ (V,E)|$ represents the number of nodes in LACC.

The illustration of LACC and SLACC is presented in Figure 2. Figures 2(a) and 2(b) present a supply network before disruption and after disruption, respectively. As presented in Figure 2(a), all 13 nodes form a connected component which contains all types of nodes. Thus, SLACC of the network in Figure 2(a) is 13. As presented in Figure 2(b), due to the disruption of node 6, the supply network presented in Figure 2(a) is divided into three connected components. Component 1 contains nodes 1, 2, 5, 8, 9, and 10. Component 2 is composed of nodes 11 and 12. Component 3 contains nodes 3, 4, 7, and 13. Among all three connected components, Component 1 and Component 3 contain all types of nodes, so they can maintain the basic function. The sizes of Component 1 and Component 3 are 6 and 4, respectively. Thus, the size of Component 1 is larger than that of Component 3. So, LACC of the network presented in Figure 2(b) is Component 1 and SLACC of it is 6.

After introducing the definition of SLACC, two robustness metrics R_r and R_t are proposed to measure the tolerance of a supply network facing random and target disruptions, respectively.

Based on the definition of SLACC and random disruption model, the robustness of supply network G against random disruptions is given as follows:

$$R_r(G)=\frac{1}{|V|}\sum_{j=1}^{|V|}\frac{\mathrm{SLACC}_r(j)}{\mathrm{SLACC}_0},\tag{7}$$

where $j=1,2,\ldots,|V|$ represents the times of random disruptions on the supply network G, $|V|$ is the number of nodes in the original network G, SLACC_0 represents the SLACC of original network G SLACC_r, (j) represents the SLACC of network G after the j^{th} random disruption, namely, removing the j^{th} nodes under random disruptions, and SLACC_r $(j)/\mathrm{SLACC}_0$ is the normalized SLACC of network G after the j^{th} random disruption.,

In the same way, the robustness of supply network G against target disruptions is defined as

$$R_t(G)=\frac{1}{|V|}\sum_{j=1}^{|V|}\frac{\mathrm{SLACC}_t(j)}{\mathrm{SLACC}_0},\tag{8}$$

where $j=1,2,\ldots,|V|$ represents the times of target disruptions on the network G, $|V|$ is the number of nodes in the original network G, $SLACC_0$ represents the SLACC of original network G. SLACC_t (j) represents the SLACC of network G after the j^{th} target disruption, namely, removing the j^{th} node under target disruptions, and $SLACC_t$ $(j)/$ SLACC_0 is the normalized SLACC of network G after the j^{th} target disruption.

4. Adaptive Variable Neighborhood Search-Based Supply Network Reconfiguration for Robustness Enhancement

In this section, an AVNS-based reconfiguration method is presented for robustness enhancement. Firstly, the problem description of supply network reconfiguration-based robustness enhancement is given. Then, an AVNS algorithm is proposed to solve the problem.

4.1. Problem Description. To enhance the robustness of a supply network, the network structure will be reconfigured by introducing a limited number of new product transmitting relations between existing entities. This is a commonly used supply network reconfiguration approach. In this study, a supply network is modeled as $G=(V,E)$, where V and E represent entities and product transmitting relations between entities. Based on the model, two robustness evaluation metrics, R_r and R_t, are proposed to describe the tolerance of a supply network facing random and target disruptions, respectively. Thus, the network reconfiguration-based robustness enhancement of a given supply network G is a typical optimization problem, which is aimed at finding a limited subset of edges S whose addition can maximize both R_r and R_t of the reconfigured network $G\cup S$. The problem is described as follows:

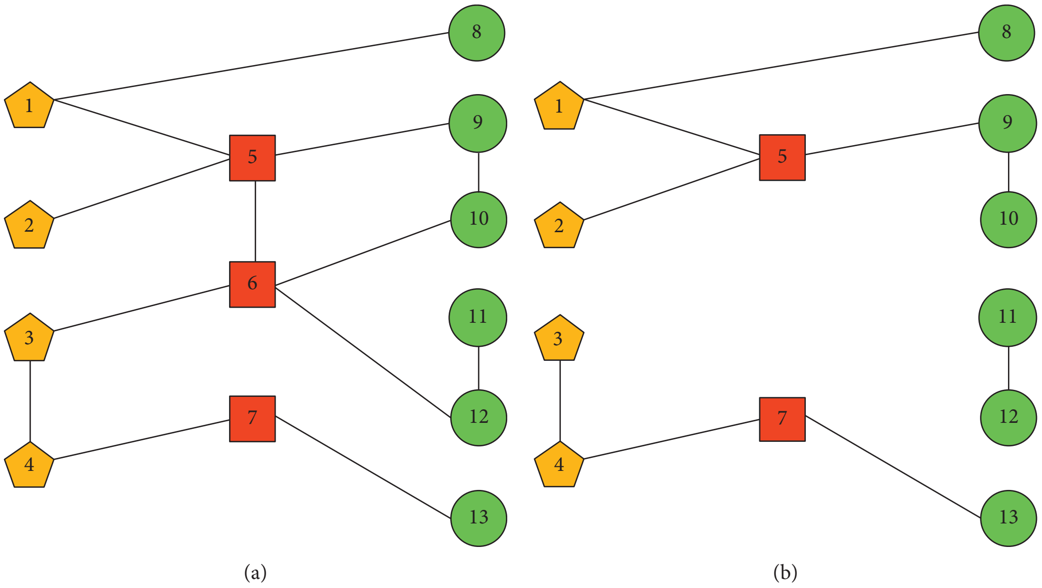


Figure 2: Illustration of LACC and SLACC. (a) Original supply network. (b) Supply network after the disruption of node 6.

$$\max_S H(S), \tag{9}$$

$$\text{s.t.} \quad |S| = K, \tag{10}$$

$$S \cap E = \varnothing, \tag{11}$$

$$H(S) = \alpha R_r(G \cup S) + (1-\alpha) R_t(G \cup S), \tag{12}$$

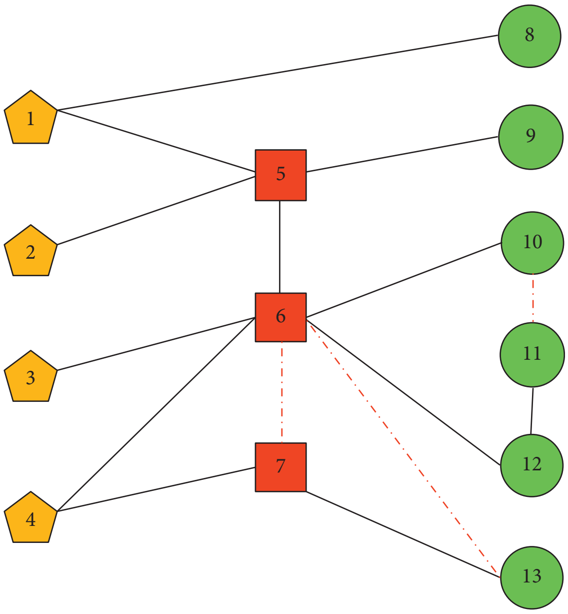
where S represents any possible subset of edges to be added into network G, $|S|$ denotes the number of edges in S, K is a predefined number of edges to be added in to G, and $G \cup S$ represents the reconfigured supply network G after adding edge set S. Constrain (10) denotes the number of added edges should be equal to the predefined number. Constrain (11) denotes the added edges cannot be edges which already exist in the network. $R_r(G \cup S)$ and $R_t(G \cup S)$ denote the tolerances of reconfigured network facing random and target disruptions, respectively. $\alpha \in [0, 1]$ is a weighting parameter. If $0 \le \alpha < 0.5$, the network's robustness mainly depends on its tolerance of random disruptions. If $0.5 < \alpha \le 1$, then the network's robustness mainly depends on its tolerance of target disruptions. In this study, the tolerances of random and target disruptions are considered to be equally important. Thus, the value of α is set to be 0.5. In the following text, $H(S)$ will be used as the objective function, namely, the fitness function in the proposed AVNS algorithm.

4.2. Adaptive Variable Neighborhood Search. Variable neighborhood search (VNS) is a type of heuristic algorithm, which is based on the idea of neighborhood change to avoid trapping in local optimums [49–51]. Due to the efficiency and effectiveness of it, it has been applied in many areas and achieved high performance. Thus, an improved VNS algorithm, namely, AVNS is proposed to solve the problem of supply network reconfiguration-based robustness enhancement. To solve the problem effectively and efficiently, an adaptive search-based solution improvement is proposed, which contains a local neighborhood search based on community closeness, a global neighborhood search and an adaptive neighborhood determination scheme.

4.2.1. Solution Representation and Fitness Evaluation. In the AVNS, each possible reconfiguration solution is coded using the string coding method. A solution can be represented as $S = [p_1, p_2, \ldots, p_K]$, where $p_i = (v_x, v_y)$ is the i^{th} element of the solution, representing an edge to be added into G and K is the predefined number of edges to be added. Figure 3 presents an example to illustrate the string-based coding. In the Figure 3, the red dotted lines represent edges to be added into the network.

In terms of searching for the optimal reconfiguration solution, operations are performed to search for the optimal edge subset whose addition will improve both robustness metrics R_r and R_t most greatly. Thus, each solution will be evaluated using a fitness value; those solutions with bigger fitness values are considered to be better ones. Thus, the fitness values are calculated using equation (12).

4.2.2. General Scheme of Adaptive Variable Neighborhood Search. As presented in Algorithm 1 and Figure 4, the proposed AVNS algorithm is mainly composed of a solution initialization procedure and an adaptive search-based solution improvement. The adaptive search-based solution improvement includes two neighborhood search methods and an adaptive neighborhood determination scheme. The two neighborhood search methods are community closeness-based local neighborhood search and global neighborhood search. To realize the adaptive neighborhood determination, a rating is associated to each neighborhood search, where P_L and P_G represent the ratings for local and global search,



Solution representation

(6, 7)	(6, 13)	(10, 11)

Figure 3: Illustration of string-based solution coding.

```
Input: G = (V, E), Role, K, $N_{\text{initial}}$, $P_L$, $P_G$, $p_1$, $p_2$,threshold
Output: S
  $S \longleftarrow$ Solution initialization (G, K, $N_{\text{initial}}$)
  while (end condition is not met) do
    if $P_L/(P_L + P_G) >$ a random number $\delta \in (0, 1)$
      $S^* \longleftarrow$ Community closeness-based local neighbourhood search (G, S)
      if fitness ($S^*$) > fitness (S)
        $S \longleftarrow S^*$;
        $P_L = P_L - p_1$;
      else
        $P_L = P_L - p_2$;
      end if
      if $P_L <$ Threshold
        $P_L =$ Threshold
      end if
    else
      $S^* \longleftarrow$ Global neighborhood search (G, S)
        if fitness ($S^*$) > fitness (S)
          $S \longleftarrow S^*$;
            $P_G = P_G + p_1$
        else
          $P_G = P_G + p_2$;
        end if
        if $P_G <$ Threshold
          $P_G =$ Threshold;
        end if
      end if
    end while
    Return S
```

Algorithm 1: Adaptive variable neighborhood search.

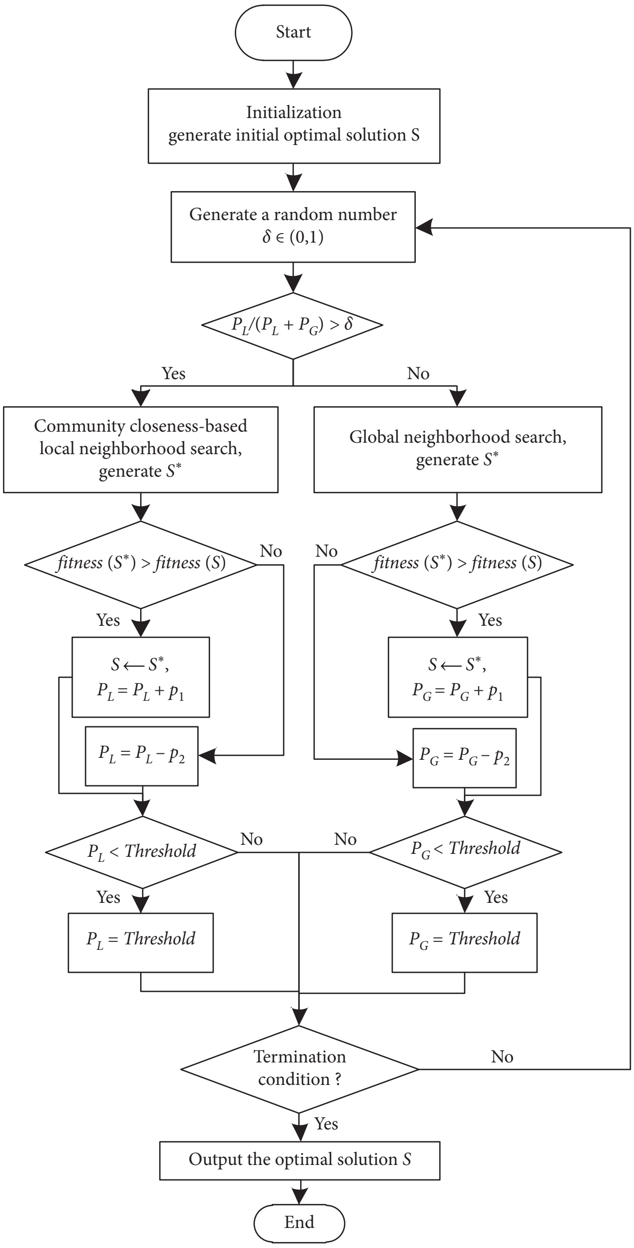


Figure 4: Flowchart of the proposed AVNS.

respectively. The rating is correlated with the possibility to perform each search method. The probability of performing local search is $P_L/(P_L + P_G)$, while the probability of performing global search is $P_G/(P_L + P_G)$. Thus, search method with a higher rating indicates a higher chance to be performed. These ratings are dynamically updated according to results encountered during the iterations. The search method leading to new optimal solutions is enhanced by increasing its rating, while the search method unable to improve solutions will be weakened by decreasing its rating.

4.2.3. Solution Initialization. The quality of an initial solution not only affects the accuracy of an algorithm but also the converging speed. An initial solution with high quality is vitally important. Thus, a random search algorithm is used to find an initial solution with high quality. Firstly, the random solution generation procedure allows solutions in the entire solution space to be obtained. Subsequently, best solution is selected from the randomly generated solutions. The solution initialization procedure is presented in Algorithm 2.

4.2.4. Community Closeness-Based Local Neighborhood Search. To ensure an effective and efficient improvement of solutions, a local neighborhood search method based on community closeness is proposed in this study. As presented in Algorithm 3, the proposed community closeness-based local neighborhood search is composed of three steps: community closeness-based neighborhood determination,

```
Input: $G = (V, E)$, Role, $K$ and $N_{\text{initial}}$
Output: $S$
  $POP = \varnothing$;
  for $i = 1$: $N_{\text{initial}}$
    $S_i \longleftarrow$ Generate a solution randomly;
    if $S_i$ is different from any solutions in $POP$;
      Add $S_i$ into $POP$;
    else
      Modify $S_i$ and add it into POP;
    end if
  end for
  evaluate solution $S_i$ according to fitness function;
  //Identify the best solution $S_b$ in the $POP$;
  $b$ = argmaxi$\in(1, 2, \ldots, N_{\text{initial}})$ fitness $(S_i)$;
  $S \longleftarrow S_{\mathrm{b}}$;
  return $S$
```

Algorithm 2: Solution initialization.

degree weighting-based candidate identification, and random swap strategy

(1) Community Closeness-Based Local Neighborhood Determination. Neighborhood refers to the solution space for candidate solutions. The performance of a local search highly depends on its neighborhood structure. Thus, a community closeness-based neighborhood determination is designed in this study, which is both smaller in size and more focused in terms of the optimization objective. In this study, performance of a supply network is measured by SLACC, which is also a network connectivity metric. Community in a network refers to groups of nodes within which connections are dense, but between which connections are sparser. Intuitively, adding edges between two unconnected communities will help to increase the connectivity. It may benefit the enhancement of supply network robustness. As a result, when swapping an edge $(v_x, v_y) \in S$ with a candidate edge (v_{x1}, v_{y1}), it may be more preferable to consider an edge connecting two unconnected communities. Based on such consideration, a local neighborhood determination method based on community closeness is proposed. As presented in Algorithm 4, the method is composed of the following steps:

(a) Community detection for $G^* = G \cup S$. Due to the accuracy and efficiency, Louvin algorithm is adopted in this study for community detection. The details of the algorithm are presented in [52].

(b) Calculate closeness for each pair of community. Closeness of a pair of communities is defined as the number of edges connecting the pair of communities.

(c) Based on the closeness of community pairs, community pair with minimal closeness is selected.

(d) Based on the community pair with minimal value of closeness, the neighborhood for generating candidate solutions is determined

(2) Degree Weighting-Based Candidate Identification. After determination of the community pair with minimal closeness, a connection will be built between them to increase network connectivity. Previous studies indicate that low degree-based edge addition can increase network robustness more effectively [53]. Thus, adding edges between less connected nodes is considered to be more satisfactory. The procedure of degree weighting-based candidate identification is presented in Algorithm 5.

4.2.5. Global Neighborhood Search. Solution improvement based on a single neighborhood search could easily lead to local optimums. To avoid trapping in local optimums, global neighborhood search is also adopted in this study. The procedure of global neighborhood search is presented in Algorithm 6.

4.3. Computational Complexity of AVNS.

To analyze the computational complexity of the proposed AVNS, we consider the main steps in one generation in the main loop of Algorithm 1.

As displayed in Algorithm 1, each generation of AVNS performs four subroutines: determination of search method, neighborhood search, optimal solution update, and rating update. The determination of search method takes time O (1). In the neighborhood search procedure, the time complexity of global neighborhood is $O\ [|V|^3]$. The time complexity of community closeness-based local neighborhood search procedure is $O\ [2\ (|V|+|E|) + K + (n) * (n-1)/2 + |V|\ ^3]$, where n denotes the current community number determined by Louvin algorithm. Thus, the time complexity of neighborhood search is bounded by $O\ [2\ (|V| + |E|) + K + (n) * (n-1)/2 + |V|^3]$. The optimal solution update and rating update take time O (1). Hence, for each generation, the total complexity of AVNS is $O\ [2\ (|V| + |E|) + K + (n) * (n-1)/2 + |V|^3]$.

```
Input: $G = (V, E)$, $S$ and $K$
Output: $S^*$
  $Neighborhood \longleftarrow$ Community closeness-based neighborhood determination $(G, S)$;
  $candidate \longleftarrow$ Degree weighting-based candidate search $(G, S, Neighborhood)$;
  //Random swap
  Generate a random integer $c \in \{1, 2, \ldots, K\}$;
  $S^* \longleftarrow S$;
  $S^* \longleftarrow S^* - \{p_c\}$;
  $S^* \longleftarrow S^* \cup$ candidate;
return $S^*$
```

Algorithm 3: Community closeness-based local neighborhood search.

```
Input: $G=(V, E)$, $K$ and $S$
Output: Neighborhood
  $G^* = G \cup S$;
  //Community detection
    $\{C_1, C_2, \ldots, C_n\} \longleftarrow$ Louvin-based community detection $(G^*)$
  //Calculate closeness for each pair of communities
    for each pair $(C_e, C_f)$ do
      Closeness $(C_e, C_f) = 0$;
      for each node $v_x \in C_e$ do
        for each node $v_y \in C_f$ do
          if $(v_x, v_y) \in E \cup S$ do
            Closeness $(C_e, C_f) =$ Closeness $(C_e, C_f) + 1$;
          end if
        end for
      end for
    end for
    //Neighborhood determination
      $(\varphi 1, \varphi 2) \longleftarrow$ find the pair of community with the minimal closeness;
      Neighborhood $\longleftarrow \varnothing$
      for each $v_x \in \varphi 1$ do
        for each $v_y \in \varphi 2$ do
          if $(v_x, v_y) \notin E \cup S$ do
            Neighborhood $\longleftarrow$ Neighborhood $\cup (v_x, v_y)$;
          end if
        end for
      end for
    return Neighborhood
```

Algorithm 4: Community closeness-based neighborhood determination.

```
Input: $G = (V, E)$, $S$ and Neighborhood
Output: candidate
  $G^* = G \cup S$;
  for each pair $(v_x, v_y) \in$ Neighborhood do
    $d\ (v_x) \longleftarrow$ Number of nodes connected to $v_x$ in $G^*$;
    $d\ (v_y) \longleftarrow$ Number of nodes connected to $v_y$ in $G^*$;
    $D\_score\ (v_x, v_y) \longleftarrow d\ (v_x) \times d\ (v_y)$;
  end for
  candidate $\longleftarrow$ Identify the node pair $(v_{x1}, v_{y1})$ with the minimal value of D_score;
  return candidate
```

Algorithm 5: Desgree weighting-based candidate identification.

```
Input: $G = (V, E)$,
Output: $S^*$
  $(v_x, v_y) \longleftarrow$ Select a pair nodes from $V \times V - (E \cup S)$ randomly;
  while $v_x == v_y$ do
    $(v_x, v_y) \longleftarrow$ Select a pair nodes from $V \times V - (E \cup S)$ randomly;
  end while
  Generate a random integer $c \in \{1, 2, \ldots, K\}$;
  $S^* \longleftarrow S$;
  $S^* \longleftarrow S^* - \{p_c\}$;
  $S^* \longleftarrow S^* \cup (v_x, v_y)$
  return $S^*$
```

Algorithm 6: Global neighborhood search.

5. Case Study

To verify the effectiveness of proposed AVNS-based supply network reconfiguration method, a case study based on three real-life supply networks is carried out. Firstly, the general characteristics of empirical supply networks are analyzed. Then, comparative experiments are performed based on the supply networks.

5.1. Three Real-Life Supply Networks. Three real-life supply networks used in this study, Chain 14, Chain 21, and Chain 25 are from an existing set of real-life cases [54]. Chain 14 describes a logistic supply network. Chain 21 presents a supply network of toilet preparations. Chain 25 is a supply network of farm machinery and equipment. The general characters of the three supply networks are presented in Table 1. All of them are composed of multiple types of entities, and the number of each type is varied. For example, in the Chain 14, the number of distributors is only 5, while the number of retailers is 66. Since the degree distribution of a supply network has been considered as a main factor affecting its robustness, the degree distributions of these networks are analyzed. It is found that all degree distributions can be fitted by truncated power-law [55]. The observed distributions and fitting curves are presented in Figure 5. Such character indicates that in these real-life supply networks, only a few nodes are intensively connected, while many others only have a few number of connections. According to the previous studies [8, 36], such a heterogeneous supply network can be robust against random disruptions but is vulnerable when entities with high degrees are damaged. In addition, the average degree [48] and H metric [56] of each network are also analyzed. The average degree can reflect the density of networks; the expression of it is presented by equation (13). The H metric is used to define the structural heterogeneity in a network; the definition of it is presented by equation (14). As presented in Table 1, Chain 25 is the most dense and heterogeneous network. Comparing with Chain 21 and Chain 25, Chain 14 is sparser and less heterogeneous:

$$\langle k \rangle = \frac{1}{N} \sum_{i}^{|V|} k_i, \tag{13}$$

where $|V|$ is denotes the total number of nodes in network and k_i is the degree value of node v_i:

$$H = \frac{\langle k^2 \rangle}{\langle k \rangle^2}. \tag{14}$$

where $\langle k \rangle$ denotes the average degree of a network, H reflects the level of the structural heterogeneity in a network, and the larger H, the more heterogeneous the network exhibits. From the definition, it is obvious that, in a homogeneous network, H is equal to one.

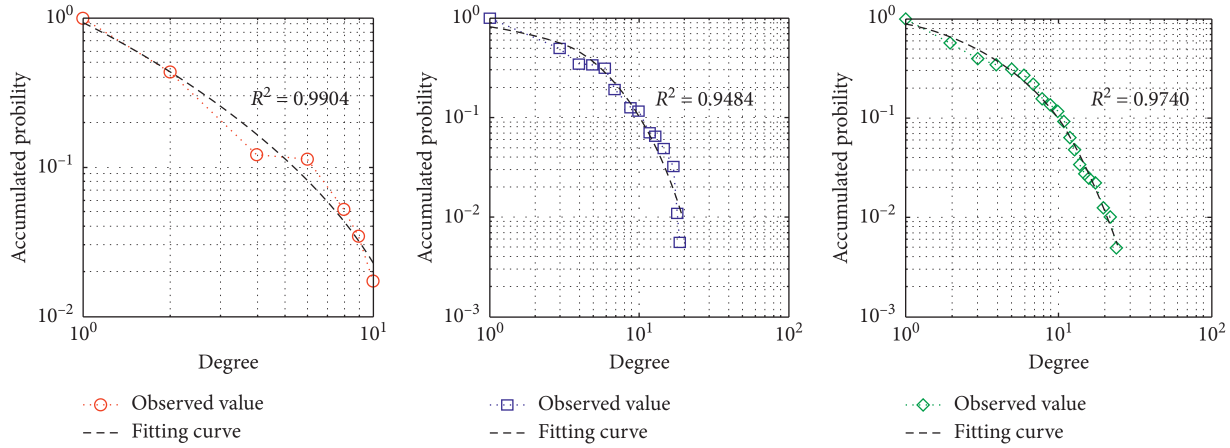
5.2. Evaluation of AVNS-Based Supply Network Reconfiguration Method. To verify the effectiveness of AVNS-based supply network reconfiguration method, comparison with other edge addition-based network reconfiguration methods is made, specifically low degree-based reconfiguration method (LD) [53], low betweenness-based reconfiguration method (LB) [57], and simulated anneal-based reconfiguration method (SA) [58].

The performances of AVNS-based and SA-based method can be influenced by several important parameters. In this study, the parameters of AVNS are set as follows: termination condition is 250 generations, $N_{\text{initial}} = 50$, $P_L = 0.7$, $P_G = 0.3$, $p_1 = 0.1$, $p_2 = 0.01$, and $\mathit{Threshold} = 0.1$. The parameters of SA are set as follows: initial temperature $T = 100$, iteration time $n = 5$, cooling factor $\theta = 0.95$, and low temperature $T_0 = 0.01$. These parameters are set based on the trial-and-error method, which has been widely used to select the parameter values for heuristic algorithms in many previous works [59].

Considering the number of added edges may affect the performance of reconfiguration methods, experiments based on the different fraction of added edges were performed. Fraction of added edge (f_a) is defined as the fraction of the number of edges of original network before edge addition. The expression of f_a is presented using equation (15). To achieve statistically significant results, each experiment was repeated 20 times. The final experimental results are calculated based on the 20 independent experiments. All experiments were performed using MATLAB R2014a and run on a PC equipped with an Intel Core i7 and 16 GB of memory, running Windows 7.

Table 1: Basic characters of the three real-life supply networks.

Network name	Number of each type of nodes					Total number of nodes	Total number of edges	$\langle k \rangle$	H
	Distributor	Manufacturer	Supplier	Retailer	Transporter				
Chain 14	5	9	—	66	36	116	119	2.052	1.983
Chain 21	17	59	76	34	—	186	359	3.860	2.158
Chain 25	31	142	94	142	—	409	853	4.171	4.653



(a) (b) (c)

Figure 5: Degree distributions of real-life supply networks. (a) Chain 14. (b) Chain 21. (c) Chain 25.

$$f_a = \frac{|S|}{|E|}, \tag{15}$$

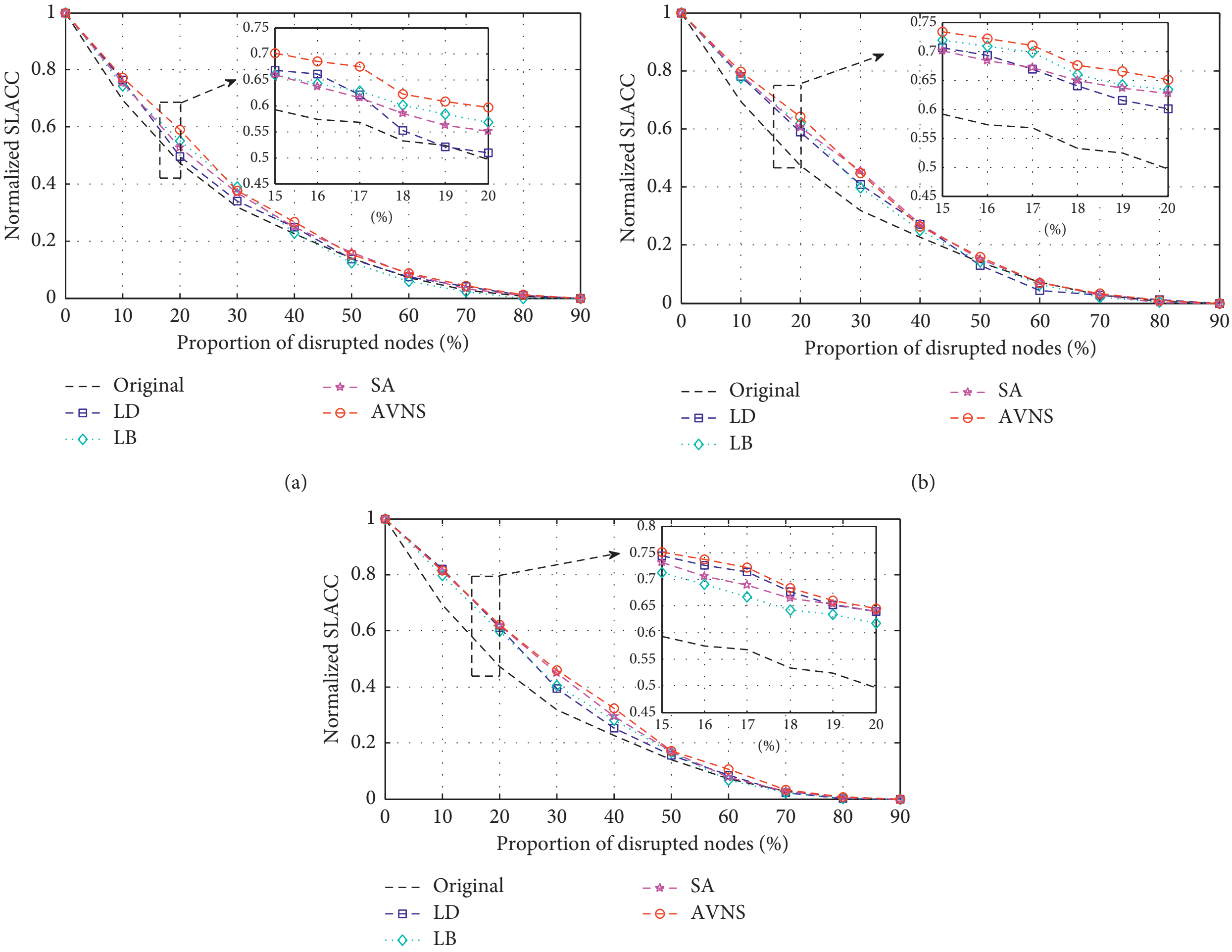
where E denote the edges in the original network, S represents the added edges, and $|E|$ and $|S|$ represent the number of edges in set E and S, respectively.

5.2.1. Experimental Results Based on Chain 14. Figures 6 and 7 illustrate the robustness of Chain 14 and the reconfigured ones facing random disruptions and target disruptions, respectively. Figures 6(a)–6(c) show the responses of five supply networks facing random disruptions, including original Chain 14 and four reconfigured ones, under $fa = 5\%$, $fa = 10\%$, and $fa = 15\%$, respectively. In Figures 6(a)–6(c), the horizontal axes denote the percentage of disrupted nodes, while the vertical axes are values of normalized SLACC. Similar to Figure 6, Figures 7(a)–7(c) show the responses of five supply networks facing target disruptions, including original Chain 14 and four reconfigured ones, under $fa = 5\%$, $fa = 10\%$, and $fa = 15\%$, respectively. For presenting a quantitative comparison, Table 2 summarizes the average values, the best values, and the worst values of R_r and R_t of the 20 independent experiments based on Chain 14.

Firstly, in both Figures 6 and 7, the performances of all networks decrease when nodes are removed sequentially from the networks. It is also observed that a higher fraction of the added edge leads to a better performance for all reconfiguration methods. Besides, by comparing Figures 6 with 7, it is found that all networks are more vulnerable to target disruptions. For example, In Figure 6(a), when 15% nodes are disrupted under random disruptions, the function of original Chain 14 is also well preserved as the majority of remaining nodes are still connected to form a functional component. As presented in Figure 7(a), the value of normalized SLACC becomes 0, when less than 15% nodes are disrupted under target disruptions. By comparing the performances of different reconfiguration methods, it is observed that the networks reconfigured by AVNS-based method are more robust than others facing both random and target disruptions, especially for target disruptions.

As presented in Table 2, the average values and the best values of R_r achieved by the proposed AVNS-based method are better than the three other methods in all of the instances. As for the worst values of R_r, only when $f_a = 10\%$, the performance of the proposed AVNS-based method is slightly worse than SA-based method. Except for the instance under $f_a = 10\%$, the AVNS-based method also achieves the best performance. As for R_t, the proposed AVNS-based method achieves the best performance with respect to all of the three indicators. Such results are consistent with Figures 6 and 7.

5.2.2. Experimental Results Based on Chain 21. Figures 8 and 9 present the robustness of Chain 21 and the reconfigured ones facing random disruptions and target disruptions, respectively. Similar to Figures 6 and 7, in all the figures of Figures 8 and 9, the horizontal axes denote the percentage of disrupted nodes, while the vertical axes are values of normalized SLACC. Table 3 also summarizes the average values,



(a)

(b)

(c)

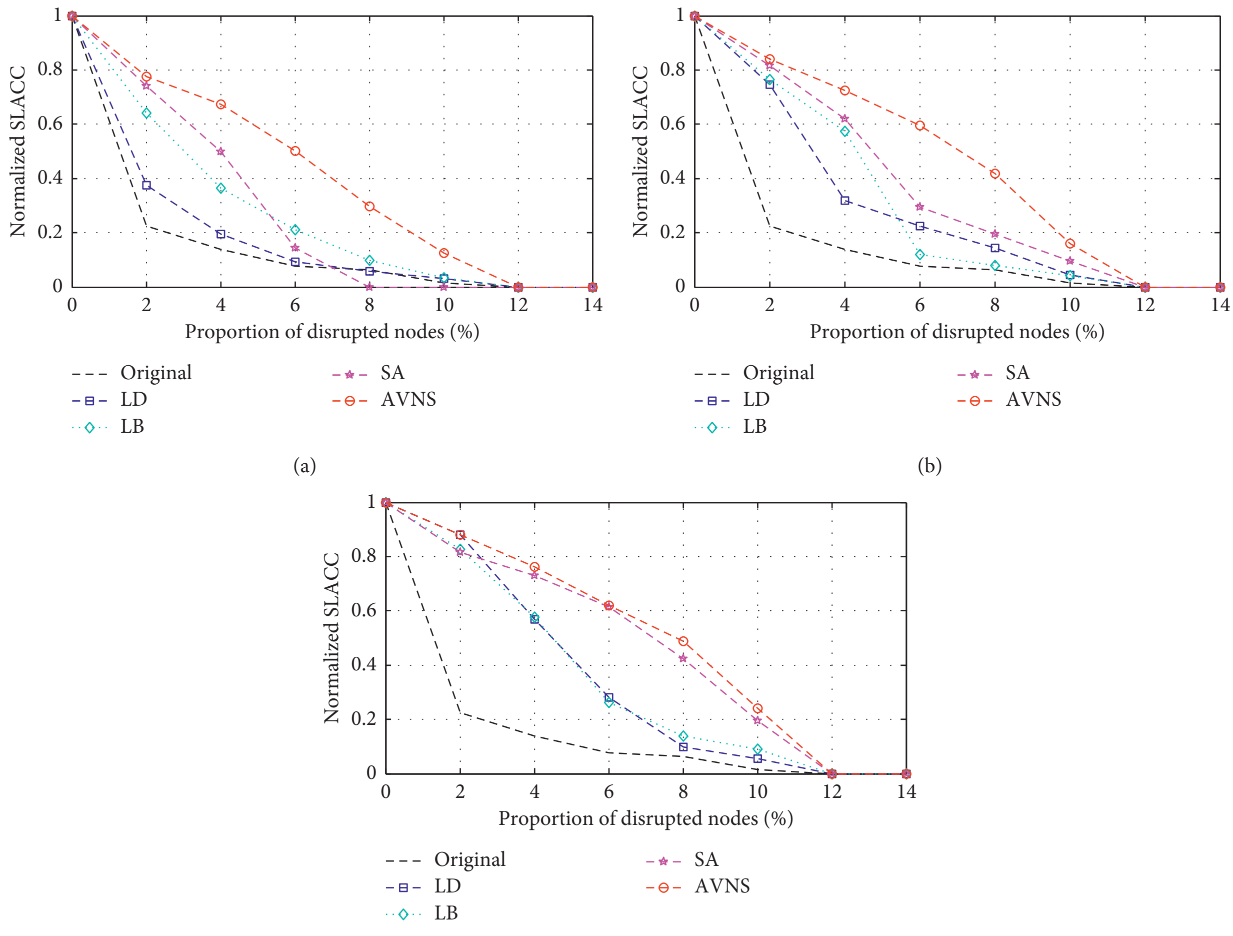
Figure 6: Responses of chain 14 and reconfigured ones facing random disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.

Table 2: Robustness comparison of chain 14 and reconfigured ones.

f_a (%)	Method	R_r			R_t		
		Average	Best	Worst	Average	Best	Worst
—	Original	0.2623	0.3465	0.1503	0.0135	0.0168	0.0114
5	LD	0.2714	0.3566	0.1535	0.0185	0.0213	0.0158
	LB	0.2772	0.3502	0.1653	0.0299	0.0357	0.0245
	AVNS	**0.2852**	**0.3587**	**0.1735**	**0.0479**	**0.0544**	**0.0385**
	SA	0.2794	0.3584	0.1615	0.0332	0.0351	0.0311
10	LD	0.2854	0.3745	0.1768	0.0370	0.0412	0.0256
	LB	0.2889	0.3877	0.1644	0.0392	0.0405	0.0335
	AVNS	**0.3049**	**0.3749**	**0.1793**	**0.0603**	**0.0612**	**0.0514**
	SA	0.2986	0.3759	0.1817	0.0477	0.0487	0.0392
15	LD	0.2981	0.3732	0.2111	0.0444	0.0487	0.0337
	LB	0.2963	0.3798	0.2055	0.0425	0.0445	0.0372
	AVNS	**0.3169**	**0.3769**	**0.2453**	**0.0635**	**0.0645**	**0.0534**
	SA	0.3070	0.3704	0.2410	0.0579	0.0608	0.0518

the best values, and the worst values of both R_r and R_t of the 20 independent experiments based on Chain 21.

As presented in Figures 8 and 9, it is observed that Chain 21 is also vulnerable to target disruptions and exhibits much stronger tolerance to random disruptions. It is also noticed that Chain 21 is more robust than Chain 14 facing both random and target disruptions. For example, when the proportion of random disrupted nodes is 20%, the normalized SLACC of Chain 14 is less than 0.5, while the normalized SLACC of Chain 21 is almost 0.7. With respect to

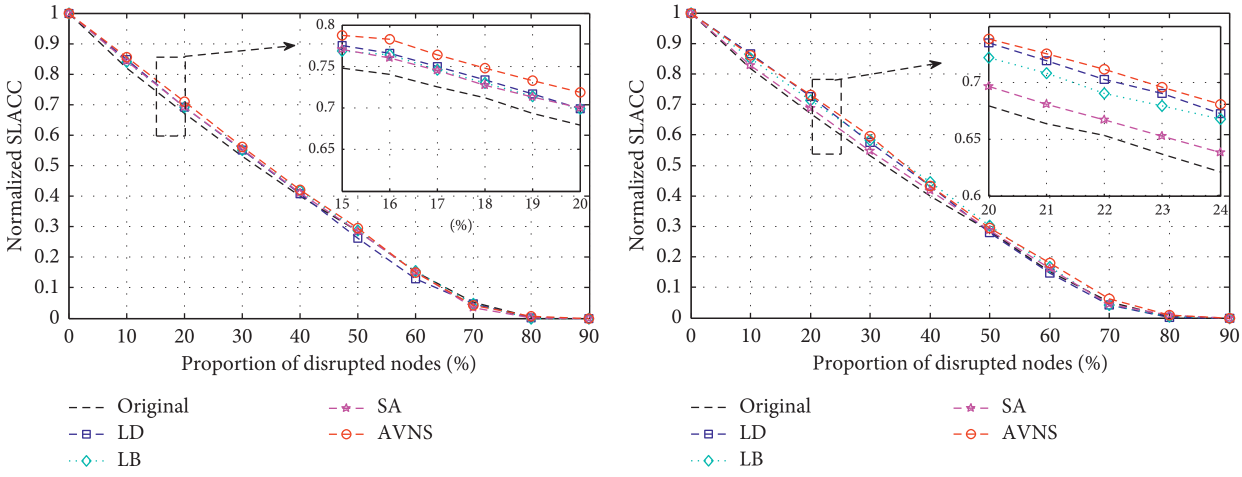


(a)

(b)

(c)

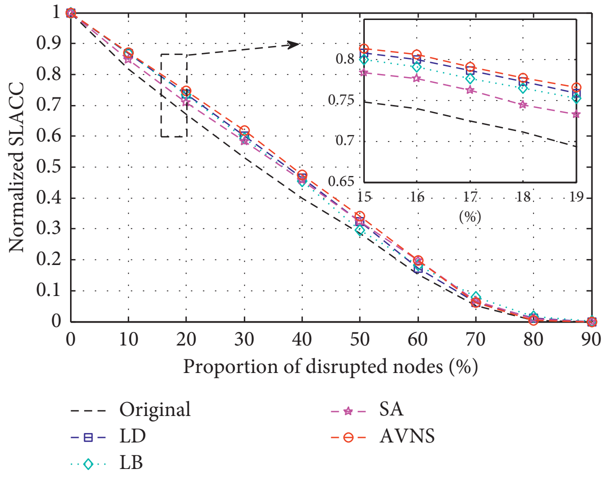
Figure 7: Responses of chain 14 and reconfigured ones facing target disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.



(a)

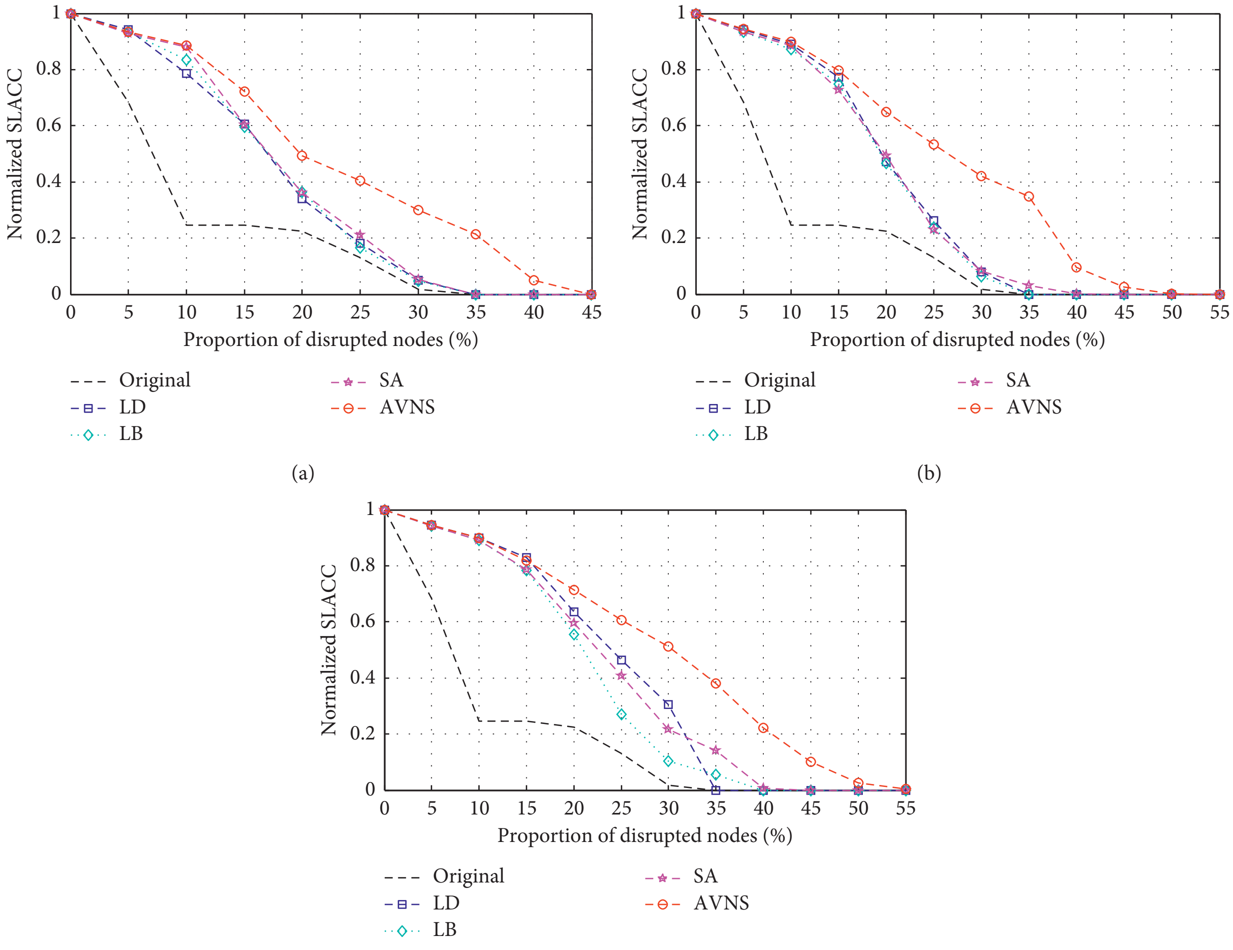
(b)

Figure 8: Continued.



(c)

Figure 8: Response of chain 21 and reconfigured ones facing random disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.



(a)

(b)

(c)

Figure 9: Response of chain 21 and reconfigured ones facing random disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.

Table 3: Robustness comparison of chain 21 and reconfigured ones.

Fa (%)	Method	R_r			R_t		
		Average	Best	Worst	Average	Best	Worst
—	Original	0.3476	0.3949	0.3165	0.0980	0.1024	0.0919
5	LD	0.3491	0.3803	0.3060	0.1652	0.1741	0.1558
	LB	0.3570	0.4035	0.3071	0.1683	0.1766	0.1518
	AVNS	**0.3611**	**0.3993**	**0.3227**	**0.2179**	**0.2255**	**0.2119**
	SA	0.3559	0.3929	0.3021	0.1694	0.1752	0.1619
10	LD	0.3652	0.4059	0.3015	0.1881	0.1934	0.1799
	LB	0.3674	0.3997	0.3094	0.1833	0.1862	0.1779
	AVNS	**0.3738**	**0.4184**	**0.3220**	**0.2518**	**0.2590**	**0.2423**
	SA	0.3537	0.4093	0.3010	0.1879	0.1939	0.1811
15	LD	0.3819	0.4146	0.3490	0.2034	0.2076	0.1980
	LB	0.3792	0.4135	0.3252	0.1972	0.2035	0.1903
	AVNS	**0.3890**	**0.4153**	**0.3583**	**0.2784**	**0.2922**	**0.2685**
	SA	0.3749	0.4079	0.3444	0.2177	0.2231	0.2112

target disruptions, when the proportion of disrupted nodes in target disruptions is less than 15%, Chain 14 loses all functional components, while the functional components of Chain 21 still remain until the proportion of target disrupted nodes reaches 35%. The main reason of such difference can be deduced that Chain 21 is denser than Chain14. By comparing the performance of different reconfiguration methods, it is also observed that networks reconfigured by AVNS-based method are more robust than others facing both random and target disruptions, especially for target disruptions.

As presented in Table 3, the average values, the best values, and the worst values of R_r achieved by the proposed AVNS-based method are better than the three other methods in all of the instances. As for R_t, the proposed AVNS-based method also achieves the best performance in all of the instances with respect to all of the three indicators. The results presented in Table 3 are also consistent with Figures 8 and 9.

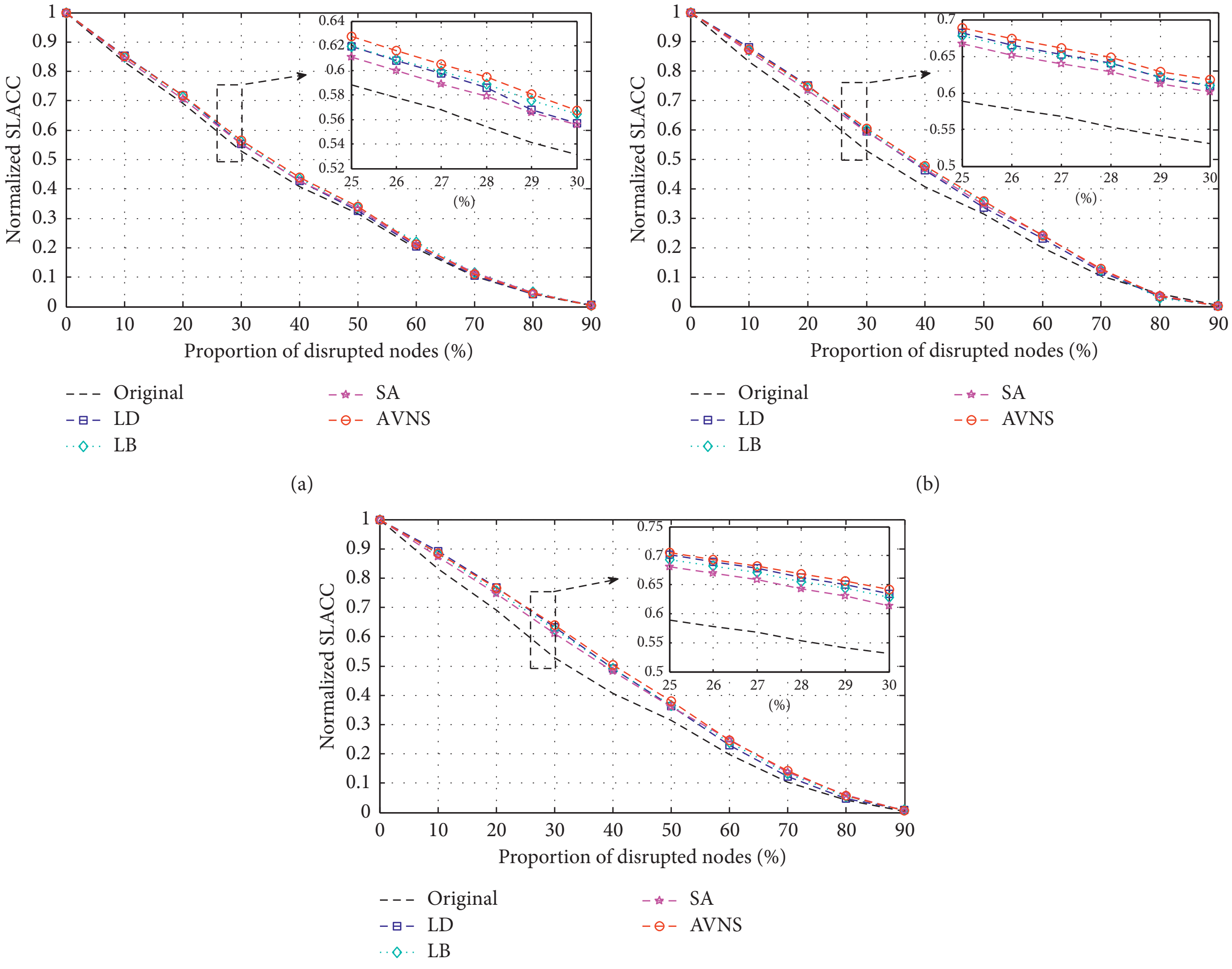
5.2.3. Experimental Results Based on Chain 25. Figures 10 and 11 also present the robustness of Chain 25 and the reconfigured ones facing random disruptions and target disruptions, respectively. In all the figures of Figures 10 and 11, the horizontal axes also denote the percentage of disrupted nodes, while the vertical axes are values of normalized SLACC. Table 4 also summarizes the average values, best values, and worst values of R_r and R_t of the 20 independent experiments based on Chain 25.

As presented in Figures 10 and 11, Chain 25 is also vulnerable to target disruptions and exhibits much stronger tolerance to random disruptions. It is also noticed that Chain 25 is more robust than Chain 14 facing both random and target disruptions. The main reason of such difference can be deduced that Chain 25 is much denser than Chain14. It can also be observed from Table 4 that Chain 25 is slightly robust than Chain 21 facing random disruptions. When facing target disruptions, Chain 25 is more vulnerable than Chain 21. Chain 25 is denser than Chain 21, which may enhance the robustness of it facing random disruptions. However, the stronger degree heterogeneity of it also weakens the robustness of it facing target disruptions. It is also observed from Figures 10 and 11 that networks reconfigured by AVNS-based method are more robust than others facing both random and target disruptions, especially for target disruptions.

As presented in Table 4, the average values, the best values, and the worst values of R_r achieved by the proposed AVNS-based method are better than the three other methods in all of the instances. As for R_t, the proposed AVNS-based method also achieves the best performance in all of the instances with respect to all of the three indicators. The results presented in Table 4 are also consistent with Figures 10 and 11.

5.2.4. Verification for Adaptive Search-Based Solution Improvement. To validate the effectiveness of proposed adaptive search-based solution improvement, a comparative experiment is also performed to compare the proposed AVNS with three alternative algorithms, GNS, LNS, and GNS + LNS. As for GNS and LNS, the adaptive search-based solution improvement is replaced by global search and community closeness-based local neighborhood search, respectively. In GNS + LNS, the adaptive neighborhood determination scheme in the solution improvement procedure is replaced by a randomized neighborhood selection, which is commonly used in VNS. Experiments were performed on 3 representative instances, namely, add 5% edges for Chain 14, Chain 21, and Chain 25, respectively. We ran each algorithm 10 times on each instance within a time limit $T_{\max} = 1800$ seconds.

The experimental results are presented in Figure 12 and Table 5. The average fitness curves of AVNS, GNS, LNS, and GNS + LNS under $fa = 5\%$ for Chain 14, Chain 21, and Chain 25 are presented in Figures 12(a)–12(c), respectively. It can be observed that AVNS can find better solutions in a shorter time in all of the instances. In addition, the experimental results are summarized in Table 5. For each instance, we report the average fitness value (f_{aver}), the best fitness value (f_{best}), and the worst fitness value (f_{worst}) of the

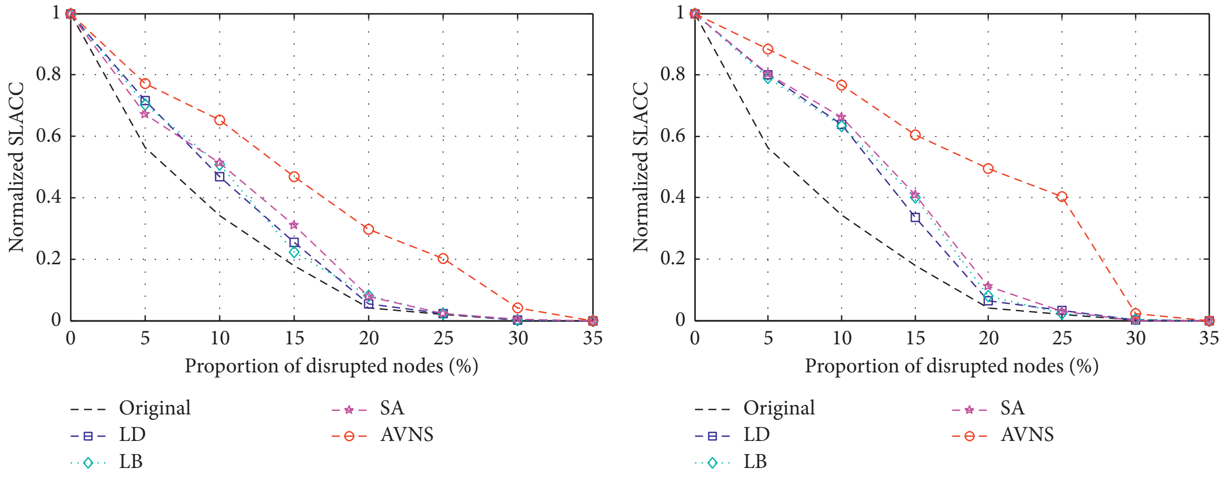


(a)

(b)

(c)

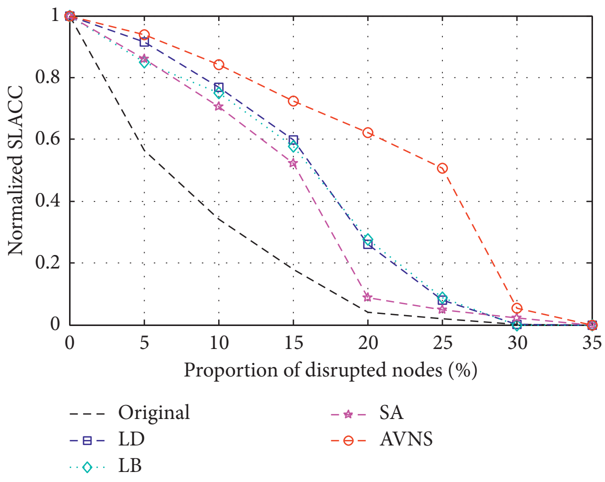
Figure 10: Response of chain 25 and reconfigured ones facing random disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.



(a)

(b)

Figure 11: Continued.



(c)

FIGURE 11: Response of chain 25 and reconfigured ones facing random disruptions. (a) $f_a = 5\%$. (b) $f_a = 10\%$. (c) $f_a = 15\%$.

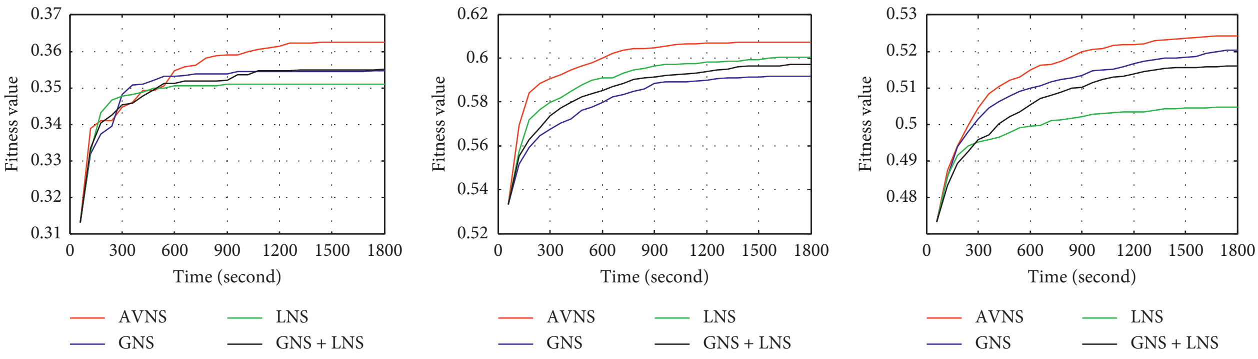
TABLE 4: Robustness comparison of chain 25 and reconfigured ones.

Fa (%)	Method		R_r			R_t	
		Average	Best	Worst	Average	Best	Worst
—	Original	0.3622	0.4252	0.2740	0.0717	0.0734	0.0695
5	LD	0.3743	0.4340	0.2954	0.0942	0.0977	0.0913
	LB	0.3761	0.4318	0.2952	0.0930	0.0953	0.0912
	AVNS	**0.3788**	**0.4344**	**0.3014**	**0.1406**	**0.1444**	**0.1371**
	SA	0.3741	0.4343	0.2931	0.0963	0.0980	0.0946
10	LD	0.3930	0.4302	0.3251	0.1121	0.1147	0.1096
	LB	0.3954	0.4301	0.3290	0.1155	0.1179	0.1130
	AVNS	**0.3977**	**0.4305**	**0.3563**	**0.1826**	**0.1867**	**0.1788**
	SA	0.3923	0.4198	0.3314	0.1203	0.1228	0.1186
15	LD	0.4057	0.4494	0.3251	0.1521	0.1563	0.1476
	LB	0.4056	0.4488	0.3324	0.1478	0.1509	0.1443
	AVNS	**0.4137**	**0.4531**	**0.3646**	**0.2079**	**0.2158**	**0.2024**
	SA	0.4032	0.4490	0.3458	0.1328	0.1345	0.1308

10 trials achieved by each algorithm. The results show that the proposed AVNS performs significantly better than other algorithms in terms of all comparison indicators. Thus, the proposed adaptive search-based solution improvement can effectively increase the performance of algorithm, suggesting that AVNS-based reconfiguration is a suitable method for supply network robustness enhancement.

5.3. Experimental Result Discussion. Structural analysis of real-life supply networks is made. It is found that the degree distribution of real supply networks obeys the truncated power-law distribution. Such a finding indicates a very few number of entities occupy the central position in a supply network. These entities play critical roles in maintaining the basic operation of a supply network. Thus, a supply network is usually robust against random disruptions but is fragile when these important entities with high degrees are damaged.

Experiments based on three real-life supply networks validate that the proposed AVNS-based reconfiguration method can enhance the robustness of supply networks effectively. In addition, it is also found that supply networks are vulnerable to target disruptions. They also exhibit comparatively stronger tolerance to random disruptions. Such experimental results consist with the structural characters of supply networks. Besides, comparing the robustness of Chain 14, Chain 21, and Chain 25, it is observed that density can affect the robustness of a supply network. A denser supply network can be more robust than a sparse supply network facing both random and target disruptions. In addition, the degree heterogeneity of a supply network can also impact the robustness of it facing target disruptions. The more heterogeneous a network is, the more fragile it is facing target disruptions. Edge addition-based supply network reconfiguration methods can enhance the robustness effectively. Along with the number of added edges increasing, the reconfigured network can exhibit a stronger robustness.



(a) (b) (c)

Figure 12: Fitness curve comparison between AVNS, GNS, LNS, and GNS + LNS: reconfiguring (a) chain 14, (b) chain 21, and (c) chain 25 by adding $f_a = 5\%$ edges.

Table 5: Performance comparison of four neighborhood searching method.

	Chain 14			Chain 21			Chain 25		
	Faver	Fbest	Fworst	Faver	Fbest	Fworst	Faver	Fbest	Fworst
AVNS	**0.3583**	**0.3860**	**0.3317**	**0.6072**	**0.6283**	**0.5781**	**0.5244**	**0.5392**	**0.5001**
GNS	0.3524	0.3792	0.3277	0.5917	0.6194	0.5586	0.5203	0.5331	0.4983
LNS	0.3478	0.3769	0.3277	0.6004	0.6264	0.5605	0.5048	0.5162	0.4826
GNS + LNS	0.3511	0.3853	0.3264	0.5973	0.6173	0.5647	0.5160	0.5293	0.4937

6. Conclusions

The structure of a supply network is critically important to its robustness. In spite of the proposed optimal structural designs, a real-life supply network can be quite different from these optimal structures. Meanwhile, real cases reveal the vulnerability of real-life supply networks. Thus, this study proposes a robustness enhancing method for supply networks by reconfiguring the existing network structure. The following can be concluded:

(1) A supply network model considering the different roles of entities in supply networks is introduced. Based on the model, two robustness metrics describing supply networks' tolerance of random and target disruptions are proposed.

(2) An AVNS-based reconfiguration method is presented for supply network robustness enhancement. In order to search for the optimal reconfiguration solution effectively and efficiently, a new variant of VNS, namely, AVNS is proposed. In the proposed AVNS, adaptive search-based solution improvement is designed, which is validated to be effectively improve algorithm performance.

(3) This study also has implications for empirical analysis of supply networks. The structural characters of three empirical supply networks are analyzed. It is found that the degree distribution of real-life supply networks obeys the truncated power-law distribution. Such finding indicates supply networks are heterogeneous. In a supply network, a very few number of entities occupy the central positions and play critically important roles to maintain the function of the supply network. While many others occupy peripheral positions and have less impact on the function of the supply network. Thus, a supply network is robust against random disruptions but is vulnerable when these important entities with high degrees are damaged.

(4) Experiments based on the three real-life supply networks were conducted. The effectiveness of the proposed AVNS-based supply network reconfiguration method is validated using comparative experiments. In addition, experimental results verify that supply networks are extremely vulnerable to target disruptions and exhibit stronger tolerance of random disruptions. And, the robustness of a supply network can be enhanced by adding a small number of edges especially for target disruptions.

However, in this study, the adaptive behavior of entities facing disruptions in a supply network is neglected. Thus, we will take the adaptive behavior of entities into consideration and analyze the effect of it on the supply network robustness in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to acknowledge the funding support from the National Natural Science Foundation Committee (NSFC) of China (grant nos. 51875429 and 51905397) as well as the contributions from all collaborators in the projects mentioned.

References

[1] C. Braziotis, M. Bourlakis, H. Rogers, and J. Tannock, "Supply chains and supply networks: distinctions and overlaps," *Supply Chain Management*, vol. 18, no. 6, pp. 644–652, 2013.

[2] E. J. S. Hearnshaw and M. M. J. Wilson, "A complex network approach to supply chain network theory," *International Journal of Operations & Production Management*, vol. 33, no. 4, pp. 442–469, 2013.

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

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

[5] T. Bier, A. Lange, and C. H. Glock, "Methods for mitigating disruptions in complex supply chain structures: a systematic literature review," *International Journal of Production Research*, vol. 58, no. 6, pp. 1835–1856, 2020.

[6] J. Yoon, S. Talluri, H. Yildiz, and W. Ho, "Models for supplier selection and risk mitigation: a holistic approach," *International Journal of Production Research*, vol. 56, no. 10, pp. 3636–3661, 2018.

[7] M. Kamalahmadi and M. M. Parast, "An assessment of supply chain disruption mitigation strategies," *International Journal Of Production Economics*, vol. 184, pp. 210–230, 2017.

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

[9] K. Zhao, K. Scheibe, J. Blackhurst, and A. Kumar, "Supply chain network robustness against disruptions: topological analysis, measurement, and optimization," *IEEE Transactions on Engineering Management*, vol. 66, no. 1, pp. 127–139, 2019.

[10] 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, Article ID 1724125, 13 pages, 2018.

[11] 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," *International Journal Of Production Economics*, vol. 138, no. 2, pp. 293–302, 2012.

[12] M. Martinez, "Supplier fire ripples across the industry," *Automotive News*, vol. 92, no. 6829, 2018.

[13] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdown," *MIT Sloan Management Review*, vol. 46, no. 1, pp. 53–62, 2004.

[14] D. Ivanov and A. Dolgui, "Low-certainty-need (LCN) supply chains: a new perspective in managing disruption risks and resilience," *International Journal Of Production Research*, vol. 57, no. 15, pp. 5119–5136, 2019.

[15] A. Brintrup and A. Ledwoch, "Supply network science: emergence of a new perspective on a classical field," *Chaos*, vol. 28, no. 3, p. 1, 2018.

[16] M. C. Dong, Z. Liu, Y. Yu, and J.-H. Zheng, "Opportunism in distribution networks: the role of network embeddedness and dependence," *Production and Operations Management*, vol. 24, no. 10, pp. 1657–1670, 2015.

[17] Y. Kim, T. Y. Choi, T. Yan, and K. Dooley, "Structural investigation of supply networks: a social network analysis approach," *Journal of Operations Management*, vol. 29, no. 3, pp. 194–211, 2011.

[18] A. Ledwoch, A. Brintrup, J. Mehnen, and A. Tiwari, "Systemic risk assessment in complex supply networks," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1826–1837, 2018.

[19] B. Adenso-Diaz, C. Mena, S. Garcia-Carbajal, and M. Liechty, "The impact of supply network characteristics on reliability," *Supply Chain Management*, vol. 17, no. 3, pp. 263–276, 2012.

[20] Y. Kim, Y.-S. Chen, and K. Linderman, "Supply network disruption and resilience: a network structural perspective," *Journal of Operations Management*, vol. 33, no. 1, pp. 43–59, 2015.

[21] F. Ma, H. Xue, K. F. Yuen et al., "Assessing the vulnerability of logistics service supply chain based on complex network," *Sustainability*, vol. 12, no. 5, p. 1991, 2020.

[22] A. Nair and J. M. Vidal, "Supply network topology and robustness against disruptions—an investigation using multi-agent model," *International Journal of Production Research*, vol. 49, no. 5, pp. 1391–1404, 2011.

[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," *Applied Network Science*, vol. 2, no. 1, 2017.

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

[25] X.-Q. Shi, W. Long, Y.-Y. Li, D.-S. Deng, Y.-L. Wei, and H.-G. Liu, "Research on supply network resilience considering random and targeted disruptions simultaneously," *International Journal of Production Research*, vol. 58, no. 21, p. 6670, 2019.

[26] A. Brintrup, Y. Wang, and A. Tiwari, "Supply networks as complex systems: a network-science-based characterization," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2170–2181, 2017.

[27] H. Liao, J. Shen, X.-T. Wu, B.-K. Chen, and M. Zhou, "Empirical topological investigation of practical supply chains based on complex networks," *Chinese Physics B*, vol. 26, no. 11, pp. 4067–4081, 2017.

[28] W. J. Tan, A. N. Zhang, and W. Cai, "A graph-based model to measure structural redundancy for supply chain resilience," *International Journal of Production Research*, vol. 57, no. 20, pp. 6385–6404, 2019.

[29] J. Blackhurst, C. W. Craighead, D. Elkins, and R. B. Handfield, "An empirically derived agenda of critical research issues for managing supply-chain disruptions," *International Journal of Production Research*, vol. 43, no. 19, pp. 4067–4081, 2005.

[30] C. S. Tang, "Robust strategies for mitigating supply chain disruptions," *International Journal of Logistics Research and Applications*, vol. 9, no. 1, pp. 33–45, 2006.

[31] S. Y. Gao, D. Simchi-Levi, C.-P. Teo, and Z. Yan, "Disruption risk mitigation in supply chains: the risk exposure index revisited," *Operations Research*, vol. 67, no. 3, pp. 831–852, 2019.

[32] S. M. Wagner and N. Neshat, "Assessing the vulnerability of supply chains using graph theory," *International Journal of Production Economics*, vol. 126, no. 1, pp. 121–129, 2010.

[33] E. Brandon-Jones, B. Squire, C. W. Autry, and K. J. Petersen, "A contingent resource-based perspective of supply chain

resilience and robustness," *Journal of Supply Chain Management*, vol. 50, no. 3, pp. 55–73, 2014.

[34] W. Klibi and A. Martel, "The design of robust value-creating supply chain networks," *OR Spectrum*, vol. 35, no. 4, pp. 867–903, 2013.

[35] B. Adenso-Díaz, J. Mar-Ortiz, and S. Lozano, "Assessing supply chain robustness to links failure," *International Journal of Production Research*, vol. 56, no. 15, pp. 5104–5117, 2018.

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

[37] H. Xia, "Improve the resilience of multilayer supply chain networks," *Complexity*, vol. 2020, Article ID 6596483, 9 pages, 2020.

[38] S. Saavedra, F. Reed-Tsochas, and B. Uzzi, "A simple model of bipartite cooperation for ecological and organizational networks," *Nature*, vol. 457, no. 7228, pp. 463–466, 2009.

[39] W. Yang, J. Wu, and J. Luo, "Effective data transmission and control based on social communication in social opportunistic complex networks," *Complexity*, vol. 2020, Article ID 3721579, 20 pages, 2020.

[40] L. Wang and J. Lu, "A memetic algorithm with competition for the capacitated green vehicle routing problem," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 2, pp. 516–526, 2019.

[41] A. R. Singh, P. K. Mishra, R. Jain, and M. K. Khurana, "Design of global supply chain network with operational risks," *The International Journal of Advanced Manufacturing Technology*, vol. 60, no. 1–4, pp. 273–290, 2012.

[42] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[43] P. Erdös and A. Rényi, "On random graphs," *Publicationes Mathematicae Debrecen*, vol. 6, pp. 290-291, 1959.

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

[45] M. Xu, S. Radhakrishnan, S. Kamarthi, and X. Jin, "Resiliency of mutualistic supplier-manufacturer networks," *Scientific Reports*, vol. 9, Article ID 13559, 2019.

[46] S. S. Perera, M. G. H. Bell, M. Piraveenan, D. Kasthurirathna, and M. Parhi, "Topological structure of manufacturing industry supply chain networks," *Complexity*, vol. 2018, Article ID 3924361, 23 pages, 2018.

[47] R. C. Basole, S. Ghosh, and M. S. Hora, "Supply network structure and firm performance: evidence from the electronics industry," *IEEE Transactions on Engineering Management*, vol. 65, no. 1, pp. 141–154, 2018.

[48] J. L. Carboni, "Balancing life on the tenure track: books to help with substance and form," *Journal of Public Administration Research And Theory*, vol. 25, no. 3, pp. 981–987, 2015.

[49] K. Gao, Z. Cao, L. Zhang, Z. Chen, Y. Han, and Q. Pan, "A review on swarm intelligence and evolutionary algorithms for solving flexible job shop scheduling problems," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 4, pp. 904–916, 2019.

[50] Z. Zhang, M. Zhou, and J. Wang, "Construction-based optimization approaches to airline crew rostering problem," *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 3, pp. 1399–1409, 2020.

[51] J. Wang, M. Zhou, X. Guo, and L. Qi, "Multiperiod asset allocation considering dynamic loss aversion behavior of investors," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 1, pp. 73–81, 2019.

[52] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of Statistical Mechanics-Theory and Experiment*, vol. 10, Article ID 10008, 2008.

[53] A. Beygelzimer, G. E. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A-Statistical Mechanics and its Applications*, vol. 357, no. 3-4, pp. 593–612, 2005.

[54] S. P. Willems, "Data set-real-world multiechelon supply chains used for inventory optimization," *Manufacturing & Service Operations Management*, vol. 10, no. 1, pp. 19–23, 2008.

[55] B. Vandermarliere, A. Karas, J. Ryckebusch, and K. Schoors, "Beyond the power law: uncovering stylized facts in interbank networks," *Physica A: Statistical Mechanics and its Applications*, vol. 428, pp. 443–457, 2015.

[56] Q. Xuan, F. Du, T.-J. Wu, and G. Chen, "Emergence of heterogeneous structures in chemical reaction-diffusion networks," *Physical Review E*, vol. 82, Article ID 46116, 2010.

[57] Z. Jiang, M. Liang, and D. Guo, "Enhancing network performance by edge addition," *International Journal of Modern Physics C*, vol. 22, no. 11, pp. 1211–1226, 2011.

[58] Y. Lu, Y. Zhao, F. Sun, and R. Liang, "Measuring and improving communication robustness of networks," *IEEE Communications Letters*, vol. 23, no. 12, pp. 2168–2171, 2019.

[59] W. Liu, M. Gong, S. Wang, and L. Ma, "A two-level learning strategy based memetic algorithm for enhancing community robustness of networks," *Information Sciences*, vol. 422, pp. 290–304, 2018.