Physica A 459 (2016) 129–139

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Robustness of assembly supply chain networks by considering risk propagation and cascading failure

Liang Tang [a,b,c], Ke Jing [d,*], Jie He [a], H. Eugene Stanley [c]

[a] School of Transportation, Southeast University, Nanjing, Jiangsu, 210096, PR China
[b] Industrial Engineering Department, Shenyang Aerospace University, Shenyang, Liaoning 110136, PR China
[c] Department of Physics, Boston University, Boston, MA 02215, USA
[d] School of Economics and Management, Shenyang Aerospace University, Shenyang, Liaoning 110136, PR China

HIGHLIGHTS

- We construct a theoretical risk model of assembly supply chain network.
- A cascading failure model based on production capability loss is developed.
- We consider different disruption scenarios and their probability.
- We assess network robustness at different node threshold and linking intensity.
- The simulation results show that 30% nodes removal cause network collapse.

ARTICLE INFO

Article history:
Received 22 December 2015
Received in revised form 17 March 2016
Available online 27 April 2016

Keywords:
ASCN
Cascading failure
Risk propagation
Network robustness

ABSTRACT

An assembly supply chain network (ASCN) is composed of manufacturers located in different geographical regions. To analyze the robustness of this ASCN when it suffers from catastrophe disruption events, we construct a cascading failure model of risk propagation. In our model, different disruption scenarios *s* are considered and the probability equation of all disruption scenarios is developed. Using production capability loss as the robustness index (RI) of an ASCN, we conduct a numerical simulation to assess its robustness. Through simulation, we compare the network robustness at different values of linking intensity and node threshold and find that weak linking intensity or high node threshold increases the robustness of the ASCN. We also compare network robustness levels under different disruption scenarios.

1. Introduction

In recent years we have begun to understand the behavior of phenomena such as natural disasters, the breakdown of technological systems, epidemic propagation, and spreading social unrest in terms of their complex network structure. During these events, supply chain systems often collapse, e.g., during the 2011 earthquake in Japan the Toyota Motor Company was forced to stop operations in twelve assembly plants and absorb a production loss of 140,000 vehicles. The influence of this production loss spread to other countries and sent shockwaves through the worldwide motor industry. The main cause was the disruption of the supply chain supporting the manufacturing subsystem. If companies transfer their

* Corresponding author. Tel.: +86 13555771799.
E-mail addresses: tangericliang@gmail.com, erictang@bu.edu (L. Tang), chloe.jingke@gmail.com (K. Jing), hejie@seu.edu.cn (J. He), hes@bu.edu (H.E. Stanley).

http://dx.doi.org/10.1016/j.physa.2016.04.030
0378-4371/© 2016 Published by Elsevier B.V.

internal risks to their supply chain partners, directly or indirectly they affect those partners [1]. The negative effects of risk are transferred to other companies because most real-world supply chain networks are geographically dispersed [2–4]. Although strong interdependencies increase supply chain efficiency, they also decrease system robustness—and when disruption occurs the negative effects are more severe. Since supply chain system becomes more and more important in current global production mode, it is necessary to do the study of supply chain robustness by considering the disruption propagation. More importantly, assembly supply chain is one of the most popular one because it is important and fundamental in manufacturing industry. Consequently, we aim to assess the robustness of ASCN.

Because all supply chains networks are vulnerable to disruption, supply chain risk management has been the subject of much recent study. The goal is to secure the uninterrupted flow of directed materials and undirected information [5]. When a firm is able to manage the risk of disruption they can better serve their customers, and thus increasing the robustness of supply chain networks is an important competitive factor in any free market [6–8]. A significant amount of empirical and quantitative research has been done on supply chain risk management, including measuring global supply chain risk, planning for catastrophic events in supply chains, increasing chain agility, and mitigating risk [9–15]. Wu et al. [16] proposed a disruption analysis network methodology for modeling how the effects of disruptions propagate through a supply chain. Oke and Gopalakrishnan [17] investigated how to classify and manage the risks in the supply chain of a large US retailer and classified risks as either inherent and of high frequency or disruptive and of low frequency. They developed risk mitigation techniques that included generic strategies for handling most types of risk and specialized strategies for handling particular risks. Marucheck et al. [18] examined how the global supply chain creates or exacerbates vulnerabilities, and they focused on how operations management science can provide fresh insights into product safety concerns and security in the global supply chain. Świerczek found that dependence relationships can cause the transmission of disruptions to "Snowball" through a supply chain network or through a portion of it. He modeled this effect by linking the disruption intensity and extent of supply chain integration to the amplification of transmitted disruptions [19].

Our goal here is to construct a cascading failure model of risk propagation that can quantify the robustness of ASCN under different disruption scenarios. Most current studies of cascading failures in complex networks have focused on single networks [20–23]. Holme and Kim [20] studied evolving networks based on the Barabási–Albert scale-free network model with vertices sensitive to overload breakdown. They considered two cases of load limitation, i.e., when the average number of connections per vertex increases with the network size and when it remains constant. They found avalanche-like breakdowns for both load limitations in their work and, to avoid these avalanches, the authors argue that the capacity of the vertices has to grow with the size of the system. The irregular dynamics of the formation of a giant component has also been studied. Moreno et al. [21] studied the tolerance to congestion failures in communication networks with a scale-free topology. They proposed that the traffic load carried by each damaged element in the network must be partially or totally redistributed among the remaining elements. Overloaded elements might fail in turn and trigger a failure cascade that isolates large portions of the network. They also found a critical traffic load above which the probability of massive traffic congestions destroying the network communication capabilities is finite. Motter and Lai showed that, for complex networks, the loads can be redistributed among the nodes, and intentional attacks can lead to a cascade of overload failures. They also demonstrated that the heterogeneity of complex networks makes them particularly vulnerable to attacks, because disabling a single key node can trigger a large-scale cascade [22]. Wang and Xu [23] investigated cascading failures in coupled map lattices with different topologies. They found that cascading failures occur much more frequently in small-world and scale-free coupled map lattices than in globally coupled map lattices. There have also been some recent studies of failure cascades in interdependent networks. Buldyrev et al. [24] recently used a one-to-one correspondence model to study the ramifications of interdependence between two networks. Their analytical framework used a generating-function formalism widely applied in studies of percolation and structure within single networks [25]. This framework for interdependent networks enables us to follow the dynamics of the failure cascades and derive analytic solutions for the final steady state. Researchers have used this work of Buldyrev in a variety of ways to study interdependent networks [26–31].

In summary, our goal is to quantify the robustness of ASCN against disruption in order to provide a scientific basis for the development of network protection. Our innovations of studying the cascading failure of ASCN are in two aspects: the risk propagation mode and the RI of ASCN. Applying cascading failure theory, we will (i) describe the concept of risk propagation in an ASCN, (ii) construct a cascading failure model to depict the dynamic process of risk propagation, and (iii) use different disruption scenarios to assess the robustness of ASCN.

2. Theoretical risk model of supply chain network

2.1. Conceptual framework for risk propagation

Every entity in a supply chain network faces risk. When a natural disaster, criminal act, or terrorist act disrupts a supply chain network, we need to be able to quantify the risk that it will propagate and to analyze its mode of propagation. Fig. 1 shows a traditional supply chain operation model.

There are four types of entity that form a single supply chain network: suppliers, production centers, distribution centers, and customers. Here we assume all entities to be network nodes [32]. The links between those nodes in the supply chain network are called connectivity links, and can transfer risk. Whenever any of the nodes in a directed supply chain network is disrupted and fails, there is a risk that they will propagate.