

EFFECT OF TOPOLOGY ON THE ROBUSTNESS OF SUPPLY NETWORKS – METRICS AND RESULTS

Kang Zhao¹, Akhil Kumar², John Yen¹

¹College of Information Sciences and Technology ²Smeal College of Business
The Pennsylvania State University, University Park, PA 16802, USA.
kangzhao@psu.edu, akhilkumar@psu.edu, jyen@ist.psu.edu

Abstract

We develop new robustness metrics for supply networks. We also propose the new ReWiSe supply network topology based on the re-wiring of the scale-free network and show that it outperforms a pure scale-free topology in some aspects when both random and targeted disruptions are likely to occur. The unique feature of our approach is that by tuning the rewiring parameter of ReWiSe it is possible to design networks with good performance on new robustness metrics in the presence of both types of disruptions. Our model is described and the experimental results and insights about choosing the right topology for achieving robustness are discussed in detail. At 20% failure rate, the ReWiSe model has higher availability and connectivity than the scale-free network by 7 to 8% and lower proximity by the same percentage. These tradeoffs are explored further.

Keywords: Robustness, connectedness, metrics, supply network, re-wiring, simulation.

1. Introduction

With globalization and the development of information technology, supply chain systems are becoming more complex and dynamic. Conceptually, a supply network is a graph of nodes and edges, where the nodes are of two types: *supply* (or *supplier*) and *demand* (or *requester*) nodes. These networks have heterogeneous nodes as opposed to homogeneous networks where all nodes are peers. Most research in the area of complex networks has focused on homogeneous networks. However, notions of network connectedness are different in these two types of networks. Therefore, metrics of connectedness, such as path length, the largest connected component, etc, have a different meaning in a supply network than they do in a homogeneous network. For example, *from a supply point of view, a disconnected network where each partition contains a supply node is still fully connected because all nodes can receive supplies.*

Moreover, supply networks, especially large or global ones, are vulnerable to a variety of disruptions, such as natural disasters and terrorist attacks. The impact of disruptions can get propagated, sometimes even with amplifications (Lee et al. 1997), among inter-connected entities. Occasionally, failures in a small portion of the system may cause the catastrophic failure of the whole system (Rice et al. 2003), seriously affecting the flow of people, goods, information and funds with adverse consequences. Therefore, designing supply chains that are robust against disruptions has high priority, and it has drawn a lot of attention from managers, shareholders and researchers (Kleindorfer et al. 2005; Wu et al. 2007). Traditional research on supply chain robustness focuses on strategies and technologies to identify, assess, and mitigate risks and problems caused by disruptions (Chopra et al. 2004; Kleindorfer et al. 2005; Wu et al. 2007). However, there is little work on the effect of topology on robustness along the lines of (Thadakamalla et al. 2004).

In this paper, we study the robustness of heterogeneous supply networks from a topological perspective, and how the network topology affects connectedness metrics of a supply network in the presence of both random and targeted disruptions. Previous research on scale-free networks (Albert et al. 2000), which are complex networks (Albert et al. 2002; Newman 2003) with power-law degree distributions, has shown that such networks perform well under random disruptions but their performance is poor under targeted disruptions. Even a few disruptions targeted at the major high-degree hub nodes can devastate these networks. One key goal in this research is to find a network design that can provide satisfactory performance under both types of disruptions. In Section 2, we first propose a new set of robustness

metrics for heterogeneous supply networks. Then a new customizable network growth model based on the re-wiring of scale-free networks is introduced. Next, in Section 3, the robustness of our new supply network topology is evaluated and compared along with other supply network topologies, through computational simulations. Section 4 provides a discussion and concludes with directions for future work.

2. Proposed approach

In this section, we present new robustness metrics for supply networks and also introduce a new general and customizable supply network growth mechanism.

2.1 New Robustness Metrics

Robustness of a network is its ability to maintain operations and connectedness under the loss of some structures or functions. A robust supply network should be able to maintain the flow of supplies even when facing disruptions. Existing robustness metrics for homogeneous networks are generic metrics from graph theory, such as *characteristic path length*, *size of the largest connected component*, *average path length in the largest connected component* and *the maximum path length in the largest connected component*. We have developed a new set of metrics for supply networks, recognizing that there are two types of nodes in such a network, supply and demand nodes, and preserving supply-demand connectivity in disruptions is critical for sustaining operations. Table 1 shows the taxonomy of system- and topology-level metrics.

Table 1. Taxonomy of the new robustness metrics for supply networks		
System-level metric	Topology-level metric	Description
Availability	Supply availability rate	The percentage of demand nodes that have access to supplies.
Proximity	Inverse average minimum supply path length	The reciprocal of the average of each demand node's shortest supply path length to its nearest supply node.
Accessibility	Adjusted average inverse supply path length	The average inverse supply path length for all possible demand-supply node pairs, adjusted by an exponent.
Connectivity	Size of the largest functional sub-network	The number of nodes in the largest functional sub-network with at least one supply node present.

Availability is interpreted as supply availability rate, which is the percentage of demand nodes that have access to supply nodes. Consider a supply network as an undirected graph $G(V,E)$ with node set V and edge set E , where $e_{i,j} \in E$ denotes an edge between nodes $v_i, v_j \in V$. V is the union of two non-overlapping subsets of demand nodes (set V_D) and supply nodes (set V_S) as defined in Equation 1.

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

Then the set of demand nodes that have access to supply nodes in the network is defined by Equation 2:

$$V'_D = \{v_i \in V_D \mid \exists v_j \in V_S: \exists path_{i,j}\} \quad (2)$$

where $path_{i,j}$ denotes a path between nodes v_i and v_j . Thus V'_D is the set of demand nodes that have access to supply nodes through the supply network. Consequently, the supply availability AV for a supply network is defined as the ratio between the cardinalities of sets V'_D and V_D (Equation 3).

$$AV = |V'_D|/|V_D| \quad (3)$$

Our second metric is *proximity*, which measures the distance between a demand node and its nearest supply node. The average of this distance across all demand nodes (Equation 4) is a measure of how fast supplies can be delivered to demand nodes across the supply network.

$$DIST = \frac{1}{|V'_D|} \sum_{i=1}^{|V'_D|} \min\{distance(v_i, v_j), \forall v_j \in V_S\}, \text{ where } v_i \in V'_D \quad (4)$$

To make the proximity metric more intuitive, we define it as the reciprocal of *DIST*, i.e.

$$PX = 1/DIST \quad (5)$$

While *PX* measures distance to the nearest supply node from a demand node, it does not capture the trade-off between having access to two support units, each at a distance of 5, versus only one support unit at a distance of 1. Thus we want another metric that combines both *the number of supply units that can be accessed* and *their distance from demand nodes*. We call this new metric *accessibility*. This metric must satisfy the following three axioms: (1) if a demand node cannot access any supply node, $AC=0$; (2) if two demand nodes can access the same number of supply nodes, *AC* should be higher for the demand node with shorter supply paths; (3) if two demand nodes have the same shortest distance to a set of supply nodes, *AC* should be higher for the demand node which can access more supply nodes. We designed supply accessibility AC_{D_i} of demand node D_i to satisfy these requirements as follows:

$$AC_{D_i} = \sum_{j=1}^k [(1/dist_{i,j})^{1/f(j)}] \quad (6)$$

Above, k is the total number of support units that D_i can access, and $dist_{i,j}$ represents the shortest path length from D_i to its j th nearest supply node. $f(j)$ is a customizable weighting exponent that specifies the relative importance of successive supply paths. Due to the page limit, we are unable to discuss how $f(j)$ can be defined here. Thus the supply accessibility for the whole supply network is the average of AC_{D_i} over all demand nodes in the supply network, as shown in Equation 7.

$$AC = \frac{1}{|V_D|} \sum_{i=1}^{|V_D|} AC_{D_i} \quad (7)$$

Lastly, network connectivity is also important. *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 the size of the largest *functional* sub-network instead of the size of the largest connected component. Nodes in the largest functional sub-network are defined as the set V_{sub} , which satisfies the following two requirements:

$$\forall v_i, v_j \in V_{sub}, \exists p_{i,j} \text{ and } \exists v_k \in V_{sub}: v_k \in V_S \quad (8)$$

2.2 Topology Designs

We consider three different supply network topologies and evaluate them with our metrics:

(1) Scale-free network (Barabasi et al. 1999). In this network, the degree distribution of nodes follows a power-law distribution, where the number of nodes of degree k is proportional to k^{-r} , where r is a scaling exponent. The edge attachment rule for a new node follows the degree-based preferential attachment, i.e., an edge is more likely to connect to a high-degree node (Equation 9).

$$P(k) = k^{-r}, (r > 0) \quad (9)$$

(2) Erdos-Renyi random (*ER-random*) network (Erdos et al. 1959). In this network, edges are connected between nodes randomly.

(3) A re-wired scale-free network (*ReWiSe*). In this proposed network topology, we start with a scale-free network, and then randomly re-wire some edges. We iterate through all edges and get the pairs of nodes at both ends of each edge. With a pre-determined re-wiring probability p_r , an edge will disconnect from one of its two endpoints, the one with higher degree, and re-wire to connect with a randomly chosen node. If $p_r=0$, no re-wiring will take place and the network remains a scale-free network. On the other hand, if $p_r=1$, all edges will go through this random re-wiring process. The re-wiring aims at adding randomness to a scale-free network. A higher p_r will bring more randomness to the network.

Supply networks with lattice and small-world topologies (Watts et al. 1998) are not included in our experiments, because they have degree distributions that are close to that of random networks. Thus their

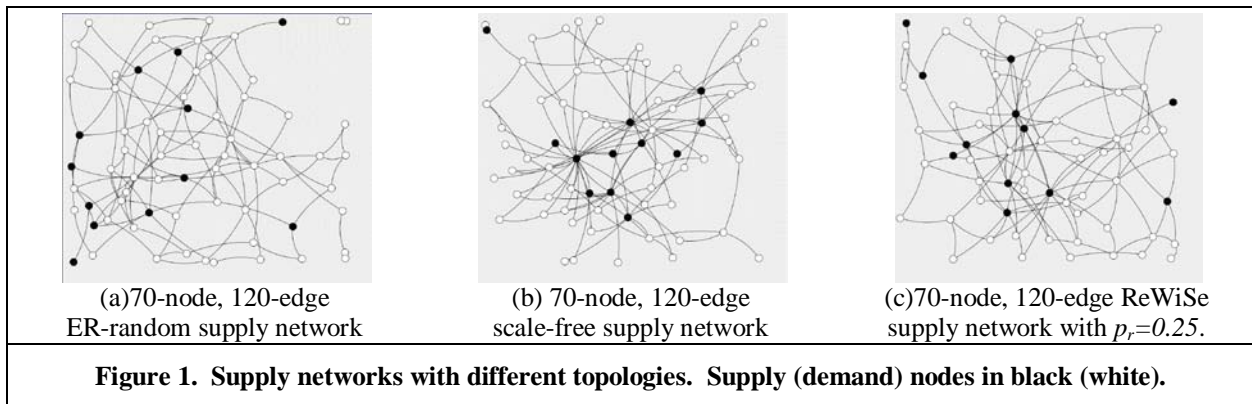
robustness is similar to that of random networks (Thadakamalla et al. 2004). In the next section, we discuss our experimental results.

3. Experimental Results

Since test attacks on real-world supply networks are inadvisable, we rely on computational simulation experiments. Agent-based simulation has become a popular choice in the study of supply chains (Swaminathan et al. 1998). In this section, we will describe our method for evaluating and comparing the robustness of different supply network topologies using agent-based computational simulations.

3.1 Simulation Settings

Our simulation scenario is based on the military supply network example in (Thadakamalla et al. 2004). The supply network consists of 1000 nodes, including 166 supply nodes and 834 demand nodes or battalions. This supply-demand ratio was estimated from a real-world military logistic system. We will compare the robustness of *ER-random*, scale-free, and *ReWiSe* supply networks with different p_r values. All the networks will have the same numbers of nodes and edges to enable a fair comparison.



When calculating distance between nodes, all edges are given a weight of 1, which means the shortest distance between nodes will be the geodesic distance in the network. For the accessibility of supply networks, we use $f(j)=1$ for Equation 5, i.e., we don't assign relative importance to supply paths. For illustrative purposes, we show the snapshots of three 70-node 120-edge supply networks with ER-random, scale-free and ReWiSe (with $p_r=0.25$) topologies in Figures 1(a), (b), and (c). The dark dots are supply nodes and the light ones are demand nodes. Notice the lower degrees of supply nodes in Figure 1(c) versus Figure 1(b) as a result of rewiring.

Table 2. Simulation settings			
Number of nodes	1000	Supply-Demand nodes ratio	1:5
Avg. number of edges per node	3.6	Accessibility weighting exponent	$f(j)=1$

Next, we simulate *random* and *targeted* disruptions. In random disruptions, random node failures are simulated, while in targeted disruptions high degree nodes fail. We only consider disruptions at the supply nodes. In our agent-based simulation, an agent represents a node in the supply network. Disruptions are simulated by the removal of agents that represent supply nodes. When an agent is removed, its connections are also removed from the multi-agent system. To simulate random disruptions, randomly chosen supply agents are removed. For targeted disruptions, supply agents are removed in decreasing order of their node degree; i.e. higher degree ones are removed earlier. 5% of all the supply nodes are removed between successive observations. We simulate disruption scenarios where the percentage of supply nodes removed lies in the 0% to 20% range. During the process of node removal, we track the robustness metrics for each network topology. Table 2 summarizes our simulation settings.

3.2 Simulation Results

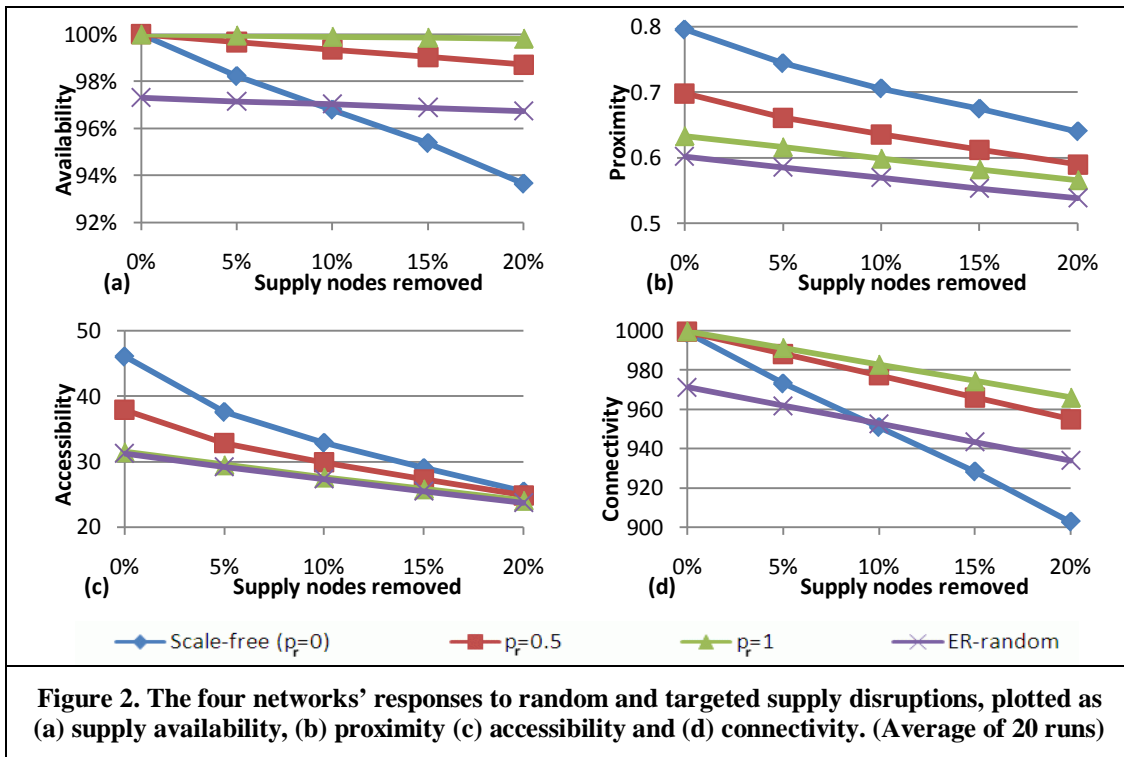


Figure 2 shows the responses of four network topologies, including scale-free, ER-random and two ReWiSe networks with $p_r=0.5$ and $p_r=1$. We averaged the results for random and targeted disruptions, assuming both types of disruptions are equally likely. The horizontal axes denote the percentage of supply nodes that have been removed, while the vertical axes show values of the proposed robustness metrics.

ER-random has relatively low values on all the four metrics, but its slope is also small. ER-random has an initial disadvantage on all metrics mainly because even when no nodes are removed the randomly generated initial network is not fully connected. The scale-free supply network excels in proximity, and its accessibility is reasonable, although its relative advantage drops when more nodes are removed. Higher p_r for ReWiSe networks leads to better availability and connectivity, but at the cost of proximity and accessibility.

We also found surprisingly good availability and connectivity from the ReWiSe network with $p_r=1$. The ReWiSe supply network offers much better availability and connectivity than scale-free networks. Figure 2(a) shows that *random disruptions of even 20% of supply units have negligible impacts on its availability*, which decreases less than 1%. Connectivity is also well preserved as almost all the remaining nodes are still connected in a functional sub-network. In terms of accessibility and proximity, its performance is not as good as scale-free but better than ER-random. Compared with scale-free networks, the ReWiSe network with higher p_r generally have a lower initial proximity and accessibility but a lower deterioration rate. $p_r=0.5$ offers a good in-between option between the fully rewired ReWiSe network with $p_r=1$ and scale-free network.

4. Discussion and Conclusions

In recent years, there has been growing interest in the research on complex networks. Studies have revealed network topologies underlying real-world complex networks. Network growth mechanisms that lead to those topologies and their properties have been studied (Albert et al. 2002; Newman 2003).

In this research, we have developed four new metrics to evaluate the robustness of heterogeneous supply networks. We also proposed the new ReWiSe topology, a supply network design that overcomes some of the drawbacks of the scale-free and ER-random networks and provides balanced robustness against disruptions. Using simulations, we compared it with scale-free and ER-random supply networks for robustness on the new metrics. Average values on the metrics for a combination of random and targeted disruptions (assuming both are equally likely) were used for understanding the trade-offs in robustness. We found that the topology choice affects robustness; ReWiSe outperforms other topologies considerably in availability and connectivity and thus is a good alternative in situations where both random and targeted disruptions can occur. It was also observed that the performance of the ER-random topology is bad. We also studied the effect of varying the re-wiring probability p_r on the performance. Increasing p_r , i.e., bring more randomness into the network, will lead to better availability and connectivity, but often at the cost of accessibility and proximity. This is intuitively meaningful. To decide the optimal value for p_r , a supply network designer should consider the trade-off between the higher cost of accessing supply nodes because of longer distances when p_r is high, versus the cost of stock outs if some nodes cannot obtain supplies when p_r is low. The research also clearly shows that supply networks that may face targeted disruptions, such as a military supply network, should avoid high-degree hub nodes.

The implications of this research are not limited to supply networks. Our robustness metrics may be modified and applied to other complex networks and infrastructure networks. For example, for a computer network like the Internet, we can use the time to transmit information between computers, as a surrogate for physical distance between nodes in our metrics. In future work, we intend to consider the effect of disruptions of edges in addition to nodes on robustness, e.g., a road that connects a manufacturer and a retailer may be blocked. Thus, it would be useful to study the effect of edge failure on the robustness of the supply network. Finally, analytical approaches for determining robustness should also be explored.

References

- Albert, R., and Barabasi, A.L. "Statistical mechanics of complex networks," *Reviews of Modern Physics* (74:1), Jan 2002, pp 47-97.
- Albert, R., Jeong, H., and Barabasi, A.L. "Error and attack tolerance of complex networks," *Nature* (406:6794), Jul 2000, pp 378-382.
- Barabasi, A.L., and Albert, R. "Emergence of scaling in random networks," *Science* (286:5439), Oct 1999, pp 509-512.
- Chopra, S., and Sodhi, M.S. "Managing risk to avoid supply-chain breakdown," *MIT Sloan Management Review* (46:1), Fall 2004, pp 53-61.
- Erdos, P., and Renyi, A. "On random graphs," *Publicationes Mathematicae*. (6) 1959, pp 290-297.
- Kleindorfer, P.R., and Saad, G.H. "Managing disruption risks in supply chains," *Production and Operations Management* (14:1), Spr 2005, pp 53-68.
- Lee, H.L., Padmanabhan, V., and Whang, S. "The bullwhip effect in supply chains," *Sloan Management Review* (38:3), Spr 1997, pp 93-102.
- Newman, M.E.J. "The structure and function of complex networks," *SIAM Review* (45:2), Jun 2003, pp 167-256.
- Rice, J.B., and Caniato, F. "Building a Secure and Resilient Supply Network," *Supply Chain Management Review* (7:5) 2003, pp 22-30.
- Swaminathan, J.M., Smith, S.F., and Sadeh, N.M. "Modeling supply chain dynamics: A multiagent approach," *Decision Sciences* (29:3), Sum 1998, pp 607-632.
- Thadakamalla, H.P., Raghavan, U.N., Kumara, S., and Albert, R. "Survivability of Multiagent-Based Supply Networks: A Topological Perspective," *IEEE Intelligent Systems* (19:5) 2004, pp 24-31.
- Watts, D.J., and Strogatz, S.H. "Collective dynamics of 'small-world' networks," *Nature* (393:6684), Jun 1998, pp 440-442.
- Wu, T., Blackhurst, J., and O'Grady, P. "Methodology for supply chain disruption analysis," Taylor & Francis Ltd, 2007, pp. 1665-1682.