Topological Resilience Analysis of Supply Networks under Random Disruptions and Targeted Attacks

Wenjun Wang, W. Nick Street, and Renato E. deMatta
Department of Management Sciences
University of Iowa
Iowa City, IA 52242, USA
{wenjun-wang, nick-street, renato-dematta}@uiowa.edu

***Abstract*—Along with the rapid advancement of information technology, the traditional hierarchical supply chain has been quickly evolving into a variety of supply networks, which usually incorporate a large number of entities into complex graph topologies. The study of the resilience of supply networks is an important challenge. In this paper, we exploit the resilience embedded in the network topology by investigating in depth the multiple-path reachability of each demand node to other nodes, and propose a novel network resilience metric. We also develop new supply-network growth mechanisms that reflect the heterogeneous roles of different types of nodes in the supply network. We incorporate them into two fundamental network topologies (i.e. random-graph network and scale-free network), and evaluate their resilience against both random disruptions and targeted attacks using the new resilience metric. The experimental results verify the validity of our resilience metric and the effectiveness of our growth model. This research provides a generic framework and important insights into the construction and resilience analysis of complex supply networks.**

I. Introduction

The supply chain is the construction and management of the flow of goods among suppliers, distributors, retailers, and customers. Traditional supply chains usually maintain a hierarchical structure with a linear flow of goods from suppliers to customers via distributors and retailers. Due to the globalization and fast development of technology, the basic supply chain system has become much more sophisticated, and it has rapidly evolved into dynamic complex networks in which links can occur not only between units of different types, but also between units of the same type. For example, some large retailers may distribute goods to small retailers.

While the supply network plays such an important role in product distribution systems, its sustainability (or say, survivability) becomes an important concern. It has also become an interesting research topic that has drawn considerable attention and extensive studies. Some of the challenging questions regarding the resilience of complex supply networks are as follows. What are the principles that govern how supply networks arise and develop? How resilient is a supply network against random and/or targeted disruptions? How do we measure resilience, and how is it related to the network topology? How can we build resiliency in a supply-network design? There are many such interesting but challenging questions regarding the resilience analysis of complex supply networks. Previous research [1][2] have revealed that supply networks share many characteristics that most real-world networks commonly have, and the graph topology of the supply network has great impact on its resilience against disruptions.

In this paper, we first propose a new resilience metric that captures the reachability-based robustness encoded in the network topology in a more accurate and comprehensive manner. Then we present new supply-network growth models that incorporate the heterogeneous roles of units of different types into two fundamental network topologies with various attachment strategies. Using a military logistic network as a case study, we analyze the resilience of different growth models by simulating the supply network under random disruptions and targeted attacks. Experimental results verify the validity of our resilience metric, and demonstrate the effectiveness of our growth model. Our approach sheds light on the construction of more realistic and robust supply networks.

II. Related Work

Supply networks are often subject to various disruptions, such as unexpected accidents, natural disasters, terrorist attacks, etc. When the disruption occurs, a few units or connections fail to operate at the onset, but the adverse impact on organizational performance may propagate in the network and eventually lead to devastating malfunction of a great component or even the entire supply system. The resilience analysis of supply-networks under random disruptions and targeted attacks has received considerable managerial attention and a lot of research work.

While conventional disruption studies focus on risk mitigation and contingency planning strategies [3][4], some researchers investigate the resilience of supply networks from a topological perspective. Criado et al. [5] define a quantitative measure of network vulnerability related to the graph topology. Using a multiagent-based simulation framework, Thadakamalla et al. [6] examine how different network topologies affect the supply-network resilience against random disruptions and targeted attacks in terms of clustering coefficient, size of the largest connected component (LCC), characteristic path length in LCC, and maximum distance in LCC. Nair and Vidal [7] adopt the multiagent model and investigate topology-associated supply-network robustness from the perspective of performance impacts in terms of inventory levels,

ASONAM '15, August 25-28, 2015, Paris, France
 ISBN 978-1-4503-3854-7/15/08 $15.00
DOI: http://dx.doi.org/10.1145/2808797.2809325

Name	Description
Size of LCC	Number of nodes in the largest connected component (LCC)
Average path length in LCC	Average of the shortest path length between any pair of nodes
Maximum path length in LCC	Maximum shortest path length between any pair of nodes

TABLE I
SOME GENERIC METRICS FOR NETWORK RESILIENCE ANALYSIS

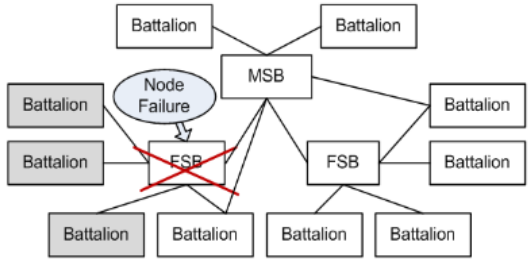

Fig. 1. A hierarchical military supply chain (given in [9])

Name	Topology-level metric	Description
Availability	Supply availability rate	Percentage of demand nodes that have access to supply nodes
Connectivity	Size of the largest functional sub-network (LFSN)	Number of nodes in LFSN, in which there is a path between any pair of nodes and there exists at least one supply node
Accessibility	Average supply path length in LFSN	Average of the shortest supply path length between *all* pairs of supply and demand nodes in LFSN
	Maximum supply path length in LFSN	Maximum shortest supply path length between *all* pairs of supply and demand nodes in LFSN

TABLE II
RESILIENCE METRICS PROPOSED BY ZHAO ET AL.[9]

Fig. 2. Example 1 of the military supply chain

Fig. 3. Example 2 of the military supply chain

backorders, and total costs. Based on the complex network theory, Chen and Lin [8] study the characteristics of the complex supply chain and present an invulnerability analysis method to evaluate its robustness against random failures and deliberate assaults. Using a military logistic network as a case study (see in Figure 1 a hierarchical illustration of it, where FSB stands for forward support battalions, and MSB for main support battalions), Zhao et al. [9] propose another taxonomy of resilience metrics that reflect the heterogeneous roles of different types of units in supply networks, and present a hybrid and tunable network growth model. Kim et al. [10] present a comprehensive conceptualization of the supply-network disruption and resilience from a network structural perspective. However, the above approaches fail to differentiate supply nodes from demand nodes in either the resilience metrics or the network growth models or both.

Table I lists some generic resilience metrics used in previous literature [6][7], which focus on the size of the largest connected component (LCC) and the average/maximum path lengths in LCC without differentiation of the roles of the nodes. When using these metrics to evaluate the supply-network resilience, it is implicitly assumed that the roles of nodes in the supply network are homogeneous. Obviously, this assumption is not realistic. For example, as illustrated in the military logistic network in Figure 1, the MSB can be regarded as the supplier or manufacturer, FSBs act as distributors or warehouses, and regular battalions as retailers or consumers. An LCC without the MSB or FSBs should not be considered resilient since the supply flow in such a sub-network is limited and unsustainable.

The resilience metrics proposed by Zhao et al. in Table II makes more sense by considering the supply-demand heterogeneous roles in supply networks. However, there are many issues on these metrics as well. First, the average/maximum supply path lengths in the largest functional sub-network (LFSN) are not defined in a sufficiently rigorous manner. We illustrate two simple examples in Figures 2 and 3 in the context of the military supply network. Using the taxonomy defined in Table II, the average/maximum supply path lengths are 1.5/2 for both examples. However, it is obvious that Example 2 has better accessibility and is more resilient than Example 1.

This inaccuracy is introduced because these two accessibility metrics are both based on *all* pairs of supply and demand nodes in the LFSN, which results in the inclusion of some *far-away* supply nodes and adversely decreases the overall accessibility. This is not reasonable. In fact, this issue can be addressed by simply defining the average/maximum supply path lengths as the average/maximum shortest supply path lengths of all demand nodes to their *nearest* supply nodes. To some extent, this helps integrate the effect of the number of supply nodes in the overall resilience analysis. Applying these new accessibility metrics to the two examples as described above, we obtain the average/maximum supply path lengths of 1.5/2 for Example 1 and 1/1 for Example 2, which practically reflects that Example 2 is more accessible (and more resilient) than Example 1.

There are other issues. For example, how do we differentiate MSBs from FSBs? Should we consider the path length in supply availability rate? Why should we only consider the LFSN but totally ignore the second largest and all other sub-networks? Should we consider also the number of supply nodes in LFSN? In addition, if the number of supply nodes

is fixed, larger LFSN is usually associated with larger average/maximum supply path lengths in LFSN. In other words, better connectivity is associated with worse accessibility. How do we evaluate the overall resilience with negatively correlated metrics? Further, now that we allow demand nodes to be connected with each other in the supply network, should we give this type of connection some resilience credit as well even though it is supposed to be much smaller than directly connecting to a supply node? All of these may imply considerable loss of information and unreliable or even misleading results when using these metrics for resilience analysis.

III. Methodology

In this section, we take into consideration the heterogeneous roles of units of different types and propose a new network resilience metric by exploiting the multiple-path reachability of each demand node to other nodes. Then we examine various attachment strategies and perform resilience analysis of supply networks that are characterized with random-graph and scale-free topologies. Our growth models differ from previous work. The key idea is that the supply-network growth model (that is always driven and investigated from the supplier's perspective) should impose few constraints on demand nodes (when they enter the network) but focus on developing effective attachment rules on supply nodes instead since the supply-network designer has little direct control over demand nodes. In fact, when a demand node enters the network, it usually does not have the global scope of the whole network, such as the shortest paths between all pairs of nodes. It makes more sense to allow them to enter or grow on their own by simply following the basic attachment rule originally proposed in constructing the respective network topology. It is not realistic to apply the same attachment rules to both demand nodes and supply nodes.

A. New Resilience Metric

Our resilience metric differs from the existing metrics in literature. Instead of only focusing on the LCC or LFSN, we consider all the nodes in the supply network. More specifically, we evaluate the network resilience based on the resilience of each demand node, which is measured by the *multiple-path reachability* of the node of interest to other nodes. We argue that it is reasonable to quantify the network resilience by the aggregated resilience of all demand nodes in the network. This approach captures an intuitive but essential notion about network resilience.

We develop a modified *depth-limited search* algorithm to exploit the multiple-path reachability of a demand node to other nodes. We do not search for any specific target nodes, but explore all the nodes that the node of interest (called *root node*) can reach in its neighborhood within a pre-specified depth limit. We have three important rules implemented in this algorithm:

1) *Cycles are avoided*. It makes sense since revisiting the same set of nodes in a loop or cycle does not improve the resilience.

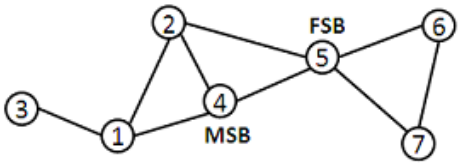

Fig. 4. Example of a simple military logistic network

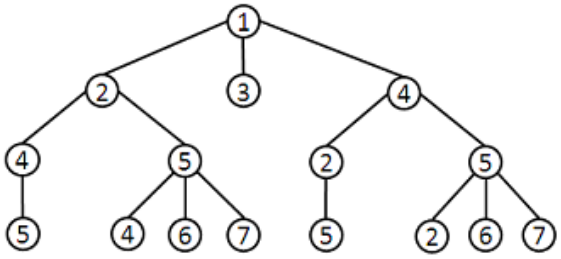

Fig. 5. Search tree of node 1

2) *Revisits along different routes are explored independently*. This mechanism allows us to examine how many different ways the root node can reach other nodes individually, which captures the essence of resilience in terms of multiple-path reachability.
3) *The path is penalized by its length*. It is reasonable to penalize longer paths since they are usually associated with longer delivery time and more transportation cost in supply networks.

As an example, we illustrate in Figure 4 a simple military logistic network, in which node 4 is a main support battalion, node 5 is a forward support battalion, and all other nodes are regular battalions. We show in Figure 5 the search tree of node 1 (with a depth limit of 3). The first two rules described above are implemented in the construction of the search tree. For example, when node 1 goes along nodes $2 \rightarrow 4$, the search path does not get back to itself at depth 3 since cycles are avoided. In fact, the loop is not even closed. On the other hand, node 5 is visited 4 times along nodes $1 \rightarrow 2 \rightarrow 5$, nodes $1 \rightarrow 2 \rightarrow 4 \rightarrow 5$, and so on.

We consider the heterogeneous roles of nodes of different types by assigning them different significance weights, and penalize the path length using a depth-associated penalty factor α ($0 < \alpha < 1$). More precisely, we define the *depth-associated penalty* to be α^{d-1}, where d is the depth from the root node to a node of interest. Whenever a node is reached along a path from the root node, we multiply the significance weight of that node by the corresponding depth-associated penalty, and add it to the resilience score of the root node. In other words, the resilience score of the root node is quantified by the summation of the depth-associated penalized significance weights of all the nodes that the root node visits in its search tree (given a pre-specified depth limit). As for the military logistic network above, if we assign a weight of 2 to the MSB, 1 to the FSB, and 0.2 to the regular battalion, then following the path from nodes $1 \rightarrow 2 \rightarrow 4 \rightarrow 5$, the resilience score of

node 1 increases by $(\alpha^0 \times 0.2 + \alpha^1 \times 2 + \alpha^2 \times 1)$. Further, it is straightforward to compute the network resilience score by summing up the resilience scores of all demand nodes.

Let D denote the set of demand nodes in the network, T_i denote all the nodes in the search tree of node i (a node may occur multiple times along different paths in the search tree), d_j denote the depth from node i to node j following a specific path in node i's search tree, and W_j denote the significance weight of node j. Then the *network resilience score* S can be written as

$$S = \sum_{i \in D} \sum_{j \in T_i} \alpha^{d_j - 1} \times W_j$$

This network resilience score gives rise to a new, more meaningful and finer metric for network resilience analysis. It differentiates the heterogeneous roles of different types of nodes, considers the resilience of all demand nodes, incorporates the reachability to both supply nodes and other demand nodes, includes not only the shortest path but also non-shortest paths, and takes into account the depth-associated penalty. We leave the significance weights, the depth-associated penalty factor, and the depth limit as user-specified tunable parameters such that supply-network designers can adjust them to achieve the desired fit for different applications or different components/paths of the supply network. In addition, an interesting byproduct of our methodology is that we not only obtain the network resilience score but also complete the resilience analysis of each individual demand node.

B. Attachment Strategies

Random-graph and scale-free networks [11] present two most fundamental and characteristically distinct topologies. Many researchers use these two network topologies to study network robustness against disruptions. It is observed that the scale-free network is highly robust against random failures but very vulnerable to targeted attacks while the random-graph network shows better performance against targeted disruptions [12]. In this paper, we develop new attachment strategies to construct various random-graph-based and scale-free-based supply networks, and evaluate their performance using the new resilience metric.

We adopt the multiagent modeling framework. Without loss of generality, we also use the military logistic network as a case study. The military logistic network consists of three types of units: regular battalions, forward support battalions (FSB), and main support battalions (MSB). In a conventional logistic scenario, the MSBs can be regarded as manufacturers, the FSBs as distributors, and the regular battalions as retailers. Both MSBs and FSBs are supply nodes, and regular battalions are demand nodes. As listed in Table III, we build the military logistic network using the same setting and parameters as those used in previous work [6][9].

As noted earlier, it makes more sense to concentrate on the development of new attachment strategies associated with supply nodes only, and let demand nodes enter the network following the pure-random and pure-preferential attachment rules in the random-graph-based and scale-free-based supply network models, respectively. Moreover, we need to consider and maintain the basic functionalities of different types of nodes when developing attachment strategies. We differentiate MSBs from FSBs in a more detailed and more realistic manner. Specifically, we allow an entering MSB to directly connect to battalions, but it has to directly connect to one or more FSBs. This is a sensible assumption to capture that the manufacturer is supposed to directly connect to at least one distributor. When an FSB enters the network, it connects directly to battalions but not to any other FSBs since a distributor is expected to directly connect to retailers instead of other distributors in general. In addition, we avoid attaching a new entering FSB/MSB to a battalion that already directly connects to an FSB or MSB. Further, we include both preferential-attachment and random-attachment rules for each entering FSB/MSB so as to balance the robustness against random failures and targeted attacks.

	Description
Nodes	Start with 10 unconnected battalions, and a new node enters the network at each step
	A total of 990 steps, which generate a network of 1,000 nodes
	The ratio for battalions/FSBs/MSBs is 25:4:1
Edges	An entering battalion initiates 1 edge to an existing node, and the 2nd edge is initiated with a probability of 0.5
	An entering FSB initiates 3 edges, and an entering MSB initiates 5 edges
	Neither multiple edges or loops are allowed when new edges are initiated
	The expected number of edges is 1,800 (average node degree is 3.6)

TABLE III
BASIC SETTING AND PARAMETERS OF THE MILITARY LOGISTIC NETWORK

We list in Table IV three attachment strategies. The first two are conventional random attachment and preferential attachment. The third is the *new supply-specific* attachment that we develop for FSBs and MSBs solely. Finally, as shown in Table V, we create four growth models by applying/combining the three attachment strategies in different ways to investigate how the new supply-specific attachment strategy interplays with the two fundamental network topologies.

IV. Simulation and Analysis

We develop a simulation program, in which we build military logistic networks based on the four growth models and evaluate the resilience of those networks under random disruptions and targeted attacks.

A. Degree Distribution

We first study the degree distribution of nodes in each network to determine how the *new supply-specific* attachment strategy affects the network topology. Figure 6 shows the log-log scatterplot of the number of nodes of degree k w.r.t degree k of the four growth models. Comparing the *New-Random* vs. the *Pure-Random* in Figure 6(a), we can tell the *New-Random*

Attachment Strategies		Description
Random		Attach to a node selected uniformly at random
Preferential		Attach to a node i of degree d_i with the probability $p_i = \frac{d_i}{\sum_j d_j}$
New Supply-specific	FSB	The first edge attaches to a demand node that has the highest degree
		The second edge attaches to a demand node preferentially to its degree
		The third edge attaches to a demand node randomly selected
	MSB	Each of the first two edges attaches to a different FSB randomly selected from the 4 newly deployed FSBs
		The third edge attaches to a demand node preferentially to its degree
		Each of the last two edges attaches to a demand node randomly selected

TABLE IV
THREE ATTACHMENT STRATEGIES

Models	Description
Pure-Random	Apply the random-attachment strategy for all nodes
New-Random	Apply the random-attachment strategy for all demand nodes, and apply the new supply-specific attachment strategy for all supply nodes
Pure-ScaleFree	Apply the preferential-attachment strategy for all nodes
New-ScaleFree	Apply the preferential-attachment strategy for all demand nodes, and apply the new supply-specific attachment strategy for all supply nodes

TABLE V
FOUR GROWTH MODELS (DEMAND = BATTALION, SUPPLY = FSB + MSB)

changes the random-graph topology with quite a few high-degree hubs that are not commonly seen in random-graph networks. For the *New-ScaleFree* vs. the *Pure-ScaleFree* in Figure 6(b), the *New-ScaleFree* also slightly changes the scale-free topology by decreasing the degree of high-degree hubs. Although these changes may not be significant, they help balance the robustness against random disruptions and targeted attacks and improve the overall resilience of the network.

B. Resilience Analysis

To evaluate the network robustness against disruptions, we simultaneously remove a batch of 50 nodes (5% of the total nodes) from the network each time and do it 16 times successively, i.e., until 80% of the total nodes are removed. When a node is removed, all of its edges are removed as well. For random disruptions, we remove the nodes uniformly at random each time, and we run the simulation 20 times for each network. For targeted attacks, we remove the nodes in descending order of the node degree. Each time after the batch of 50 nodes are removed, we measure the resilience of the disrupted network using different resilience metrics. Each data point is the average of 10 networks built from the respective growth model.

First, we evaluate the resilience using the 4 resilience metrics presented in Table II. The first two, i.e., the *supply availability rate* and the *size of LFSN*, are used as they are originally defined. But as discussed earlier, for the *average/maximum supply path lengths in LFSN*, we use the average/maximum shortest supply path lengths of all demand nodes to their *nearest* supply nodes.

As we can see in Figure 7, all four models are fairly resilient against random disruptions. The *New-Random* has almost the same supply availability rate as the *Pure-Random*, but is slightly worse in terms of the size of LFSN. It outperforms the *Pure-Random* in terms of the average/maximum supply path lengths. However, given that the size of LFSN of the *New-Random* is smaller than that of the *Pure-Random*, it is expected that the average/maximum supply path lengths of the *New-Random* are shorter than those of the *Pure-Random*. Similarly, it seems that the *New-ScaleFree* dominates the *Pure-ScaleFree* in terms of the supply availability rate and the average/maximum supply path lengths, but it is inferior to the *Pure-ScaleFree* in terms of the size of LFSN. It turns out that we are not able to arrive at a definite or comprehensive resilience ranking of the four models. It even fails to demonstrate that the scale-free network is more robust against random disruptions than the random-graph networks.

For targeted attacks, as shown in Figure 8(a) and 8(b), both the supply availability rate and the size of LFSN decrease sharply, which reflects that targeted attacks are more damaging than random disruptions to all the four models and that the scale-free networks are even more vulnerable than the random-graph networks. While the *New-Random* shows similar performance to the *Pure-Random*, the *New-ScaleFree* clearly outperforms the *Pure-ScaleFree*.

It is noticed that the supply availability rate and the size of LFSN both decrease monotonically as nodes are removed. However, the average/maximum supply path lengths initially increase and then decrease continuously. That is because the LFSN increasingly gets sparser and leaner, which leads to longer average/maximum supply path lengths. After the sparsity of LFSN reaches some threshold, the LFSN becomes fragmented. Then the average/maximum supply path lengths decrease and keep getting shorter. In addition, from Figure 8(c) and 8(d), one may arrive at a plausible argument that the two scale-free models exhibit better accessibility than the two random-graph models in terms of shorter average/maximum supply path lengths. However, this argument is misleading. As we can see from Figure 8(b), the scale-free models have much smaller LFSN (worse connectivity) than the random-graph models, which results in shorter average/maximum supply path lengths in both scale-free models. In fact, these four resilience metrics are closely correlated. It is hard to piece them together to provide a comprehensive and reliable judgement on the network resilience.

Next we evaluate the network resilience using our proposed metric, i.e., the network resilience score defined in Section III. We assign a significance weight of 2 to each MSB, 1 to each FSB, and 0.2 to each regular battalion. We set the depth limit

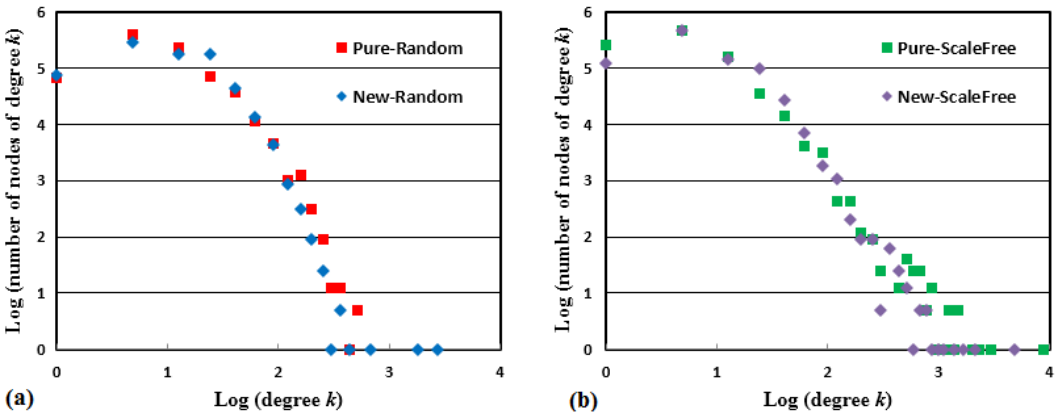

Fig. 6. Log-Log of the degree distribution of the four models

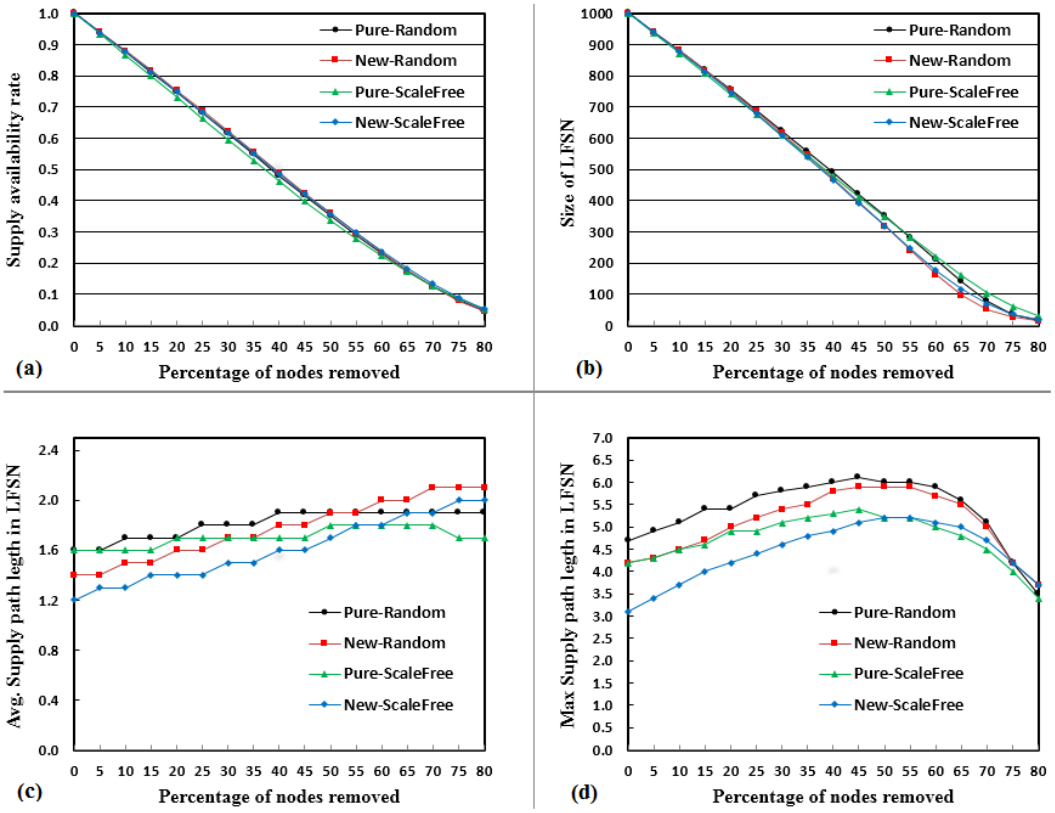

Fig. 7. Responses of the four growth models to random disruptions, plotted as (a) supply availability rate, (b) size of LFSN, (c) average supply path length in LFSN, and (d) maximum supply path length in LFSN

to 3 and the depth-associated penalty factor to 0.5. Figures 9 and 10 illustrate the changes of the network resilience score along with the percentage of nodes removed in the event of random disruptions and targeted attacks, respectively.

In general, networks with high-degree hubs are more resilient since the hubs make the network diameter shorter. As we can see in Figure 9, the resilience scores of the four models vary considerably at the onset. The ranking agrees with the degree-distribution analysis on these models. The *Pure-Random* has the lowest resilience score since hubs rarely occur in random-graph networks. The *New-Random* achieves higher resilience score than the *Pure-Random* since it changes the random-graph topology with quite a few hubs. The *Pure-ScaleFree* reaches the highest resilience score due to its scale-free property. The resilience score of the *New-ScaleFree* is a little bit lower than that of the *Pure-ScaleFree*. That is because the hubs of the *New-ScaleFree* have relatively lower degrees than those of the *Pure-ScaleFree*.

As shown in Figure 9, four models are all fairly resilient to random failures. The resilience scores show alignments

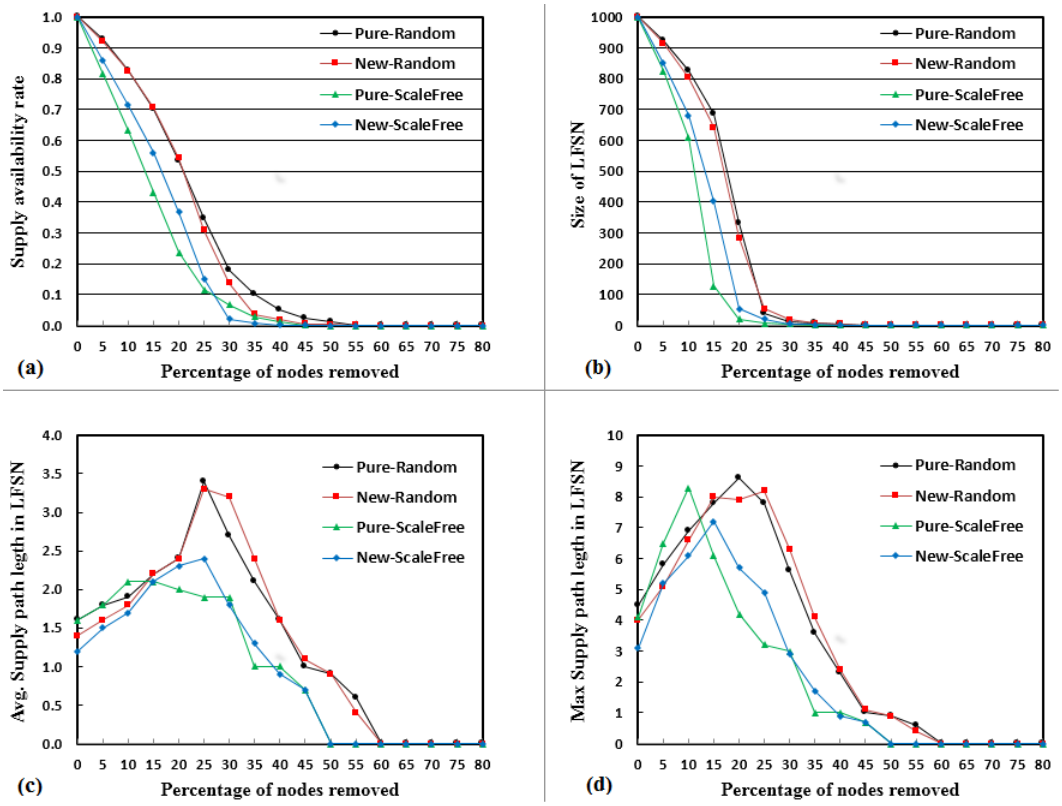

Fig. 8. Responses of the four growth models to targeted attacks, plotted as (a) supply availability rate, (b) size of LFSN, (c) average supply path length in LFSN, and (d) maximum supply path length in LFSN

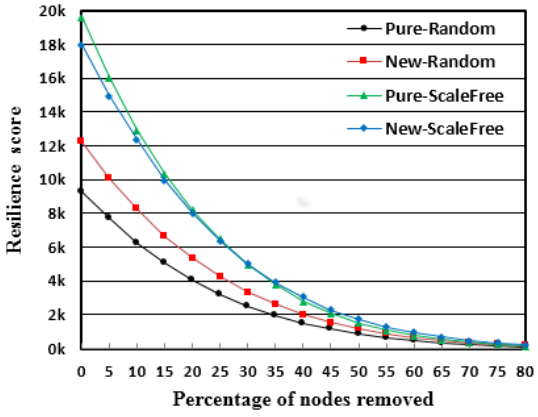

Fig. 9. Resilience scores of the four growth models to random disruptions

with our observation that scale-free networks are much more robust than random-graph networks under random disruptions. The *New-Random* consistently outperforms the *Pure-Random*. The resilience scores of the *New-Random* are 32.6%, 32.5%, and 35.1% higher than those of the *Pure-Random* when 10%, 20%, and 40% of nodes are removed, respectively. The *New-ScaleFree* has almost the same performance as the *Pure-ScaleFree*. The *New-ScaleFree* is slightly worse when less than 20% of nodes are removed, but gets a little better when more than 35% of nodes are removed.

Our network resilience scores support our observation that the damage due to targeted attacks is devastating to all the four models. As shown in Figure 10, when only 5% of nodes are removed, the resilience scores of the *Pure-Random*, the *New-Random*, the *Pure-ScaleFree*, and the *New-ScaleFree* drop 62.5%, 72.9%, 88.3%, and 84.8%, respectively. The scale-free networks are more vulnerable and become inferior to the random-graph networks immediately in spite of great advantages at the onset. While the *New-Random* shows slightly better performance than the *Pure-Random*, the *New-ScaleFree* obviously beats the *Pure-ScaleFree*. The resilience scores of the *New-ScaleFree* are 18.9%, 36.7%, 32.2%, and 18.9% higher than those of the *Pure-ScaleFree* when 5%, 10%, 15%, and 20% of nodes are removed, respectively.

Further, we can aggregate the random-disruption resilience score with the targeted-attack resilience score using different weights. Considering that targeted attacks are much more damaging than random disruptions, it is reasonable to assign a higher weight to the targeted-attack resilience score to favor stronger robustness against targeted attacks. We assign a weight of 0.2 to the random-disruption resilience score and 0.8 to the targeted-attack resilience score, and illustrate the aggregated resilience scores in Figure 11. As we can see, the *New-Random* obviously beats the *Pure-Random*, the scale-free networks outperform the random-graph networks, and the *New-ScaleFree* has the best performance overall.

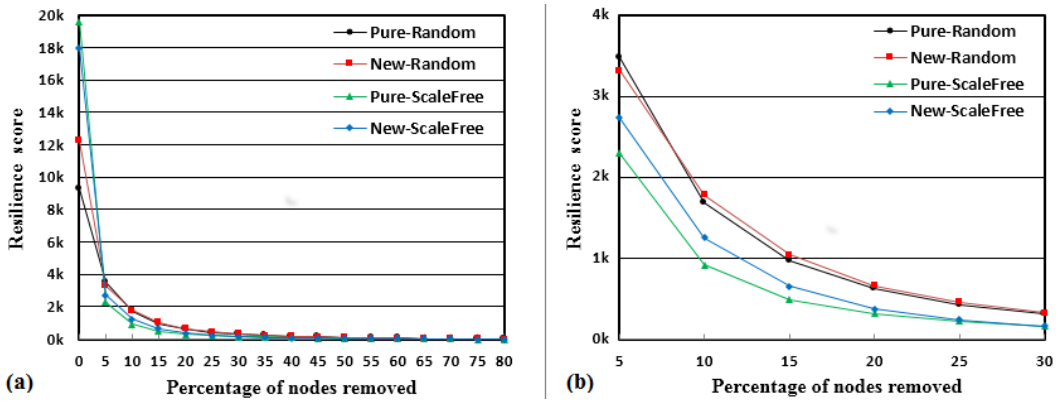

Fig. 10. Resilience scores of the four growth models to targeted attacks, plotted as (a) 0-80 percent of nodes removed, and (b) 5-30 percent of nodes removed

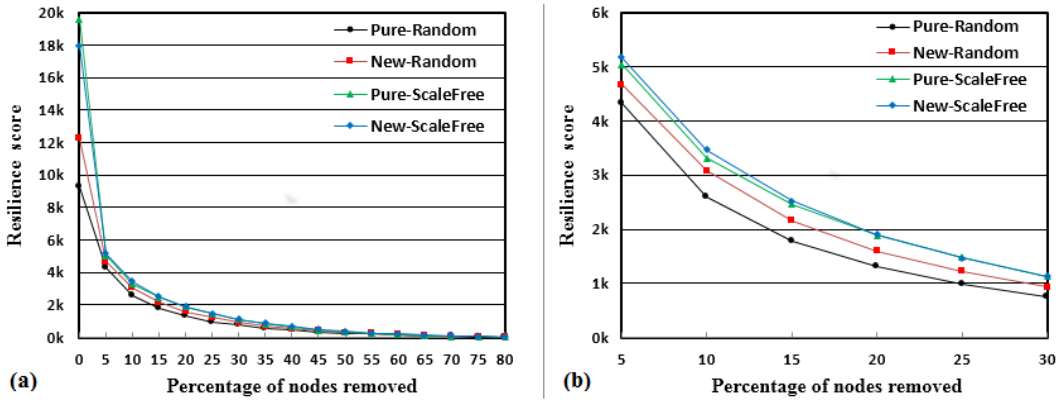

Fig. 11. Aggregated resilience scores of the four growth models under random disruptions and targeted attacks, plotted as (a) 0-80 percent of nodes removed, and (b) 5-30 percent of nodes removed

V. Conclusion and Future Work

In this paper, we exploit the multiple-path reachability of each demand node to other nodes in the supply network, and propose a novel network resilience metric. We also develop new attachment strategies that differentiate the heterogeneous roles of different types of nodes. We incorporate them into two fundamental network topologies, and analyze the network resilience against random disruptions and targeted attacks. The experimental results demonstrate the validity of our resilience metric and the effectiveness of our growth model.

For the future work, it is desirable to take into account inventory levels, backorders, total costs, and inventory reassignment to arrive at a more realistic and more robust growth model. One promising direction is to convert those factors into the weights on the edges of the supply network. The approach introduced in this paper can be easily extended to weighted networks. Another interesting direction is to investigate the cascade-based attack vulnerability on supply networks and/or adapt this approach to other complex networks.

References

[1] H. Sun and J. Wu, "Scale-free characteristics of supply chain distribution networks," *Modern Physics Letter B*, vol. 19, no. 17, pp. 841–848, 2005.

[2] Q. Xuan, F. Du, Y. Li, and T. Wu, "A framework to model the topological structure of supply networks," *IEEE Transactions on Automation Science and Engineering*, vol. 8, no. 2, pp. 442–446, 2011.

[3] P. R. Kleindorfer and G. H. Saad, "Managing disruption risks in supply chains," *Production and Operations Management*, vol. 14, no. 1, pp. 53–68, 2005.

[4] B. Tomlin, "On the value of mitigation and contingency strategies for managing supply chain disruption risks," *Management Science*, vol. 52, pp. 639–657, 2006.

[5] R. Criado, J. Flores, B. Hernandez-Bermejo, J. Pello, and M. Romance, "Vulnerability of complex networks under random and intentional attacks," in *CMMSE*, 2004, pp. 1–8.

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

[7] A. Nair and J. M. Vidal, "Supply network topolgy and robustness against disruptions - An investigation using multiagent model," *Int. J. Production Research*, vol. 49, no. 5, pp. 1391–1404, 2011.

[8] H. Chen and A. Lin, "Complex network characteristics and invulnerability simulating analysis of supply chain," *J. of Networks*, vol. 7, no. 3, pp. 591–597, 2012.

[9] 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 J.*, vol. 5, no. 1, pp. 28–39, 2011.

[10] Y. Kim, Y. Chen, and K. Linderman, "Supply network disruption and resilience: A network structural perspective," *J. of Oper. Manag.*, vol. 33, no. 34, pp. 43–59, 2015.

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

[12] R. Albert, H. Jeong, and A. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 27, pp. 378–382, 2000.