http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (8): 1614-1619, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1614.1619

Supply-chain Dynamic Invulnerability Research Based on Node Failure

Hong Liu and Biwei Li
College of Computer and Information Engineering, Zhejiang Gongshang University Hangzhou, 310018, People's Republic of China

Abstract: The unexpected incident in supply chain is occurred unexpectedly under some control of certain accident factors, causes serious damage or effect and need immediate processing. However, this tendency of supply chain network complexity intensifies the uncertainty of supply chain network's operating environment; any node in the supply chain network occurs unexpected incident which will soon affect the associated upstream and downstream enterprises and then affect the all enterprises on the network. For cascading problems of supply chain, this study proposed a capacity reallocation strategy with local and global information integrated. Based on this strategy, three attacking methods were adopted to simulate emergency events of supply chain and the vulnerability of supply chain network is measured through maximum connected subgraph and network efficiency. The experimental results show that the reallocation strategy put forward is practical and highly efficient.

Key words: Supply chain, node failure, capacity allocation, network attacks

INTRODUCTION

Supply chain is a complex network composed by suppliers, manufacturers, distributors, logistics providers, wholesalers and retailers, etc. The chain transforms the raw materials into finished products to meet customer demands and each node enterprise has a certain degree of relevance. For highly competitive product market, the processing of the supply chain system is rather interdependent. The collapse of a specific node will not only affect its normal operation, but may also result in supply interruptions or demand fluctuations through infection mechanism of accumulation, enlarging or mutation. The failure could interrupt the normal functioning of upstream or downstream enterprises and sometimes evolve into a crisis throughout the supply chain. Therefore, there is great practical and theoretical significance in improving the network quality in order to cope with various failure impacts.

Many scholars have done some research of supply chain invulnerability. Christopher (2003) infered that quick responsive network after status change is the most powerful way to realize supply chain resilience. Mixed flexible and redundancy methods is put forward by Rice and Caniato (2003) to enhance the resilience of the supply chain. Haywood and Peck (2003) found that when the supply chain status changes, the supply chain is more vulnerable to attacks. Muckstadt *et al.* (2001) put forward the strategy of increasing supply chain partnerships and cooperation intensity and reducing the uncertainty of the operating environment in order to create the supply chain resilience. Helbing *et al.* (2006) found that a good supply chain structure could increase the network stability and attack resistance. In the supply chain network, subtle changes of any nodes may bring changes to other node, which is closely related to the topology and macroscopic properties of the supply chain. Kuhnert *et al.* (2006) discovered that the material supply network obeys scale-free distribution, within which a small number of core nodes plays an important material scheduling and distributing role. Laumanns and Lefeber (2006) considered the supply chain network as a dynamic flowing process of material, in which each node is regarded as a converter and the material transforms when passing through a specific node. The first-order differential equation could be adopted to simulate the process and the supply chain could be optimized by the robust optimal control method. The robustness to random failure and the vulnerability to targeted attacks are defined by Albert *et al.* (2000) as basic characteristics of scale-free network, while the heterogeneity of the degree distribution of scale-free network is the source. In the studies above-mentioned, the flexible supply chain and various quantitative methods were qualitatively discussed or proposed, enhancing supply chain resilience under uncertainties or disturbances. For these studies, only one specific enterprise was taken into considered, without considering the concatenating failure problem of the other enterprises.

Corresponding Author: Hong Liu, College of Computer and Information Engineering, Zhejiang Gongshang University Hangzhou, 310018, People's Republic of China

In this study, a node capacity allocation strategy is proposed, with global and local information integrated for the multi-vendor and multi-manufacturer supply chain. The strategy could analyze the stability and resistance of the supply chain network, under circumstances such as node failure and chain interruption of complex network.

PROBLEM DESCRIPTION

The stability of supply chain network structure refers to keeping the fluctuation of some major macroeconomic statistics within pre-specified ranges. The common statistics include the size of the largest connected subgraph, the shortest path and the maximum distance and etc. When supply chain system is influenced by factors such as emergent events or frequent changes, the statistics would change accordingly. Obviously, within a certain time period, if these macro statistics fluctuates widely, the structural stability of system is substantially lower; and vice versa. In supply chain management, there exists primarily following types of emergencies: (1) Random emergent event, which randomly damages the production of a specific enterprise or the supply relationships between enterprises; (2) Targeted emergent event, which deliberately undermines the core enterprises or key supply relationships in the supply chain network and (3) Mixed emergent event, which contains the characteristics of both random and targeted attacking emergent events, undermining not only the production of a specific enterprise or supply relationships between enterprises but also the core enterprises or key supply relationships (Jian and Jian, 2009).

For the complex network theory, it is mainly through eliminating points (or sides) to simulate the impact of emergent events. Usually, the entire stability and responsiveness of supply chain network is analyzed when the number of eliminated points (or sides) steadily increases. In this study, three ways of point elimination (random elimination, targeted elimination and mixed elimination) are adopted to carry out such the analysis. To prevent the possible cascading failure of nodes, load-preference capacity allocation strategy with integrated global and local information is analyzed.

SUPPLY CHAIN INVULNERABILITY

The model of supply chain network: Supply chain network is a typical complex economic network. The rapid development of electronic commerce has exacerbated the complexity of its structure. Suppose the network have suppliers (a = 1, 2… A), manufacturers (b = 1, 2…, B), distributors (c = 1, 2, ..., C) and d retailers and users (d = 1, 2, ..., D). The raw materials is input into the entire network by (a) (supplier) and meets the user demands after sequentially passing through (b) (manufacturing), (c) (distribution) and (d) (retailing). Assume that each node has limited capacity of supply (or production, distribution, inventory) and due to the geographical location each node has different transportation cost. During the functioning of supply chain network, some outside irresistible factors (such as earthquakes, floods, hurricanes, etc.) may result in the sudden failure of a node in the supply chain (Yan *et al*., 2010).

The network can be described as the form:

$$G^W = (V, E, W)$$

where, $V = (v_1, v_2,..., v_N)$ denotes the set of nodes, representing the four categories of enterprises in the supply chain, namely supplier, manufacturer, distributor and retailers. Each node is dynamically interconnected through logistics, information and capital flow. $E = (e_1, e_2,..., e_M)$ is the set of edges and $e_i = (v_i, v_j)$ is the supply relationship between enterprises v_i and v_j. $W = (w_1, w_2,..., w_M)$ denotes the set of weight values of edges and each element w_{ij} ($w_{ij} \geq 0$) denotes the weight of the specific edge connecting v_i and v_j (weight value can be trading volume).

According to above description, the evolutionary model of supply chain network G is described as follows:

- **Initial conditions:** Network initial state is set (t = 0) and there are m_0 initial nodes (including four types of nodes). Considering the universal applicability of network, it is assumed that edge weights are randomly generated and normalized as $w_i \in (0, 1)$ Within each time step, a node with m degrees ($m \leq m_0$) is added to such the network and so m edges connecting m different existing nodes are also added into the network
- **Optimal choice:** In the t time step, a new enterprise node makes connections with m different existing enterprise nodes with weight values g(t). The new node will optimally choose to establish supply relationships with target node according to the following degree preferential probability:

$$\pi_i = \frac{k_i}{\sum_i k_i}$$

After t time steps, there comes to a network with $N = m_0+t$ nodes and $M = mt$ edges.

The strategy set of network attacking: Supply chain networks often encounter some unexpected events of attacking, in some severe cases the network could be

paralyzed or even disintegrated. This study focuses on analyzing three types of emergent events: random, targeted and mixed, which can be simulated using Random, targeted and mixed attacking in the complex network. For complex network invulnerability study, it adopts node degrees or betweenness as the basis for node elimination. However, for supply chain network, node degree cannot fully represent the importance of node itself, since it ignores the network traffic and loading condition. But, betweenness can relatively describes the dominance and influence of the corresponding node in the entire network and the larger the node betweenness, the greater the role of the node in the network since more data packets flow through it. The study adopts node betweenness as the basis for node elimination. The specific attack strategy is described as follows:

- **Random attack strategy:** The attacking principle is to randomly select a node v_i according to its betweenness and remove the node and remove all the associated edges from the network
- **Targeted attack strategy:** The attacking principle is to arrange the node betweenness in the descending order and then choose the node with maximum betweenness as the attacking target. If some nodes happen to have identical number of betweenness, randomly choose one of the nodes as the attacking target
- **Mixed attack strategy:** The attacking principle is decomposed into several rounds and each round would be assigned as random or targeted according to its probability, which could be described as:

$$MA = \begin{cases} p_a \rightarrow RA \\ (1-p_a) \rightarrow TA \end{cases}, p_a \in (0,1)$$

The capacity allocation strategy of node failure: For a given network with N nodes, it is assumed that information or energy always interchanges along the shortest path between node pairs. In the initial stage, the load of each edge is below its processing capacity, so the network is in steady state. Node elimination will shift the load to its neighbor nodes and when the assigned nodes cannot handle the additional load, it will further lead to the collapse of the other nodes. Under the premise of constant network capacity, the study considers the capacity redistribution of the expired node.

Node load is defined as the node betweenness (Holme *et al*., 2002; Newman, 2001), while the capacity of node j is proportional to its initial node load, defined as c_j, j = 1, 2,..., N. In this study, the preferential load redistribution rule with integrated global and local information is put forward. The capacity of the failure node is redistributed to neighboring nodes according to its load preference, while non-adjacent nodes would not be influenced. Load preference is defined as follows:

$$L_i = f(IG, Il_i) = Ig_i * IL_i$$

where, Ig_i and IL_i are the global and local parameters of node i. The redistribution of the capacity of failure node j to neighboring nodes can be expressed as:

$$C_i = \begin{cases} C_i + C_j * \frac{L_i}{\sum_{n \in \Gamma_j} L_n}, i \in \Gamma_j \\ C_i, \quad i \notin \Gamma_j \end{cases} \quad (1)$$

where, node n is the neighboring node of expired node j and Γ_j represents the set of neighboring nodes of node j.

Invulnerability model: For the above-mentioned supply chain network, the network invulnerability model Ψ is defined as:

$$\Psi = F(G, A, V_A, r)$$

where, G denotes the network model, A represents the set of network attacking strategy, V_A refers to the set of failure nodes and r denotes the capacity redistribution strategy. The specific process of the model is described as follows:

Step 1: **Initial conditions:** for the initial network G, with N nodes and M edges. Set two constants p_a, $p_b \in (0, 1)$ and generate two random real numbers a, $b \in (0, 1)$

Step 2: When the network is under attack, different treatment is chosen according to the different attack strategies

Step 3: **Random attack:** Calculate the betweenness of each node and one node is randomly selected and eliminated and then calculate the network performance. Turn to step (3)

Step 4: **Targeted attack:** The betweenness of each node is calculated and arranged in the descending order. The node with maximum betweenness is selected and eliminated. If there are nodes with identical maximum betweenness, one of the nodes would be randomly selected and eliminated. And then calculate the network performance. Turn to step (3)

Step 5: **Mixed attack:** Randomly generate b. If $b<p_b$, the random attack is performed and turn to process (1), otherwise turn to process (2)

Step 6: Randomly generate α and p_a are, when $\alpha<p_a$, the capacity of the failure node is redistributed and the resulting network is used for next round of attack. Repeat the attack process until (4) ends

Step 7: Ending conditions of the simulation: The network collapses completely or betweenness of the remaining nodes is zero

The measure of network invulnerability: Because of the particularity and complexity of supply chain network as well as the interaction and collaboration among network nodes, the supply chain network emerges as a complex network structure. Understanding and measuring the invulnerability performance of network after emergent events or attack would exert great influence on the design and operating of the network. This study introduces two measure indexes, named structural stability index and network robustness index, to evaluate the network invulnerability of supply chain network in case of attack.

Structural stability: The structural stability analysis of supply chain network adopts two measure indexes, maximal connected subgraph and network efficiency. Of which, the maximal connected subgraph denotes that after attacks, network G is decomposed into several connected subgraphs and the number of nodes contained in the maximal connected subgraph is used to measure the network performance. And the efficiency of supply chain network E(G) stands for the average of the multiplicative inverse of the distances between any two nodes in the network, namely:

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \quad (2)$$

where, $1/d_{ij}$ represents the inverse of the shortest distance between nodes i and j. If there is no path between nodes i and j, then d_{ij} is defined as ∞ and $\frac{1}{d_{ij}} = 0$. It is obvious that $E(G) \in (0, 1)$.

Network robustness: For network robustness, the study uses the measurement of connection robustness. The connection robustness refers to the ability of the remaining nodes in the network keep connected after the attack, which is defined as:

$$R = \frac{C}{(N - N_r(n))} \quad (3)$$

where, N denotes the initial network size, $N_r(n)$ denotes the number of nodes eliminated from the network and C is the number of nodes contained in the maximal connected subgraph after node elimination.

RESULTS AND DISCUSSION

The experiment is carried out under the environment of MATLAB7.0 and adopts scale-free directed network with parameters of N = 1000, m_0 = m = 4 and $p \sim k^{-T}$, $\gamma = 2.5$ to simulate the supply chain network mentioned above. For a given attack combination, nodes are eliminated in accordance with the attack strategy. Once a node is eliminated, capacity redistribution is performed according to the predetermined probability and measure indexes are computed. To eliminate the influence of random factors in the simulation, for a given network configuration parameter, the experiment is performed 20 times and then the results is averaged.

The response speed and flexibility analysis of supply chain network: It can be seen from Fig. 1. When supply chain network suffers an attack, the whole network would disintegrate after a critical threshold. For targeted attack, the number of nodes contained in the maximal connected subgraph converges to zero after about 160 steps, while for mixed attack and random attack, it is after about 220 and 815 steps, respectively. At the same time, the network efficiency declines to zero after the peak and the specific situation is shown in Fig. 2. For target attack, mixed attack and random attack, the critical point of declining happens at the 195, 1800 and 1000 steps, respectively. What's more, for cases of targeted attack and mixed attack, the phenomenon is more obvious when the network efficiency increases to the maximum value, while the network efficiency declines dramatically to zero after the peak under targeted attack.

When supply chain network is under random attack, the whole network disintegrates slowly and the number of nodes contained in the maximal connected subgraph declines to zero at a slow rate. When the network efficiency slowly decreases, it indicates the decline of response speed and flexibility of the supply chain is slowly and after a certain threshold, it drops quickly to zero.

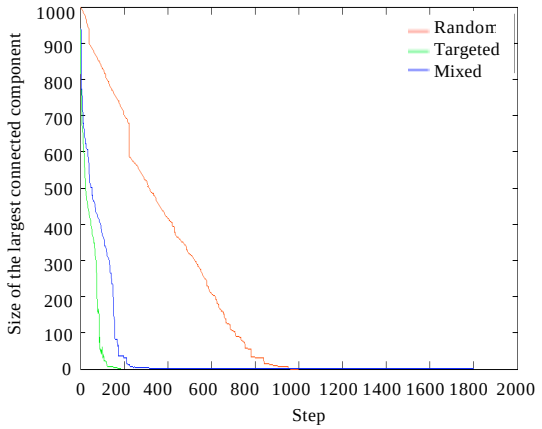

Fig. 1: No. of nodes contained in the maximal connected subgraph under various attacks

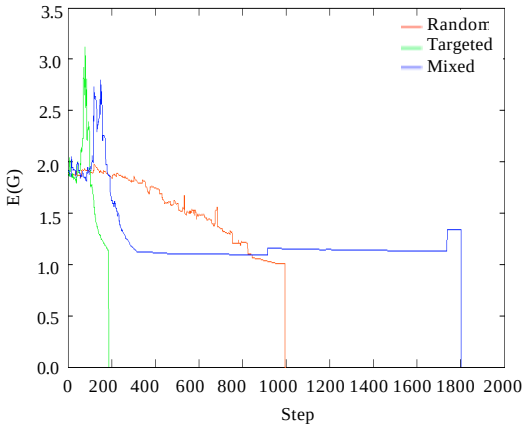

Fig. 2: Network efficiency under various attacks

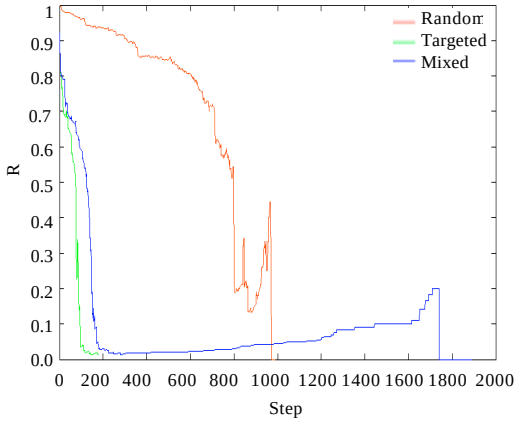

Fig. 3: Network connection robustness under various attacks

After encountering emergent attacks, the network efficiency of supply chain rapidly increases within a short period, which means that supply chain network is getting worse after the attack. But the performance of the supply chain under various attacks is quite different. For targeted attack, the response speed declines and reaches the critical threshold in a short period and then the whole network completely collapses and the response speed drops to zero. For random attack, though the response speed deteriorates, the whole network still has a certain degree of responsiveness and flexibility within a long period. When mixed attack is encountered, the response speed and network efficiency of supply chain lies between random and targeted attacks. After the network efficiency reaches a critical threshold, the response speed and flexibility of supply chain remains steady for some times and then it declines rapidly to zero, which is mainly caused by the capacity redistribution rule of the failure nodes.

The connection robustness analysis of supply chain network: The changes of connection robustness as the number of eliminated nodes under different attacks are shown in Fig. 3. For random attack, the network connectivity deteriorates relatively slowly as the number of eliminated nodes increases. After 980 steps, the network connectivity converges to zero. It is concluded that though some enterprises in the supply chain network fail quickly, for most supply chain enterprises, the chain processing continues properly for a while. But for targeted attack, the network connectivity declines between 0 and 200 steps and the performance of the supply chain is relatively more vulnerable. Within a certain range, the connectivity declines quickly while the node is eliminated. For extreme circumstances, the core enterprises and key supply chains are completely destructed by targeted attack. For mixed attack, the connectivity of the network stops deteriorating after 200 steps, where the supply chain crashes more slowly than under targeted attack. The network maintains some network connectivity even it decreases to a certain level, namely some enterprises still maintain supply relationships after the attack.

CONCLUSION

Based on the structural characteristics of supply chain network, this study introduced complex network theory and graph theory into analyzing the network invulnerability of supply chain with node failure under three emergent events. Meanwhile, the load preferential capacity redistribution rule with global and local information integrated is proposed. From the experimental results, it is concluded that the network structure of supply chain has high structural stability and robustness under random attack, but with low structural stability and robustness under targeted attacks, which is mainly caused by the network heterogeneity among the member enterprises of the supply chain.

ACKNOWLEDGMENTS

This study was supported by the Zhejiang Provincial Natural Science Foundation of China (No.Y1090688, Y1110995, Z1110551), the Humanity and Social Science on Young Fund of the Ministry of Education (No.12YJC630170), the Education Fund of Zhejiang province, P.R.China (No. Y201017626). This study is supported by National Natural Science Fund of China (No. 71071142, 71171178).

REFERENCES

Albert, R., H. Jeong and A.L. Barabasi, 2000. Error and attack tolerance of complex networks. Nature, 406: 378-381.

Christopher, M., 2003. Creating resilient supply chain. Int. J. Oper. Prod. Manage., 24: 589-601.

Haywood, M. and H. Peck, 2003. Improving the management of supply chain vulnerability in UK aerospace manufacturing. Proceedings of the 1st Conference on European Operations Management Association/Production and Operations Management Society, June 16-18, 2003, Como, Italy, pp: 121-130.

Helbing, D., D. Armbruster, A.S. Mikhailov and E. Lefeber, 2006. Information and material flows in complex networks. Phys. A: Stat. Mech. Appli., 363: 11-14.

Holme, P., B.J. Kim, C.N. Yoon and S.K. Han, 2002. Attack vulnerability of complex networks. Phys. Rev. E, 65: 1-14.

Jian, H. and L. Jian, 2009. Supply chain network mutation and control policy. J. Nanjing Univ. Technol., 4: 63-69.

Kuhnert, C., D. Helbing and G.B. West, 2006. Scaling laws in urban supply networks. Phys. A: Stat. Mech. Appli., 363: 96-103.

Laumanns, M. and E. Lefeber, 2006. Robust optimal control of material flows in demand-driven supply networks. Phys. A: Stat. Mech. Appl., 363: 24-31.

Muckstadt, J.A., D.H. Murray, J.A. Rappold and D.E. Collins, 2001. Guidelines for collaborative supply chain system design and operation. Inform. Syst. Front., 3: 427-453.

Newman, M.E.J., 2001. The structure of scientific collaboration networks. Proc. Nat. Acad. Sci., 98: 404-409.

Rice, J.B. and F. Caniato, 2003. Building a secure and resilient supply network. Supply Chain Manage. Rev., 7: 22-30.

Yan, Y., X. Liu and X.T. Zhuang, 2010. Resilient supply chain emergency management strategy based on node fails. Control Decision, 25: 25-30.