

Analyzing the Trade-offs in the Robustness of Supply Networks against Disruptions

Kang Zhao, Akhil Kumar, and John Yen

Abstract

Supply chain systems often face disruptions, which may lead to the catastrophic failure of the whole system. In this paper, we study robustness of supply chains from the perspective of complex network topologies. Using a military supply network as a case study, we propose taxonomy of supply network robustness metrics that reflect the heterogeneous roles (e.g. supply, demand) of entities in supply networks. We also design a novel hybrid supply network growth mechanism called DLA that combines degree-based and locality-based preferential attachment. Moreover, it can be tuned to provide balanced robustness against different disruption scenarios. Using agent-based simulations, we compare the robustness of several supply network topologies. Our results show that the new robustness metrics could capture important robustness requirements for supply networks very well. It was also found that the supply network topology generated by our new mechanism provides satisfactory robustness against both random and targeted types of disruptions.

Keywords: Complex network topology, disruption, robustness, supply network, agent-based simulation.

1. Introduction

With globalization and the development of information technology, supply chain systems are becoming more complex and dynamic. Today's supply chain systems often feature a network of interacting entities, such as suppliers, manufacturers, retailers, customers, etc. Many researchers have suggested that supply chains should be considered as supply networks [1] and the analysis and design of supply chains should incorporate the concepts of complex systems, especially complex networks [2, 3].

Meanwhile, supply chains, especially large or global ones, are often embedded in dynamic environments and may face disruptions, such as natural disasters, economic recessions, unexpected accidents or terrorist attacks. A disruption may initially attack or disable only one or few entities in the system, but its impact may also extend further. Disruptions can get propagated, sometimes even with amplifications [4], among inter-connected entities. Such disruptions will thus affect the normal operations of many other entities. Occasionally, failures in a small portion of the system may cause the catastrophic failure of the whole system [5]. Those events may seriously disrupt or delay the flow of people, goods, information and funds, and thus lead to higher costs or lower sales [6]. Disruptions in a company's supply chains may also affect its long-term stock performance [7]. Therefore, designing supply chains that are robust against disruptions becomes a high priority, and it has drawn a lot of attention from managers, shareholders and researchers [8, 9].

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 [6, 8, 9]. However, even though research has revealed that the topology of a supply network will affect its robustness [10], we found little research following this direction. In this paper, we will adopt the complex network view of supply chains and study the robustness of supply networks from a topological perspective.

The remainder of the paper is organized as follows. We will first briefly review related research on supply network robustness. Using a military supply network as a case study, we then propose the new

taxonomy of robustness metrics for supply networks. After that, a new customizable network growth model is introduced. Through agent-based computational simulations, the robustness of our new supply network topology, along with other supply network topologies, is evaluated and compared. The paper will end with a conclusion and discussion of future research directions.

2. Related Work

Complex networks such as small-worlds, scale-free networks, etc., are ubiquitous in nature and society. Examples include, but are not limited to, social networks, the World Wide Web, biological cellular network, etc. During recent years, there has been growing interest in the research on complex networks. Network topologies underlying real-world complex networks and the corresponding network growth mechanisms have been revealed [11, 12]. Their statistical characteristics and structures have also been studied [13, 14]. Research on complex networks has also inspired research in various domains, such as social norms [15], organizational coordination [16], the spread of diseases [17] and computer virus [18], viral marketing [19], and academic community discovery [20], etc.

Specifically, the robustness of a complex network topology against errors and attacks has been analyzed. It was found that scale-free networks have very high tolerance against random failures. Nevertheless, networks with the scale-free topology are fragile to disruptions that target the most connected nodes [21, 22]. Other topologies and statistical characteristics that affect the network's robustness have also been studied [23, 24]. In [25], a review of approaches to assess network vulnerability and robustness is provided.

The research in [10] introduced the topological perspective into the study of supply networks survivability. In this work, robustness was considered as an important component of survivability. It was argued that traditional supply chains with hierarchical topologies are subject to disruptions or attacks. A military supply network, consisting of *battalions*, *forward support battalions (FSB)* and *main support battalions (MSB)* was used as an example. As shown in Fig. 1, the failure of a single FSB in the hierarchical supply chain disconnects about 25% of the battalions from military supplies. Therefore, the

authors proposed a network growth mechanism that assigns different attachment rules to different types of units in the military supply network. Agent-based computational simulations were used to compare the performance of military supply networks with various topologies in two types of node removal attack scenarios. The simulation results showed that the survivability of supply networks can be improved by concentrating on the network topology and its interplay with function. Our study of supply network robustness will extend this research further.

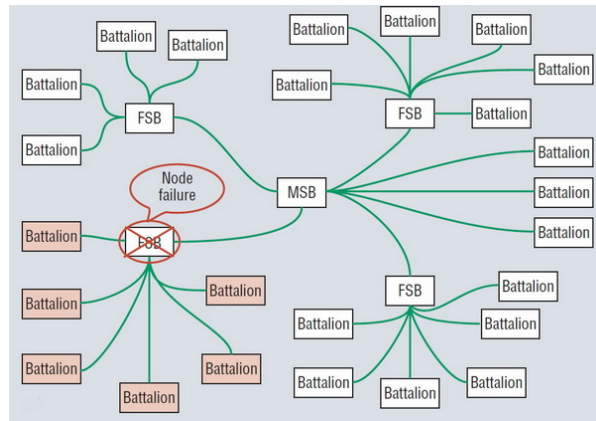


Figure 1. A hierarchical military supply chain [10].

3. Proposed Approach

In this section, we will present the taxonomy of robustness metrics for supply networks. The new taxonomy includes system-level and topology-level metrics, which reflect the heterogeneous roles of different types of entities in supply networks. We also introduce a new general and customizable supply network growth mechanism and evaluate multiple supply networks' performance against disruptions.

3.1. New Robustness Metrics

Robustness of a network is the ability to maintain operations and connectedness under the loss of some structures or functions. In the research of complex network robustness, the evaluation of robustness focuses on the largest connected component in which there is a path between any pair of nodes. Existing robustness metrics are generic topological metrics, including size of the largest connected component,

average path length in the largest connected component and the maximum path length in the largest connected component. The metrics are explained in Table 1.

Applying these generic metrics to the evaluation of supply network robustness is largely based on the assumption that roles and functions of entities in a supply network are homogeneous. However, in real-world supply networks, different types of entities play different roles in the system. Often times, the normal functioning of downstream entities may be highly dependent on the operations of upstream entities. 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 [25]. As a result, preserving this type of connectivity in disruptions is critical for maintaining the operations of the whole supply chain.

Table 1. Some generic metrics for network robustness.	
Name of the metric	Brief explanations of the metric
Size of the largest connected component of a network	The number of nodes in the largest connected component of a network.
Average path length in the largest connected component	The average of the shortest path length between any two nodes in the largest connected component of a network.
Maximum path length in the largest connected component	The maximum path length between any two nodes in the largest connected component of a network.

Taking the military supply network in [10] as an example, support units such as FSB and MSB play a different role from battalions in the supply network. Often battalions cannot perform their military duties without supplies from support units. Therefore, a large connected component in which there is no support unit, or where battalions are far from support units, should not be considered as robust because there is none or limited supply flow in such a sub-network. Similarly, the distance between battalion and support units is generally more important for a robust supply chain than the distance among battalion units. Therefore, the heterogeneous roles (as supply and demand nodes) of different types of entities in a supply network must be taken into consideration when evaluating the robustness of a supply chain.

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

First, we introduce *availability* as a critical robustness metric for supply networks, because it shows whether entities in the supply network can get the supplies they need to maintain normal operations. At the topological level, availability can also be interpreted as supply availability rate, which is the percentage of "Destination" nodes that have access to "Origin" nodes. In the face of disruptions this rate reflects the robustness of the supply network. In the context of the military supply network, the supply availability rate is the percentage of battalions that have access to support units.

Consider the military supply 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 battalion nodes (set V_B) and supply support nodes (set V_S).

$$V = V_B \cup V_S, \text{ where } V_B \cap V_S = \emptyset \quad (1)$$

Then the set of battalion units 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 battalion nodes that have access to support nodes through the supply network. Consequently, the supply availability A for a military supply network is defined as the ratio between the cardinalities of sets V_{BS} and V_B , as shown in (3) below.

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

$$A = |V_{BS}|/|V_B| \quad (3)$$

Second, the connectivity of the system is also important. Flows of goods or services are often limited and less fluid in supply networks that are isolated into various components. *Topological connectivity* is often measured by the size of the largest connected component. Here, we incorporate the idea of availability into this metric and will use size of the largest functional sub-network instead of the size of the largest connected component. For the military supply network, nodes in the largest functional sub-network are defined as the set V_{sub} , which satisfies the following two requirements.

$$\forall v_i, v_j \in V_{sub}, \exists p_{i,j} \quad \text{and} \quad \exists v_k \in V_{sub}: v_k \in V_S \quad (4)$$

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

Last, but not least, we extend and group two generic topological metrics to reflect the *accessibility* of supplies in supply networks. As we mentioned earlier, from the perspective of supply network robustness, the distance between battalions is not as important as the distance between battalions and support units in the military supply network. Consequently, we propose the metric of *supply path length* to replace *path length*. A supply path is the path between a support unit and a battalion. Thus the *average supply path length in the largest functional sub-network* is the average of the minimum supply length between all possible pairs of support units and battalions in the sub-network. Moreover, the *maximum supply path length in the largest functional sub-network* in the largest functional sub-network is the longest supply length between any (support unit and battalion) pair in the sub-network. Naturally, shorter average and maximum supply path lengths mean that supplies can be more easily accessed in the network.

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 largest functional sub-networks into consideration because a larger supply network with more nodes will have longer average paths than a network with fewer nodes. The existence of a few supply nodes that are far away from some battalions may increase the average and maximum supply path length in a large sub-network. We will illustrate this with our experiments in Section 4.

It is also possible to combine those metrics into a single objective function in order to optimize the overall performance of a supply network. However, we decide 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 one knows very well the context in which a specific supply network operates, one is in a better position to determine the single objective function for optimization.

Our new metrics are summarized in Table 2. The metrics reflect the heterogeneous roles of different types of entities in supply networks and can more accurately measure supply network robustness. Thus we believe the new taxonomy is more systematic and realistic as compared to the metrics in previous work such as [10].

Table 2. Taxonomy of the new robustness metrics for supply networks.		
System-level metric	Topology-level metric	Brief explanations of the topology-level metrics
Availability	Supply availability rate	The percentage of demand nodes that have access to supplies.
Connectivity	Size of the largest functional sub-network	The number of nodes in the largest functional sub-network, 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 the largest functional sub-network*	The average of the shortest supply path length between all pairs of supply and demand nodes in the largest functional sub-network.
	Maximum supply path length in the largest functional sub-network*	The maximum path length between any pair of supply and demand nodes in the largest functional sub-network.

* for comparison purposes, the largest functional sub-networks should be of similar sizes.

3.2. New Hybrid Growth Mechanism (DLA)

To realize a supply network topology, we must start with its growth mechanism, which describes how new nodes get connected with existing nodes in a network. [10] presented a network growth mechanism for a military network that is survivable under the old robustness metrics in Table 1. According to the mechanism, different types of nodes have different attachment rules. For example, when a new battalion joins the network, it is allowed to create 1 or 2 connections with existing units in the network. A new FSB and MSB can create 3 and 5 new edges, respectively. The authors did not name their approach, but for the purpose of clarification and convenience, we will call this mechanism Prioritized Attachment for Support Units (PASU). The supply network generated by PASU is called PASU network in this paper.

While PASU uses arbitrary numbers of edges and ad-hoc attachment rules for different types of entities in the supply network, we propose a more general hybrid mechanism that incorporates both degree and locality called *Degree and Locality-based Attachment (DLA)* growth mechanism. This mechanism does not require special attachment rules for different types of units and may be applied to other types of complex networks in general. The DLA growth mechanism starts with a small number of disconnected nodes, say N_0 . Assume that when a new node enters the system, it initiates edges to connect to or attach with k existing nodes in the system, where $k < N_0$. The general attachment rules for a new node are specified as follows:

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

$$P_i = k_i^u / \sum_i (k_i^u), \text{ where } u \geq 0 \quad (5)$$

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

$$P_j = (d_j^{-r}) / \sum_j (d_j^{-r}), \text{ where } r \geq 0 \quad (6)$$

Equation (5) describes the attachment preference of the first edge of a new node. u is the customizable degree preference parameter. Given the same u , the new node will preferentially connect to

existing nodes with higher degrees. When $u=0$, the attachment rule is similar to that of random networks, as every other node in the network has the same probability of being connected by the new node. When $u=1$, the attachment occurs by the rules of a scale-free network where the probability of a new node being connected to an existing node is proportional to the existing node's degree. A larger u gives even higher P_i to highly connected nodes. Therefore, as u becomes larger it is more likely that the new node will connect to an existing node with very high degree. 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 (6) above specifies the attachment preference 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 equation (6), the non-negative integer distance d_j and the customizable locality preference parameter r constitute the locality-based 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 to new nodes. In other words, local nodes are preferred over distant nodes when new nodes initiate connections. 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 local nodes which are close to the new node, 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, for obvious reasons multiple links to the same node are disallowed.

Fig. 2 illustrates a simple example for the DLA growth mechanism with $u=1$ and $r=1$. In this example, each new node will have two edges. At Step 1, the network starts with three disconnected initial nodes, namely nodes 1, 2 and 3. Node 4 is the first new node that enters the system and will randomly choose two nodes to connect to. In our example, the new node chooses nodes 1 and 2. When node 5

comes in, its first edge will prefer existing nodes with high degrees and thus node 4 has the highest probability to be connected to it. Node 5's second edge will prefer nodes that are close to it. Nodes 1 and 2 then have the same probability to be chosen. In this example, node 5 chooses node 4 for the first edge and node 1 for the second edge. Similarly, node 6 connects to nodes 4 and 2 in Step 4. The supply network topology that emerges from this mechanism is called a DLA network. As noted above, the hybrid DLA is more general than PASU. In fact, the PASU mechanism is a special case of the DLA growth mechanism and can be realized with a suitable choice of parameters. In the next section, we will evaluate the robustness of DLA network and compare it with other topologies using the new robustness metrics.

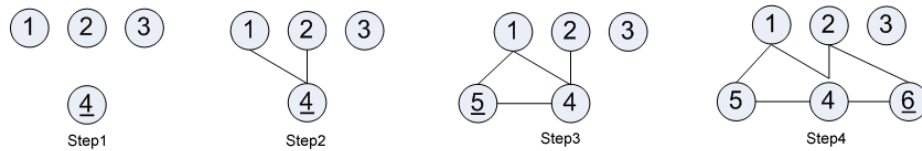


Figure 2. An example of the DLA growth mechanism. ID for the new node is underscored.

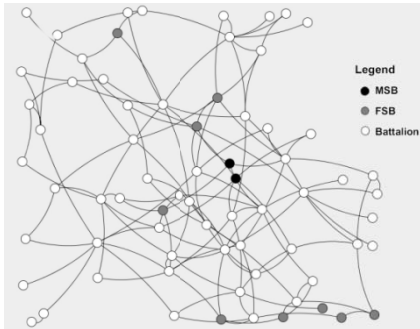
4. Experimental Results

As it is very difficult, if not impossible, to construct a real-world supply network and generate disruptions of nodes within it to evaluate its robustness, we have to rely on computational simulations. Agent-based simulation has become a popular choice in the study of supply chains [26-28]. This approach can simulate system structures or patterns resulting from micro-level interactions and behaviors of heterogeneous agents within complex systems [29]. Hence, it is very suitable for our analysis. In this section, we will describe our method for evaluating and comparing the robustness of different supply network topologies using agent-based computational simulations. The results from the simulations of the military supply network will be illustrated and discussed.

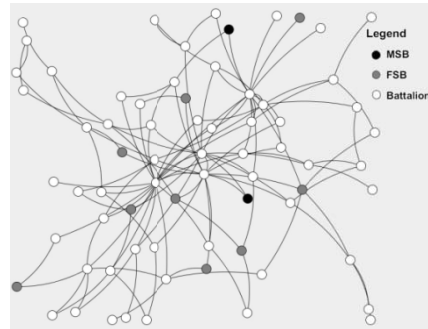
4.1. Simulation Setup

Our agent-based simulation is developed using the Java Universal Network/Graph Framework [30]. We adopt the military supply network example in [10] in our simulation. The military supply network

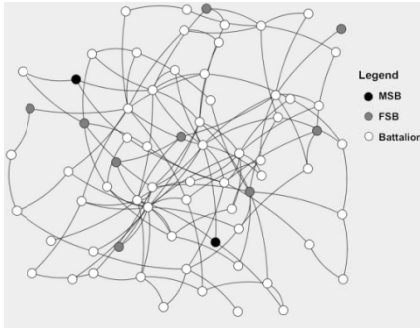
consists of 1000 nodes and 1815 edges. Battalions, FSB and MSB units enter the system following the ratio of 25:4:1, which was estimated from a military logistic system. This ensures a consistent comparison with the previous work in [10]. We will compare the robustness of supply networks with *random*, *scale-free*, *PASU* and *DLA* topologies. For each supply network topology, we will first construct the network using corresponding network growth mechanism and the military supply network configuration. For the DLA growth mechanism, we use $u=1/2$ and $r=2$.



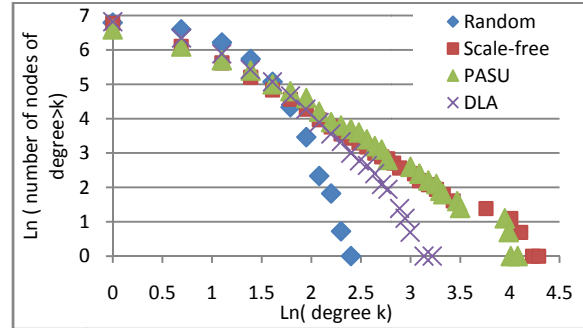
(a) A snapshot of a 70 node random supply network.



(b) A snapshot of a 70 node scale-free supply network.



(c) A snapshot of a 70 node DLA supply network with $u=1/2$ and $r=2$.



(d) The log-log degree distribution of the four supply networks with 1000 nodes each.

Figure 3. Simulated supply networks with various topologies.

Fig. 3(a), 3(b), and 3(c) show the snapshots of supply networks with random, scale-free and DLA topologies (the legend is shown alongside). This small-scale DLA supply network features some hub nodes and also some highly connected clusters, but the connection to the hubs are not as concentrated as in scale-free networks. Fig. 3(d) illustrates the log-log degree distributions of the four networks. A scale free network [12] is characterized by a power law distribution in the node degree, while in a random network all pairs of edges are equally likely.

Next, we need to simulate disruptions. In research on network robustness, two types of disruptions based on node removal are commonly studied: *random and targeted disruptions*. In random disruptions, nodes are removed randomly from the network. Edges that are connected to them are also removed. This scenario corresponds to natural disasters (e.g., earthquakes, hurricanes and floods), accidents (e.g., fires and power outage), and unexpected economic events (e.g., recessions and bankruptcy). On the other hand, in targeted disruptions important nodes are more likely to be removed than unimportant ones. Examples of targeted disruptions include terrorist and military attacks, which often target critical entities in the system such as network hubs.

In our agent-based simulation, an agent represents a node in the supply network. Disruptions are simulated by the removal of agents. As in [10], 50 agents are removed between successive observations. When an agent is removed, its connections are also removed from the multi-agent system. To simulate random disruptions, randomly chosen agents are removed. For targeted disruptions, agents are removed in order of decreasing node degree. In other words, nodes with higher degrees are removed earlier. During the process of node or agent removal, we track the robustness metrics for each network topology. In the end, we will compare the robustness metrics for all the topologies. To ensure a fair comparison, each network topology will have the same number of edges. On average, each new node will initiate about 1.8 new edges in our simulations to correspond with the PASU network in [10]. Thus the total number of edges will be around 1800 and the average degree is 3.6 edges per node. Our simulation settings are summarized in Table 3.

Number of nodes	1000	Ratio of Battalion, FSB and MSB	25:4:1
Average number of degree per node	3.6	Parameters for the DLA mechanism	$u=1/2$, $r=2$
Node removal between observations	50	Parameter for the scale-free (all edges)	$u = 1$

4.2. Simulation Results for Random Disruptions

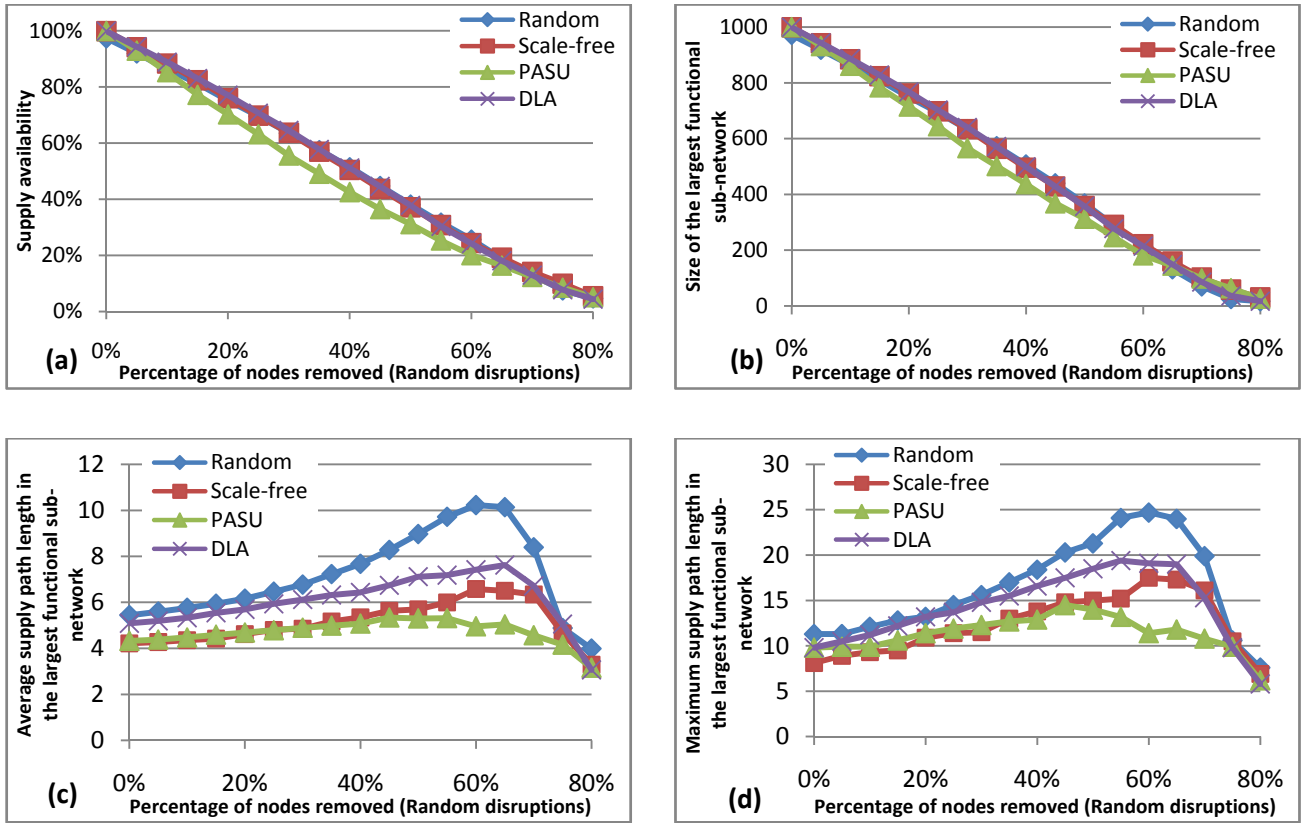


Figure 4. The four networks' responses to random disruptions, plotted as (a) supply availability, (b) size of the largest functional sub-network, (c) average supply path length in the largest functional sub-network, and (d) maximum supply path length in the largest functional sub-network. Each data point is the average of 20 runs.

Fig. 4 shows the responses of the four network topologies to random disruptions. The X-axes denote the percentage of nodes that have been removed, while the Y-axes are values of the topology-level supply network robustness metrics that we proposed in Table 2. The graphs are not extended beyond the 80% mark on the X-axis because they converge after this point. Fig. 4(a) and 4(b) show that for all the four network topologies, supply availability rate and the size of the largest functional sub-network decrease almost linearly as nodes are removed from the network. On the two metrics, the performance of random, scale-free and DLA networks is very close. However, PASU's robustness in terms of availability and connectivity is slightly worse than of the other three, as indicated by its steeper slope. In addition, since

the four networks are similar in the size of their largest functional sub-network, the comparison on their two accessibility metrics is reasonable.

Nevertheless, the accessibility metrics in Fig. 4(c) and 4(d) point towards different conclusions. In general, when nodes are removed from a network, the accessibility of supplies gets worse because the average and maximum supply path length in the largest functional sub-network increase as more nodes are removed. Almost all supply path lengths reach their peak values at 50-60% node removal, and then start to fall. The decreases are most likely caused by the smaller size of the largest functional sub-network (less than 200 nodes). The PASU's supply path lengths are the most resilient, which indicates that the PASU network is the most robust in terms of preserving good supply accessibility. Even when 40-50% of nodes are removed, there is no dramatic increase in the average supply path length in the largest functional sub-network. On the other end of the spectrum, supply 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 supply accessibility.

Considering all robustness metrics, the PASU supply network is generally the most robust against random disruptions. The robustness of other three network topologies against random disruptions can be ranked in a descending order as scale-free, DLA and random networks.

4.3. Simulation Results for Targeted Disruptions

Arguably, robustness against targeted disruptions is more important than against random disruptions, because military supply networks often face more targeted attacks than random attacks from opponents. Also, targeted attacks are usually more damaging than random attacks. Fig. 5 shows the responses of the four network topologies to targeted disruptions. Similar to the figures for random disruptions, the X-axes denote the percentage of nodes that have been removed, while the Y-axes are the topology-level supply network robustness metrics. The graphs are not shown beyond the 45% mark on the X-axis because they converge after this point. As expected, robustness of all the four supply networks suffers different levels of deteriorations when compared with the case of random disruptions.

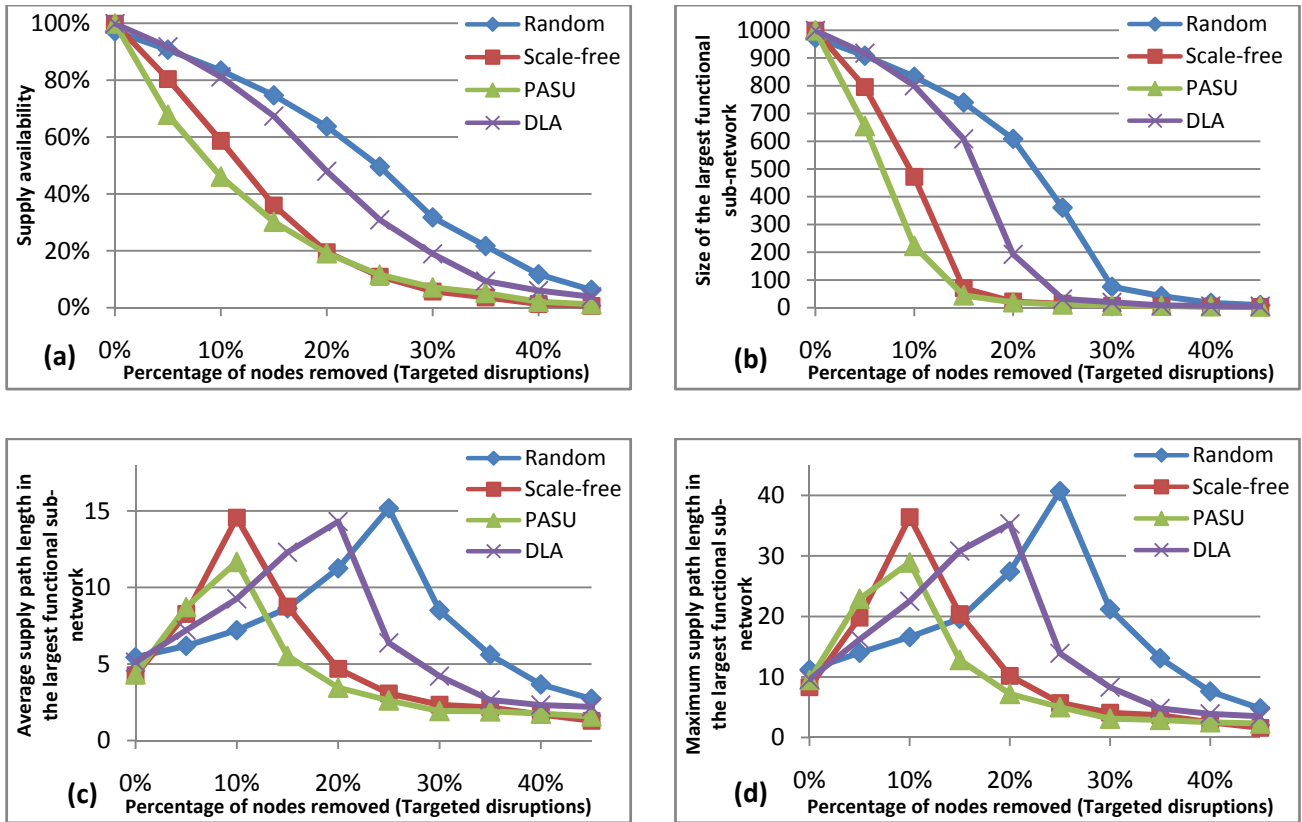


Figure 5. The four networks' responses to targeted disruptions, plotted as (a) supply availability, (b) size of the largest functional sub-network, (c) average supply path length in the largest functional sub-network, and (d) maximum supply path length in the largest functional sub-network. Each data point is the average of 20 runs.

We first examine supply availability. Unlike the uniformly near-linear decreases found for random disruptions, the four supply networks show significant difference on this metric in targeted disruptions. In Fig. 5(a), all the four networks have very low supply availability when only 45% of the nodes are removed. On the contrary, in random disruptions, supply availability of all networks at this point is around 40%. Among the four networks, only the random network and the DLA network can still maintain near linear decreases in supply availability. DLA's supply 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.

At the same time, the scale-free and PASU networks see significant decay in supply availability from the very beginning of targeted disruptions. For example, *10% node removal in the PASU network*

leads to a near 60% drop in supply availability. When 20% of the nodes are removed, only 20% of the battalions can still get supplies from support units in the scale-free and the PASU supply networks. By comparison, *the random and the DLA networks can still maintain their supply availability at 64% and 48% respectively.*

We then turn to connectivity. According to Fig. 5(b), the deterioration in robustness is even worse in terms of connectivity. Even the random network, which is the best performer on this metric, cannot maintain a linear decrease. The size of its largest functional network is only 8% of its original size when 30% of the nodes are removed. *We also observe very poor performance from the PASU network, whose largest functional sub-network 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 PASU supply networks in availability and connectivity when facing targeted disruptions. What about accessibility? Similar to Fig. 4(c) and 4(d), the plots of average and maximum supply path lengths in Fig. 5(c) and 5(d) are also bell-shaped. Actually, the average and maximum supply path lengths of the largest functional sub-network have very similar graphs, except that the two graphs use different Y-axes scales.

Intuitively, we would like to compare values of each network's supply path lengths in the largest functional sub-network, but such a comparison is not very fair if the largest functional sub-networks do not have similar sizes. While this condition was satisfied in the results from random disruptions, however, as shown in Fig. 5(b), the sizes of the largest functional sub-networks 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 largest functional sub-network of the PASU network are about 26% shorter than those of the DLA network, which may suggest that the PASU network has better accessibility than DLA at this point. However, at the same point, *the size of PASU's largest functional sub-network turns out to be only 7% of the size of DLA network's largest functional sub-network.* Therefore, it is not possible to conclude that PASU has an

advantage in terms of accessibility since this likely advantage may be due to the much smaller size of its largest functional sub-network.

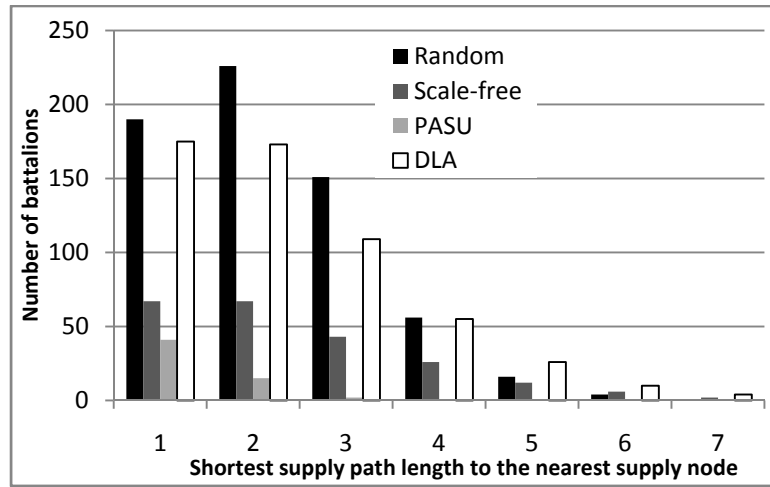


Figure 6. The distribution of battalions' shortest supply path to the nearest supply node in the four networks' largest functional sub-network (15% targeted disruption)

To better highlight the issue of accessibility for the four supply networks in the 0% to 25% disruption range, we draw the distributions of the shortest supply path lengths in the four networks' largest functional sub-network at the 15% disruption point in Fig. 6. The horizontal axis denotes all the possible shortest supply path lengths from a battalion to its nearest supply node, while the vertical axis represents the numbers of battalions that have a certain shortest supply path length to its nearest supply node in the largest functional sub-network. The figure reveals that, in PASU's 45-node largest functional sub-network all battalions are within a distance of 1 to 3 from the nearest supply node. Meanwhile, in DLA's much larger sub-networks, there are many more battalions, which are within a distance of 1 or 2 than in PASU. At the same time, a number of battalions are far away from a supply node, with distance up to 7. Those long supply paths contribute to DLA's higher average and maximum supply path length when 15% of the nodes are attacked. Yet DLA has far more battalions than PASU that can obtain supplies within the same shortest supply path length as PASU can.

Nevertheless, the value of Fig. 5(c) and (d) lies in illustrating the rate at which the supply path lengths increase in the largest functional sub-network, i.e., how fast the accessibility deteriorates when disruptions occur. Although the largest functional networks of scale-free and PASU start with a relatively shorter supply path length, their supply path lengths increase faster than of DLA and random networks. The supply path lengths of scale-free and PASU 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 PASU networks deteriorates faster than of the DLA and the Random networks*. It is also found that those supply path lengths reach peak values when another round of node removal makes the size of largest functional sub-networks drop below 100, which is about 10% of their original sizes. For example, in the PASU network, the supply path lengths reach peak values when 10% of nodes are removed and the largest functional sub-network has a size of 222. If an additional 50 nodes are removed, the largest functional sub-network retains only 45 nodes, while the supply path lengths see significant drops. We argue that by the time the size of the largest functional sub-network falls below 10% of its original size, the network has already been decomposed into many isolated components, 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 supply accessibility followed by the DLA network. The scale-free and PASU networks show similar supply accessibility.

Overall, the random network is the most robust against targeted disruptions, with the DLA network a close second. The PASU network is the least robust against targeted disruptions among the four, while the scale-free network is only slightly better.

5. Discussions

Scale-free supply networks are very brittle in the presence of targeted disruptions. This is largely because the operations of scale-free supply networks rely heavily on hub nodes, which have very high degrees and thus are removed at early stages of targeted disruptions. Besides confirming some previous research results, our study based on new supply network robustness metrics also provides some new and surprising insights. For example, in earlier work, PASU supply networks were shown to be reasonably robust against both random disruptions and targeted disruptions [10]. By our new robustness metrics, PASU supply networks still retain very good robustness against random disruptions. However, we found that the robustness of PASU supply networks against targeted disruptions, which are even 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 supply chains for military logistic systems.

The reason for the PASU's brittleness against targeted disruptions lies in its growth mechanism, which intentionally assigns more edges to support units. In a PASU supply network, support units will naturally become topological hubs in the supply network. As a result, 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 nice property of DLA supply networks is that they show good robustness against both types of disruptions. The robustness of the DLA network often lies in between that of the random and the scale-free networks. Specifically, in random disruptions, it is more robust than the random supply network. In targeted disruptions, it is more robust than the scale-free network. Thus, it is an excellent option when one cannot predict the probability of either type of attack.

More importantly, the customizable DLA is not limited to providing only one type of supply network topology. By manipulating the degree preference parameter u and the locality preference

parameter r , we are able to generate different supply network topologies. Generally, larger u leads to stronger preference for high degree nodes in edge attachments. Consequently, the resulting supply network will incorporate more degree-based preferential attachment and deviate farther from randomness, which means it will rely heavily on few "super hub" nodes that have very high degrees. Larger r means more local edge attachments. The resulting supply network will feature more clusters and fewer connections that bridge nodes that previously have long distance between them. Next we briefly examine the sensitivity of DLA's robustness to u and r parameter values.

As mentioned earlier, the DLA network in our simulations was generated with $u=1/2$ and $r=2$. To better understand how the tuning of the two parameters will affect the resulting DLA supply network's robustness, we conducted a simple sensitivity analysis. We will analyze the effect of changing u and r on supply availability rates when 10% of the nodes are removed in each disruption scenario. Node removal rates higher than this are not likely to occur in practice. For random disruptions, the supply availability ratio falls between 86% and 89% and is not much sensitive to changes in u and r parameters. 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 4. Each value in the table is the average of results from 100 runs.

	$r = 0$	$r = 0.5$	$r = 1$	$r = 2$	$r = 3$	$r = 4$
$u = 0$	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%

From Table 4, we see that as u increases, the supply availability decays. On the other hand, 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 attachment 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 become the new node's 2-hop neighbors. In this case, the preference for local nodes becomes less important because most of the other nodes have the same distance to this new node.

The results agree with our previous finding that random supply networks (i.e. DLA with $u=0$ and $r=0$) have better availability than scale-free supply networks and DLA networks with $u=1/2$ and $r=2$ in targeted disruptions.

It should also be noted that in our analysis the impact of locality on availability in targeted disruptions 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 [10]. In the DLA mechanism, the first edge attachment is based on degree, while subsequent edge attachments are based on locality. This means that edge attachments based on locality are about 20% fewer than edge attachments based on degree in our simulation. We believe that given more edge attachments based on locality, the impact of locality on availability may be even more pronounced.

The sensitivity analysis shows that the DLA mechanism can be tuned to generate supply network topologies that have different levels of robustness against different types of disruptions. This customizability of DLA has important implications for the design and management of supply chains. As our results suggested, there is no single supply network topology that dominates all other topologies for both random and targeted disruptions. Meanwhile, we would like to have a supply network topology that is robust against both types of disruptions. Therefore, in the design of supply chains one needs to seek a balance or trade-off between the robustness against random disruptions and the robustness against targeted disruptions. The DLA network growth mechanism provides the opportunity for the supply chain designer or manager to choose support network topologies, based on what type of supply network they

are building and the balance of possible disruptions that the supply network will face. For instance, a military logistic officer may prefer a DLA supply network with lower u , as military systems often need to handle targeted attacks from the enemy. An automaker may choose a DLA supply network with higher u as targeted disruptions are generally rare, if not impossible, for this type of supply chain.

6. Conclusions and Future Work

In this paper, we study the robustness of supply networks against disruptions from the perspective of complex network topologies. We first propose the new taxonomy of supply network robustness metrics to reflect the fact that, unlike in many other networks, entities or agents play heterogeneous roles in a supply network. Hence, the notions of connectedness change. The taxonomy consists of system-level metrics, including availability, connectivity and accessibility, and corresponding topology-level metrics. The second contribution of this paper is to propose a new general and hybrid supply network growth mechanism called DLA. This mechanism is based on combining preferential attachment with distance based attachment, and it offers an excellent *in-between option* when it is not possible to predict whether a random or a targeted attack will occur. We found that it has nice robustness properties under both types of attacks. The properties of the proposed network were compared with the random, scale-free, PASU networks in detail using agent-based computational simulation experiments. We also showed that by adjusting the parameters of the growth mechanism for creating a DLA network it is possible to tune its relative performance against the two types of disruptions. Recall that the multiple robustness metrics can be combined to generate a single objective function for a specific supply chain. Consequently, the designer or manager of the supply chain may be able get Pareto-optimal supply network topologies, which can provide balanced robustness in the supply chain's operational context.

Although we use the military supply network as a case study, the implications of our research are not limited to military logistic systems and have many other applications. The taxonomy of robustness metrics and the DLA network growth mechanism may also provide insights to the study and design of robust supply networks in other domains or industries. In addition, our research may also be applicable in

other complex networks whose operations rely on flows of people, information, goods or services between entities with heterogeneous roles. Example networks with similar features may include communication networks such as the Internet (with servers and clients), and infrastructure networks such as power grids.

There are several areas that we would like to address in future. In our simulation of disruptions, we only consider the removal of nodes, which corresponds to the failures of entities in a supply network. Actually, a real-world supply network may also face disruptions of connections, e.g. a road that connects a manufacturer and a retailer may be blocked due to traffic accidents. In this case, the manufacturer may need to find an alternative path to deliver the goods. Thus, it would be useful to study the removal of edges from the supply network. Other possible research directions include analyzing the performance of DLA networks with higher average degrees, exploring variants of DLA, and also modifying the way in which critical nodes are selected for a targeted disruption.

Footnotes Page:

Manuscript received ...

Authors' affiliation:

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 is 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.

List of figure and table captions:

Figure 1: A hierarchical military supply chain [10].

Figure 2: An example of the DLA growth mechanism. ID for the new node is underscored.

Figure 3: Simulated supply networks with various topologies.

Figure 4: The four networks' responses to random disruptions, plotted as (a) supply availability, (b) size of the largest functional sub-network, (c) average supply path length in the largest functional sub-network, and (d) maximum supply path length in the largest functional sub-network. Each data point is the average of 20 runs.

Figure 5: The four networks' responses to targeted disruptions, plotted as (a) supply availability, (b) size of the largest functional sub-network, (c) average supply path length in the largest functional sub-network, and (d) maximum supply path length in the largest functional sub-network. Each data point is the average of 20 runs.

Table 1: Some generic metrics for network robustness.

Table 2: Taxonomy of the new robustness metrics for supply networks.

Table 3: Simulation settings.

Table 4: Sensitivity analysis for supply availability rate (10% targeted node removal).

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, pp. 4235-4265, Oct 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, pp. 547-580, Nov 2007.
- [3] T. Y. Choi, K. J. Dooley, and M. Rungtusanatham, "Supply networks and complex adaptive systems: control versus emergence," *Journal of Operations Management*, vol. 19, pp. 351-366, May 2001.
- [4] H. L. Lee, V. Padmanabhan, and S. Whang, "The bullwhip effect in supply chains," *Sloan Management Review*, vol. 38, pp. 93-102, Spr 1997.
- [5] J. B. Rice and F. Caniato, "Building a Secure and Resilient Supply Network," *Supply Chain Management Review*, vol. 7, pp. 22-30, 2003.
- [6] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdown," *MIT Sloan Management Review*, vol. 46, pp. 53-61, Fall 2004.
- [7] K. B. Hendricks and V. R. Singhal, "An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm," *Production and Operations Management*, vol. 14, pp. 35-52, Spr 2005.
- [8] P. R. Kleindorfer and G. H. Saad, "Managing disruption risks in supply chains," *Production and Operations Management*, vol. 14, pp. 53-68, Spr 2005.
- [9] T. Wu, J. Blackhurst, and P. O'Grady, "Methodology for supply chain disruption analysis," 2007, pp. 1665-1682.
- [10] 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, pp. 24-31, 2004.
- [11] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440-442, Jun 1998.
- [12] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509-512, Oct 1999.
- [13] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, pp. 167-256, Jun 2003.
- [14] R. Albert and A. L. Barabasi, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, pp. 47-97, Jan 2002.
- [15] J. Delgado, "Emergence of social conventions in complex networks," *Artificial Intelligence*, vol. 141, pp. 171-185, Oct 2002.
- [16] K. Zhao, J. Yen, C. Maitland, A. Tapia, and L.-M. N. Tchouakeu, "A Formal Model for Emerging Coalitions under Network Influence in Humanitarian Relief Coordination," in *Proceedings of the Spring Simulation Multi-conference*, San Diego, CA, 2009.
- [17] R. M. Anderson and R. M. May, *Infectious Diseases of Humans: Dynamics and Control*: Oxford University Press, 2002.
- [18] C. Griffin and R. Brooks, "A note on the spread of worms in scale-free networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 36, pp. 198-202, 2006.
- [19] J. Leskovec, L. A. Adamic, and B. A. Huberman, "The dynamics of viral marketing," *ACM Trans. Web*, vol. 1, p. 5, 2007.
- [20] H. Zhang, C. L. Giles, H. C. Foley, and J. Yen, "Probabilistic Community Discovery Using Hierarchical Latent Gaussian Mixture Model," in *Proceedings of the 22nd Association for the Advancement of Artificial Intelligence Conference (AAAI 2007)*, 2007, pp. 663-668.
- [21] R. Albert, H. Jeong, and A. L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378-382, Jul 2000.
- [22] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, p. 056109, 2002.
- [23] G. Paul, T. Tanizawa, S. Havlin, and H. E. Stanley, "Optimization of robustness of complex networks," *European Physical Journal B*, vol. 38, pp. 187-191, Mar 2004.
- [24] M. E. J. Newman, "Assortative mixing in networks," *Physical Review Letters*, vol. 89, p. 4, Nov 2002.
- [25] T. H. Grubestic, T. C. Matisziw, A. T. Murray, and D. Snediker, "Comparative Approaches for Assessing Network Vulnerability," *International Regional Science Review*, vol. 31, pp. 88-112, January 1, 2008 2008.

- [26] J. M. Swaminathan, S. F. Smith, and N. M. Sadeh, "Modeling supply chain dynamics: A multiagent approach," *Decision Sciences*, vol. 29, pp. 607-632, Sum 1998.
- [27] J. S. K. Lau, G. Q. Huang, K. L. Mak, and L. Liang, "Agent-based modeling of supply chains for distributed scheduling," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 36, pp. 847-861, 2006.
- [28] F.-r. Lin and Y.-H. Pai, "Using multi-agent simulation and learning to design new business processes," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 30, pp. 380-384, 2000.
- [29] B. J. L. Berry, L. D. Kiel, and E. Elliott, "Adaptive agents, intelligence, and emergent human organization: Capturing complexity through agent-based modeling," *Proceedings of the National Academy of Sciences*, vol. 99, pp. 7187-7188, May 14, 2002 2002.
- [30] J. O'Madadhain, D. Fisher, T. Nelson, S. White, and Y.-B. Boey, "The Java Universal Network/Graph Framework (JUNG): A Brief Tour," in *Music-to-Knowledge North American Workshop*, University of Illinois, 2005.