Research Article

Performance Evaluation and Disruption Recovery for Military Supply Chain Network

Biao Xiong, Rong Fan, Shuai Wang, Bixin Li, and Can Wang

Oil Department, Army Logistics University of PLA, Chongqing 401311, China

Correspondence should be addressed to Rong Fan; frfr1002@126.com

Received 30 November 2019; Revised 11 April 2020; Accepted 30 April 2020; Published 20 May 2020

Copyright © 2020 Biao Xiong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The performance of military supply chain networks (MSCNs) against disruptions is an important consideration for defense logistics decision making, and it is crucial to evaluate it scientifically and accurately. This paper highlights the problem from the perspective of targeted defense strategies before being attacked and analyzes the acceptable recovery time against attacks. A topological structure model, with three exclusive features, in contrast with traditional networks, is used to describe the structure of military supply chain networks. In order to provide a platform for evaluating performance, a simulation method based on exploratory analysis is presented. Considering supply capability against disruptions and the acceptable recovery time for an MSCN after disruptions, evaluation metrics including supply capability and disruption recovery are proposed. By applying the model and algorithms to a POL supply network in a theater, we obtain the values of supply capability and disruption recovery against different disruptions. We also identify the key entities which can easily cause catastrophic failure to this network and which need to be protected against carefully. The results show that new evaluation metrics can capture important performance requirements for military supply chain networks. We also find that the proposed method in this paper can solve the problem of evaluating performance and analyzing disruption recovery in a feasible and effective manner.

1. Introduction

Sun Tzu said: generally, a war operation requires one thousand swift chariots, as many chariots and a hundred thousand armored soldier’s with provisions enough to carry them a thousand li (500 meters). What with the expenses at home and in the field, including entertainment of guests, small items such as glue and paint, and sums spent on chariots and armor. The total expenditure will amount to one thousand pieces of gold a day. Only after all this money is in hand can an army of one hundred thousand men be raised to fight. Such is the cost of raising an army of 100,000 men [1].

With the development of military equipment and wide use of modern high technology weapons in warfare, the consumption of military materials has exploded sharply, which makes the military logistics supply system more and more complex. The dependence of war on logistics makes logistical activities, equipment, and facilities become priority attack targets for opponents [2]. For example, in order to destroy the Iraqi army’s military supply networks, the allied troops sent thousands of aircraft to bomb oil refineries, transportation facilities, and other logistics facilities in the Gulf War, which resulted in the destruction of 90% of Iraqi oil refineries. “To fight is to fight on logistics” has once again been verified.

In other words, as a priority target, military supply chain networks often face disruptions [3, 4]. These disruptions affect the performance of MSCNs [5]. For example, a disruption may initially destroy or disable only one or few entities in the system, but its impact may propagate further, sometimes even with amplifications, among interconnected entities. Such disruption will thus affect the normal operations of the supply chain system [6]. Occasionally, failures in a small portion of the system may affect the whole system. Such events may seriously disrupt and delay the flow of logistics, leading to the failure of the war effort [7]. Therefore, it is crucial to discern the key entities which can
easily cause catastrophic failure when disrupted, evaluate the performance and resilience to damage of the MSCN, and then carry out targeted defense in wartime. In this way, the reliability of MSCNs will be improved effectively. In this paper, we consider the problem of reducing the impact of disruptions on MSCNs study the performance of MSCNs against disruptions and provide insights on how to identify key vulnerabilities which can easily cause catastrophic failure, and determine which entities in a MSCN need to be protected. This approach suggests that it is not necessary to fully prevent disruptions, but more precisely to determine the recovery time of the MSCN following a worst-case disruption pattern.

The rest of the paper is organized as follows. In Section 2, we briefly review the relevant literature. In Section 3, we define the MSCN and analyze three exclusive features which make it different from traditional networks. In Section 4, a simulation method with exploratory analysis is put forward to evaluate the performance of MSCNs against disruptions. In Section 5, we construct performance evaluation metrics for MSCNs. Section 6 discusses simulation analyses based on a case study. Finally, Section 7 presents conclusions.

2. Literature Review

Military operations, in particular at remote locations, require a robust and well-managed supply chain network. In order to establish strong and sustainable MSCNs, the US Defense Department introduced the concept of sustainable operations [8]. Some advanced manufacturing and management techniques like additive manufacturing have been introduced to reduce delivery times and logistic costs [9, 10]. However, these techniques are only applied to the supply chain network for special products, not to the supply chain networks for ammunition and petroleum. So, we review the literature on performance evaluation of supply networks, which is closely related to the methodology used in the current papers [11, 12]. Scholars’ research [7, 13, 14] on the structure, resilience, and reliability of supply chain networks can be summarized as a category of this issue. Existing literature [15–17] contains ways to evaluate and optimize the performance of supply networks. Thomas [18] proposed a model for quantifying supply chain reliability for contingency operations. A mixed-integer nonlinear model [15] for optimizing and allocating the road network has been introduced. Additionally, other traditional optimization methods are applied to optimize the small-scale system with a mononetwork such as storage, location, route, or cost in logistic supply systems [19–21]. Supply chain network (SCN) optimization is one of the most crucial planning problems in supply chain management [22, 23]. We found these methods can solve supply chain network optimization problems with few entities and a static structure, but have difficulties in dealing with problems related to the large-scale, multiattribute, and multitarget features of MSCNs [24]. In fact, most studies (e.g., [25, 26]) conclude that the SCN is affected by several uncertainty parameters like costs, demand, and supply, especially for the military supply chain network. Many researchers have suggested that supply chains should be considered as supply networks [27] and that the analysis of supply chain networks should be incorporated with the concepts of complex systems, especially dynamic complex networks [28].

To solve these problems, simulation techniques are applied. Some experts [29–31] use Monte Carlo simulation, Bayesian networks, or system dynamics method to build simulation models, but these kinds of simulation models, which can simulate static structures, are not suitable for simulating the dynamic variation process of the MSCN’s structures. Compared with a traditional supply chain, the MSCN has more entities, and its dynamic feature is more obvious. In a MSCN, supply units and battalions rely on supply orders to connect dynamically. At some point, a connection is established when a supply unit places an order of goods to a battalion. Without the order, there is no connection between them [24].

With the development of complex network technology, some researchers have attempted to apply these methods to evaluate and optimize structural properties of supply chain networks while regarding them as continuous networks [32–34]. Zhao [35] proposed a new method for analyzing the resilience of complex supply network topologies against random and targeted disruptions. However, military supply chain networks are discrete networks in practice. Continuous networks and discrete networks have very different characteristics, and attempting to use continuous network performance evaluation techniques on discrete networks presents difficulties [36]. If the attributes of the network are indiscriminate, wrong conclusions can easily be made. And if the evaluation metrics of continuous networks are used to evaluate discrete networks, errors could appear in the evaluation results. Therefore, a topological structure model [24] with the characteristics of dynamic and discreteness is proposed to describe the structure of MSCNs, and simulation algorithms for effectiveness evaluation are presented. Simulation approaches have been proved to be a suitable tool for evaluating the performance of MSCNs.

Meanwhile, supply chain networks, especially military supply chain networks, often face disruptions, such as natural disasters, enemy strikes, or unexpected accidents. A disruption may initially attack or disable one or a few nodes in the system, but its influence may spread further among interrelated entities and sometimes even amplify [37]. Such disruptions will thus affect the normal operations of many other entities. In many cases, preventive steps can be taken so that if disruptions occur, the ensuing downtime of affected entities will be reduced. The obvious benefits are the improved speed at which the supply chain network can be restored to full operational status and the overall loss control during system downtime. In the best case, it is sometimes possible to reduce recovery time to zero, in which case an entity becomes fully protected from disruption [38]. So far, few people have analyzed the disruption recovery of military supply chain networks from the perspective of discrete networks, and no literature has proposed a method to determine key entities which can cause catastrophic network failure. In this paper, we will present our research on these problems and will provide some useful suggestions for military logistics decision makers while identifying which entities
in a MSCN need to be protected carefully and the max recovery time for repairing them.

3. Definition of MSCN

A military logistic supply system is a complex system comprising several factories, supply storage, demand storage, and logistic devices. Thus, a model description is the foundation to analyze and evaluate that system. Figure 1(a) indicates a logistic supply system in a theater, which can be defined as a directed weighted network \( G = G (V, E, R, \psi) \) (Figure 1). In the directed weighted network \( G, V \) stands for the node set representing factories, depots, demanded forces, etc. \( E \) stands for the connection of nodes formed by traffic networks and the relationship of supply entities. \( R \) represents attributes of supply entities such as physical capacity, location, cargo loading cases, and others; \( \psi \) is a relationship function between nodes and edges. Figure 1 shows MSCN structural evolution established by the complex network model [24].

A military supply chain network not only shares the basic complex system features with traditional complex networks such as complexity and dynamic extensibility but also possesses exclusive features which make it differ from traditional networks.

3.1. Node Heterogeneity. The differences in the forms and the attributes of the entities make the functions and features of the nodes different from each other in the directed weighted network \( G \), which vests the military supply chain network with heterogeneity. Taking Figure 1(a) as an example, there are 3 kinds of entities (factories, supply depots, and demand depots) in the theater, where the factories are mainly responsible for production and delivery of goods, the supply depots receive the goods from the factories and deliver them to the demand depots, and the demand depots receive the goods from the supply depots and distribute them to the troops. The differences in function cause the differences in attributes and attribute weights of different entity nodes. Therefore, as shown in Figure 1(b), the system could be described as the different functional nodes \( V \):

\[
V = V_S \cup V_D \cup V_F,
\]

\[
V_S \cap V_D \cap V_F = \phi,
\]

where \( V_S \) denotes the node set of supply depots, \( V_D \) denotes the node set of demand depots, and \( V_F \) denotes the node set of factories.

3.2. Dynamic Discreteness. Distinguished from traditional continuous networks such as communication networks or molecule networks, a MSCN is a kind of discrete system network. As shown in Figure 1(b), there would be a connection edge \( E_{27} \) when the supply activity between supply node \( V_{S2} \) and demand node \( V_{D7} \) occurs at time \( t \). If the supply activity finishes at time \( t + n \), the edge disappears.

3.3. Time Variation. Because they are affected by supply mechanisms and other factors, the relationships between nodes in the MSCN change dynamically. As shown in Figure 2(a), a supply relationship exists between \( V_{D7} \) and \( V_{S2} \) at time \( t \); however, at a later time \( t + n \), because of the change of supply activities, a new supply relationship between \( V_{D7} \) and \( V_{S3} \) is founded, while the former relationship between \( V_{D7} \) and \( V_{S2} \) disappears. There are two prerequisites for these changes. One is that there must be traffic accessibility between the supply and demand nodes in the logistic system; the other is that the new relationship conforms to the relation-founding rules, such as the organic supply mechanism and regional supply mechanism.

4. Proposed Approach

4.1. Simulation Framework and Algorithm. In this section, we establish a simulation framework based on exploratory analysis, as shown in Figure 3. Firstly, we identify exploratory factors and scenario parameters according to the simulation framework. In the MSCN, disruption time, targets, and so on can be described as exploratory factors and supply environment, tasks, and inventory are scenario parameters. Second, we construct an exploratory analysis model based on the mathematical and simulation models. Then, we analyze the performance of the MSCN and generate feasible solution sets using exploratory analysis with different inputs. Lastly, the feasible solution sets will be inputted into the exploratory analysis model, and the exploratory factors which satisfy all feasible solution sets will be found. The problems of disruption recovery will be solved.

The algorithm is as follows:

1. Initialization.
2. Input the scenario parameters of MSCN, such as supply environments, tasks, and relationships.
3. Input the exploratory factors, such as disruption time, disruption targets, and number of disruptions.
4. Computer simulation and performance evaluation. Output the feasible solution sets.
5. The feasible solution sets are inputted into the exploratory analysis model in reverse.
6. The best values of exploratory factors and the optimal solution set are found.

4.2. Exploratory Analysis Model. An exploratory analysis model is needed for evaluating the performance of an MSCN. The modeling can be divided into three steps: analysis of exploratory factors, determination of exploratory objectives, and the establishment of a basic analytical model.

4.2.1. Exploratory Factors. There are many factors that affect the performance of an MSCN, and we cannot study all of them. In order to evaluate the performance against disruptions and analyze disruption recovery of an MSCN, we chose the following three factors as exploration factors:

exploratory factor index : \( EI = \langle DT, DV, DN \rangle \),

\( DT \), \( DV \), and \( DN \) represent disruptions time, disruptions volume, and disruptions number of disruptions, respectively.
where DT indicates the actual time when disruptions occurred; DV indicates the nodes disrupted; and DN indicates the number of disruptions.

4.2.2. Exploratory Objectives. The exploratory objectives of exploratory analysis for the MSCN can be summarized as follows: the first objective is to determine the reliable time...
interval which cannot affect the performance of MSCN when disrupted, and the other is evaluating the performance of MSCN when disrupted.

4.3. Performance Evaluation Metrics. The performance evaluation for the MSCN should consider both supply capability metrics and disruption recovery metrics.

4.3.1. Supply Capability Metrics. The highest concern of military evaluation metrics of MSCNs is their supply capability, i.e., the capability to fulfill the support mission and the degree to which the mission can be completed through the existing logistic supply resources in war. In a MSCN, if the logistic materials needed by the demand nodes surpass the specified threshold (ex. 0 or 10% of the storage amount) throughout the entire war, the supply capability can be defined as strong. Otherwise, the longer the logistic materials needed by the demand node remain below the specified threshold, the weaker the supply capability would be. The following formula shows the above perspectives:

\[ \Delta P_j = \frac{DT_j}{\text{SumTime}} \]  

where \( \Delta P \) represents the supply capability sum of all the demand units \( V_j \). The smaller the value of \( \Delta P \) is, the more competent the supply capability is.

\[ DT_j = \sum_{i=1}^{\text{SumTime}} \text{Time}(VD_j \leq \rho \cdot \text{Volume}_j), \]  

where \( VD_j \) is the storage amount of the demand node \( V_j \) at time \( t \); \( \rho \) is the specified threshold ratio; \( \text{Volume}_j \) is the total storage amount of all the demand units \( V_j \); and \( \text{SumTime} \) stands for the total time of war.

4.3.2. Disruption Recovery Metrics. Under wartime conditions, nodes and edges in the MSCN are important targets for combat opponents. Emergency rescue and repair will be carried out to restore the supply capability of disrupted nodes and edges after being attacked, such as establishing a field emergency facility to replace the damaged facility. If the damage can be repaired within the time interval \( \Delta t \), the performance cannot be affected during war time. We call this phenomenon disruption recovery, and the time interval \( \Delta t \) is the disruption recovery metric. The greater the value of \( \Delta t \), the stronger the ability of disruption recovery.

4.3.3. Basic Analytical Model. The basic analytical model for analyzing the performance of MSCN can be described as follows:

\[ OS = \{Q, N, Z\}, \]  

where \( Q \) is a set of variables, which usually includes a set of known variables and a set of exploratory factors; \( N \) is a set of constraints; and \( Z \) is the objective set.

(1) Variable Set \( Q \). \( Q \) includes both deterministic known variable set \( MI \) and uncertain exploratory factor set \( EI \).

\[ Q = MI \cup EI, \]  

where, \( MI = \{V_S, V_D, D, TR, H\} \).

Set \( MI \) contains demand nodes \( V_S \), supply nodes \( V_D \), distances \( D \), the total amount of traffic \( TR \), and transportation network \( H \).

(2) Constraint Set \( N \). The constraint set \( N \) describes the constraints of the basic analytical model, including time constraint, capacity constraint, and inventory constraint. Its mathematical expression is

\[ N = \{\text{DTime}, \text{TRS}, \text{LS}\}, \]  

where \( \text{DTime} \) is the constraint of supply time; \( \text{TRS} \) represents the transport capacity constraint of MSCN; and \( \text{LS} \) is the inventory of the MSCN.

\[ \text{DTime}: T_{ij} \leq \text{DTime}_j, \quad \forall j = 1, 2, \ldots, m, \exists i \in (1, n), \]  

\[ \text{TRS}: \sum_{i=1}^{T} \text{TRSD}^i \geq \sum_{i=1}^{T} \text{TRSS}^i, \]  

\[ \text{LS}: \sum_{i=1}^{T} \sum_{j=1}^{n} \text{VS}^i_j \geq \sum_{i=1}^{T} \sum_{j=1}^{m} \text{VD}^i_j, \]  

where \( \text{VS}^i_j \) stands for the available storage amount of supply node \( i \) at time \( t \); \( \text{VD}^i_j \) is the demand amount of demand node \( j \) at time \( t \); \( T_{ij} \) is the actual time of transporting from supply node \( i \) to demand node \( j \); \( \text{TRSD}^i \) is the available transport capacity at time \( t \); and \( \text{TRSS}^i \) is the demand for transport capacity at time \( t \).

(3) Objective Set \( Z \). \( Z \) is the objective set of exploratory analysis for the MSCN, which contains supply capacity and an acceptable time interval. Supply capability \( \Delta P \) is the quantitative performance of the MSCN when disrupted, and an acceptable time interval \( \Delta t \) stands for the acceptable time span for the MSCN’s performance that cannot be affected by disruptions.

\[ Z = \{\Delta P, \Delta t\}. \]

5. Simulation Example

Oil is the blood of war. Oil consumption during wartime makes up 60% of all material costs. The oil supply network of our simulated theater comprises 3 supply oil depots (SODs) and 16 demand oil depots (DODs) in this example. With a constant pipeline between SOD 1 and an oil refinery, SOD 1 is supported by the refinery directly, while SOD 2 and SOD 3 are supplied by SOD 1 through field pipelines, respectively. The SODs support the demand oil depots using oil trucks. The oil supply network of this theater is shown in Figure 4. The basic parameters such as storage capacity, support ability, distance, and expected costs in the network are omitted. Given: all depots are at full load before the war; there are 150 oil trucks to deliver oil; and the operation lasts for 20 days.
5.1. Data Assumptions. Related simulation assumption data shown in Table 1 mainly include the DOD inventory capacity (Volume) and consumption.

Consumption refers to consumption and provisioning of POL (petrol oil and lubricant) from each DOD that supplies other troops. For example, assuming that DOD 16 consumes 5 m³/h, this number shows that the average consumption per hour is 5 m³ when it sends POL to the front line troops.

5.2. Transportation Hypothesis. Suppose that pipeline 1 (from the oil refinery to SOD 1) has a throughput of 30 m³/h. SOD 1 provides POL to SOD 2 and SOD 3 through pipelines at 20 m³/h.

This MSCN contains 150 vehicles in total, which are initially deployed in SODs. The running speed of each vehicle is 30 km/h. The simulation process does not consider vehicle damage.

5.3. Simulation Data Analysis. It is very difficult to construct a real-world POL supply chain network and generate disruptions within it to evaluate its performance, so we rely on computer simulations. In this section, we describe our method for evaluating the performance and recovery time of the POL supply chain network against pipeline and node disruptions.

5.3.1. Recovery Time Analysis for Pipeline Disruptions. Because of the characteristics of strong conveying capacity, safety, and reliability, pipelines are the main way of oil transportation from one oil depot to another. Therefore, each pipeline is an important target for combat opponents in wartime, so we must analyze the performance of an MSCN when the pipeline is disrupted and determine the recovery time interval $\Delta t$ with the simulation method in this example.

In order to study the performance of the MSCN when the pipeline is disrupted, we simulate a situation where No. 2 pipeline is disrupted by one attack at different times. The attack time (AT) and recovery time interval $\Delta t$ are chosen as exploratory factors in this section. Then, we carry out a computer simulation based on the proposed approach, and 480 sets of feasible solutions are generated. The partial simulation results are shown in Table 2.

As shown in the first row of data in Table 2, if the recovery time for repairing the interrupted time of pipeline is less than 159 hours, the network performance will not be affected by the attack and when it happened at the 100th hour of simulation, all demands in MSCN can be satisfied. That is to say, if disruption happened at the 100th hour of simulation and if we can repair the pipeline before the 259th hour of simulation, the supply capability metric $\Delta P$ will be equal to 0. Otherwise, the supply capability metric $\Delta P$ will not be equal to 0, which means that at least one demand node is out of supply during the simulation time.

In the simulation, we also found that if the time of the attack is different, the acceptable recovery time will also be different. For example, the acceptable recovery time is reduced to 67 hours when the attack happens at the 250th hour of simulation.

We use the method described in this paper to analyze the optimal recovery time ($\Delta t$) value which was satisfactory for any attack in this example, and we found when $\Delta t$ is less than 62 h, the performance cannot be affected by the attack for No. 2 pipeline. In other words, if we can repair the disrupted pipeline in less than 62 h when interrupted by

| Depot | Inventory capacity (m³) | Consumption (m³/h) |
|-------|-------------------------|--------------------|
| DOD 1 | 150                     | 3                  |
| DOD 2 | 125                     | 2                  |
| DOD 3 | 880                     | 3                  |
| DOD 4 | 245                     | 3                  |
| DOD 5 | 480                     | 4                  |
| DOD 6 | 560                     | 4                  |
| DOD 7 | 260                     | 5                  |
| DOD 8 | 250                     | 5                  |
| DOD 9 | 320                     | 4                  |
| DOD 10| 1600                    | 5                  |
| DOD 11| 100                     | 2                  |
| DOD 12| 850                     | 4                  |
| DOD 13| 650                     | 5                  |
| DOD 14| 850                     | 6                  |
| DOD 15| 325                     | 6                  |
| DOD 16| 300                     | 5                  |
one attack, there will not be any DT$_j$ greater than 0. As a result, the simulation method can be used to provide maintenance decision supports for actual MSCNs against disruptions.

5.3.2. Node Disruption Analysis. Node disruption means that an oil depot is disrupted by the enemy, one of the most common disruptions for this type of MSCN. In wartime conditions, once the oil depot is disrupted, its supply function will be difficult to repair or even directly destroyed because of the flammability of oil. In view of this, we usually set up field oil depots (FODs) nearby to satisfy the demands of the region. In this example, we simulate this situation and prepare enough FODs near SODs 1, 2, and 3, and once a DOD is disrupted, the nearest FOD will be sent to replace it.

In this paper, we first simulate that a DOD in MSCN is disrupted by one attack separately shown in Figure 5. The horizontal axis of this chart is the simulation time when a disruption happened, and the vertical axis is DT$_{sum}$ which means the total time for all demand nodes to drop to zero inventory in simulation time. Take DOD 5 as an example: the total times of zero inventory are 18.3 hours when DOD 5 is disrupted at the 150th hour of simulation time. We also found that the trends of zero-inventory time for this example change periodically, which are caused by the demands to be constantly replenished in fixed time cycles.

How do multiple disruptions change the performance of the MSCN? The MSCN is attacked by 5 random disruptions 100 times in this section. In Table 3, we select 7 sets of simulation results with larger values of DT$_{sum}$, and the attack times are described in Table 4. We use S.2 row as an example, and S.2 represents the second largest value set of DT$_{sum}$ in simulation results. As shown in Table 4, we can see that DOD 3, DOD 5, DOD 10, DOD 13, and DOD 15 are disrupted at different times. For example, we found that DOD 3 is disrupted at the 60th hour of simulation time as shown in Table 4. The value of DT, which represents the total time for demand nodes to drop to zero inventory, can be found in Table 3. Taking the value of DT$_j$, in S.2 row as an example, the value of DT$_j$ is 11, which means the total time for DOD 3 to drop to zero inventory is 11 hours.

We found DOD 16 is not attacked in S.2, but it has also been affected; the total time for DOD 16 to drop to zero inventory is equal to 20 hours. This shows that there is a connection between the nodes. Damage to one node may cause disruption to other nodes; we call this phenomenon cascading failure in complex networks.

Through data analysis, we found if DOD 13 is disrupted, it had the greatest impact on network reliability, followed by DOD 10 and DOD 16. At the same time, DOD 13, DOD 10, and DOD 16 are critical nodes in the MSCN. Therefore, when protecting against network disruptions, it is important to consider the protection of DODs 10, 13, and 16.

6. Discussion

In this section, the results of our study are discussed and linked with the existing body of knowledge.

The topological structure is addressed as the research focus for the performance of MSCN against disruptions [7, 35], while in our study, the attack time is equally important. Simulation results show that if the attack time for the same node in an MSCN is different, the performance is also different under the same conditions. So, we can no longer treat the network as a continuous network and only consider the effect of the structure on the network performance. We must recognize the characteristics of dynamic discreteness and time variation for MSCNs which are described in Section 3.2 and treat it as a discrete network. Although this paper has not been able to formalize the relationship between node disruption time and performance impact, it is enough to show that an MSCN has the characteristic of time variation. Therefore, we recommend further research into the effect of node disruption on performance.

Availability and connectivity have been considered as performance evaluation metrics for MSCNs in earlier studies [7], while the current study did not take them into consideration. From the perspective of discrete networks, even if there is no supply node connected to a demand node, as long as the inventory of all demand nodes is not equal to zero, the performance of an MSCN is strong. As a result, we chose supply capability metrics to evaluate performance. However, there is no proper metric to evaluate the resilience of an MSCN, which is recommended for further research.

While previous research often focused on the hub nodes which have high degrees for protecting against disruptions, we think this is not enough. Through simulation, we found
there are still some nonhub nodes that once struck will also quickly reduce the performance of the MSCN, such as DOD 13 mentioned above. We call this phenomenon cascade failure of a weighted discrete network, which still exists in the MSCN. Therefore, we should not only focus on the key nodes in theory but also focus on the key nodes in reality. This is the key discrepancy between our finding and the theory.

7. Conclusion

The aim of this paper was to study how enemy attacks affect the performance of MSCNs and how to deal with these attacks from the perspective of targeted defense strategies before attacks and analyze the acceptable recovery time against attacks. We first adopted the complex network view of supply chains and studied the performance of military supply chain networks from the perspective of discrete networks, which can describe the dynamic and discrete characteristics of MSCNs. Then, we established an exploratory analysis model for performance evaluation and disruption recovery. Thirdly, we proposed a new taxonomy of performance evaluation metrics to reflect the fact. The taxonomy consists of supply capability metrics and disruption recovery metrics.

For simulation, we used the proposed approach to evaluate the performance of a POL supply chain network in theater and analyzed the disruption recovery metric by using exploratory analysis. The simulation results show that if the attack time for MSCNs is different, the damage and the recovery time will also be different, which proves that MSCNs are typical discrete networks. Moreover, although the value of recovery time for MSCN against disruptions changed without rules to follow, we have found that each node has a different impact on the performance of MSCN against disruption, and it has a different weight. This means our model can give some useful advice for network defense. In an actual MSCN, we can use the proposed approach in this paper to analyze which nodes are important, and then we can focus on the protection of these critical nodes. As a result, the network performance will not decline significantly when an unimportant node is destroyed. We can also use this approach to analyze disruption recovery for MSCN. The simulation example shows that the approach proposed in this paper is workable and effective for dealing with discrete network performance evaluation and disruption recovery analysis.

There are several areas that we would like to address in the future. In this paper, we only consider node disruptions without considering the effects of edge disruptions. If a road in an MSCN is interrupted, we must find an alternative path to fulfill the task. The alternative road will be blocked when additional vehicles use it. Then, cascading failures of the MSCN may occur. Another limitation is that we proposed a method for performance evaluation of MSCN, but it is not an optimization model for improving the performance. After all, the ultimate goal of our work for performance evaluation is to optimize it.

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

This study was supported by the National Social Science Fund of China under grant no. 2019-SKJJ-C-013.
References

[1] T. Shapiro and M. John, *The Art of War: Bilingual Chinese and English Text*, Tuttle Publish, Clarendon, VR, USA, 2017.

[2] G. Kovács and P. Tatham, “Responding to disruptions in the supply network-from dormant to action,” *Journal of Business Logistics*, vol. 30, no. 2, pp. 215–229, 2009.

[3] E. Ozceylan and T. Paksoy, “Interactive fuzzy programming approaches to the strategic and tactical planning of a closed-loop supply chain under uncertainty,” *International Journal of Production Research*, vol. 52, no. 8, pp. 2363–2387, 2014.

[4] A. M. Ross, Y. Rong, and L. V. Snyder, “Supply disruptions with time-dependent parameters,” *Computers & Operations Research*, vol. 35, no. 11, pp. 3504–3529, 2008.

[5] F. Pan and R. Nagi, “Robust supply chain design under uncertain demand in agile manufacturing,” *Computers & Operations Research*, vol. 37, no. 4, pp. 668–683, 2010.

[6] L. Özdamar and M. A. Ertem, “Models, solutions and enabling technologies in humanitarian logistics,” *European Journal of Operational Research*, vol. 244, no. 1, pp. 55–65, 2015.

[7] Q. Zhou, B. Xiong, and B. Li, “Analysing the resilience of military supply network and simulation against disruptions,” *International Journal of Engineering Systems Modelling and Simulation*, vol. 8, no. 3, pp. 195–204, 2016.

[8] M. Goltz and N. Turek, “Sustainable military operations,” in *Sustainability Practice and Education*, Bentham Science Publisher, Sharjah, UAE, 2017.

[9] J. D. Boer, W. Lambrechts, and H. Krikke, “Additive manufacturing in military and humanitarian missions: advantages and challenges in the spare parts supply chain,” *Journal of Cleaner Production*, vol. 257, no. 1, pp. 1–11, 2020.

[10] L. F. C. S. Durao, A. Christ, E. Zancul, R. Anderl, and K. Schützer, “Additive manufacturing scenarios for distributed production of spare parts,” *International Journal of Advance Manufacturing Technology*, vol. 93, no. 1–4, pp. 869–880, 2017.

[11] E. Burshtein and J. Goubault-Larrecq, “A logical framework for evaluating network resilience against faults and attacks,” *Lecture Notes in Computer Science*, vol. 4846, no. 4, pp. 212–227, 2007.

[12] H. P. Thadakamaila, U. N. Raghavan, S. Kumara, and R. Albert, “Survivability of multi-agent based supply networks: a topological perspective,” *IEEE Intelligent System*, vol. 19, no. 5, pp. 24–31, 2004.

[13] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Limited, Aldershot, UK, 2006.

[14] R. Klimov and Y. Merkuryev, “Simulation model for supply chain reliability evaluation/tiekimo grandinės patikimumo iveritimo imitacinis modelis,” *Technological and Economic Development of Economy*, vol. 14, no. 3, pp. 300–311, 2008.

[15] A. S. Mohaymany and M. Babaei, "An approximate reliability evaluation method for improving transportation network performance," *Transport*, vol. 25, no. 2, pp. 193–202, 2010.

[16] T. Santos, S. Ahmed, and M. Goetschalckx, “A stochastic programming approach for supply chain network design under uncertainty,” *European Journal of Operational Research*, vol. 167, no. 1, pp. 96–115, 2005.

[17] W.-C. Yeh, “A hybrid heuristic algorithm for the multistage supply chain network problem,” *The International Journal of Advanced Manufacturing Technology*, vol. 26, no. 5-6, pp. 675–685, 2005.

[18] M. U. Thomas, “Supply chain reliability for contingency operations,” *Proceedings Annual Reliability and Maintainability Symposium*, vol. 32, pp. 61–67, 2002.

[19] C. Gershenson and M. Prokopenko, “Complex networks,” *Artificial Life*, vol. 17, no. 4, pp. 259–261, 2011.

[20] S. H. Strogatz, “Exploring complex networks,” *Nature*, vol. 410, no. 8, pp. 268–276, 2001.

[21] S. Huang, C. K. M. Lee, K. Wu, and K. L. Choy, “Multi-objective optimization for sustainable supply chain network design considering multiple distribution channels,” *Expert Systems With Applications*, vol. 65, no. 1, pp. 87–99, 2016.

[22] E. Aghezzaf, “Capacity planning and warehouse location in supply chains with uncertain demands,” *Journal of the Operational Research Society*, vol. 56, no. 4, pp. 453–462, 2005.

[23] K. Govindan, M. Fattahi, and E. Keyvanshokooh, “Supply chain network design under uncertainty: a comprehensive review and future research directions,” *European Journal of Operational Research*, vol. 263, no. 1, pp. 108–141, 2017.

[24] B. Xiong, B. X. Li, R. Fan, Q. Z. Zhou, and W. Li, “Modeling and simulation for effectiveness evaluation of dynamic discrete military supply chain networks,” *Complexity*, vol. 2017, Article ID 6052037, 9 pages, 2017.

[25] H. M. Bidhandi and R. M. Yussuf, “Integrated supply chain planning under uncertainty using an improved stochastic approach,” *Applied Mathematical Modelling*, vol. 35, no. 6, pp. 2618–2630, 2011.

[26] E. H. Sabri and B. M. Beamon, “A multi-objective approach to simultaneous strategic and operational planning in supply chain design,” *Omega*, vol. 28, no. 5, pp. 581–598, 2000.

[27] A. Surana, S. Kumara, M. Greaves, and U. N. Raghavan, “Supply-chain networks: a complex adaptive systems perspective,” *International Journal of Production Research*, vol. 43, no. 20, pp. 4235–4265, 2005.

[28] S. D. Pathak, J. M. Day, W. J. Sawaya, A. Nair, W. J. Sawaya, and M. M. Kristal, “Complexity and adaptivity in supply networks: building supply network theory using a complex adaptive systems perspective,” *Decision Sciences*, vol. 38, no. 4, pp. 547–580, 2007.

[29] A. Jabbarzadeh, B. Fahimnia, and S. Seuring, “Dynamic supply chain network design for the supply of blood in disasters: a robust model with real world application,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 70, pp. 225–244, 2014.

[30] A. Jabbarzadeh, S. G. Jalali Naini, H. G. Jalali, and N. Azad, “Designing a supply chain network under the risk of disruptions,” *Mathematical Problems in Engineering*, vol. 2012, no. 1, pp. 1–23, 2012.

[31] L. Sawaya and Z.-J. M. Shen, “A supply chain design model with unreliable supply,” *Naval Research Logistics*, vol. 54, no. 8, pp. 829–844, 2007.

[32] R. Albert, H. Jeong, and A. L. Barabasi, “Error and attack tolerance of complex network,” *Nature*, vol. 406, no. 4, pp. 378–382, 2000.

[33] A. L. Barabási, H. Jeong, Z. Néda, and E. Ravasz, “Evolution of the social network of scientific collaborations,” *Physica A: Statistical Mechanics and Its Applications*, vol. 311, no. 3-4, pp. 590–614, 2002.

[34] P. Erdos and A. Renyi, “On random graphs,” *Publicationes Mathematicae*, vol. 11, no. 6, pp. 290–297, 1959.

[35] 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. 23, no. 5, pp. 28–39, 2011.
[36] S. Vicsek, V. Latora, Y. Moreno, M. Chavez, and D. Hwang, “Complex networks: structure and dynamics,” *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.

[37] H. L. Lee, V. Padmanabhan, and S. Whang, “The bullwhip effect in supply chains,” *MIT Sloan Management Review*, vol. 38, no. 3, pp. 93–102, 1997.

[38] C. Losada, M. P. Scaparra, and J. R. O’Hanley, “Optimizing system resilience: a facility protection model with recovery time,” *European Journal of Operational Research*, vol. 217, no. 3, pp. 519–530, 2012.