Analyzing the Resilience of Complex Supply Network Topologies against Random and Targeted Disruptions

Kang Zhao, *Member, IEEE,* Akhil Kumar, *Member, IEEE,* Terry P. Harrison, and John Yen, *Fellow, IEEE*.

***Abstract*—In this paper, we study the resilience of supply networks against disruptions and provide insights to supply chain managers on how to construct a resilient supply network from the perspective of complex network topologies. Our goal is to study how different network topologies, which are created from different growth models, affect the network's resilience against both random and targeted disruptions. Of particular interest are situations where the type of disruption is unknown. Using a military logistic network as a case study, we propose new network resilience metrics that reflect the heterogeneous roles (e.g. supply, relay, and demand) of nodes in supply networks. We also present a hybrid and tunable network growth model called Degree and Locality-based Attachment (DLA), in which new nodes make connections based on both degree and locality. Using computer simulations, we compare the resilience of several supply network topologies that are generated with different growth models. The results show that the new resilience metrics can capture important resilience requirements for supply networks very well. We also found that the supply network topology generated by the DLA model provides balanced resilience against both random and targeted disruptions.**

***Index Terms*—Complex network, growth model, random disruption, targeted disruption, resilience, supply network topology.**

I. Introduction

OUR daily life relies on the operations of supply chains, which distribute goods and services, such as groceries, water and electricity, from suppliers to consumers. With globalization and the development of technology, structures of supply chains are constantly evolving and becoming more complex, as new entities join the system and new connections form between them. As a result, today's supply chain systems are shifting away from the "chain" structure. Instead, they often feature a network of interacting *entities*, such as manufacturers, distributors, and retailers in a distribution network. In a military logistics network the corresponding entities might be supply units and battalions. Since entities may take different forms in various application domains, we refer to them simply as *nodes* in a network. Many researchers have suggested that supply chains should be considered as supply networks [1], and that the analysis and design of supply chains should incorporate the concepts of complex systems, especially dynamic complex networks [2].

Meanwhile, supply networks, especially large or global ones, often face disruptions, such as natural disasters, economic recessions, unexpected accidents, or terrorist attacks. A disruption may initially attack or disable only one or few nodes in the system, but its impact may propagate further, sometimes even with amplification [3], among inter-connected nodes. Such disruptions will thus affect the normal operations of many other nodes. Occasionally, failures in a small portion of the system may cause the catastrophic failure of the whole system [4]. Such events may seriously disrupt or delay the flow of people, goods, information and funds, and thus lead to higher costs or reduced sales [5]. A supply network's *resilience against disruptions* lies in its ability to maintain operations and connectedness under the loss of some structures or functions [6]. Therefore, building resilient supply networks has high priority, and it has attracted the attention of managers, shareholders, and researchers [7].

Traditional research on supply chain disruptions often adopts the risk management perspective and focuses on strategies and technologies to identify, assess, and mitigate risks and problems caused by disruptions [5], [7], [8]. Previous research [9] has revealed that the *topology* of a supply network has great impact on its resilience. In other words, the way individual nodes are organized and connected, and the resulting network structure, e.g., random, hierarchical, etc., will affect the supply network's performance when disruptions occur. However, we found little research following this direction. In this paper, we adopt the complex-network view of supply chains and study the resilience of supply networks from a topological perspective. Assuming the homogeneous roles of nodes, the existing literature of network attachment strategies is often limited in application as the resilience of a supply network is measured inappropriately. By contrast, because we take into consideration the heterogeneous roles of nodes when evaluating supply network resilience, our heuristic strategy is more general and effective than those described in extant literature.

The remainder of the paper is organized as follows. We first briefly review related research. Using a military logistic network as a case study, we propose a new taxonomy of resilience metrics for supply networks. Following that, a new network growth model is introduced. Through computer simulations, the resilience of the supply network topology generated with

K. Zhao and J. Yen are with the College of Information Sciences and Technology, the Pennsylvania State University, University Park, PA 16802, USA, e-mail: kangzhao@psu.edu, jyen@ist.psu.edu.

A. Kumar and Terry P. Harrison are with the Department of Supply Chain and Information Systems, Smeal College of Business, the Pennsylvania State University, University Park, PA 16802, USA, e-mail: akhilkumar@psu.edu, tharrison@psu.edu

The work of A. Kumar was supported by the Smeal College of Business through a summer research grant.

the new growth model is evaluated and compared with the topologies of other networks. Finally, the paper will give a conclusion and discuss future research directions.

II. Related Work

The literature contains ways to evaluate and optimize the resilience of networks [10], [11]. However, these network optimization problems are generally NP-hard [12], [13]. As a result, when the network is complex and evolving, finding the optimal network configuration is computationally expensive. While techniques, such as simulated annealing [14], genetic algorithms [15], and heuristic procedure [16], have been used in the design of supply chain and distribution networks, this stream of work focuses mainly on location of facilities, capacity planning and minimizing transportation costs, instead of the resilience of supply networks when some nodes fail to operate. Most of the related work on resiliency also does not consider the twin goals of maintaining resilience under random failures and targeted attacks.

Moreover, the optimization-based approaches are generally centralized in nature, because a supply network manager is required to have complete knowledge and control of the whole network to optimize it. However, it is often difficult to meet this requirement in the real world. Researchers have found that the structure of a supply network often emerges from the distributed decisions of individual nodes, regardless of the centralized nature of the design [17], because some heuristic strategies are often used when a node decides which nodes to connect to. Further, a manager only knows and controls the network of its corporation or organization, but the supply network at a macro level consists of networks from different corporations or organizations. Corporations' or organizations' optimization of their own networks may not necessarily lead to a globally resilient network. Therefore, managers' awareness of how network design strategies at the micro level affect the resilience of the whole supply network at the macro level is also important.

At the outset, we also distinguish our work from that in the area of social network theory. Social network theory views the attributes of individuals as less important than their relationships and ties with other actors within the network. It has been useful for explaining many real-world phenomena, but it leaves less room for individual agency, so much of it rests within the structure of the network(s) that they are part of. Some sample references in this area are [18], [19], [20].

Complex networks are defined as networks whose "structure is irregular, complex and dynamically evolving in time" [21]. They are ubiquitous in nature and society. Examples include social networks, the Internet, biological cellular networks, etc. Research has revealed topologies of many real-world networks [22], [23]. For example, some supply networks have scale-free topologies [24], which feature few high-degree hub nodes and power-law degree distributions. The research on complex network growth models reveals distributed strategies and heuristics that underlie many real-world networks.

Network growth models study the evolution of complex networks by specifying how new nodes connect with existing ones through a process of "attachment". As new nodes enter a network, the network topology emerges from the distributed attachment decisions of individual nodes. Different growth models follow different attachment rules and lead to different network topologies. For instance, the *random-attachment model* randomly connects two pair of nodes with a pre-defined probability and generates an ER random network [25]. The growth models are often simple, yet they can produce complex network topologies [26]. For example, in the *preferential-attachment model* [23], the probability that a new node attaches to an existing node is proportional to the existing node's degree. This leads to the well-known scale-free topology that can explain many real-world networks, such as the Internet. It is also one of the key underlying principles that guides the evolution of supply networks [27].

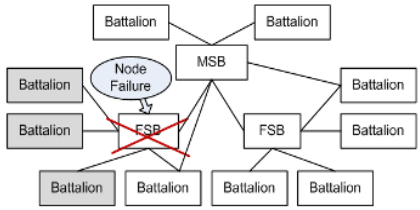


Fig. 1. A hierarchical military supply chain

Specifically, when the resilience of complex networks against errors and attacks was analyzed, it was found that scale-free networks offer high tolerance against random failures. However, networks with scale-free topologies are vulnerable to disruptions that target the most connected nodes [28]. Thadakamalla et al. introduced the topological perspective into the study of supply network resilience [9]. It was argued that traditional hierarchical supply chains, in which an edge can only exist between two units of different types, are vulnerable to disruptions. A military logistic network, consisting of *battalions, forward support battalions (FSB) and main support battalions (MSB)* was used as an example. In the hierarchical supply network in Fig.1, the failure of a single FSB disconnects about 30% of the battalions from supplies. Therefore, the authors proposed a new network growth model (henceforth referred to as the **Hierarchy+** model) that extends the hierarchical model by allowing edges between nodes of the same type. However, it still arbitrarily creates more edges for support units than for battalions. The supply network generated by this model is called the Hierarchy+ network. Computer simulations showed that Hierarchy+ supply networks have satisfactory resilience against disruptions. Our study will extend this research further.

III. Proposed Approach

In this section, we first present a taxonomy of resilience metrics for supply networks. The new metrics reflect the heterogeneous roles (such as supply, relay and demand) of different types of nodes in supply networks. We then introduce a new hybrid and tunable supply-network growth model to generate a new supply network topology, and evaluate multiple supply network topologies' resilience against disruptions using the new metrics.

TABLE I
SOME GENERIC METRICS FOR NETWORK RESILIENCE

Name	Brief description
Size of the LCC	The number of nodes in the LCC of a network.
Average path length in the LCC	The average of the shortest path length between any two nodes in the LCC of a network.
Maximum path length in the LCC	The maximum path length between any two nodes in the LCC of a network.

A. New Resilience Metrics

In complex network research, the evaluation of resilience focuses on the largest connected component (LCC), in which there is a path between any pair of nodes. Existing resilience metrics are generic topological metrics, including size of the LCC, average path length in the LCC, and the maximum path length in the LCC. Table I explains these metrics.

Applying these generic metrics to the evaluation of supply network resilience is largely based on the assumption that roles and functions of nodes in a supply network are homogeneous. However, in real-world supply networks, different types of nodes play different roles. Often times, the normal functioning of downstream nodes may depend on the operations of upstream nodes. In addition, one of the fundamental purposes of a supply chain is to connect suppliers with consumers. This type of "Origin-Destination" connection is the prerequisite for the flow of goods or services [29]. As a result, preserving this type of connection in disruptions is critical for maintaining the operations of the whole supply network.

In the military logistic network in [9], support units, such as FSB and MSB, play a different role from regular battalions. MSBs are supply providers and regular battalions are consumers. FSBs act as distribution centers and forward supplies to consumers. Battalions often cannot perform their duties without supplies. Therefore, an LCC, in which there is no support unit, or where battalions are far from support units, should not be considered resilient because there is no or limited supply flow in such a sub-network. Similarly, the distance between battalions and their support units is generally more important for a resilient supply chain than the distance among battalions. Therefore, the heterogeneous roles (as supply and demand nodes) of different types of nodes in a supply network must be considered when evaluating the resilience of a supply chain.

The proposed taxonomy consists of system- and topology-level metrics. We will use the military logistic network as an example to illustrate our metrics.

First, we introduce *availability* as a critical resilience metric for supply networks, because it shows whether nodes in the supply network can get the supplies that they need to maintain normal operations. At the topological level, availability is interpreted as *supply availability rate*, which is the percentage of demand nodes that have access to supply nodes. In the context of the military supply network, the supply availability rate is the percentage of battalions that have access to MSBs.

Consider the military logistic network as an undirected graph G with node set V and edge set E, where $e_{i,j} \in E$ denotes an edge between nodes $v_i, v_j \in V$. As shown in (1), V is also the union of two non-overlapping subsets of battalions (node set V_B) and support units (node set V_S).

$$V = V_B \cup V_S, where\ V_B \cap V_S = \phi \tag{1}$$

Then the set of battalions that have access to support units in the network is defined by (2), where $p_{i,j}$ denotes a path between nodes v_i and v_j. Thus V_{BS} is the set of battalions that have access to support untis through the supply network. Consequently, the supply availability A for a military logistic network is defined as the ratio between the cardinalities of sets V_{BS} and V_B, as shown in (3) below.

$$V_{BS} = \{v_i \in V_B \mid \exists v_j \in V_S :\ \exists p_{i,j}\} \tag{2}$$

$$A = |V_{BS}| \,/\, |V_B| \tag{3}$$

Second, the *connectivity* of the system is also important. Topological connectivity is often measured by the size of the **LCC**. In a supply network whose LCC contains all nodes, a node can access any other node through the network. On the contrary, if a supply network's LCC contains, say, only 40% of all nodes, the network may be partitioned into several isolated sub-networks, which means flows of goods or services are limited to within a smaller sub-network. Here, we extend the metric of LCC and use size of the largest *functional* sub-network (**LFSN**) instead. For the military logistic network, a functional sub-network $V_m \in V_{sub}$ (V_{sub} is the set of all functional sub-networks) satisfies the requirements in (4). Thus the LFSN is the V_m with the largest size (5).

$$\forall v_i, v_j \in V_m : \exists p_{i,j}\ and\ \exists v_k \in V_m : v_k \in V_s \tag{4}$$

$$V_L = \{V_m \in V_{sub} | \forall V_n \in V_{sub} (n \neq m) : |V_m| \geq |V_n|\} \tag{5}$$

The difference between the old and the new connectivity metrics is that there must be at least one supply node in the LFSN. A sub-network of a military logistic network cannot function and maintain the flow of supplies without a support unit in it. When nodes fail during disruptions, a supply network that features a larger functional sub-network can maintain a higher level of connectivity and is considered more resilient.

We also describe two metrics for *accessibility* of supplies. Higher accessibility means that supplies are closer to consumers, and they can receive them at lower cost or in lesser time. As mentioned earlier, from the perspective of supply network resilience, the distance between a pair of demand nodes is not as important as that between a supply and a demand node. Consequently, we propose *supply path length* as the length of the path between a demand and a supply node (denoted by $dist(x, y)$). Thus, the *average supply-path length* in the LFSN is the average of the minimum supply-path lengths between all pairs of supply and demand nodes in the LFSN (see Equation 6). Moreover, the *maximum supply-path length* in the LFSN is the longest supply-path length between any supply and demand pair in the sub-network (see Equation 7). Naturally, shorter average and maximum supply-path lengths mean better average- and worst-case accessibility.

$$C_{avg} = \frac{\sum_{v_i \in {V'}_S} \sum_{v_j \in {V'}_B} dist(v_i, v_j)}{|{V'}_S| * |{V'}_B|}, \quad \text{where } {V'}_S = V_L \cap V_S, {V'}_B = V_L \cap V_B \tag{6}$$

TABLE II
TAXONOMY OF THE NEW RESILIENCE METRICS FOR SUPPLY NETWORKS

Name	Topology-level metric	Description
Availability	Supply availability rate	The percentage of demand nodes that have access to supplies (Equation 3).
Connectivity	Size of the largest functional sub-network (LFSN)	The number of nodes in the LFSN, in which there is a path between any pair of nodes and there exists at least one supply node (Equation 5).
Accessibility	Average supply-path length in the LFSN	The average of the shortest supply-path length between all pairs of supply and demand nodes in the LFSN (Equation 6).
	Maximum supply-path length in the LFSN	The maximum path length between any pair of supply and demand nodes in the LFSN (Equation 7).

$$C_{max} = max(dist(v_i, v_j)), \text{where } v_i \in V'_S, v_j \in V'_B \quad (7)$$

However, there is a caveat when using the two accessibility metrics. In general, the comparison between the average and maximum supply-path lengths of different supply networks (or sub-networks) are fair and meaningful only when the networks are of similar sizes. We have to take the sizes of the LFSNs into consideration because a larger supply network with more nodes will often have longer average paths than a network with similar topology but fewer nodes. The existence of a few supply nodes that are far away from some demand nodes may increase the average and maximum supply-path length in a large sub-network. We will illustrate this with our experiments in Section IV.

It is also possible to combine these metrics into a single objective function in order to compare the overall performance of different supply networks more directly. However, we decided to use multiple metrics instead of a single objective function to gain a better understanding of a supply network's performance from different perspectives. When the context in which a specific supply network operates is known, one is in a better position to determine a single objective function.

Table II summarizes our new metrics. We believe they can more accurately measure supply network resilience, and are more systematic and realistic as compared to the metrics in previous work such as [9].

B. New Hybrid Growth Model (DLA)

As noted earlier, the topology of a complex network depends on its growth model. In the context of supply networks, growth models represent distributed connection strategies that a node uses to decide which other nodes to connect to. For example, in the preferential-attachment model [23], new nodes prefer to connect to existing high-degree nodes. Thus, they can access other nodes efficiently and at lower cost. The random-attachment model is a strategy that randomly selects nodes to attach a new node to. The Hierarchy+ [9] model allows connections between nodes at the same level in the hierarchy.

While Hierarchy+ uses ad-hoc attachment rules for different types of nodes, we propose a more general model called *Degree and Locality-based Attachment (**DLA**)* growth model.

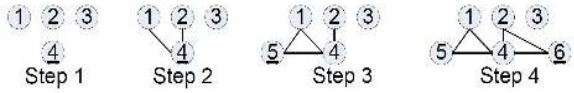


Fig. 2. An example of the DLA growth model. ID for the new node is underscored.

In this model, a node considers not only the connectedness, but also the distance of a candidate node when establishing connections. This model does not require special attachment rules for different types of nodes and may be applied to other types of complex networks in general. The DLA growth model starts with a small number of disconnected nodes, say N_0. We assume that when a new node enters the system it initiates edges to connect to k existing nodes ($k < N_0$). The *attachment rules* for a new node are as follows:

The first edge connects to a node i of degree k_i with probability P_i where:

$$P_i = {k_i}^u / \Sigma_i {k_i}^u, \text{ where } u >= 0 \quad (8)$$

The remaining edge(s) will connect to a node j, which has a shortest distance of d_j to the new node, with probability P_j where:

$$P_j = {d_j}^{-r} / \Sigma_j {d_j}^{-r}, \text{ where } r >= 0 \quad (9)$$

Equation (8) describes the degree-based attachment preference of the first edge of a new node, and u is the customizable degree preference parameter. Given the same u, the new node will prefer connecting to existing higher degree nodes. When $u = 0$, the rule is similar to that of random networks, as every other node in the network has the same probability of being connected with the new node. When $u = 1$, the connection occurs by the preferential-attachment model of a scale-free network. A larger u gives even higher P_i to high-degree nodes. Therefore, as u becomes larger, it is more likely that the new node will connect to an existing node with higher connectedness. It is worth noting that, at the very beginning of the growth process, all the existing nodes are disconnected from each other, i.e., $\forall k_i : k_i = 0$. In this case, when the first new node enters the system, it will randomly choose an existing node to connect to.

On the other hand, Equation (9) gives preference to locality for the attachment of a new node's remaining edges if it is allowed to initiate more than one connection. As the node is already connected to the network through the first edge, we can then calculate the shortest distances from this node to all the other nodes. In (9), the non-negative integer distance d_j and the customizable locality preference parameter r constitute the attachment rule for the remaining edges of a new node. Given the same r, candidate nodes with smaller d_j will have a higher probability of being connected with new nodes. In other words, *the new node prefers nodes in its neighborhood over distant nodes*. When $r = 0$, every other node in the network has the same probability of being connected by the new node as in a random network. A larger r will reinforce the relative advantage of nearby nodes, while a smaller r will increase the new node's chance of connecting to more distant nodes. Additionally, in the special case of a sparse network, where

no existing node is connected to the new node via any path, a node is chosen randomly. Lastly, and for obvious reasons, multiple links to the same node are disallowed. Also, because a new node does not need the exclusive access to other nodes when establishing connections, deadlocks will not happen in our model.

Fig. 2 illustrates a simple example for the DLA growth model with $u = 1$ and $r = 1$. In this example, each new node will establish two edges. Initially, the network starts with three disconnected nodes 1, 2, and 3. Node 4 is the first new node that enters the system and it randomly chooses two nodes to connect to, say, nodes 1 and 2. When node 5 comes in, its first edge will prefer existing high degree nodes, and thus node 4 has the highest probability to be chosen. The second edge of node 5 will prefer nodes that are close to it. Nodes 1 and 2 then have equal probability of being chosen. In this example, node 5 chooses node 4 for the first edge and node 1 for the second. Similarly, node 6 connects to nodes 4 and 2 in Step 4. As more nodes are added, a DLA network will emerge from this attachment process. As noted above, the "hybrid" DLA is more general than Hierarchy+. In fact, the Hierarchy+ model is a special case of the DLA growth model and can be realized with a suitable choice of parameters. In the next section, we will evaluate the resilience of DLA networks, and compare it with other topologies using the new resilience metrics.

IV. Experimental Results

As it is very difficult to construct a real-world supply network and generate disruptions within it to evaluate its resilience, we rely on computer simulations. In this section, we describe our method for evaluating and comparing the resilience of different supply network topologies using simulation. The results from the simulation of a military logistic network are illustrated and discussed.

A. Simulation Setup

We performed a discrete event simulation study based on the method described in [30]. The main steps are: design a valid conceptual model, develop a program so simulate the model, design and run experiments, and perform output data analysis. We simulated the military logistic network example in [9], so as to directly compare Hierarchy+, which is designed for military logistic networks, with other topologies. The network is based on a real-world military logistic system. It consists of 1000 nodes and 1815 edges (the average degree is about 3.6). Battalions, FSB and MSB units enter the system following the ratio of 25:4:1, which was estimated from a real-world military logistic system. In other words, for every 25 newly-deployed battalions, we added 4 FSBs and then 1 MSB into the supply network. In reality, other deployment schemes, such as deploying all support units before any battalions are deployed, are also possible and may lead to different supply network topologies. However, we choose this scheme to ensure a consistent comparison with the previous work. We will then compare the resilience of supply networks with *Random, Scale-free, Hierarchy+ and DLA topologies*. Each topology is generated with the corresponding growth model and the military logistic network configuration. For the DLA growth model, we use $u = 1/2$ and $r = 2$.

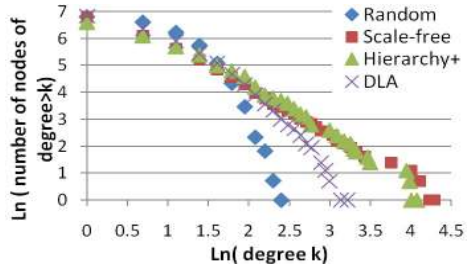
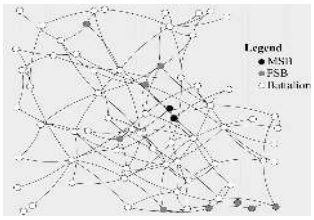


Fig. 3. Cumulative degree distributions for supply networks with 1000 nodes.

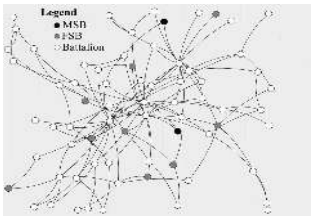
Fig. 3 illustrates the log-log degree distributions of four simulated 1000-nodes networks. A scale-free network is characterized by the famous power-law distribution. Fig. 4(a), 4(b), and 4(c) show the snap shots of simulated small-scale supply networks with random, scale-free and DLA topologies (the legend is shown alongside). The DLA supply network features some hub nodes and also some highly connected clusters, but connections to the hubs are not as concentrated as in the scale-free network.

The next step is to simulate disruptions. The research on complex network resilience often studies two types of disruptions based on node removals: *random and targeted disruptions*. Random disruptions correspond to natural disasters (e.g., earthquakes and hurricanes), accidents (e.g., fires and power outrage), and unexpected economic events (e.g., recessions and bankruptcy) in which every node has similar probabilities of being disrupted. We simulate such disruptions by randomly choosing nodes and removing them from the network, so that each node has the same probability of being removed. On the other hand, in *targeted disruptions*, "important" nodes are more likely to fail than unimportant ones. Such failure might result from, for example, terrorist and military attacks, which are aimed at critical nodes in the system, such as network hubs, to inflict maximum damage.

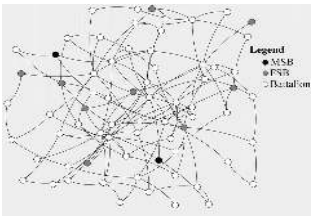
Among the many metrics to measure a node's importance in a network, we choose the widely-used *degree centrality* in line with previous research [9], [28]. In other words, we assume that the higher the node degree is, the more important it is. The reason for picking degree as the indicator of importance is that it is easier for attackers to find than other metrics. High-degree nodes are often more visible because they are in contact with many other nodes [31]. Other centrality measures, such as closeness, betweenness, and eigenvector centrality [32], require knowledge of the network topology, which is usually difficult for attackers to obtain. To simulate targeted disruptions, we remove nodes in the order of decreasing node degree, and update the degrees of all nodes after each removal. In addition, edges that are connected to the removed nodes are also removed in both simulation scenarios. While simulating disruptions with node removals has limitations (e.g., it assumes that disruptions will stop a node's operation, while in the real world an entity may only lose some of its capacities after disruptions), a great number of previous studies on complex network have shown that this simple and intuitive approach can



(a) A 70-node Random supply network.



(b) A 70-node Scale-free supply network.



(c) A 70-node DLA supply network with $u = 1/2$, $r = 2$.

Fig. 4. Simulated supply networks with various topologies.

TABLE III
95% CONFIDENCE INTERVALS FOR SUPPLY AVAILAIBILITY RATES(%) IN RANDOM DISRUPTIONS

Nodes removed	Random	Scale-free	Hierarchy+	DLA
5%	91.7-92.3	94.0-94.3	92.5-93.3	94.1-94.5
10%	86.1-86.8	88.0-88.6	84.7-85.9	88.5-89.2
15%	80.8-81.5	82.2-82.6	76.5-77.9	82.7-83.3
20%	74.7-75.6	75.7-76.3	69.4-71.0	76.7-77.5
25%	69.1-70.0	69.4-70.2	62.3-64.0	70.3-71.1
30%	63.1-64.0	63.2-64.2	54.0-57.1	64.0-65.1
35%	57.2-57.9	56.1-57.8	47.9-50.2	57.1-58.4
40%	51.0-51.8	49.7-51.2	41.5-43.6	50.4-51.8

help to reveal important properties on a network's resilience against disruptions [9], [28].

In our simulation, we remove 50 nodes (5% of the total nodes) between successive observations to correspond to previous research [9] and to balance the simulation running time and the granularity of the results. During node removal, we track the resilience metrics for each network topology. In the end, we compare the networks' resilience using the metrics. To ensure a fair comparison, each network has the same number of nodes and edges. On average, each new node initiates 1.8 new edges to correspond with the military logistic network in [9]. Thus the total number of edges will be around 1800 and the average degree is 3.6 edges per node.

B. Simulation Results for Random Disruptions

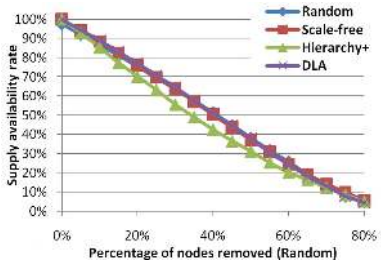
Fig. 5 shows the responses of the four network topologies to random disruptions. The horizontal axes denote the percentage of nodes that were removed, while the vertical axes are values of the topology-level supply network resilience metrics from Table II. The graphs are not extended beyond the 80% mark on the horizontal axis because they converge after this point. Fig. 5(a) and 5(b) show that for all the four network topologies, supply availability rate and the size of the LFSN decrease almost linearly as nodes are removed from the network. In terms of availability and connectivity, the performance of random, scale-free and DLA networks is very close, while the resilience of Hierarchy+ is slightly worse than of the other three, as indicated by its steeper slope. The 95% confidence intervals for the four networks' availability in Table III confirm our observation that Hierarchy+ falls a little behind in terms of maintaining supply availability. In addition, since the four networks are similar in the size of their LFSN, it allows us to make a fair comparison of accessibility next.

Nevertheless, the accessibility metrics in Fig. 5(c) and 5(d) point toward different conclusions. In general, when nodes are removed, the accessibility of supplies worsen because the average and maximum supply-path lengths in the LFSN increase as more nodes are removed. This is intuitive, since disruptions make it increasingly difficult for demand nodes to receive supplies. At the 60% node removal point, almost all supply-path lengths reach their peak values and then start to fall. The decreases are most likely caused by the fragmentation of the network and the isolation of "hard-to-reach" demand nodes.

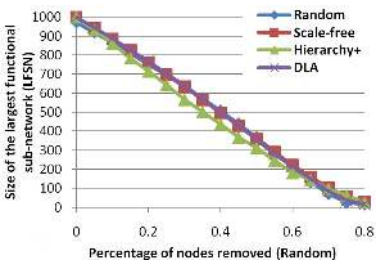
Before disruptions happen, the network is well-connected. A demand node may have multiple supply paths available, leading to different supply nodes. When some nodes fail, supply can still reach many demand nodes through alternative, albeit longer, supply paths. The existence of those "hard-to-reach" demand nodes that are still connected in the LFSN leads to the increase in supply path length. However, the longer a demand node's supply path is, the more this demand node depends on other nodes to receive supplies. As each node has the same probability to fail in random disruptions, the more dependent a demand node is, the more likely it is to get disconnected from supplies when additional nodes are removed. Thus a "hard-to-reach" demand node has higher probably to be isolated from the LFSN as more nodes are removed. After more than 60% of node removal, many "hard-to-reach" demand nodes are no longer in the LFSN. Instead, the remaining demand nodes in the LFSN are close to supply nodes. Meanwhile, the supply network becomes very fragmented. The LFSN only has fewer than 200 nodes (20% of the original size). We believe the smaller LFSN and the disappearance of "hard-to-reach" demand nodes in the LFSN contribute to the decrease in supply path length when more than 60% nodes are removed.

In any case, the supply-path lengths of Hierarchy+ are the shortest, indicating that the Hierarchy+ network is able to preserve good supply accessibility. Even when 40-50% of nodes are removed, there is no dramatic increase in its supply-path length. On the other end of the spectrum, accessibility in the random network has the most serious degradation. The DLA is better than the Random network, but not as good as the Scale-free network, on accessibility.

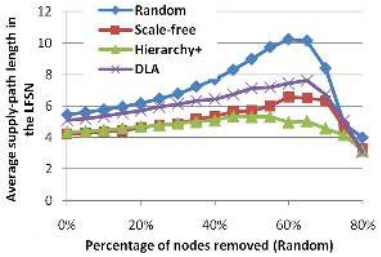
Considering all resilience metrics, we believe the Hierarchy+ supply network is generally the most resilient against random disruptions. The resilience of other three network topologies against random disruptions can be ranked in a descending order as Scale-free, DLA and Random networks.



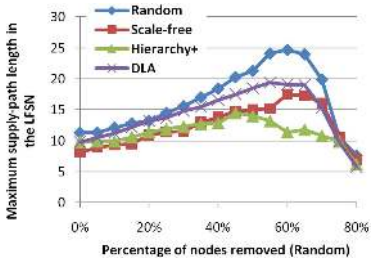
(a) Supply availability rate



(b) Size of the LFSN.

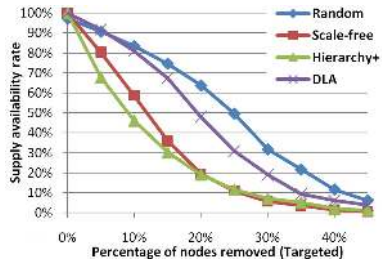


(c) Average supply-path length in the LFSN.

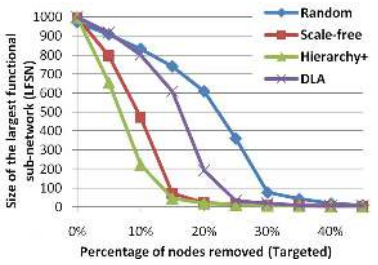


(d) Maximum supply-path length in the LFSN.

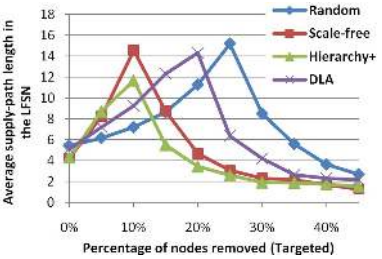
Fig. 5. The four networks' responses to random disruptions. Each data point is the average of 20 runs.



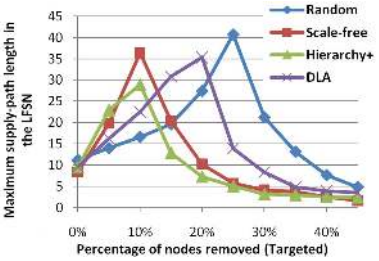
(a) Supply availability rate



(b) Size of the LFSN.



(c) Average supply-path length in the LFSN.



(d) Maximum supply-path length in the LFSN.

Fig. 6. The four networks' responses to targeted disruptions. Each data point is the average of 20 runs.

C. Simulation Results for Targeted Disruptions

Arguably, resilience against targeted disruptions is more important than against random disruptions, because military logistic networks often face more targeted attacks than random attacks from opponents. Also, targeted attacks are generally more damaging than random attacks. Fig. 6 shows the responses of the four network topologies to targeted disruptions. Similar to Fig. 5, the horizontal axes denote the percentage of removed nodes, and the vertical axes display the resilience metrics. The graphs are not shown beyond the 45% mark on the horizontal axis because they converge after this point. As expected, resilience of all the supply networks suffers different levels of deteriorations when compared with the case of random disruptions.

TABLE IV
95% CONFIDENCE INTERVALS FOR SUPPLY AVAILAIBILITY RATE(%) IN TARGTED DISRUPTIONS

Nodes removed	Random	Scale-free	Hierarchy+	DLA
5%	90.4-91.1	79.7-81.1	67.0-68.6	91.4-92.1
10%	83.0-83.8	57.6-59.9	45.1-47.1	80.7-81.5
15%	74.1-75.2	34.3-37.6	29.2-31.2	66.7-68.0
20%	63.0-64.4	17.9-21.1	18.2-20.1	46.9-49.0
25%	47.8-51.5	9.8-12.0	10.9-12.3	28.1-29.8
30%	30.0-33.5	5.2-6.3	6.7-7.5	18.0-19.9

We first examine availability. Unlike the uniformly near-linear decreases found for random disruptions, the four supply networks show significant differences on this metric in targeted disruptions. In Fig. 6(a), all four networks have very low supply availability when 45% of the nodes are removed, while in random disruptions, availability of all networks is around 40% at this point. Among the four networks, only the random network and the DLA network can still maintain near linear decreases. DLA's availability is close to that of the random network at the early stage of the disruption (from 0 to 15%), but drops faster than for the random network after 20% of nodes are removed. Meanwhile, the Scale-free and Hierarchy+ networks see significant decay in availability from the very beginning of targeted disruptions. For example, *10% node removal in the Hierarchy+ network leads to a near 60% drop in availability*. When 20% of the nodes are removed, only 20% of the battalions can still get supplies in the scale-free and the Hierarchy+ supply networks. By comparison, *the Random and the DLA networks can still maintain their supply availability at 64% and 48% respectively.* 95% confidence intervals in Table IV further illustrate that the four networks' availabilities are very different in targeted disruptions than in random disruptions.

We also consider connectivity. As demonstrated in Fig. 6(b), the deterioration in resilience is even worse in terms of connectivity. Even the random network, the best performer on this metric, cannot maintain a linear decrease. The size of its LFSN is only 8% of its original size when 30% of the nodes are removed. *We also observe very poor performance from the Hierarchy+ network, whose LFSN drops to 22% of its original size with only 10% nodes removed.*

Clearly, the Random and DLA supply networks show a considerable advantage over the Scale-free and Hierarchy+ supply networks in availability and connectivity when facing targeted disruptions. What about accessibility? Similar to Fig. 5(c) and 5(d), the plots of average and maximum supply-path lengths in Fig. 6(c) and 6(d) are also bell-shaped. Actually, Fig. 6(c) and 6(d) have very similar graphs, except that they use different vertical axes scales. Intuitively, we would like to compare values of each network's supply-path lengths in the LFSN, but such a comparison is not representative if the LFSNs have various sizes. While this condition was satisfied in the results from random disruptions, however, as shown in Fig. 6(b), the sizes of the LFSNs in the four networks differ significantly for the same disruption rate (especially when the disruption rate lies between 0% and 25%). For example, when 15% of the nodes are attacked, the supply-path lengths in the LFSN of the Hierarchy+ network are about 26% shorter than those of the DLA network. However, at the same point, *the size of Hierarchy+'s LFSN turns out to be only 7% of the size of DLA network's LFSN.* Therefore, one cannot conclude that Hierarchy+ has better accessibility since this likely advantage may be due to the much smaller size of its LFSN.

To better highlight the issue of accessibility comparison in the 0% to 25% disruption range, we draw the distributions of the shortest supply-path lengths in the four networks' LFSN at the 15% disruption point in Fig. 7. The horizontal axis denotes the shortest supply-path lengths from a battalion to its nearest supply unit, and the vertical axis represents the numbers of battalions that can access its nearest supply unit with a given shortest supply-path length in the LFSN. In Hierarchy+'s LFSN with 45 nodes, a nearest supply unit is always within a distance of 1 to 3 to a battalion. Meanwhile, in DLA's much larger sub-networks, more battalions can access the nearest supply unit within a distance of 1 or 2 than in Hierarchy+. However, a number of battalions are far away from a supply unit, with distance up to 7, thus contributing to DLA's higher average and maximum supply-path length. Yet, compared with Hierarchy+, DLA has far more battalions that can easily obtain supplies within the same distance as Hierarchy+ can.

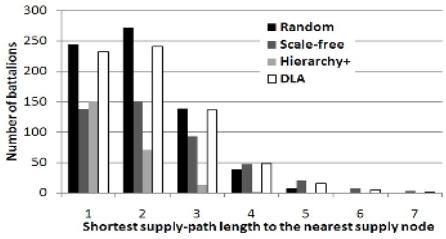


Fig. 7. The distribution of shortest supply-path length in the four networks' largest functional sub-network (15% targeted disruption).

Fig. 6(c) and 6(d) still contribute to our analysis, because they illustrate the rate at which the supply-path lengths increase in the LFSN, i.e., how fast the accessibility deteriorates when disruptions occur. Although supply-path lengths of scale-free and Hierarchy+ start with relatively lower values, they increase faster than of DLA and Random networks. The supply-path lengths of Scale-free and Hierarchy+ networks also reach their peaks very early. By the 10% point, the supply-path lengths have almost tripled. On the other hand, the peaks of DLA and Random come at 20% and 25% points respectively. In other words, *the supply accessibility of the Scale-free and Hierarchy+ networks deteriorates faster than of the DLA and the Random networks*. We found that supply-path lengths reach peak values when another round of node removal makes the size of LFSNs drop below 100, which is about 10% of their original sizes. For example, in the Hierarchy+ network, the supply-path lengths reach peak values when 10% of nodes are removed and the LFSN has a size of 222. If an additional 50 nodes are removed, the LFSN retains only 45 nodes, while the supply-path lengths see significant drops. We argue that by the time the size of the LFSN falls below 10% of its original size, the network has already been decomposed into many isolated sub-networks, and the normal operations of the whole supply network have also been seriously disrupted. Consequently, supply-path lengths after their peak values are not as meaningful to consider as those before the peaks. Therefore, we believe the random network has the best accessibility followed by the DLA network. The Scale-free and Hierarchy+ networks show similar accessibility.

Overall, the Random network is the most resilient against targeted disruptions, with DLA a close second. Hierarchy+ is the least resilient against targeted disruptions among the four, while the Scale-free network is only slightly better.

V. Discussion

Scale-free supply networks are very vulnerable to targeted disruptions. This is largely because their operations rely heavily on hub nodes, which have very high degrees and are removed at early stages of targeted disruptions. Recall that scale-free networks' preferential-attachment growth model corresponds to the strategy that nodes focus mainly on efficiency and cost. The results suggest if nodes make connection decisions solely based on efficiency and cost, the resulting network may be vulnerable to targeted disruptions.

Besides confirming previous research results, our study based on new resilience metrics also provides some new and surprising insights. For example, earlier work showed that Hierarchy+ supply networks were reasonably resilient against both random and targeted disruptions [9]. By our new resilience metrics, they still retain very good resilience against random disruptions. However, their resilience against targeted disruptions, which are more likely than random attacks in a military environment, is very disappointing. They have the worst availability and connectivity among the four supply networks. Removal of only a small percentage of nodes will disastrously fragment the network and disrupt its flows and operations. Hence, they are unsuitable against targeted disruptions which may well arise in military logistic systems.

The reason for the Hierarchy+'s vulnerability against targeted disruptions lies in its growth model, which intentionally assigns more connections to support units. Therefore, support units will naturally become topological hubs in the supply network. When target disruptions strike, support units will have higher probabilities of being attacked. The failures of support units, which act as both functional hubs and topological hubs, will inevitably hurt the availability and connectivity. The implication is that always assigning more connections to supply nodes may not be the best strategy to improve a supply network's resilience against targeted disruptions.

The merit of DLA supply networks is that they show good, although *not necessarily the best*, resilience against both types of disruptions. The resilience of the DLA network often lies in between that of the Random and the Scale-free networks. Specifically, in random disruptions, DLA is more resilient than the Random supply network, while in targeted disruptions it is more resilient than the Scale-free network. Thus, it offers a balanced option when one cannot predict the probability of either type of disruption.

While previous research often improves resilience by introducing redundant capacities in manufacturing, transportation, and storage, etc, the approach taken by DLA is slightly different because it does not require a node or edge to reserve redundant capacities. Instead, it changes the way that a supply network is constructed and consequently the network topology. *Admittedly, DLA is not a clearly dominant method.* Similar to redundancy-based approaches, it also requires more investment to operate and maintain a supply network. This is because, when no disruption occurs, DLA's accessibility is not as good as that of Scale-free and Hierarchy+, which implies that it may cost more to deliver supplies to demand nodes in a DLA network.

TABLE V
NUMERICAL ANALYSIS FOR SUPPLY AVAILABILITY RATE (10% TARGETED NODE REMOVAL)

	r = 0	**r = 0.5**	**r = 1**	**r = 2**	**r = 3**	**r = 4**
u = 0	86.12%	85.87%	85.68%	85.13%	84.50%	82.88%
u = 0.5	83.55%	83.21%	82.96%	82.24%	81.24%	79.32%
u = 1	78.65%	78.05%	77.37%	76.29%	74.72%	72.36%
u = 1.5	64.43%	63.36%	61.97%	59.63%	57.25%	52.93%
u = 2	31.69%	31.65%	31.80%	31.50%	30.80%	30.58%
u = 3	28.11%	29.11%	28.74%	28.61%	28.62%	28.59%
u = 4	28.57%	28.50%	28.48%	28.84%	28.74%	28.93%

DLA's attachment rules also reflect the distributed nature of supply network evolution. A new node entering a supply network has only local information. Therefore, connecting with nearby nodes in its neighborhood is much easier and less expensive. In fact, the performance of DLA suggests that when nodes consider both efficiency and distance while making connection decisions, the resulting supply network will have balanced resilience against both types of disruptions. Thus DLA represents a cost-effective strategy to build efficient yet resilient supply networks.

Moreover, by tuning the degree preference parameter u and the locality preference parameter r, we are able to generate different supply network topologies. Generally, a larger u leads to stronger preference for high degree nodes. Consequently, the resulting supply network will deviate farther from randomness and rely more heavily on few "super hub" nodes that have very high-degrees. Larger r means more local connections. The resulting supply network will feature more clusters and fewer connections that bridge nodes that previously have long distance between them. We conducted a simple numerical analysis to understand how the tuning of parameters u and r affects the resulting DLA supply network's resilience.

As an example, we analyzed the effect of changing u and r on supply availability rates when 10% of the nodes are removed in each disruption scenario. Node removal higher than this is not likely to occur in practice. For random disruptions, the supply availability rate falls between 86% and 89% and is only slightly affected by changes in u and r. On the other hand, for targeted disruptions availability is much more sensitive to u and r values. Supply availability rates of DLA supply networks with 10% targeted node removal are summarized in Table V. Each value in the table is the average of results from 100 runs.

From Table V we see that as u increases, the availability decays. Meanwhile, given the same degree preference u, higher preference for locality-based attachment, i.e. increasing r, will generally lead to slightly lower availability. Some may notice that when u is high, r has little impact on availability. This may be explained by the very strong preference for high-degree nodes. As a result, there emerge one or few "super hub" nodes that are connected to almost all the other nodes. When a new node enters the network, it will most likely establish the first connection with a "super hub" node. Then most of the other nodes have the same distance of 2 to this new node, so the preference for local nodes becomes less important. The results also agree with our previous finding that random supply networks (i.e. DLA with $u = 0$ and $r = 0$) have better

availability than scale-free and DLA networks with $u = 1/2$ and $r = 2$ in targeted disruptions.

It should also be noted from our analysis that the impact of locality on resilience is weaker than that of degree. This can be attributed to the fact that on average each new node initiates only 1.8 new edges in our experiments in order to ensure a fair comparison with the previous work [9]. In the DLA model, the first edge attachment is based on degree, while subsequent edge attachments are based on locality. This means that attachments based on locality are about 20% fewer than those based on degree. We believe that given more attachments based on locality, the impact of locality on availability might even be more pronounced.

The numerical analysis shows that one can tune the DLA model to generate supply network topologies with different levels of resilience against different types of disruptions. This customizability has important implications for the design and management of supply chains. As there is no single supply network topology that dominates all others in both random and targeted disruptions, one needs to seek a balance or trade-off between the resilience against random disruptions and targeted disruptions. The DLA network growth model provides the opportunity for nodes to make connection decisions based on what type of supply network they are in and the balance of possible disruptions the supply network will face. For instance, a DLA model with lower u is more appropriate for military logistic networks, which often handle targeted attacks from the enemy. A DLA model with higher u may be better for an automaker or a retailer as targeted disruptions are less likely for this type of supply chain.

VI. Conclusions and Future Work

Our objective for this paper was to study how topological considerations affect supply network resilience when both random and targeted disruptions can occur. We first propose a new taxonomy of supply-network resilience metrics to reflect the fact that, unlike in many other networks, nodes play heterogeneous roles in a supply network. The taxonomy consists of system-level metrics, including availability, connectivity and accessibility, as well as corresponding topology-level metrics. The second contribution of this paper is a new general and hybrid supply-network growth model called DLA, whose attachments are based on both degree and locality. Compared with other growth models, DLA represents a different strategy for distributed connections: nodes consider both efficiency and distance when deciding which nodes to connect to.

Using simulation, we compared the resilience of supply networks generated with various network growth models. The results reveal that DLA networks have desirable resilience properties in both random and targeted disruptions. Even though DLA is not the dominant model in terms of resilience against all types of disruptions, it offers an excellent *compromise strategy* to establish connections in supply networks when it is not possible to predict whether a random or a targeted attack will occur, which is often the case in the real world. We also showed that by adjusting the parameters of the DLA model, one is able to tune DLA networks' relative performance against the two types of disruptions. Recall that the multiple resilience metrics can be combined to generate a single objective function for a specific supply chain. Consequently, for supply network managers or individual decision-makers, the DLA model represents a simple yet effective heuristic strategy to build a Pareto-optimal supply network with balanced resilience in the supply network's operational context.

Although we used a military logistic network as a case study, our research is also relevant for non-military supply networks. A typical distribution network consists of plants, warehouses and retail outlets, which mirrors the three level structure of the military logistic network. By choosing appropriate parameters it is possible to apply our results in those scenarios, and this is a subject for future work. Other scenarios where our approach and insights about resilience can be applied include the Internet (with servers and clients as supply and demand nodes), and infrastructure networks such as power grids.

Meanwhile, we realize that it is not always possible to build a supply network from scratch using the new growth model or change existing supply networks that have evolved over a long period of time to conform to a new topology. Nevertheless, by shedding new light on the resilience of supply networks with different topologies, our growth model and resilience analysis could help to understand how an existing supply network evolved over time and how different micro-level paradigms to design a supply network will affect its resilience at a macro level. With these topological considerations in mind, managers are also better informed in the future expansion of existing supply networks.

There are several areas that we would like to address in future. As in other complex network research, we have focused mainly on network topologies, and neglected some operational details such as the flow of goods and capacity limits on various links and nodes. We aim to address this shortcoming in future work. Our expectation is that the resilience ranking of different network topologies will not change significantly even after taking those into account. Another limitation is that we only consider node failures, whereas a real-world supply network may also face disruptions to connections or edges, e.g., traffic accidents may block a road that connects a manufacturer and a retailer. Then the manufacturer may need to find an alternative path to deliver the goods. Thus, it would be useful to simulate the removal of edges from the supply network. We also plan to incorporate the dynamic behaviors of entities after disruption into the evaluation of resilience. Other possible research directions include analyzing the performance of DLA networks with higher average degrees and exploring variants of DLA.

Acknowledgment

The authors would like to thank Dr. Hing Kai Chan and anonymous reviewers for their insightful comments, which helped us to improve the quality of the paper.

References

[1] 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.

[2] S. D. Pathak, J. M. Day, 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.

[3] H. L. Lee, V. Padmanabhan, and S. Whang, "The bullwhip effect in supply chains," *Sloan Mgmt. Rev.*, vol. 38, no. 3, pp. 93–102, 1997.

[4] J. Rice and F. Caniato, "Building a secure and resilient supply network," *Supply Chain Management Review*, vol. 7, no. 5, pp. 22–30, 2003.

[5] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdown," *Sloan Management Rev.*, vol. 46, no. 1, pp. 53–61, 2004.

[6] G. W. Klau and R. Weiskircher, "Robustness and resilience," in *Network Analysis*. Springer Berlin/Heidelberg, 2005, pp. 417–437.

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

[8] J. Wu, H. Z. Deng, Y. J. Tan, and D. Z. Zhu, "Vulnerability of complex networks under intentional attack with incomplete information," *Journal of Physics A*, vol. 40, no. 11, pp. 2665–2671, 2007.

[9] 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.

[10] S. H. Lee, "Reliability evaluation of a flow network," *IEEE Transactions on Reliability*, vol. 29, no. 1, pp. 24–26, 1980.

[11] Y. K. Lin, "A simple algorithm for reliability evaluation of a stochastic-flow network with node failure," *Computers and Operations Research*, vol. 28, no. 13, pp. 1277–1285, 2001.

[12] M. O. Ball, "Complexity of network reliability computations," *Networks*, vol. 10, no. 2, pp. 153–165, 1980.

[13] A. Konak and M. R. Bartolacci, "Designing survivable resilient networks: A stochastic hybrid genetic algorithm approach," *Omega-Intl. Journal of Management Science*, vol. 35, no. 6, pp. 645–658, 2007.

[14] V. Jayaraman and A. Ross, "A simulated annealing methodology to distribution network design and management," *European Journal of Operational Research*, vol. 144, no. 3, pp. 629–645, 2003.

[15] F. Altiparmak, M. Gen, L. Lin, and T. Paksoy, "A genetic algorithm approach for multi-objective optimization of supply chain networks," *Computers and Industrial Engineering*, vol. 51, no. 1, pp. 196–215, 2006.

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

[17] T. Y. Choi and Y. Hong, "Unveiling the structure of supply networks: case studies in honda, acura, and daimlerchrysler," *Journal of Operations Management*, vol. 20, no. 5, pp. 469–493, 2002.

[18] M. E. Burkhardt, "Social interaction effects following a technological change: A longitudinal investigation," *The Academy of Management Journal*, vol. 37, no. 4, pp. 869–898, 1994.

[19] H. Ibarra and S. Andrews, "Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions," *Administrative Science Quarterly*, vol. 38, no. 2, pp. 277–303, 1993.

[20] G. Meyer, "Social information processing and social networks: A test of social influence mechanisms," *Human Relations*, vol. 47, no. 9, pp. 1013–1047, 1994.

[21] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.

[22] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

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

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

[25] P. Erdos and A. Renyi, "On random graphs," *Publicationes Mathematicae*, vol. 6, pp. 290–297, 1959.

[26] R. Albert and A. L. Barabasi, "Statistical mechanics of complex networks," *Rev. of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[27] S. D. Pathak, D. M. Dilts, and G. Biswas, "On the evolutionary dynamics of supply network topologies," *IEEE Trans. on Engineering Management*, vol. 54, no. 4, pp. 662–672, 2007.

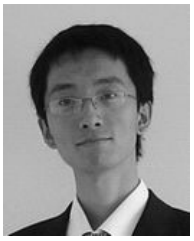
[28] R. Albert, H. Jeong, and A. L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[29] T. H. Grubesic, T. C. Matisziw, A. T. Murray, and D. Snediker, "Comparative approaches for assessing network vulnerability," *International Regional Science Review*, vol. 31, no. 1, pp. 88–112, 2008.

[30] A. Law and W. Kelton, *Simulation modeling and analysis*, 3rd ed., ser. Industrial Engineering and Management Science Series. New York: McGraw-Hill, 2000.

[31] V. Latora and M. Marchiori, "Vulnerability and protection of infrastructure networks," *Phys. Rev. E*, vol. 71, no. 1, p. 4, 2005.

[32] M. E. J. Newman, "Mathematics of networks," in *The New Palgrave Encyclopedia of Economics*, 2nd ed., L. E. Blume and S. N. Durlauf, Eds. Basingstoke, UK: Palgrave Macmillan, 2008.



Kang Zhao is a Ph.D. candidate at the College of Information Sciences and Technology, the Pennsylvania State University. He received his M.S. in Computer Science from Eastern Michigan University, USA, and B.E. in Electrical Engineering from Beijing Institute of Technology, China. He was the recipient of the Robert W. Graham Endowed Graduate Fellowship (2007-2008). His research interests include the simulation and analysis of complex multi-dimensional social and organizational networks, social computing, agent-based models, and complex systems.

Akhil Kumar is a Professor of Information Systems at the Smeal College of Business at the Pennsylvania State University. He received his Ph.D. from the University of California at Berkeley, and has previously been on the faculties at Cornell University and University of Colorado. He has done pioneering work in data replication and XML based workflows. His research interests are in workflow systems, e-services, distributed information systems and intelligent systems. He has published more than 80 scientific papers in academic journals and international conferences, and also held many editorial positions.

Terry P. Harrison is the Earl P. Strong Professor of Executive Education and Professor of Supply Chain and Information Systems in the Smeal College of Business at Penn State University. His primary teaching interest is in the area of large-scale production and distribution systems, and supply chain management and design. He has created seven new courses at the undergraduate and graduate levels, in areas such as optimization, operations, manufacturing, supply chain management and computing. His research interests match his teaching interests. He has authored many papers on various aspects of optimization and its use in manufacturing, distribution and supply chain management. He currently is investigating questions relating to the performance of service supply chains, "green" procurement and SKU rationalization in product portfolios. Currently, Professor Harrison serves as Vice President of Publications for INFORMS. He is a past editor-in-chief of the journal Interfaces.

John Yen is the University Professor and the Director for Strategic Initiatives at College of Information Sciences and Technology at the Pennsylvania State University. He received his Ph.D. in Computer Science from University of California, Berkeley, M.S. in Computer Science from Santa Clara University, and B.S. in Electrical Engineering from National Taiwan University. His research interests are intelligent agents, decision supports, and social network analysis, especially within the context of extreme events and social dynamic modeling. He received the NSF Young Investigator Award in 1992, and is a Fellow of IEEE.