

Author:

Kang Zhao*
College of Information Sciences and Technology,
The Pennsylvania State University,
University Park, PA 16802

Corresponding author e-mail address: kangzhao@psu.edu

Title:

Robustness of Heterogeneous Supply Networks against Random and Targeted Disruptions

Long Abstract:***Introduction***

Nowadays, supply chain systems are becoming more complex and dynamic. These 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 (Surana et al. 2005) and the analysis and design of supply chains should incorporate the concepts of complex systems, especially complex networks (Choi et al. 2001; Pathak et al. 2007).

Meanwhile, supply chains are often embedded in dynamic environments and may face disruptions, such as natural disasters, economic recessions, unexpected accidents or terrorist attacks. Disruptions at one or few entities in the system can get propagated, sometimes even with amplifications, and thus affect the normal operations of many other entities. Occasionally, failures of a small portion of the system may cause the catastrophic failure of the whole system (Rice et al. 2003). Therefore, designing supply chains that are robust against disruptions becomes has drawn a lot of attention from managers, shareholders and researchers (Kleindorfer et al. 2005; Wu et al. 2007).

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 (Chopra et al. 2004; Kleindorfer et al. 2005; Wu et al. 2007). The research of (Thadakamalla et al. 2004) introduced the topological perspective into the study of supply networks 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. They proposed a network growth mechanism that assigns different attachment rules to different types of units in the military supply network. 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.

New Robustness Metrics

Robustness of a network is the ability to maintain operations and connectedness under the loss of some structures or functions. However, previous research on network robustness often uses generic network metrics, such as size of the largest connected component, average path length in the largest connected component, etc. 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. Nevertheless, 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 (Grubestic et al. 2008). As a result, preserving this type of connectivity in disruptions is critical for maintaining the operations of the whole supply chain.

Taking the military supply network in (Thadakamalla et al. 2004) 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 battalions are far from support units, should not be considered as robust as there is none or limited supply flow in such a sub-network. Similarly, the distance between battalion and support units is 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.

Therefore, we proposed the new taxonomy of robustness metrics for supply networks (Table 1). 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 (Thadakamalla et al. 2004).

Table 1. 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.

New Hybrid Network Growth Mechanism

While the network growth mechanism in (Thadakamalla et al. 2004) 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. In the DLA mechanism, when a new node enters the system, its first edge attachment is based on the degrees of existing nodes. The subsequent edge attachments are based on locality, i.e., how far the new node is from existing nodes.

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 attachment rules for a new node can be generally specified as follows:

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

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

- 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:

$$P_j = (d_j^{-r}) / \sum_j (d_j^{-r}), \text{ where } r \geq 0 \text{ and } d_j > 1$$

This mechanism does not require special attachment rules for different types of units. It also provides customizability so that the preference for degree and locality can be tuned by using different combinations of u and r .

Preliminary Results

We evaluate and compare the robustness of different supply network topologies using computational simulations. Our simulation is developed using the Java Universal Network/Graph Framework (O'Madadhain et al. 2005). We adopt the military supply network example in (Thadakamalla et al. 2004) in our simulation. The military supply network consists of 1000 nodes. 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. We will compare the robustness of supply networks with random, scale-free, (Thadakamalla et al. 2004) and DLA (with $u=2$ and $r=1/2$) topologies.

For each supply network topology, we will first construct the supply network using corresponding network growth mechanism and the military supply network configuration. Then two types of disruptions are simulated: 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. As in (Thadakamalla et al. 2004), our simulations remove 50 nodes between successive observations. 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 node will have 1.8 edges in our simulations to correspond with the network in (Thadakamalla et al. 2004).

Our simulation results suggest that the (Thadakamalla et al. 2004) supply network is 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. On the other hand, the random supply 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.

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 combines the best of both worlds.

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 deviates 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.

Conclusion

In this research, 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 connectivity change. The taxonomy consists of system-level metrics, including availability, connectivity and accessibility, and corresponding topology-level metrics. The second contribution of this research is to propose a new general and hybrid supply network growth mechanism called DLA. This mechanism is based on combining preferential attachment with locality based attachment, and it has nice robustness properties under both random and targeted attacks.

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, and infrastructure networks such as power grids.

References:

- Choi, T.Y., Dooley, K.J., and Rungtusanatham, M. "Supply networks and complex adaptive systems: control versus emergence," *Journal of Operations Management* (19:3), May 2001, pp 351-366.
- Chopra, S., and Sodhi, M.S. "Managing risk to avoid supply-chain breakdown," *MIT Sloan Management Review* (46:1), Fall 2004, pp 53-61.
- Grubestic, T.H., Matisziw, T.C., Murray, A.T., and Snediker, D. "Comparative Approaches for Assessing Network Vulnerability," *International Regional Science Review* (31:1), January 1, 2008, pp 88-112.
- Kleindorfer, P.R., and Saad, G.H. "Managing disruption risks in supply chains," *Production and Operations Management* (14:1), Spr 2005, pp 53-68.
- O'Madadhain, J., Fisher, D., Nelson, T., White, S., and Boey, Y.-B. "The Java Universal Network/Graph Framework (JUNG): A Brief Tour," in: *Music-to-Knowledge North American Workshop*, University of Illinois, 2005.
- Pathak, S.D., Day, J.M., Nair, A., Sawaya, W.J., and Kristal, M.M. "Complexity and adaptivity in supply networks: Building supply network theory using a complex adaptive systems perspective," *Decision Sciences* (38:4), Nov 2007, pp 547-580.

- Rice, J.B., and Caniato, F. "Building a Secure and Resilient Supply Network," *Supply Chain Management Review* (7:5) 2003, pp 22-30.
- Surana, A., Kumara, S., Greaves, M., and Raghavan, U.N. "Supply-chain networks: a complex adaptive systems perspective," *International Journal of Production Research* (43:20), Oct 2005, pp 4235-4265.
- 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.
- Wu, T., Blackhurst, J., and O'Grady, P. "Methodology for supply chain disruption analysis," Taylor & Francis Ltd, 2007, pp. 1665-1682.