SUPPLY NETWORK TOPOLOGY AND ROBUSTNESS AGAINST DISRUPTIONS – AN INVESTIGATION USING MULTIAGENT MODEL

Anand Nair *
Department of Management Science
Moore School of Business
University of South Carolina
Columbia, SC - 29208, USA
Phone: (803) 777-2648
Fax: (803) 777-3064
E-mail: nair@moore.sc.edu

José M. Vidal
Department of Computer Science and Engineering
Swearingen Engineering Center
University of South Carolina
Columbia, SC - 29208, USA
Phone: (803) 777-0928
Fax: (803) 777-3767
E-mail: vidal@sc.edu

* Corresponding Author

(Forthcoming)
International Journal of Production Research

Supply Network Topology and Robustness against Disruptions – an investigation using multiagent model

In this study we examine the relationship between supply network's topology and its robustness in the presence of random failures and targeted attacks. The agent based model developed in this paper uses the basic framework and parameters in the experimental game presented in Sterman (1989) for modeling adaptive managerial decision making in an inventory management context. The study extends the linear supply chain context to a complex supply network and undertakes a rigorous examination of robustness of these supply networks that are characterized by distinct network characteristics. We theorize that network characteristics such as average path length, clustering coefficient, size of the largest connected component in the network and the maximum distance between nodes in the largest connected component are related to the robustness of supply networks, and test the research hypotheses using data from several simulation runs. Simulations were carried out using twenty distinct network topologies where ten of these topologies were generated using preferential attachment approach (based on the theory of scale-free networks) and the remaining ten topologies were generated using random attachment approach (using random graph theory as a foundation). These twenty supply networks were subjected to random demand and their performances were evaluated by considering varying probabilities of random failures of nodes and targeted attacks on nodes. We also consider the severity of these disruptions by considering the downtime of the affected nodes. Using the data collected from a series of simulation experiments, we test the research hypotheses by means of binomial logistic regression analysis. The results point towards a significant association between network characteristics and supply network robustness assessed using multiple performance measures. We discuss the implications of the study and present directions for future research.

Keywords: Supply networks, Topology, Disruptions, Robustness, Scale-free Networks, Random Networks, Agent-based model, Binomial Logistics Regression

Introduction

In recent times, supply disruptions are receiving considerable managerial attention due to their adverse impact on organizational performance. Sheffi and Rice (2005) highlight the supply chain implication of the terrorist attack on September 11, 2001 by giving the examples of adverse effect on Ford's and Toyota's operations. Chozick (2007) report that 70% of Japan's auto production was temporarily paralyzed for a week due to the disruptions in the supply of piston ring caused by a 6.8-magnitude earthquake that hit central Japan thereby damaging Riken Corp.'s production plant, the supplier that makes custom piston rings for most of the car makers in Japan.

The increased interest in supply chain disruptions is also evident in research studies. For instance, studies have examined the financial implications of supply chain disruptions (e.g., Hendricks & Singhal, 2003; 2005) and investigated risk mitigation and contingency planning strategies in the presence of supply chain disruptions (e.g. Sodhi, 2005; Tomlin, 2006). There is also a growing research stream that examines disruption and related supply chain issues by using a multiagent-based simulation framework (e.g. Thadakamalla et al., 2004).

Our paper fits within this multiagent based approach. In this study we examine how supply network topology is associated with its robustness in the event of disruptions. It has been observed that several supply networks exhibit incredible robustness in the presence of disruptions while others fail to survive random failures or targeted attacks. Sheffi and Rice (2005) provide examples of firms, whose supply networks are characteristically distinct from each other, making their levels of resilience and robustness to random failures and targeted attacks to be considerably different. This study builds on the extant literature in statistical physics that examine the error and attack tolerance of complex networks (Albert et al., 2000; Thadakamalla et al., 2004), and consider the impact of supply network characteristics, such as average path length, clustering coefficient, size of the largest connected component, and maximum distance between two nodes in the largest connected component, on performance measured in terms of inventory levels, backorders and total costs within a supply network.

Literature review and research hypotheses

Modeling of complex networks has focused on three main classes: (i) random graphs: these variants of Erdős – Rényi model (Erdős and Rényi, 1959; Bollobás, 1985) are still widely used in many fields and serve as a benchmark for many modeling and empirical studies; (ii) small-world models: these models interpolate between the highly clustered regular lattices and random graphs; and (iii) scale-free models (Barabási and Albert, 1999): these are motivated by the power-law degree distribution of the nodes in complex networks as evident in several networks such as the World Wide Web (Albert et al., 1999), the Internet (Faloutsos et al., 1999), or metabolic networks (Jeong et al., 2000). When viewed from the perspective of robustness to failures, it is observed that random networks and small-world networks have similar properties due to the similarity in their degree distribution (Thadakamalla et al., 2004). Meanwhile, scale-free networks are highly robust to random failures but are sensitive to targeted attacks. Thus, random networks and scale-free networks present two characteristically distinct topologies, a systematic examination of which can provide deeper insights regarding the association of network characteristics with its robustness against disruptions.

Studies, such as Albert et al. (2000), have focused on random graphs and scale-free network topologies to discern the error and attack tolerances of these networks. Consistent with this stream of research and with literature emphasizing that supply networks follow topologies commonly observed in complex adaptive systems (Surana et al., 2005; Sun and Wu, 2005; Pathak et al., 2007; Wang et al., 2008; Bichou et al., 2007), in this paper we consider random and scale-free network topologies for our research investigation of robustness of supply networks.

The theory of random networks has its origin in the use of probability methods in problems related to graph theory. Erdős and Rényi (1959) define a random graph to be one in which *N* nodes are connected to *n* edges, chosen randomly from *N(N-1)/2* possible edges. There are $C^{n}_{[N(N-1)/2]}$ possible graphs that can be formed with all graphs having equal probability of being realized in the probability space. The theory of random graphs concerns with an examination of this probability space as $N \to \infty$.

The scale-free networks were motivated from a mismatch between the clustering coefficients found in real-world network and those predicted by random graphs. Also, it has been observed that even for those networks for which *P(k)* (a distribution function representing the probability that a randomly selected node has exactly *k* edges) has an exponential tail, the degree distribution do not follow Poisson distribution as suggested in random graphs theory. Barabási and Albert (1999) present the idea of scale-free network by considering the power-law degree distribution that is observed in several real world networks. The networks grow by continuous addition of new nodes. Instead of following a random-attachment of nodes, these networks follow a preferential attachment logic whereby new nodes join a node that is already highly connected (i.e. exhibit high degree). Formally, the probability Π that a new node *n* will connect to a node *i* in the network depends on the degree k_i of node *i*: $\Pi(k_i) = \dfrac{k_i}{\sum_j k_j}$.

Further details on the analytical and empirical developments in the random graphs and scale-free network theory are presented in Albert and Barabasi (2000) and Dorogovtsev and Mendes (2002). In the following subsections we present details regarding network characteristics that are used for our research investigation.

Average path length

The average path length presents an approach to characterize the spread of a network by calculating the average distance between any pair of nodes. For a network with *N* nodes, it is likely that not all nodes will have the same number of edges (also referred as node degree). The spread of the node degrees is characterized in terms of the distribution function *P(k)*. The degree distribution of most random networks can be approximated by binomial distribution (with Poisson distribution being a more appropriate approximation for very large number of nodes). The average path length of a network is related to the number of nodes, *N*. The average path length of scale-free networks examined by Barabasi and Albert (1999) increases approximately logarithmically with the number of nodes, *N*. It can be argued that with a low average path length, the nodes within a supply network are able to transport products and communicate information more quickly thereby aiding in its robustness against disruptions. Based on this reasoning we hypothesize:

H1: In the presence of disruptions, the robustness of supply network is negatively associated with its average path length.

Clustering coefficient

Clustering coefficient capture the small-world nature inherent in several real-world networks. Specifically, this measure suggests that the probability of the nearness of two nodes is related to the nearness of these nodes to a third node. In a random network the probability that nearest neighbors of a node are connected is equal to the probability that two nodes in the network are connected. The clustering coefficient of scale-free networks proposed by Barabasi and Albert (1999) are higher than that of the random networks and

this difference increase as the number of nodes increase. The cliquish property represented by clustering coefficient is expected to be useful in the normal operations of a supply network. However, in the event of disruptions it could result in high level of vulnerability due to the high levels of dependency among the nodes. The disruption of any node will adversely impact the functioning of all nodes that are closely connected to it. We hypothesize:

H2: In the presence of disruptions, the robustness of supply network is negatively associated with its clustering coefficient.

Largest connected component – Size and maximum distance

A connected, isolated subgraph or cluster of a network is defined as its component. Several simulation studies have highlighted the importance of the size of the largest connected component within a network and the maximum distance between the nodes in the largest connected component, particularly in the context of robustness against random failures and targeted attacks (see for example, Albert et al., 2000; Cohen et al., 2000; Moreno et al., 2002; Thadakamalla et al., 2004). With a large connected component, a supply network is able to manage disruptive events relatively better. In spite of the loss of some of its structures or loss of functionalities of some of its nodes, it is able to maintain a fair amount of connectedness among nodes (Thadakamalla et al., 2004) due to the existence of a path between the pair of nodes in the component. Further, as the size of the largest connected component increase the maximum distance between any two nodes in the component increase. This allows a node to have a farther reach in the event of disruption. Drawing on this reasoning we hypothesize:

H3: In the presence of disruptions, the robustness of supply network is positively associated with the size of its largest connected component.

H4: In the presence of disruptions, the robustness of supply network is positively associated with the maximum distance in its largest connected component.

We consider robustness of the supply network in terms of three performance measures: inventory levels (H1a – H4a), backorders (H1b – H4b) and total costs (H1c – H4c). Specifically, we examine if the topological characteristics of a supply network explain the significant differences in these performance measures in the presence and absence of disruptions.

Research Design

The use of agent-based simulation model in supply chain context is gaining research interest (e.g. Moyaux, et al., 2007). In this study we develop multi-agent model using the NetLogo modeling platform (Wilensky, 1999). The approach enables us to capture the complexities and dynamics associated with network topologies and examine the evolutionary nature of choices made by firms within these supply networks. It also allows an investigation of the impact of failure of a node (representing a supply chain entity) on the overall behavior of the supply network.

Agent-Based Model

Our model extends the experimental game presented in Sterman (1989) by allowing for more complex network topologies. The dynamic decision making model has four players - factory, distributor, wholesaler and retailer – linked in the form of a serial supply chain. We model the stock and flow structure of the system, the decision rule used by managers, and the values for characterizing the parameters and costs similar to that in Sterman (1989). As an initial validation check we use the basic experimental setup and subject it

to a step demand function as studied in Sterman (1989), i.e. a constant demand of four cases and a one-time increase in customer demand to eight weeks in week 5. The results obtained from the agent-based model provide a satisfactory replication of the results in Sterman (1989).

Once the validity of the results for the basic experimental setup was established, we extended it by considering multiple distributors, retailers, and customers. The model allows the network to evolve until a specified number of nodes (i.e. factories, distributors, warehouses and retailers) are created. During the evolution, we can specify the logic by which the nodes attach to other nodes. We subject the network formation process with certain conditions to ensure that the resulting network represents a valid supply network. In particular, we consider a single factory who can supply to warehouse, distributors or retailers depending upon the specific network topology (i.e. random network or scale free network) that is under consideration. The supplies to the factory are modeled with a lead time without explicitly modeling the raw materials and component suppliers. In our network considerations, the end customer demand is always satisfied from a retail location.

Since in a network setup each supply chain entity (i.e. factory, distributors, warehouses, and retailers) can supply to more than one demand source, we had to add some extra rules that are not present in the basic experimental game setup presented in Sterman (1989). The supply chain entities satisfy orders they receive on a first-come first-serve basis, regardless of the amount in the order. The quantity that a factory, distributor or wholesaler is unable to fulfill is treated as backorder. The shortages at the retail location are lost orders. In the model presented in Sterman (1989) all players start with

the same inventory since each has only one customer. In our model the initial inventory at each supply chain entity is proportional to the number of demand sources that it supplies to.

Two supply chain entities that are directly connected to each other are at a distance of one. More generally, the distance between any pair of supply chain entities is the smallest number of edges which one would need to traverse in the graph to go from one node to the other. The calculation of these values is the classic max-flow problem in graph theory that can be solved using Dijkstra's algorithm (Cormen et al., 2003). Our model implements Dijkstra algorithm to find the shortest path between all pairs of nodes and then uses these values to determine the average path length and the largest connected component.

With the overall framework and constraints presented earlier, scale-free networks were generated by using the preferential attachment logic (Barabási and Albert, 1999), and the random networks are generated by following a random attachment of nodes. We generate ten network topologies representing random networks and ten network topologies representing scale-free networks. To generate a new network we start with one node, the factory, and then create new nodes one at a time connecting them to existing nodes. In the random network topology each new node is connected to one randomly chosen existing node where all existing nodes have equal probability of being chosen. In the preferential attachment topology we follow the standard algorithm (Barabasi and Albert, 1999) and connect each new node to one existing node but now each node's probability of being chosen is directly proportional to the number of edges that it has. For example, if there are three nodes with 1, 2, and 3 edges respectively, then each will be

chosen with a probability of 1/6, 2/6, and 3/6. We measure the network characteristics, i.e. average path length, clustering coefficient, size of the largest connected component and maximum distance between nodes in the largest connected component by using the definitions as discussed earlier in the paper.

In an agent based model all the facilities as well as the customers (modeled as a random demand function that sets the value of demand at every time step as a number between 0 and 8) are treated as agents. To ensure consistency and comparability between the various topologies considered in the study, each topology consists of 18 facilities comprising of one factory, five intermediaries acting as distributors or warehouse, and twelve retail locations that are directly facing the customer demand. The choice of the scale (i.e. one factory, five intermediaries and twelve retailers) is arbitrary and the model can be scaled to higher and lower number of nodes.

In the event when a facility fails due to random failure or targeted attack, the purchase orders and deliveries arriving to the facilities accumulate until the facility becomes functional. Once the facility is operational, the purchase orders and deliveries are attended to on a first-come first-serve basis. The timing in our model is the same as in the experimental setup presented in Sterman (1989). The unit of analysis is in weeks and all facilities take decisions on a weekly basis. Both orders and deliveries have to spend one week in transit and the total replenishment cycle (from order to receipt) is 4 weeks.

Experimental Design

The development of the simulation model and the analysis of the data gathered from simulation runs follow the systematic approach suggested in literature (Kelton, 1997; Sargent, 1998; Nance and Sargent, 2002; Law, 2004). The overall experimental design

and parameters used for the study are reported in table 1. We ran the agent based simulation model for 105 time ticks; each time tick corresponds to a week. We collect data from twenty replications of each scenario of the simulation model, and use the average of the weekly data obtained from these 20 replications for analysis.

[Table 1 about here]

Results and Discussion

We examine the robustness of individual topologies by undertaking paired sample t-test for each network topology considered in the study. The performance of a network in the absence of both random failures and targeted attacks is used as the base case. The performance of all twenty network topologies considered in this study in the presence of varying degrees of random and targeted disruptions are compared with the base case. In total 24 paired sample t-tests (for each disruption scenario explained in the experimental design) were conducted for each topology. Robustness of a network topology against disruptions is gauged by a non significant difference in the mean for the performance measures as reported by the paired sample t-test (i.e. p-value > 0.05). The topologies that exhibit significant difference of performance (i.e. p-value $\leq$ 0.05) are considered as vulnerable to disruptions.

As a next step, we utilize the information from the paired t-test and categorize the topologies as robust (coded as 1) or vulnerable (coded as 0). We use binomial logistics regression analysis to examine how the robustness of supply network against disruptions is associated with average path length, clustering coefficient, size of the largest connected component within the network, and the maximum distance between nodes in the largest

connected component of the network. Initially, we undertake the binomial logistics regression analysis for the entire sample of network topologies considered in this study. We use the topology type (categorical variable denoting scale-free and random network) as a control variable. Subsequently, we split the sample into scale-free and random-networks and investigate the hypothesized relationships in these network topologies separately. The sample size, mean, standard deviation, minimum and maximum values for the independent and dependent variables used for binomial logistics regression analysis are presented in table 2.

[Table 2 about here]

Overall Sample

The results of the binomial logistics regression analysis for the overall sample are presented in table 3.

[Table 3 about here]

The pseudo R-square value (Nagelkerke R-square) suggest that the independent variables explain almost 11.8%, 35.2% and 19.2% of variations in the robustness of supply networks from the perspectives of performance impacts measured in terms of inventory levels, backorders and total costs, respectively. The results emphasize the important role played by network characteristics and topology type in determining the robustness of supply networks.

From the results of the analysis we fail to find an association between maximum distance between the nodes in the largest connected component and the robustness of the network topology examined in terms of change in inventory levels in the presence of disruptions (hypothesis H1c). All other hypothesized relationships are strongly supported

($p<0.05$). The results in table 3 also show that scale-free networks are relatively more robust from the inventory perspective, however, when viewed from the backorders and total cost perspectives, random networks are more robust.

The results present a compelling evidence of the association between network characteristics and robustness of supply networks. We find that a unit increase in average path length and clustering coefficient substantially increase the odds of making the supply network vulnerable from the point of view of inventory levels, backorders and total costs. As shown in table 3, for every unit increase in the size of the largest connected component the odds of having a robust supply network from the perspectives of inventory levels, backorders and total costs increase by about 1.6 times, 3 times and 2.6 times respectively. A unit increase in the maximum distance between nodes in the largest connected component increases the odds of a robust supply network from backorders and total cost perspective by a factor of 8.7 and 10.2, respectively.

Scale-free Networks

The results of the binomial logistics regression analysis for the scale-free network topology sub-sample are presented in table 4.

[Table 4 about here]

The pseudo R-square values (Nagelkerke R-square) suggest that the average path length, clustering coefficient, size of the largest connected component and the maximum distance between nodes in the largest connected component explain almost 21.9%, 24.5% and 26.3% variation in the robustness of supply networks characterized in terms of inventory levels, backorders and total costs, respectively. These values highlight that

topological considerations are extremely valuable in understanding the robustness of supply network.

The results suggest that the average path length, clustering coefficient and size of the largest connected component are significantly associated with deterioration of inventory levels in the presence of disruptions, as hypothesized in H1a, H2a and H3a. We do not find support for the association of maximum distance between nodes in the largest connected component with deterioration in inventory levels in the presence of disruptions. Hypotheses H1b-H4b are supported, suggesting that all network characteristics considered in this study are significantly associated with robustness of supply networks evaluated from the perspective of deterioration in backorders in the presence of disruptions. Finally, we do not find support for hypotheses (H1c and H4c) linking average path length and maximum distance between nodes in the largest connected component with deterioration of total costs in the supply network in the presence of disruptions. However, clustering coefficient and the size of the largest connected component were significantly associated with robustness from total cost perspective (H2c and H3c).

We find that a unit increase in clustering coefficient substantially increase the odds of making the supply network vulnerable. A unit increase in average path length also substantially increase the odds of making the supply network vulnerable from the point of view of inventory levels and backorders. Table 4 indicates that as the size of the largest connected component of scale-free networks increase by one unit the robustness of the network from inventories, backorders and total costs perspectives increase by almost 2, 2.7 and 5 times, respectively. While the maximum distance between nodes in

the largest connected component is not significantly associated with inventory and total cost based robustness measures, a unit increase in this variable increases robustness from backorders perspective by almost 5 times.

Random Networks

We present the results of the binomial logistics regression analysis for the sub-sample comprising of random networks in table 5.

[Table 5 about here]

The Nagelkerke R-square values suggest that the network characteristics considered in this study explain almost 8%, 33.8% and 13.6% variation in the robustness of supply networks from inventory, backorders and total cost perspectives.

We find a weak association of clustering coefficient and maximum distance between nodes in the largest connected component with robustness of supply networks in terms of inventory levels (H2a and H4a). The results do not support an association of average path length and size of the largest connected component with robustness in terms of inventory levels. All hypothesized relationships for robustness, measured in terms of backorders and total costs, were supported (H1b – H4b & H1c-H4c).

We find that similar to scale-free networks, a unit increase in clustering coefficient substantially increases the odds of vulnerability of random networks against random failures and targeted attacks. A unit increase in average path length substantially increases the odds of vulnerability from backorders and total cost perspectives. Table 5 shows that a unit increase in the size of the largest connected component increases supply network robustness, viewed from backorders and total cost perspectives, by a factor of 3.2 and 2.1 times, respectively. A unit increase in the maximum distance between nodes

in the largest connected component was found to increase the odds of a robust supply network by 3.7 times, 14.1 times and 16.9 times when the robustness is evaluated from inventory, backorders and total cost perspectives respectively.

Implications and directions for future research

Based on the findings from this study we emphasize that long average path lengths between nodes in a supply network are detrimental for its robustness against disruptions. Shorter average distances between nodes in the network allow faster propagation of products and information and thus aid in enhancing the responsiveness of supply network in the event of disruption. A clustered form of supply network has been widely adopted by several firms due to its advantages in terms of consolidation, efficiency and quick response. The results of this study suggest careful examination of the nature of connection between nodes within clusters as well as in the overall supply network. Managers ought to balance the advantages of a clustered configuration of facilities in the supply network with the potential disadvantages in the presence of disruptions. Finally, the reach of a facility in the largest sub-structure plays a positive role in enhancing the robustness of a supply network. The study's findings motivate the need for an evaluation of supply network robustness from multiple outcome metrics. It is important to give consideration to various performance metrics, such as inventories, backorder, total costs, to get a better understanding of the robustness of the supply network.

There are a few limitations of this study that provide directions for future research. In this study we do not consider the aspect of rewiring of nodes that often provide an adaptive mechanism in the event of disruptions. Future studies can examine how inventories could be reassigned in the event of disruptions and investigate efficient

heuristics for such reassignments. It would also be worthwhile to examine the implications of fortifying certain nodes, identifying the nodes that are most suitable to be fortified and examining the implications of such actions on the relationship between network characteristics and robustness of supply network. Finally, empirically validation of the relationship examined in this paper from real-world supply networks would be a fruitful area of research investigation.

References

1. Albert, R., Jeong, H. and Barabasi, A., 2000. Error and attack tolerance of complex networks. *Nature*, 406(27), 378-382.
2. Barabási, A. and Albert, A., 1999. Emergence of scaling in random networks. *Science*, 286 (5439), 509-512
3. Bichou, K., Bell, M.G.H., and Evans, A., 2007. *Risk management in port operations, logistics, and supply chain security*. London: Informa.
4. Bollobás, B. (1985). *Random Graphs*. Academic Press, London, 1985.
5. Choi, T.Y., Dooley, K.J, and Rungtusanatham, M., 2001. Supply Networks and Complex Adaptive Systems: Control versus Emergence. *Journal of Operations Management*, 19, 351-366.
6. Chozick, A. 2007. A Key Strategy of Japan's Car Makers Backfires. *Wall Street Journal*, July 20, B1.
7. Cohen, R., Erez, K., ben-Avraham, D., & Havlin, S. (2000). Resilience of the Internet to random breakdowns. *Phys. Rev. Lett.*, 85, 4625
8. Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C. 2003. *Introduction to Algorithms*. Cambridge, MA: MIT Press.
9. Dorogovtsev, S.N. and Mendes, J.F.F., 2002. Evolution of networks. *Advances in Physics*, 51(4), 1079-1187.
10. Erdős, P. and Rényi, A., 1959. On random graphs. *Publiationes Mathematicae*, 6, 290-297.
11. Faloutsos, M., Faloutsos, P. and Faloutsos, C., 1999. On power-law relationships of the internet topology, ACM SIGCOMM '99. *Comput. Commun. Rev.* 29, 251–263.
12. Hendricks, K. and Singhal, V., 2003. The effect of supply chain glitches on shareholder wealth. *Journal of Operations Management*, 21, 501–522.
13. Hendricks, K. and Singhal, V., 2005. 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*, 14(1), 35–52.
14. Jeong, H, Tombor, B, Albert, R, Oltvai, Z.N., and Barabasi, A., 2000. The large-scale organization of metabolic networks. *Nature*, 407(6804), 651-654.
15. Kelton, W.D., 1997. Statistical analysis of simulation output. *Proceedings of the 1997 Winter Simulation Conference*, 23-30.
16. Law, A.M., 2004. Statistical Analysis of Simulation Output Data: The Practical State of the Art. *2004 Winter Simulation Conference*, 67-72.
17. Moreno, Y., Gomez, J. B., and Pacheco, F. K. (2002). Instability of scale-free networks under node-breaking avalanches. *Europhys. Lett*, 58, 630-636.
18. Moyaux, T, Chaib-draa, B., and D'amours, S., 2007. Information sharing as a coordination mechanism for reducing the bullwhip effect in a supply chain. *IEEE Transactions on Systems, Man, and Cybernetics*. 33(3), 396-409.
19. Nance, R.E and Sargent, R.G., 2002. Perspectives on the evolution of simulation. *Operations Research*, 50(1), 161-172.
20. Pathak, S.D., Day, J.M., Nair, A., Sawaya, W., and Kristal, M.M. 2007. Complexity and Adaptivity in Supply Networks: Building Supply Network

Theory Using a Complex Adaptive Systems Perspective. *Decision Sciences*, 38(4), 547-580.
21. Sargent, R.G. 1998., Verification and validation of simulation models. *Proceedings of the 1998 Winter Simulation Conference*, 121-130.
22. Sheffi, Y. and Rice, J., 2005. A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1), 41–48.
23. Sodhi, M., 2005. Managing demand risk in tactical supply chain planning for a global consumer electronics company. *Production and Operations Management*, 14(1), 69–79.
24. Sterman, J.D., 1989. Modeling managerial behavior: Misperceptions of feedback in a dynamic decision making context. *Management Science*, 35(3), 321-339.
25. Sun, H. and Wu, J., 2005. Scale-free characteristics of supply chain distribution systems. *Modern Physics Letters B*, 19(17), 841-848.
26. Surana, A., Kumara, S., Greaves, M, and Raghavan, U.N., 2005. Supply-chain networks: a complex adaptive systems perspective. *International Journal of Production Research*, 43(20), 4235-4265.
27. Thadakamalla, H.P., Raghavan, U.N., Kumara, S., and Albert, R., 2004. Survivability of multiagent-based supply networks: A topological perspective. *IEEE Intelligent Systems*, 19, 24–31.
28. Tomlin, B., 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science*, 52, 639–657.
29. Wang, K., Zeng, Z., and Sun, D., 2008. Structure Analysis of Supply Chain Networks Based on Complex Network Theory. 2008 *Fourth International Conference on Semantics, Knowledge and Grid.*
30. Wilensky, W. 1999. *NetLogo*. Center for Connected Learning and Computer-Based Modeling, Northwestern University. Evanston, IL.

Table 1: Experimental Design*

No. of Experiments	(A) Network topologies	(B) Probability of random failure of nodes	(C) Probability of targeted attack on nodes	(D) Severity of disruption
500 experiments* conducted by using different permutations of values for variables: (A) – (D)	20 (10 topologies with preferential attachment and 10 topologies with random attachment logic	0, 5%, 10%	0, 5%, 10%	1 week, 2 weeks, 3 weeks

*For each topology the experimental design provides 27 potential scenarios. When the probability of random failure of nodes and probability of targeted attack on nodes is 0, the severity of disruption is redundant. We consider this "no disruption" scenario as a base case. In total we have 24 scenarios that represent varying degrees of disruption faced by each network topology. We examine the robustness of each network topology in the presence of disruption by undertaking 24 paired-samples t-tests using the no disruption case as reference. When the probability of random failure and targeted attack on nodes is 0, the severity of disruption does not have any consequence on the results. Thus, when the probability of random failure and targeted attack on nodes is 0 we consider only one instance of severity of disruption and remove the remaining redundant experiments from further consideration. In total, this provides data from 500 experiment for further analysis.

Table 2: Descriptive Statistics for the Overall Sample and the Sub-sample comprising of scale-free networks and random networks

	Average Path Length	Clustering Coefficient	Size of the largest connected component	Maximum distance in the largest connected component	Total inventory in the supply network	Total backorders in the supply network	Total costs in the supply network
OVERALL SAMPLE (Sample Size 480)							
Mean	3.057	0.377	22.203	6.654	1372.579	943.369	3044.701
Std. Dev.	0.577	0.022	3.897	0.795	2793.159	1842.997	5813.443
Min.	1.733	0.320	14.470	4.635	57.668	181.144	498.695
Max.	4.462	0.436	29.324	8.865	18444.936	15407.885	41363.915
SCALE-FREE NETWORKS (Sample Size 240)							
Mean	2.921	0.384	22.219	6.420	732.798	516.000	1656.374
Std. Dev.	0.556	0.021	3.800	0.800	705.310	307.749	1102.047
Min.	1.733	0.332	14.470	4.635	57.668	181.144	498.695
Max.	4.057	0.436	29.079	8.697	3499.485	2406.916	7339.194
RANDOM NETWORKS (Sample Size 240)							
Mean	3.193	0.371	22.186	6.888	2012.360	1370.739	4433.027
Std. Dev.	0.566	0.215	3.999	0.718	3783.727	2519.120	7915.055
Min.	2.122	0.320	14.648	5.451	177.528	340.353	991.714
Max.	4.462	0.416	29.324	8.865	18444.936	15407.885	41363.915

Table 3: Binary Logistics Regression Analysis Results (Overall Sample)

INVENTORY

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-2.409	.831	8.412	***	.090
Clustering Coefficient	-32.629	8.554	14.550	***	.000
Size of the largest connected component	.466	.098	22.632	***	1.594
Max. distance in largest connected component	.024	.395	.004	-	1.024
Topology type^	-0.447	0.269	2.773	*	0.639

Nagelkerke R-square: 0.118; Hosmer and Lemeshow Test (χ^2): 14.519 (p-value = not significant)

BACKORDERS

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-6.420	1.150	31.152	***	.002
Clustering Coefficient	-93.508	17.203	29.545	***	.000
Size of the largest connected component	1.109	.154	51.592	***	3.031
Max. distance in largest connected component	2.160	.546	15.679	***	8.673
Topology type^	1.730	.351	24.349	***	5.643

Nagelkerke R-square: 0.352; Hosmer and Lemeshow Test (χ^2): 4.655 (p-value = not significant)

TOTAL COST

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-5.056	2.176	5.399	**	.006
Clustering Coefficient	-106.712	36.582	8.509	***	.000
Size of the largest connected component	.954	.291	10.738	***	2.595
Max. distance in largest connected component	2.326	1.084	4.602	**	10.239
Topology type^	1.064	.633	2.830	*	2.899

Nagelkerke R-square: 0.192; Hosmer and Lemeshow Test (χ^2): 3.473 (p-value = not significant)

***Significant at p<0.01; **Significant at p<0.05; *Significant at p<0.10

^Scale-free network is used as a reference for the categorical variable "Topology Type"

Table 4: Binary Logistics Regression Analysis Results (Scale-free Networks)

INVENTORY

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-3.588	1.117	10.311	***	.028
Clustering Coefficient	-42.353	11.119	14.508	***	.000
Size of the largest connected component	.702	.129	29.658	***	2.017
Max. distance in largest connected component	-.122	.511	.057	-	.885

Nagelkerke R-square: 0.219; Hosmer and Lemeshow Test (χ^2): 4.638 (p-value = not significant)

BACKORDERS

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-5.570	1.821	9.351	***	.004
Clustering Coefficient	-87.722	25.477	11.855	***	.000
Size of the largest connected component	.988	.230	18.544	***	2.687
Max. distance in largest connected component	1.630	.831	3.845	**	5.101

Nagelkerke R-square: 0.245; Hosmer and Lemeshow Test (χ^2): 9.011 (p-value = not significant)

TOTAL COST

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-5.657	4.177	1.835	-	.003
Clustering Coefficient	-202.191	102.440	3.896	**	.000
Size of the largest connected component	1.633	.729	5.019	**	5.121
Max. distance in largest connected component	2.136	1.965	1.182	-	8.466

Nagelkerke R-square: 0.263; Hosmer and Lemeshow Test (χ^2): 0.847 (p-value = not significant)

***Significant at p<0.01; **Significant at p<0.05; *Significant at p<0.10

Table 5: Binary Logistics Regression Analysis Results (Random Networks)

INVENTORY

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	1.082	1.595	.460	-	2.952
Clustering Coefficient	-35.244	19.811	3.165	*	.000
Size of the largest connected component	-.254	.191	1.764	-	.776
Max. distance in largest connected component	1.309	.762	2.949	*	3.703

Nagelkerke R-square: 0.080; Hosmer and Lemeshow Test (χ^2): 10.371 (p-value = not significant)

BACKORDERS

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-6.981	1.577	19.609	***	.001
Clustering Coefficient	-102.510	23.801	18.551	***	.000
Size of the largest connected component	1.178	.214	30.174	***	3.248
Max. distance in largest connected component	2.647	.777	11.613	***	14.109

Nagelkerke R-square: 0.338; Hosmer and Lemeshow Test (χ^2): 9.521 (p-value = not significant)

TOTAL COST

Variable	Beta	Std Err	Wald	Sig.	Exp(Beta)
Average Path Length	-5.223	2.668	3.832	**	.005
Clustering Coefficient	-83.064	39.926	4.328	**	.000
Size of the largest connected component	.743	.334	4.955	**	2.103
Max. distance in largest connected component	2.827	1.401	4.073	**	16.891

Nagelkerke R-square: 0.136; Hosmer and Lemeshow Test (χ^2): 4.475 (p-value = not significant)

***Significant at p<0.01; **Significant at p<0.05; *Significant at p<0.10