Disruption Information, Network Topology and Supply Chain Resilience

Yuhong Li

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Business Information Technology

Christopher W. Zobel, Chair
Roberta S. Russell
Loren P. Rees
Onur Seref
G. Alan Wang

June 14, 2017
Blacksburg, VA

Keywords: Supply Chain Disruption, Information Accuracy, Network Structure, Supply Chain Resilience, Simulation

Disruption Information, Network Topology and Supply Chain Resilience

Yuhong Li

ABSTRACT

This dissertation consists of three essays studying three closely related aspects of supply chain resilience.

The first essay is “Value of Supply Disruption Information and Information Accuracy”, in which we examine the factors that influence the value of supply disruption information, investigate how information accuracy influences this value, and provide managerial suggestions to practitioners. The study is motivated by the fact that fully accurate disruption information may be difficult and costly to obtain and inaccurate disruption information can decrease the financial benefit of prior knowledge and even lead to negative performance. We perform the analysis by adopting a newsvendor model. The results show that information accuracy, specifically information bias and information variance, plays an important role in determining the value of disruption information. However, this influence varies at different levels of disruption severity and resilience capacity.

The second essay is “Quantifying Supply Chain Resilience: A Dynamic Approach”, in which we provide a new type of quantitative framework for assessing network resilience. This framework includes three basic elements: robustness, recoverability and resilience, which can be assessed with respect to different performance measures. Then we present a comprehensive analysis on how network structure and other parameters influence these different elements. The results of this analysis clearly show that both researchers and practitioners should be aware of the possible tradeoffs among different aspects of supply chain resilience. The ability of the framework to support better decision making is then illustrated through a systemic analysis based on a real supply chain network.

The third essay is “Network Characteristics and Supply Chain Disruption Resilience”, in which we investigate the relationships between network characteristics and supply chain resilience. In this work, we first prove that investigating network characteristics can lead to a better understanding of supply chain resilience behaviors. Later we select key characteristics that play a critical role in determining network resilience. We then construct the regression and decision tree models of different supply chain resilience measures, which can be used to estimate

supply chain network resilience given the key influential characteristics. Finally, we conduct a case study to examine the estimation accuracy.

Disruption Information, Network Topology and Supply Chain Resilience

Yuhong Li

GENERAL AUDIENCE ABSTRACT

With the trend of industry globalization and regional specification, supply chain networks are becoming more complex and thus more vulnerable to disruptions. The situation is potentially worsened because of dynamic risk diffusion, which is a phenomenon that involves the propagation of a disruption from a company to its suppliers and customers. Disruptions in complex supply chain networks, together with this dynamic risk diffusion process, are hard to predict and difficult to manage. Thus, it is particularly important for supply chains to have resilience capabilities.

Supply chain resilience has been a fast-evolving research topic in recent years. Compared with traditional supply chain risk management, which focuses on controlling the risk of disruptions, supply chain resilience emphasizes a supply chain's capability to be well prepared for, quickly respond to, and recover from a disruption. This forward-looking perspective requires supply chain managers to have a good understanding of both disruptions and their supply chain network in order to build resilience.

Based on this perspective, we conduct three studies on disruption information and supply chain network structure in order to contribute to a better understanding of the concept of supply chain resilience. In the first chapter, we aim to provide insights into how information accuracy influences the value of disruption information, which can support better decision making about information investment. As network structure is also critical to supply chain resilience, we then examine the relationship between network structure and supply chain resilience in chapters 3 and chapter 4. Understanding how network structure and, in particular, the key characteristics that define that structure impact supply chain resilience can allow practitioners to design more resilient supply chain networks and achieve resilience without too many additional resources.

Although our models are simplified versions of reality, these studies establish a solid foundation for understanding supply chain resilience, and for evaluating different risk mitigation and recovery strategies, hence they can support more effective decision making in practice.

Acknowledgments

My journey of pursuing a Ph.D. degree is full of challenges and joys. I treasure all the moments that life have given me. Challenges make me a better person and stronger, and joys make my life sparkle and meaningful. I am especially touched by the unconditional support I have received during this journey; here I thank everyone for his or her efforts on me.

First of all, I am deeply indebted to the department of Business Information Technology, for admitting me to this program, and providing various resources through my study at Virginia Tech.

My sincere gratitude goes to my advisor, Dr. Christopher Zobel, for his mentorship, encouragement, and support. Dr. Zobel is the one who have been inspiring my interest in academic. Under his guidance, doing research is an enjoyable thing, and it is always a great pleasure to work with him.

I would also like to thank all other members on my dissertation committee. Dr. Alan Wang introduced me to the door of research and greatly supported my first paper. Dr. Loren Rees provided invaluable, insightful comments on my dissertation. I have benefited tremendously from Dr. Roberta Russell and Dr. Onur Seref from their advice on my dissertation.

I want to extend my gratitude to all other faculty members, Ph.D. students and my friends in Blacksburg. Special thanks to Lina Zhou, Wenjing Xue, Huijuan Shao, Stephane Collignon, Franklin Warren, Jay Teets, Zhilei Qiao for their unconditional support.

Finally and most importantly, I am very grateful to my husband, my daughter and my parents, for their continuing love, companion and support. It is good to have them around through happiness and toughness.

Table of Contents

Chapter 1: Introduction

Supply chain networks are becoming more complex and thus more vulnerable to disruptions, given the trend of industry globalization and regional specification. Furthermore, high-profile disaster events, such as Hurricane Sandy in 2012 and the Tohoku Earthquake in 2011, have brought disruptions into public attention and thus supply chain risk management (SCRM) has experienced a recent explosion of interest. Also, new techniques, such as big data analysis and social media analysis, and new methods as exemplified by sustainability risk analysis, have stimulated research interest in this area.

Supply chain resilience is a fast evolving yet largely unexplored research topic in the supply chain risk management field. The concept of supply chain resilience assumes that supply chain disruptions are unavoidable, and therefore a resilient supply chain should be able to not only reduce disruption risks but also quickly respond to and recover from disruptions. In contrast, traditional supply chain risk management focuses primarily on risk control when given a disruption.

This dissertation consists of three essays studying three closely related aspects of supply chain resilience: the value of disruption information, the measurement of overall network resilience, and the effect of network structure on supply chain resilience.

The first essay is “Value of Supply Disruption Information and Information Accuracy”, in which we investigate how information accuracy influences the value of supply disruption information (VOI). This work is inspired by the fact that obtaining disruption information is widely recognized as an important risk mitigation method to enhance supply chain resilience. With accurate information, companies can gain benefits through choosing better strategies to mitigate supply chain risks. However, fully accurate disruption information may be difficult and costly to obtain, and inaccurate disruption information can decrease the financial benefit and even lead to negative performance. This deterioration of benefits comes from the fact that underestimation of the disruption influence can make it more difficult to recover, while overcautious actions can cost money without providing benefit.

To study the value of disruption information, we develop a newsvendor model with one product setting where the focal firm can source from one main supplier and one backup supplier.

We define disruption information as the estimated fractional supply amount influenced by the disruption, where the difference between disruption information and actual supply influence is the information error. Then we calculate the focal company's profits both with and without disruption information separately. The difference between these two profits is the value of that information. The results show that information accuracy, specifically information bias and information variance, plays an important role in determining the value of disruption information. However, this influence varies at different levels of disruption severity and resilience capacity. Our results imply that higher resilience capacity may cause detrimental effects if there is no quality disruption information. Thus, for companies with a high resilience capacity, obtaining quality information is critical to effectively cope with disruptions.

The second essay is "Quantifying Supply Chain Network Resilience: A Dynamic Approach", in which we provide a quantitative framework for assessing network resilience. Current supply chain networks of many companies are becoming increasingly complex, and thus more vulnerable to disruptions. These disruptions can be further exacerbated by risk diffusion – poor performance of its suppliers can cause financial loss to a company, and eventually affect other companies in the same network. Supply chain resilience, a holistic tool to measure supply chain health, can assist practitioners in different decision making efforts. Therefore, quantitative analysis of supply chain resilience is of great research interest.

Under this background, we develop a resilience framework that takes a dynamic approach and considers risk propagation in the network. This framework includes three basic elements: robustness, recoverability and resilience, which can be assessed with respect to different performance measures. We then conduct a controlled experiment to investigate how network structure and the risk diffusion process influence different aspects of supply chain resilience. The results show that both researchers and practitioners should be aware of the possible tradeoffs among different resilience measures. Later we illustrate how this framework can support better decision making through a case study.

This study can enrich the supply chain resilience literature by focusing on network level resilience, contribute to the limited quantitative research on supply chain network resilience from a dynamic perspective, and enhance our understanding of the impact of network structure on supply chain resilience. This study also can help practitioners better understand the health status of the supply chain network, and how certain network types influence the supply chain network resilience, and thus assist managerial decision making in terms of disruption mitigation and recovery.

The third essay is “Network Characteristics and Supply Chain Disruption Resilience”, which is a follow up study of the second essay. This study is inspired by the needs of studying a detailed level of network structure. Current studies have been performed at the network type level (e.g., scale free, small world, and random networks), and ignore the complex nature of a supply chain network. Many real supply chain networks do not belong to a certain type of network, and networks may have different structures even if they belong to the same network type. Furthermore, a network type level approach fails to provide a prescription to improve the network structure because one company in a complex supply network has almost no power to change the whole network type.

To address these limitations, therefore, this third chapter will focus on the network *characteristic* level and we will investigate the relationships between network characteristics and supply chain resilience. Through in-depth analysis of simulated data, we prove that network characteristics, in general, are better than network types in terms of their explanatory power for describing supply chain resilience. We then select a set of key influential characteristics that can most effectively represent network resilience, and based on the large simulated data set, we construct predictive regression and decision tree models to estimate the supply chain resilience. At the end, we use a real supply chain network to compare the estimation accuracy of the different models.

Findings from the third essay suggest that we could focus on the key influential characteristics when investigating supply chain resilience, and show that implementing a decision tree model can provide a rule of thumb estimation of the supply chain resilience.

Chapter 2: Value of Supply Disruption Information and Information Accuracy

2.1 Introduction

With the growing complexity of current global supply networks, managing supply disruptions is becoming increasingly challenging (Basole and Bellamy, 2014; Hübner et al., 2014). These disruptions largely come from the intricate interactions among suppliers that make supply chains more vulnerable (Wagner and Bode, 2006), and are often driven by events such as labour strikes, natural disasters, terrorism, and supplier bankruptcies. The situation is further complicated by the fact that 42% of such disruptions have been shown to originate below the first tier of suppliers (Business Continuity Institute, 2013), and most companies have very little visibility into their supply network beyond the first tier (Basole and Bellamy, 2014).

Increasing supply visibility, specifically the obtaining of disruption information and risk evaluation in the context of supply chain risk management, is widely recognized as an important supply chain risk mitigation strategy (Craighead et al., 2007; Kirilmaz and Erol, 2015; Kleindorfer and Saad, 2005; Saghafian and Van Oyen, 2012; Tang, 2006; Tomlin and Snyder, 2006; Yang et al., 2008). In today's complex and dynamic business environment, researchers and practitioners are looking for different ways to increase supplier visibility, including visual analysis of supply networks (Basole and Bellamy, 2014), investigation of the supply chain network risk propagation mechanism (Basole and Bellamy, 2014; Garvey et al., 2015), identification of critical nodes in a supply network, and implementation of new technologies to mine information (Sanders, 2014). A recent example is IBM's announcement in 2015 of a $3 billion investment in its "Internet of Things" (IoT) unit over the next four years (IBM, 2015). This investment aims to provide real-time and accurate information to firm clients from mining sources of big data. One of IBM's IoT focus areas is supply disruption information.

Given the significance of supply disruption information, obtaining *quality* information is one of the most important investments for practitioners to make (Landwehr and Carley, 2014; Accenture, 2014; Sanders, 2014). Although timely access to accurate disruption information can allow the focal firm in the supply chain to better prepare for or respond to a potential disruption, fully accurate disruption information is hard to retrieve and costly to obtain in reality, and inaccurate disruption information can decrease the financial benefit of prior knowledge and even lead to negative performance. This is because underestimation of the disruption influence can make it more difficult to recover, while overcautious actions can cost money without providing benefit (Hübner et al., 2014). For example, the 2015 Nepal earthquake was successfully predicted to happen by seismologists (Mazza, 2015), and the World Food Programe (WFP) had supplies stored and a response plan in place (Page, 2015). Nevertheless, WFP still faced challenges in meeting local needs because they underestimated the disruption influence on the transportation network (Page, 2015).

The trade-off between information cost and information accuracy leads to questions about how much should be invested to increase supply visibility and the best approach to making such investments. To answer these questions, we need to clearly understand the value of disruption information given a certain level of accuracy. We thus aim to investigate the relationship between information accuracy and the value of disruption information, in order to gain insights into the managerial implications of investing in disruption information.

In this study, we define "*disruption information"* to be information about the estimated influence of a supply disruption on the focal company. There are many types of information about supply disruptions, including information related to supplier reliability, disruption type, disruption influence, and the timing of the disruption. In particular, it is important to consider the likelihood of a disruption occurring and the influence on the focal company if it does occur. Our approach to determining this influence will be to calculate the ratio between the unfulfilled supply and the contracted supply from the main supply source. This allows for measuring both the *estimated influence* of a disruption, which is calculated before the impact of the disruption is actually known, and the *actual influence* of that disruption, which can be measured after the disruption's impact has been experienced.

The remainder of the paper is organized as follows: Section 2 provides a review of the literature on supply chain disruption information. Section 3 discusses the modelling framework and the newsvendor model that is used to formally calculate the value of such disruption information. In Section 4, we provide an analysis of the value of the disruption information construct given the estimated influence and the actual influence of the disruption. Then, in Section 5, assuming the information error is a variable, we analyze how the expected value of the disruption information changes with the mean and standard deviation of the information error.

Finally, we summarize our findings and discuss a number of managerial implications, along with potential future work, in Section 6.

2.2 Literature Review

Current research in supply chain risk management emphasizes the importance of supply disruption information using both qualitative (Craighead et al., 2007; Kleindorfer and Saad, 2005) and quantitative methodologies (Saghafian and Van Oyen, 2012; Tomlin and Snyder, 2006; Yang et al., 2008).

The qualitative studies tend to develop conceptual frameworks to derive new insights into supply chain risk management. For example, Kleindorfer and Saad (2005) highlight the importance of specifying the disruption source and assessing the disruption influence on managing supply chain disruption risks. Similarly, Craighead, Blackhurst, and Rungtusanatham (2007) present six propositions that relate to the severity of a supply chain disruption. One of the propositions states that a disruption in a supply chain with certain warning capabilities is less likely to be severe than the same supply chain with little or no capability to warn.

Comparatively, the quantitative studies tend to focus on mathematical modelling and on estimating the quantitative impact of the disruption information. Tomlin and Snyder (2007) build an inventory model to investigate how inventory systems can take advantage of a threat advisory system. Their study shows that supplier capacity and the structure of the disruption risk process significantly influence the value of a threat advisory system. Yang et al. (2008) take a different approach by studying the value of symmetric supply reliability information in a mechanism design theory framework. They investigate how the value of risk management strategies changes with asymmetric information. Saghafian and Van Oyen (2012) develop a newsvendor model to quantify the value of flexible suppliers and disruption risk information.

In this current study, we apply a newsvendor model to investigate the relationship between information accuracy and the value of disruption information. This work falls into the category of quantitative research, and is expected to contribute to the literature in the following ways:

First of all, existing studies on the value of disruption information (Saghafian and Van Oyen, 2012; Tomlin and Snyder, 2006; Yang et al., 2008) define disruption information as information about supply reliability, and assume an all-or-nothing influence of the disruption on the supply chain (i.e., the supply chain only has two states: fully functioning or non-functioning). In contrast, our work focuses on the fractional amount by which a disruption influences supply flow, and thus disruption influence is a continuous number between 0 and 1. By incorporating fractional disruption influences in the model, our study is able to better reflect reality and mainstream supplier disruption classifications. For example, many conceptual and empirical studies (Oke and Gopalakrishnan, 2009; Simchi-Levi et al., 2014) classify disruption risks into three categories: low-impact & high-likelihood, medium-impact & moderate-likelihood, and high-impact & low-likelihood. Such a classification scheme requires the consideration of different fractional levels of disruption influence.

Secondly, our study focuses on how information *accuracy* influences the value of disruption information. Although qualitative studies emphasize the importance of disruption identification and risk evaluation (Craighead et al., 2007; Kleindorfer and Saad, 2005; Tang, 2006), few quantitative studies consider the impact of information accuracy about disruptions. The disruption information (i.e., disruption influence in this context) depends on many elements, including cognitive limitations and capabilities, the information source, the information perception process, and decision maker subjectivity. With the existence of information error, companies tend to be either overly cautious or underestimated in their actions. Both of these actions can cause potential economic loss; thus, studying the impact of disruption information error on the value of disruption information has practical significance.

To the best of our knowledge, among the quantitative studies on disruption information, only Saghafian and Van Oyen (2012) touch on the area of inaccurate disruption information. Defining the disruption information to be the estimated disruption reliability, Saghafian and Van Oyen (2012) briefly show that the value of disruption information is non-increasing with the absolute value of information error. Our work, on the other hand, views disruption information as a variable of the estimated disruption influence, and thus we can measure how the information bias and information variance influence the value of disruption information. This approach supports the development of a number of managerial implications that can be used to further improve decision making in this context.

As a third significant contribution to the literature, our study fills a gap in supply chain disruption research by focusing on disruption information from suppliers. Literature about inaccurate information in supply chains has two streams. One stream focuses on inaccurate internal information, specifically information about inventory (Cannella et al., 2015; Fleisch and Tellkamp, 2005; Kang and Gershwin, 2005; Kwak and Gavirneni, 2015; Sahin and Dallery, 2009; Sahin et al., 2008); the other focuses on the demand side, which is the quality of forecasted demand information (Chen et al., 2000; Forslund and Jonsson, 2007; Kerkkänen et al., 2009; Zhao and Xie, 2002). None of this existing literature addresses inaccurate supply disruption information and how information quality influences supply chain performance.

2.3 Modelling Framework

In the following analysis, we apply a newsvendor model to calculate the value of disruption information. This supply chain model consists of one focal company, sourcing from one main supplier with known resilience capacity. This main supplier can be viewed as a black box of an actual supply network that is exposed to various disruption risks, where different risks have distinct influences on the focal company. The focal company's resilience capacity, which is measured by the available resources Q, represents its ability to cope with disruptions by temporarily replacing lost supply. These available resources can come from excess inventory levels, self-production capacity, available backup suppliers or substitutable products, for example.

For the sake of this analysis, we further assume that only one disruption can happen in a given time period. As discussed above, our use of the term *disruption information* refers to the estimated disruption influence, θ, which is calculated as the percentage of estimated unfulfilled supply from the main supply source caused by the disruption. We then use the abbreviation VOI to represent the value of this disruption information.

Letting V be the contracted delivery amount from the main supply source and letting π be the actual disruption influence, the estimated delivery from the main supply source is $(1-\theta)V$, while the actual delivery from the main supply source is $(1-\pi)V$. The difference between θ and π is the information error ε, $\theta = \pi + \varepsilon$. Considering the fact that a disruption can only influence the purchasing amount from zero to the contracted supply amount, we have $\pi, \theta \in [0,1]$. When π (or θ) equals zero, the actual (or estimated) disruption influence is zero. When π (or θ) equals one, supply is totally disrupted and the focal company receives nothing from the main supply source.

Figure 1 depicts this supply chain disruption model. The focal company receives the contracted amount of supply from the main supply source, and the supply is supplemented by their additional resilience capacity if a disruption happens.

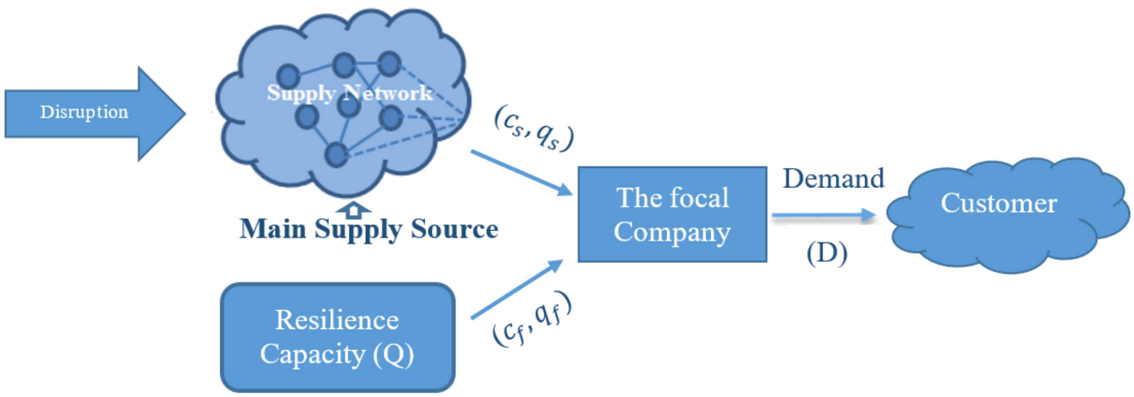


Figure 1. Supply Chain Disruption Model

Given this model, we first examine $VOI_\pi(\theta)$, the value of the disruption information given disruption information θ and actual disruption influence π. $VOI_\pi(\theta)$ is an observation of the disruption information value for a given disruption influence π, where θ is a variable. To incorporate uncertainty into the model, we also consider VOI_π, the expected value of the disruption information given the actual disruption influence π. The mathematical notation used in the following discussion is summarized in Table 1.

2.3.1 Calculating $\boldsymbol{VOI_\pi(\theta)}$

To calculate the value of the disruption information for a given θ and π, we follow the decision process depicted in Figure 2.

Step 1, the focal company observes demand D and receives the disruption information θ.

Table 1. Model Notation

Symbol	Definition
θ	Estimated disruption influence on the main supplier, $\theta \in [0,1]$.
π	Actual disruption influence on the main supplier, $\pi \in [0,1]$.
ε	Information error, $\varepsilon = \theta - \pi$.
V	Contracted purchase amount from the main supplier.
c_s	Unit purchasing cost from the main supplier.
c_f	Unit purchasing cost from the flexible supplier.
r	Unit selling price.
h	Unit inventory holding cost.
p	Unit penalty cost of unsatisfied demand.
Q	Maximal available purchase amount from the flexible supplier.
α	Ratio of Q over V, $\alpha = Q/V$.
q_s^θ	Estimated delivery amount from the main supplier given disruption information θ, $q_s^\theta = (1-\theta)V$.
q_s'	Actual delivery amount from the main supplier given actual disruption influence π, $q_s' = (1-\pi)V$.
q_f	Purchase amount from the flexible supplier.
q_f^*	Optimal purchase amount from the flexible supplier given disruption information θ.
q_f^0	Optimal purchase amount from the flexible supplier without disruption information.
P_θ	Actual profit realized given disruption information θ.
P_0	Actual profit realized without disruption information.
$VOI_\pi(\theta)$	Value of the disruption information given disruption information θ and actual disruption influence π.
VOI_π	Expected value of the disruption information given actual disruption influence π.

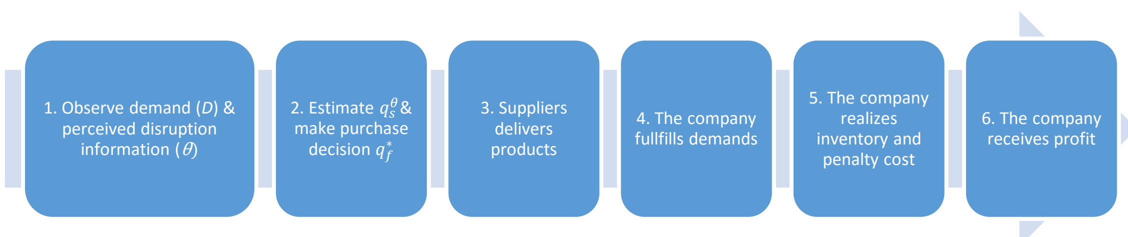


Figure 2. Decision Process Sequence

Step 2, the focal company calculates the *estimated* delivery amount from the supply network based on disruption information θ, $q_s^\theta = (1-\theta)V$. Then the company decides the purchase amount from its resilience capacity q_f^* based on the following nonlinear programming model:

$$\max_{0 \le q_f \le Q, q_s^\theta = (1-\theta)V} \{r * \min\{D, q_f + q_s^\theta\} - (c_f q_f + c_s q_s^\theta) - h * \max\{q_f + q_s^\theta - D, 0\} - p * \max\{-q_f - q_s^\theta + D, 0\}\} \quad (3.1.1)$$

where r is the revenue, h is the holding cost, and p is the penalty (shortage) cost per unit. The objective of this model is to find the optimal purchase amount from the resilience capacity q_f^* to maximize the focal company's profit. Here the penalty cost is the aggregated unit cost from various sources, including lost sales, customer waiting cost, price discounts, and any other cost related to product shortages. This penalty cost can vary widely depending on the industry as well as on the level of competition.

Step 3, the focal company receives the supplies. As the actual disruption influence is π, the actual delivery amount from the supply network is $q_s' = (1-\pi)V$. In total, the focal company actually gets q_s' from the supply network and q_f^* from the resilience capacity, and the total purchasing cost, which includes the cost of material from each source, respectively, is $c_s q_s' + c_f q_f^*$.

Step 4, the focal company attempts to fulfil demand. The actual amount fulfilled is $min\{D, q_s' + q_f^*\}$ and the total revenue is $r * min\{D, q_s' + q_f^*\}$.

Step 5, the focal company realizes the inventory holding cost and the shortage penalty cost, which is $h * max\{q_s' + q_f^* - D, 0\} + p * max\{-q_s' - q_f^* + D, 0\}$.

Step 6, the focal company realizes the actual profit P_θ.

$$P_\theta = r * min\{D, q_f^* + q_s'\} - (c_f q_f^* + c_s q_s') - h * max\{q_f^* + q_s' - D, 0\} - p * max\{-q_f^* - q_s' + D, 0\}. \quad (3.1.2)$$

The value of the disruption information is the profit difference between the outcome with disruption information and the outcome without such information. In the case of no disruption information, the focal company expects no disruption influence and behaves as if the estimated disruption influence is zero ($\theta = 0$). Therefore, given $\theta = 0$, the optimal purchase amount from the resilience capacity q_f^0 is the solution to (3.1.1), and the corresponding profit is:

$$P_0 = r * min\{D, q_f^0 + \mathrm{q}_s'\} - (c_f q_f^0 + c_s \mathrm{q}_s') - h * max\{q_f^0 + \mathrm{q}_s' - D, 0\} - p * max\{-q_f^0 - \mathrm{q}_s' + D, 0\}. \quad (3.1.3)$$

We thus have:

$$VOI_\pi(\theta) = P_\theta - P_0 \quad (3.1.4)$$

2.3.2 Calculating VOI_π, the expected value of $VOI_\pi(\theta)$

The estimate of actual disruption influence, θ, is a variable because uncertainties exist during the information estimation process. For example, the technique used and knowledge limitations, the sample bias, and the decision maker's subjectivity can all influence the estimation. In terms of evaluating the relative value of different information sources, therefore, it is the expected value of the disruption information that is most important.

The disruption information, θ, is totally dependent on ε for a given π, since $\theta = \pi + \varepsilon$, and the shape of ε determines the quality of the disruption information. In our model, we assume that ε is an independent and identically distributed random variable with mean μ_ε, standard deviation σ_ε, and probability density function $f(\varepsilon)$. Thus, the expected value of the disruption information for a specific π can be expressed as:

$$VOI_\pi = \int VOI_\pi(\pi + \varepsilon) f(\varepsilon) d\varepsilon \qquad (3.2.1)$$

As π is exogenous, our analysis of VOI_π focuses on how the mean and the standard deviation of the information error influence the value of the disruption information.

2.4 Analysis of $VOI_\pi(\theta)$

To simplify the following analysis, we make three important assumptions:

(1) $c_s < c_f$. In our model, the company always receives the products from the main supply source first and then considers the resilience capacity only if it is needed. This assumption is based on the common supposition that the company is rational and always chooses suppliers with lower cost as the main supply source if product value is homogeneous.

(2) $r + p - c_f > 0$. If the purchase price from the resilience capacity is too high, then the company will lose money for every unit purchased from that source. The focal company typically would then choose to not fulfil the demand instead of purchasing from the source of resilience capacity. In this situation, we always have $q_f^* = q_f^0 = 0$ and $VOI_\pi(\theta) = 0$. To avoid it, we assume $r + p - c_f > 0$.

As a special case of this situation, it is important to recognize that while a supplier is recovering from a disruption a firm could instead decide to take a loss in order to maintain their market share, since losing market share can be very expensive in the long run. This condition also can be included in the model, however, by allowing for the cost of lost sales to be increased appropriately, as part of the overall penalty cost. The model will then reflect the relative importance of the current customers to the decision making process while still satisfying the given purchase price constraint.

(3) $D = V$. Because we are focusing on how information error influences VOI, we assume $D = V$ in order to eliminate the influence from other perturbations. This assumption also makes sense from a practical perspective. A company usually makes purchase decisions based on demand estimation, thus they would adjust their purchase contract unless the expected value of D is equal to V.

Based on the above assumptions, we calculate the optimal purchase amount from the resilience capacity with and without disruption information, as $q_f^* = \min\{Q, \theta V\}$ and $q_f^0 = 0$, respectively. $q_f^* = min\{Q, \theta V\}$ means the purchase amount from the backup resources is restricted by both the available resources and the estimated disruption influence, hence it is the smaller of the two values. $q_f^0 = 0$ means that the purchase amount from the backup resources is zero when there is no disruption information. Substituting these values into formula (3.1.4), we therefore have:

$$VOI_\pi(\theta) = P_\theta - P_0 = r * \left(min\left\{V, q_s' + q_f^*\right\} - q_s'\right) - c_f q_f^* - h * max\left\{q_s' + q_f^* - V, 0\right\} - p * \left(max\left\{V - q_s' - q_f^*, 0\right\} - \pi V\right) \qquad (4.1)$$

Since $Q = \alpha V$, then V is simply a multiplier in equation (4.1). If we normalize the influence of V by setting $V = 1$, then:

when $q_s' + q_f^* > V = D => min\{\alpha, \theta\} > \pi$,

$$VOI_\pi(\theta) = (r + h + p)\pi V - \left(c_f + h\right)q_f^* = (r + h + p)\pi - \left(c_f + h\right) * min\{\alpha, \theta\} \qquad (4.2)$$

and when $q_s' + q_f^* \leq V = D => min\{\alpha, \theta\} \leq \pi$,

$$VOI_\pi(\theta) = \left(r + p - c_f\right)q_f^* = \left(r + p - c_f\right) * min\{\alpha, \theta\} \qquad (4.3)$$

From formulas (4.2) and (4.3), we can see that, given π and θ, VOI is dependent on parameters α, c_f, r, h and p. Here α represents the company's resilience capacity, or flexibility;

c_f describes the company's procurement power from the source of resilience capacity; *r* describes the company's pricing power; and *h* and *p* describe the company's cost management capability.

We now show several important properties of the information error ε, and other exogenous factors, on the value of disruption information. Proofs for each of these Properties are included in Appendix A.

Property 1. When π is small enough, $VOI_\pi(\theta) < 0$ exists. The condition of $VOI_\pi(\theta) < 0$ is: $\pi < \frac{c_f+h}{r+h+p} * min\{\alpha, \theta\}$.

This property demonstrates that disruption information is not always helpful in the presence of information error. This property also provides the conditions when the value of the disruption information becomes negative. It shows that when π is small enough, the company will not benefit from the disruption information.

Property 2. When $\theta = \pi$ $(\varepsilon = 0)$, the company benefits the most from the disruption information. When $\theta > \pi$ $(\varepsilon > 0)$, $VOI_\pi(\theta)$ is non-increasing with the information error *ε*. When $\theta < \pi$ $(\varepsilon < 0)$, $VOI_\pi(\theta)$ is non-decreasing with information error *ε*.

This property demonstrates the intuition that the company obtains the highest benefit when there is perfect disruption information, and that the benefit is non-increasing with increasing information error.

To illustrate Property 1 and Property 2, we generate Figure 3 below with parameters $D = V = 200$, $\alpha = 0.5$, $c_f = 5$, $c_s = 3$, $r = 6$, $h = 0.5$ and $p = 1$. We select three different levels of π to represent three different scenarios: high-impact disruption $(\pi = 0.9)$, medium-impact disruption $(\pi = 0.5)$ and low-impact disruption $(\pi = 0.1)$.

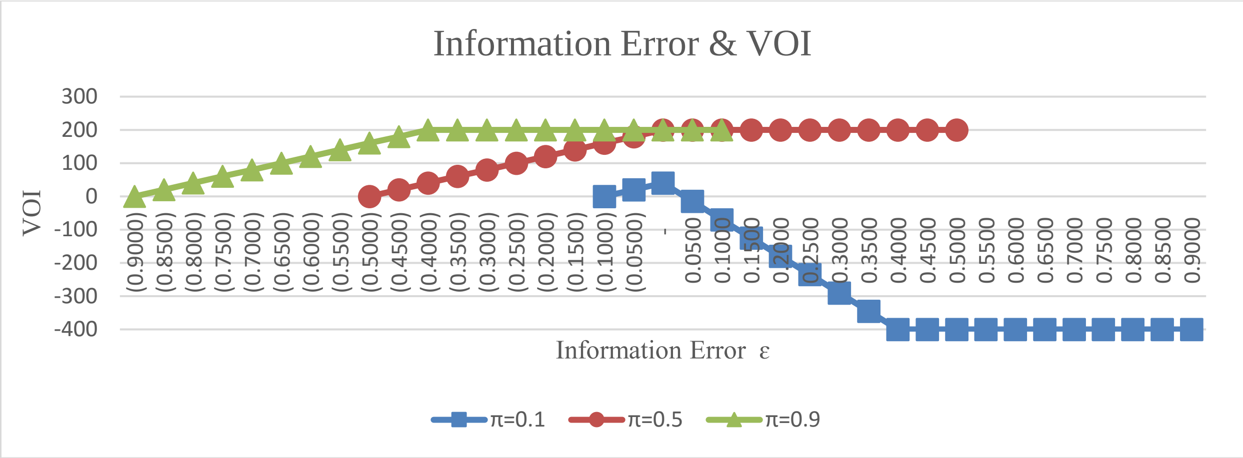


Figure 3. Information Error and VOI

Figure 3 shows that when $\pi = 0.1$, the line of VOI falls below zero except when ε is small. Thus, when π is small enough, the company can only benefit from disruption information with high accuracy.

We also can see that $\varepsilon = 0$ is not the only point that reaches the highest VOI for higher values of π. Unless $VOI_{\pi}(\theta)$ satisfies the condition given in Property 1 and is negative for a given θ, it will achieve its highest value whenever $\varepsilon \geq \alpha - \pi$, thus $\theta \geq \alpha$ and $q_f^* = min\{Q, \theta V\} = Q$. Thus, once the maximum available amount has been purchased from a backup supplier (i.e. from the source of resilience capacity), then there is no additional value gained in attempting to further improve information accuracy. This result has a significant impact on the trade-offs between cost and accuracy. Figure 3 helps to illustrate this result by showing that for $\pi = 0.9$, any estimate of θ greater than or equal to $\alpha = 0.5$ will generate the same maximal level of $VOI_{\pi}(\theta)$.

Given this initial indication of the impact of α on $VOI_{\pi}(\theta)$, we may further clarify the relationship of the two concepts as follows:

Property 3. The influence of α on $VOI_{\pi}(\theta)$ is complex and we separate it into three cases. Case 1, $VOI_{\pi}(\theta)$ is decreasing with α when $\pi \leq \alpha \leq \theta$. Case 2, $VOI_{\pi}(\theta)$ is increasing with α when $\alpha \leq \theta$ and $\alpha \leq \pi$. Case 3, for the rest of the circumstances, $VOI_{\pi}(\theta)$ does not change with α.

This property shows that when the available purchase amount is smaller than both the expected disruption influence and the actual disruption influence, increasing α can increase $VOI_{\pi}(\theta)$. Therefore, increasing α is a good strategy for mitigating supply disruption.

Property 4. With the value of other parameters fixed, the value of the disruption information $VOI_{\pi}(\theta)$ is non-decreasing with unit selling price r and unit penalty cost p, and non-increasing with purchasing cost from the backup resources c_f and unit holding cost h.

This property provides the following justifications: If the purchasing price from the backup resources is high, then the company tends to benefit less from disruption information. If the holding cost is high, the company tends to hold less stock and make conservative purchasing decisions. Thus higher holding cost has less $VOI_{\pi}(\theta)$. On the other hand, increasing the unit selling price r can increase $VOI_{\pi}(\theta)$, and increasing the unit penalty cost p will lead the company to purchase more to avoid this penalty. Thus, increasing r and p can lead to higher $VOI_{\pi}(\theta)$.

2.5 Numerical Analysis of VOI_{π}

The analysis in section 4 shows that information error is an important factor that influences the value of disruption information, together with the resilience capacity level α and other parameters. In reality, supply chain managers will not know the exact value of the information error before the disruption occurs, but they may know the information error distribution from historical data, or through a process of estimation. By viewing information error as a variable, we can calculate the expected value of disruption information, VOI_{π}, and also evaluate the VOI associated with different information sources.

In this section, therefore, we present a numerical study to gain insight into how information accuracy influences VOI. To capture the characteristic of information accuracy, we assume (as stated above) that information error ε is an identically and independently distributed random variable that follows a truncated normal distribution for $\varepsilon \in [-1,1]$. The mean of the information error, μ_{ε}, represents the expected estimation bias of the disruption influence, and the standard deviation, σ_{ε}, represents its variability. The following analyses focus on the impact of these two parameters, and their interaction, on VOI_π.

From Section 4, we know that the contracted amount with the main supply source V is a multiplier of the formula of $VOI_\pi(\theta)$, and therefore the value of V changes the scale but not the shape of VOI. Also from Property 4 above, we know that the unit selling price r, the unit penalty cost p, the purchasing cost from the backup supplier c_f and the unit holding cost h, also only change the scale of VOI. This behaviour was validated by performing a series of sensitivity analyses for each of these parameters. For the sake of the following analysis, therefore, we choose representative parameter values that satisfy the assumptions in Section 4: $V = 200$, $c_f = 5$, $c_s = 3$, $r = 6$, $h = 0.5$ and $p = 1$.

Because the influences of the actual disruption influence π and the resilience capacity level α are complex, we use different levels of π and α in order to observe a range of behaviours for VOI for different combinations of π and α. In particular, we set $\pi = \{0.1, 0.5, 0.9\}$ and $\alpha = \{0.1, 0.3, 0.5, 0.7, 0.9, 1.1\}$, where the π levels are selected to reflect the disruption types of low-impact, medium-impact and high-impact, and the α levels are based on subdividing $\alpha = 1.1$ in order to observe the behaviour of the *VOI* value when there are abundant backup resources. To isolate the influence of the demand perturbation, we assume $D = V$ as before.

2.5.1 Effect of the variability of the information error on VOI_π

We use the standard deviation of the information error σ_ε to describe the variability of the information error, and we use $\mu_\varepsilon = 0$ to minimize the influence of the estimation bias. In Figure 4, we plot VOI_π as a function of σ_ε, where $\sigma_\varepsilon = \{0, 0.1, 0.2, 0.3, 0.4, 0.5\}$, at different levels of α, given $\alpha = Q/V$. Figure 4(a) represents a low-impact disruption situation ($\pi = 0.1$), Figure 4(b) displays a medium-impact situation with $\pi = 0.5$ and Figure 4(c) shows a high-impact situation with $\pi = 0.9$. The main insights that can be derived from this analysis are as follows:

<u>Insight 5.1.1</u>: As expected, VOI is decreasing with σ_ε. This result is in accordance with our intuition that sources of disruption information with less variability are more valuable.

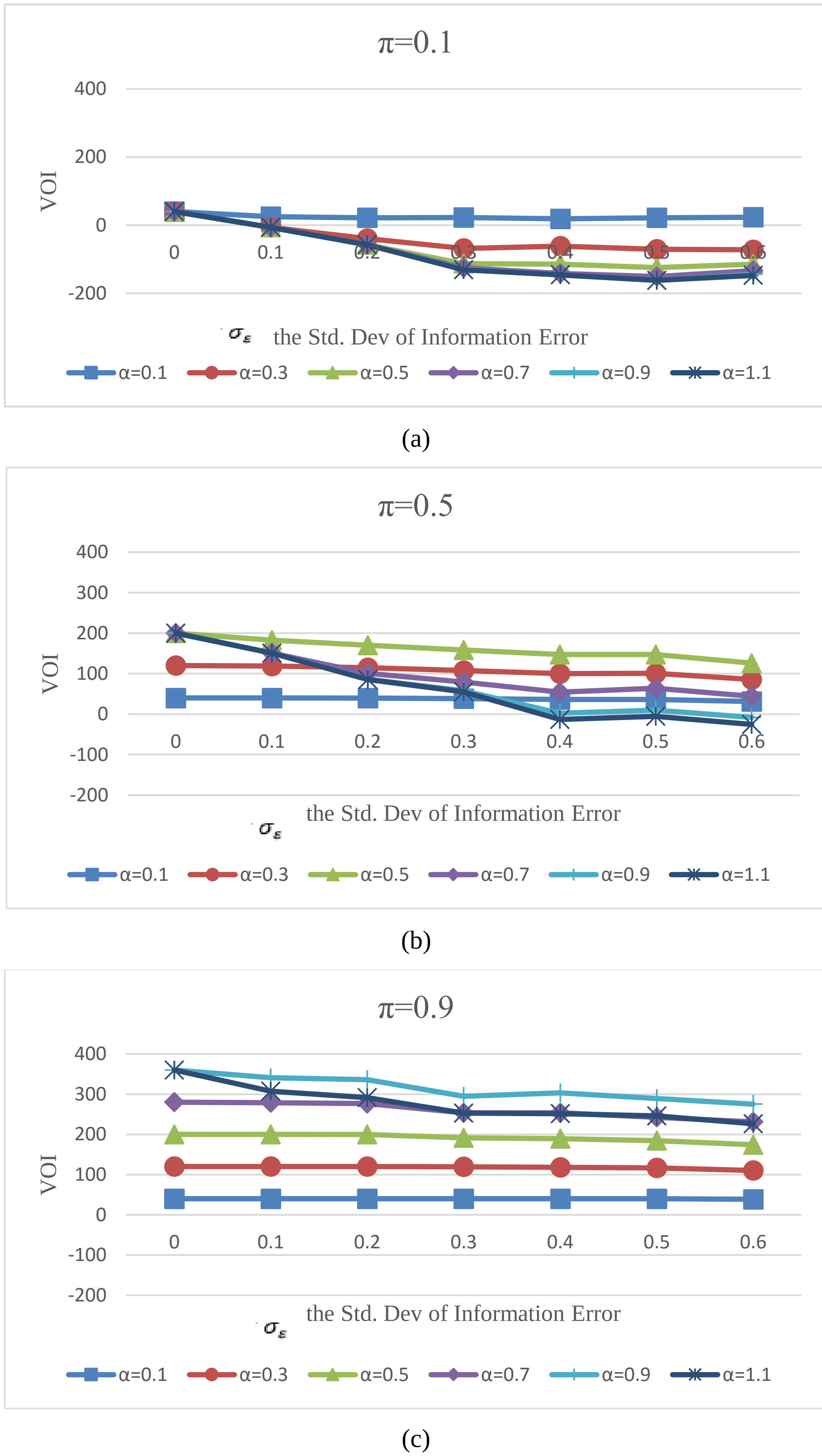


Figure 4. VOI with respect to σ_ε for different levels of α

Insight 5.1.2: VOI is more sensitive to σ_ε in situations where $\pi \leq \alpha$ than when $\pi > \alpha$. When $\pi > \alpha$, the value of the disruption information changes only slightly with σ_ε. Comparatively, when $\pi \leq \alpha$, the value of the disruption information decreases significantly with σ_ε. To clarify, when $\pi > \alpha$, overestimating the disruption influence does not change the disruption information value, and underestimating the disruption influence can have a small negative effect only when $\theta < \alpha$. Comparatively, when $\pi \leq \alpha$, then the company always suffers loss if there is any amount of overestimation or underestimation of the disruption influence. Therefore, from a practical perspective, we believe that choosing a source of disruption information with smaller σ_ε is better, especially when the resilience capacity is abundant. This insight actually implies that higher disruption information accuracy is preferred in situations with higher resilience capacity α, especially relative to the disruption influence π.

Insight 5.1.3: In a low-impact situation, the focal company should be very careful about the information accuracy, while in a high-impact situation, having disruption information is in general beneficial, even given low information accuracy. In Figure 4(a), the low-impact situation, the focal company has positive VOI only when σ_ε is small, if $\pi > \alpha$, which means the company can only benefit from very accurate disruption information. Comparatively, in the high-impact situation shown in Figure 4(c), the value of the disruption information does not change much with σ_ε, but it increases steadily with the α levels until $\pi < \alpha$.

2.5.2 Effect of the mean of the information error on VOI_π

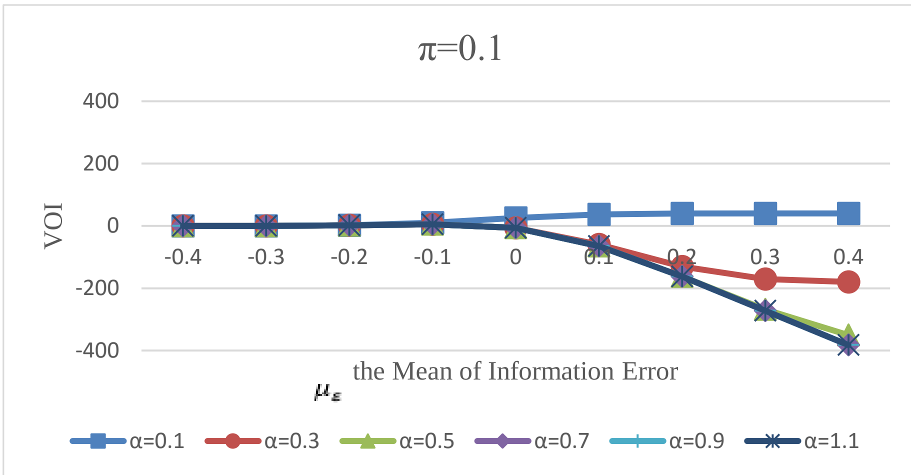
The mean of the information error μ_ε represents the historical record of information bias, where information with a smaller absolute value of μ_ε is more accurate. To isolate the effect of μ_ε, we assume low variability of the information error, such that $\sigma_\varepsilon = 0.1$. For other parameters, we still use the previous settings.

In Figure 5, we plot VOI with respect to μ_ε for different levels of α, where $\mu_\varepsilon = \{-0.4, -0.3, -0.2, -0.1, 0, 0.1, 0.2, 0.3, 0.4\}$. In general, the main insights that we can derive from this analysis are as follows:

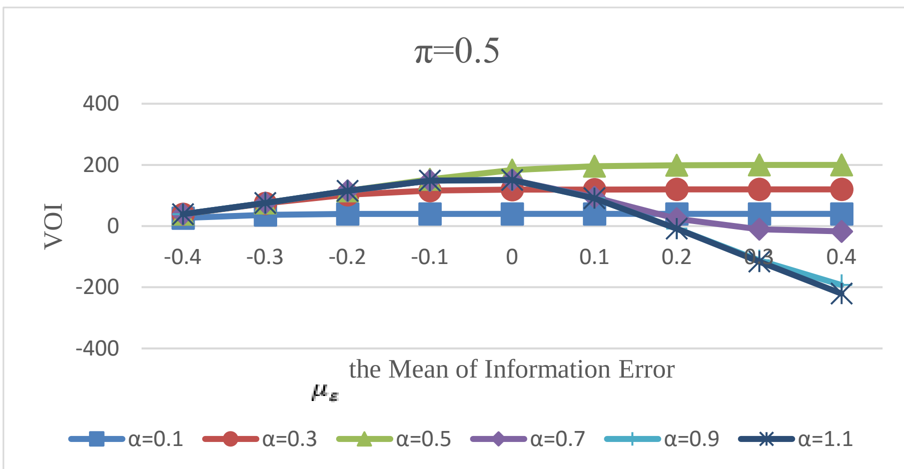
Insight 5.2.1: In most cases, the expected value of disruption information reaches the highest point at $\mu_\varepsilon = 0$ for a given α level, however, one exception is that when $\alpha = \pi$, VOI reaches the highest at some point $\mu_\varepsilon > 0$. This result is due to the existence of information error variability. We conclude that a slight overestimation of disruption influence is better with the existence of disruption variance.

Insight 5.2.2: The impact of μ_ε is not symmetric about $\mu_\varepsilon = 0$. When $\mu_\varepsilon < 0$, the VOI is non-decreasing with μ_ε. When $\mu_\varepsilon > 0$, there are two cases: when $\pi \geq \alpha$, the VOI does not change substantially with μ_ε, and when $\pi < \alpha$, the VOI decreases sharply with μ_ε. The reason is that underestimation ($\mu_\varepsilon < 0$) of the disruption influence can decrease the potential benefit, while overestimation ($\mu_\varepsilon > 0$) can cause detrimental effect when $\pi < \alpha$. This reason is the same as that provided by Insight 5.1.2.

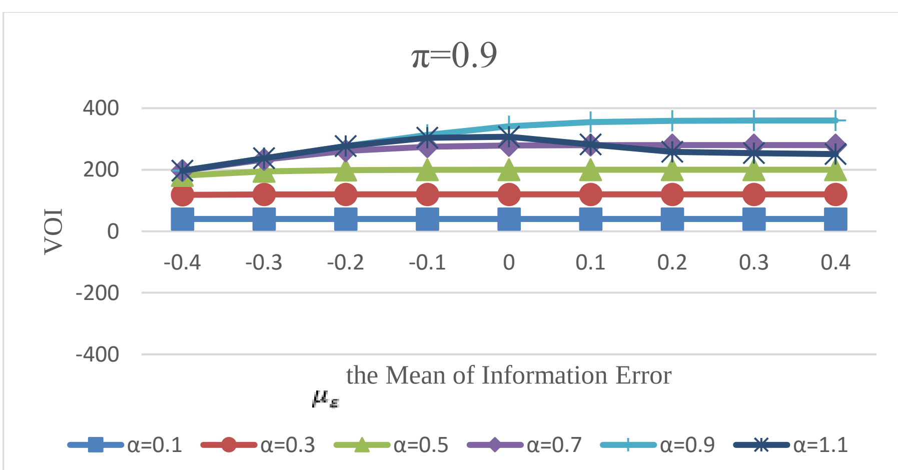
Insight 5.2.3: When the actual disruption influence π exceeds the available resource level α by a large amount, the mean of the information error μ_ε does not have a significant impact on VOI. For example, when $\pi = 0.9$ and $\alpha \leq 0.5$, the value of the disruption information changes only slightly with μ_ε. In reality, this situation occurs when the company has very limited backup resources. In this case, information accuracy does not play an important role on the value of the disruption information. Since the resilience capacity is the bottleneck, having a higher α level can increase VOI. This insight echoes Insight 5.1.3.



(a)



(b)



(c)

Figure 5. VOI with respect to μ_ε for different levels of α

2.5.3 Interaction effect of the variability and the mean of the information error on VOI_π

This interaction effect analysis is complementary to the analyses in Section 5.1 and Section 5.2. We aim to show how the interaction between the mean and variability of information error influences the value of the disruption information. In support of this contention, three different levels each of π and α are selected, $\pi = \{0.1, 0.5, 0.9\}$ and $\alpha = \{0.1, 0.5, 0.9\}$, and the results are displayed in Figure 6.

Each subplot in Figure 6 depicts the relationship between information error bias μ_ε and VOI for different levels of σ_ε. The main insights that we can derive from this analysis are the following:

<u>Insight 5.3.1</u>: VOI is more sensitive to both σ_ε and μ_ε with higher α levels. A company with high resilience capacity has more flexibility to make purchasing decisions; therefore, it tends to have a broader range of VOI, and VOI is more sensitive to σ_ε and μ_ε. This insight enhances our conclusion in Insight 5.1.2 that information accuracy is important to a company with higher resilience capacity.

<u>Insight 5.3.2</u>: In most instances, VOI is decreasing with σ_ε for a given μ_ε. The only exception is when the α level is significantly bigger than π, VOI is actually increasing with σ_ε when the value of μ_ε is big enough, such as when $\pi = 0.5$, $\alpha = 0.9$ and $\mu_\varepsilon = 0.4$. To clarify, the detrimental effect of a high level μ_ε is offset by high level of σ_ε, which implies that decreased information variability may not be beneficial when the disruption influence is significantly overestimated.

<u>Insight 5.3.3</u>: In general, VOI is very sensitive to information accuracy in low-impact situations and only high quality information benefits the company. VOI is moderately sensitive to both information accuracy and α levels in a medium-impact situation. VOI is much less sensitive to information accuracy in a high-impact situation. This insight is consistent with Insight 5.1.3 and Insight 5.2.3.

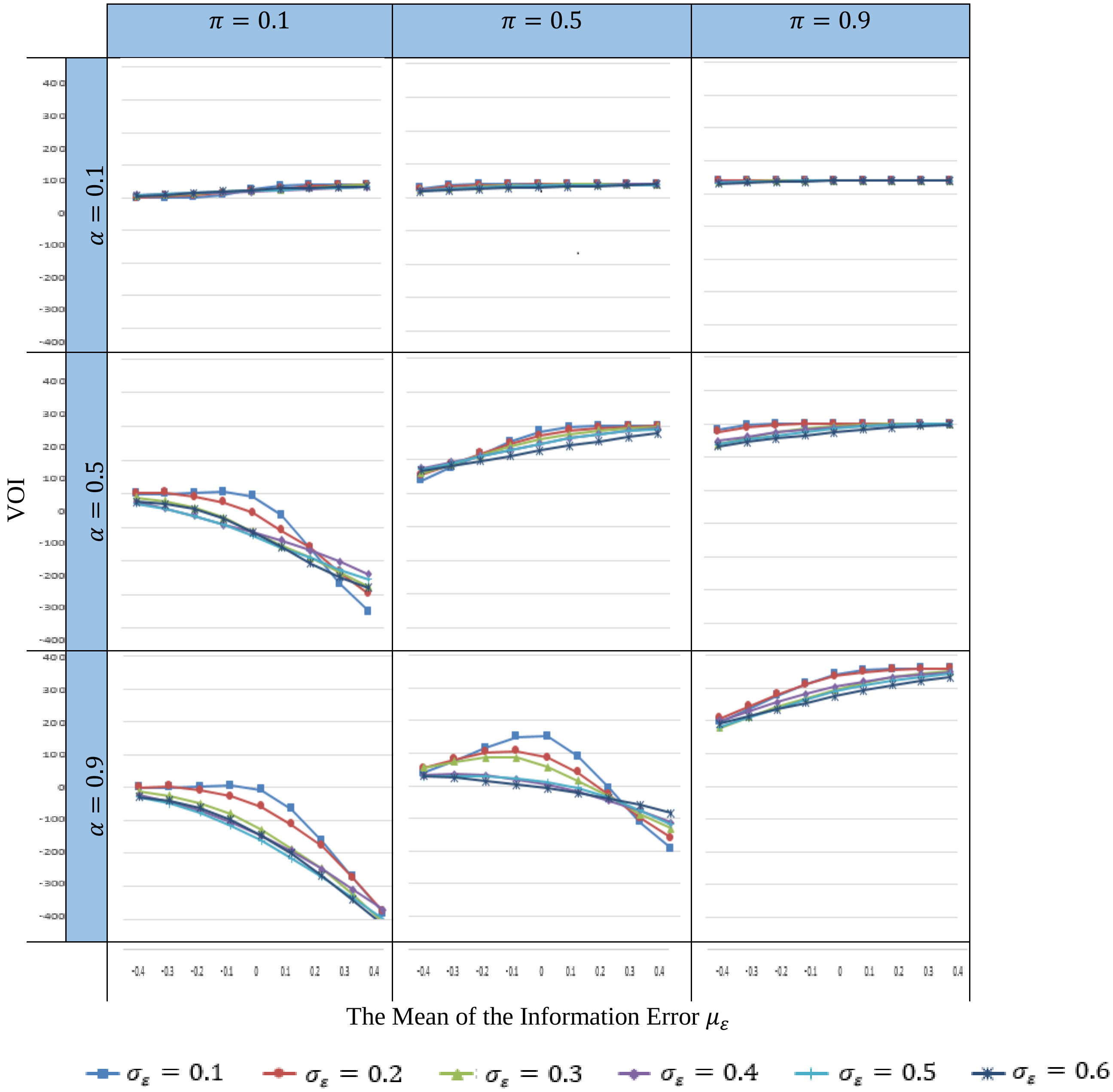


Figure 6. Interaction effect *of* μ_ε and σ_ε on VOI

Insight 5.3.4: In general, the company can benefit more from disruption information at a higher level of actual disruption influence π, which implies that companies tend to perform better if they are warned before a high-impact disruption. A high-impact disruption can cause a high level disruption influence, and thus the company can have higher potential gains from the disruption information.

2.5.4 Effect of the demand fluctuation

The previous analyses are each based on the assumption that $D = V$. But in reality, many factors beyond a manager's control can cause fluctuations in demand. Examples of external factors include currency fluctuations, general economic conditions, competitor actions and technology innovations. Here we want to investigate how demand fluctuation influences the value of the disruption information, and whether the insights in Section 5 still hold with the existence of such demand fluctuation.

To examine the impact of demand fluctuation, we first assume demand is normally distributed with mean V and standard deviation σ_D. Furthermore, we use $\mu_\varepsilon = 0$ in this analysis. We then plot the expected value of the disruption information against σ_D with respect to different levels of σ_ε, as shown in Figure 7. From Figure 7, we can derive the following insights:

Insight 5.4.1: In general, demand fluctuation, σ_D, changes the scale of the value of the disruption information. Specifically, when $VOI > 0$, VOI is decreasing with σ_D, while when $VOI < 0$, VOI is increasing with σ_D.

Perhaps more importantly, however, we also have the following:

Insight 5.4.2: When $\mu_\varepsilon = 0$, the main findings in Section 5.1 still hold even in the presence of demand fluctuation.

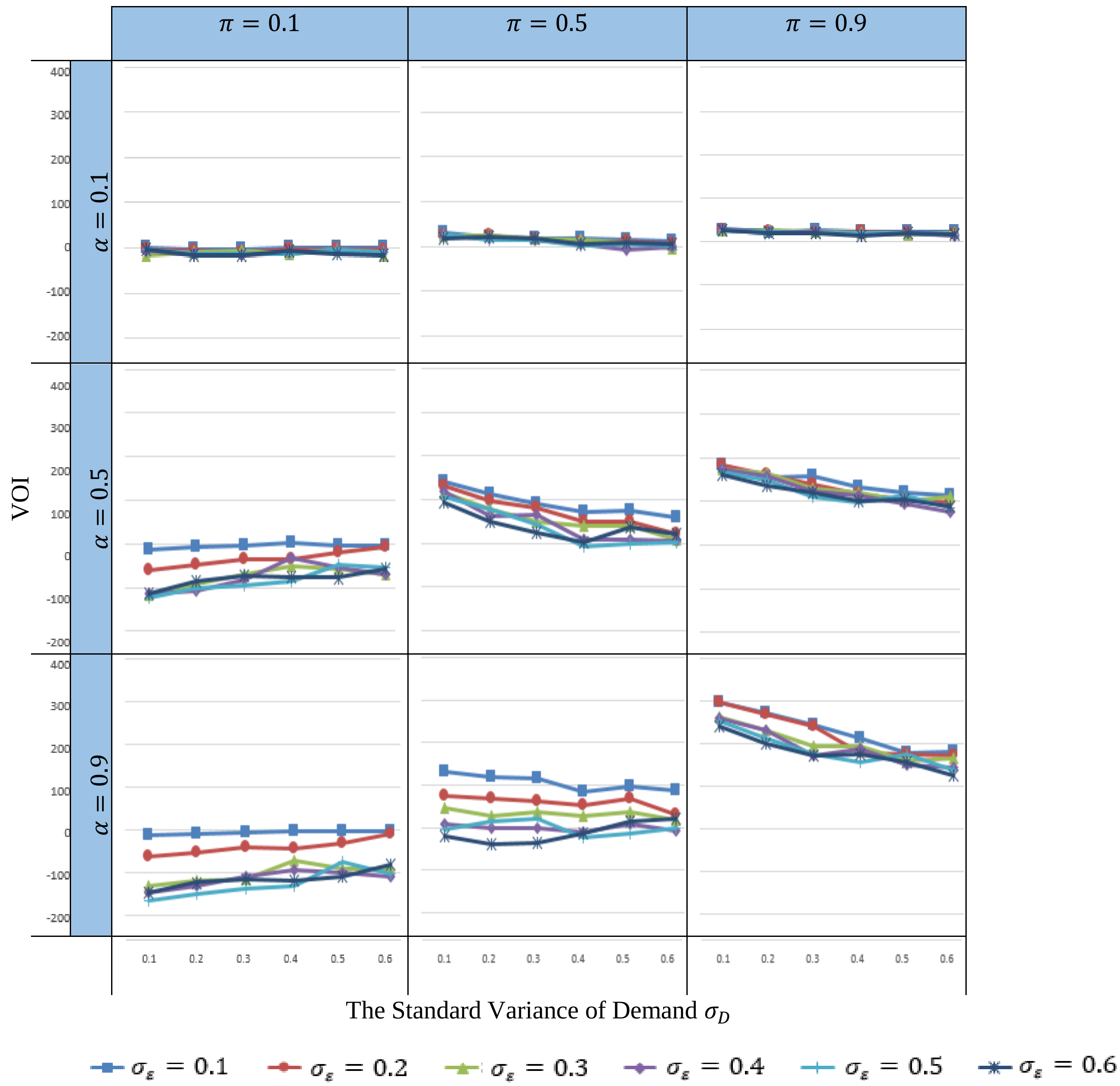


Figure 7. Effect of the demand perturbation

2.6 Conclusions and Implications

In this study, we investigated the factors that influence the value of disruption information, and carefully evaluated the relationship between information accuracy and the value of disruption information at different resilience capacity and disruption severity levels. Based on our analysis above, we have developed the following main findings.

To start, we recognize that there are many factors that influence the value of disruption information, including both non-information related factors and information related factors. Non-information related factors we consider in this study include actual disruption influence, available substitute resources, purchasing price, contracted purchase amount, selling price, holding cost, penalty cost, and demand perturbation. For information related elements, we focus on factors of information bias and information variance, which are measured, respectively, by the mean and the variance of the information error.

For non-information related factors, our analyses in Section 4 show that the value of the disruption information is non-decreasing with selling price and penalty cost, and non-increasing with the purchase price from the source of resilience capacity (such as a backup supplier) and with the holding cost. Our extended analysis in Section 5.4 shows that when the estimation bias is zero ($\mu_\varepsilon = 0$) and the demand is normally distributed with mean V, the demand perturbation decreases the scale of the value of the disruption information, but does not change the other main findings about the effect of the information error variability.

For information related factors, our analyses show that both information bias and information variance have an impact on the value of disruption information; however, these influences vary across different levels of disruption influence and the available substitute resource levels. Our numerical analyses illustrate that accurate disruption information is better in general, but achieving the highest possible level of performance does not necessarily require fully accurate information. Thus, understanding how information accuracy influences the VOI can help practitioners making managerial decisions. For example, if a company is going to invest in obtaining more accurate disruption information, it should consider how much to invest to obtain that information, while also considering the trade-offs associated with additional inventory or shortage costs. The company should also consider how accurate the information ultimately needs to be to make it cost-effective, as well as which information provider should be selected.

Based on our analyses, we summarize the main implications, limitations and future work of this study, as follows:

2.6.1 Implication of Identifying Disruption Risk

Identifying disruption risk is important, even if at low accuracy levels, especially in the case of large disruptions (see Insights 5.1.3 and 5.3.4). With such disruption information, the focal company can better prepare for and respond to a disruption. When a disruption is estimated to be very large, the company might use up all available backup resources. In this situation, improving information accuracy might not then provide additional benefit. The importance of identifying disruption risk, especially that with a large influence, provides a theoretical foundation for the recent emphasis on enhancing visibility in complex, global supply networks (Basole and Bellamy, 2014a, 2014b; Harland et al., 2003; Kim et al., 2015). There are several common ways to increase supply visibility, including identifying the critical points in the supply network, understanding the structure of the supply network, and gaining insight into the risk diffusion mechanism of the supply network.

2.6.2 Implication of Information Accuracy

Our analyses show that although information accuracy plays an important role in determining the value of disruption information, this influence varies for different resilience capacity and disruption severity levels. The implementation of a disruption information strategy should therefore consider the focal company's own conditions and the type of disruption risk that they want to mitigate. Information accuracy in this context is measured by information bias and information variance, and a source of information with less bias and less variance is defined to be more accurate.

Insight 5.1.2 and Insight 5.3.3 illustrate that information accuracy is especially important for companies with abundant resilience capacities. Such companies tend to be larger and thus have enough resources to make the necessary investments. Those higher resilience capacities then allow those companies to have enough flexibility to mitigate disruption risk and to achieve better performance with more accurate information. Comparatively, a company with a lower resilience capacity has less room to mitigate the risk, hence the accuracy of the information has less impact on its value. In the extreme situation that a company has no resilience capacity, obtaining disruption information does not help the current situation at all even if the company has complete information, since the company does not have the capability to cope with the ensuing disruption. It is possible, however, that the company may still want this information for other business considerations such as making a decision to continue investing in a given product.

Insight 5.1.3, Insight 5.2.3, and Insight 5.3.3 further show that information accuracy is more important when there is a lower disruption influence, especially when compared with the available capacity for resilience. This is because when the disruption influence is small, the benefit of disruption information tends to be small and can be largely offset by the cost due to inaccurate influence estimation. Practitioners should therefore be cautious when using disruption information in situations when there is a low disruption influence.

2.6.3 Implication of Resilience Capacity

Resilience capacity also has a significant impact on the value of disruption information, and thus on a company's performance in a disruption situation. Our results in Section 5 show that having a high resilience capacity might actually cause detrimental results if a company does not have the corresponding ability to obtain disruption information. This conclusion contradicts the general statement that a higher resilience capacity is better.

A recent example of this phenomenon occurred in the context of the 2010 Haiti earthquake. Although many resources were available to be shipped to the disrupted area, the lack of clear information about the type or amount of goods needed resulted in all kinds of unwanted materials (including untrained and ineffective volunteers) showing up in the impacted area (Fessler, 2013), and even hindering help (JoNel, 2010). This result could have been offset with access to better and more accurate information.

Although good information about the extent of a disruption can improve the overall performance of a company or organization, this example helps to illustrate that overestimating the disruption influence can cause an organization to suffer excess purchasing and storage costs without receiving additional benefits. Thus, for big companies or organizations with a high resilience capacity, obtaining more accurate disruption information is very important in allowing them to more effectively cope with disruptions.

2.6.4 Limitations and Future Research

There are several related areas of research that we would like to explore in the future. First of all, our analysis so far only considers information quality in terms of the mean and variability of the information error, whereas another important aspect of information quality is the timing of the information. The *advance time* is the time difference between when the disruption information is available and when the actual disruption occurs. It would be interesting to investigate how the advance time, and the trade-off between the advance time and the information accuracy, influence VOI.

Secondly, our study assumes that the available backup resources are static. A company tends to be better prepared, however, and can get access to more substitute resources, if the disruption information is provided earlier. In this sense, the level of available backup resources, α, is dynamic and is a function of the advance time, τ, and disruption information, θ.

Thirdly, in this study we assume that the information error follows a truncated normal distribution. Further investigating VOI under the assumption that the information error follows other distributions, especially asymmetric ones, is another area of future research.

Finally, it is important to note that in this study we are assuming the occurrence of only one disruption at a time, in order to focus our discussion on underlying principles. In reality, however, because companies may be exposed to a large number of different risks, they may actually experience multiple overlapping disruptions within a given decision period. To help companies deal with such situations, future research could make a worthwhile contribution by extending the work above so that it can support decision making in even more complex and uncertain environments. The importance of acquiring disruption information as a risk mitigation method makes such further investigation of its value a matter of both theoretical and practical significance.

References

Accenture. (2014), *Accenture Global Operations Megatrends Study*, available at: www.accenture.com/megatrends (accessed 28 November 2015).

Basole, R.C. and Bellamy, M.A. (2014a), "Visual analysis of supply network risks: Insights from the electronics industry", *Decision Support Systems*, Vol. 67, pp. 109–120.

Basole, R.C. and Bellamy, M.A. (2014b), "Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach", *Decision Sciences*, Vol. 45 No. 4, pp. 1–49.

Business Continuity Institute. (2013), *Supply Chain Resilience 2013 Annual Survey*, available at: http://www.zurich.com/internet/main/sitecollectiondocuments/insight/Supply-Chain-Resilience-2013.pdf (accessed 12 November 2015).

Cannella, S., Framinan, J.M., Bruccoleri, M., Barbosa-Póvoa, A.P. and Relvas, S. (2015), "The effect of Inventory Record Inaccuracy in Information Exchange Supply Chains", *European Journal of Operational Research*, Vol. 243, pp. 120–129.

Chen, F., Drezner, Z., Ryan, J.K. and Simchi-levi, D. (2000), "Quantifying Supply Chain : Lead the Bullwhip The Impact and Effect of in a Simple Forecasting , Times , Information", *Management Science*, Vol. 46, pp. 436–443.

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J. and Handfield, R.B. (2007), "The severity of supply chain disruptions: Design characteristics and mitigation capabilities", *Decision Sciences*, Vol. 38, pp. 131–156.

Fessler, P. (2013), "The 'Second Disaster': Making Well-intentioned Donations Useful", *NPR*, 12 January, available at: http://www.npr.org/2013/01/12/169198037/the-second-disaster-making-good-intentions-useful (accessed 23 June 2016).

Fleisch, E. and Tellkamp, C. (2005), "Inventory inaccuracy and supply chain performance: A simulation study of a retail supply chain", *International Journal of Production Economics*, Vol. 95, pp. 373–385.

Forslund, H. and Jonsson, P. (2007), "The impact of forecast information quality on supply chain performance", *International Journal of Operations & Production Management*.

Garvey, M.D., Carnovale, S. and Yeniyurt, S. (2015), "An analytical framework for supply network risk propagation: A Bayesian network approach", *European Journal of Operational Research*, Vol. 243 No. 2, pp. 618–627.

Harland, C., Brenchley, R. and Walker, H. (2003), "Risk in supply networks", *Journal of Purchasing and Supply Management*, Vol. 9 No. 2, pp. 51–62.

Hübner, D., Larsson, T., Wagner, S.M. and Christ, A. (2014), "Costly Supply Chain Disruptions", *Industrial Engineer*, Vol. 46 No. 3, pp. 32–38.

IBM. (2015), “IBM Connects ‘Internet of Things’ to the Enterprise”, available at: http://www-03.ibm.com/press/us/en/pressrelease/46453.wss (accessed 14 June 2016).

JoNel, A. (2010), “Disaster do-gooders can actually hinder help”, *NBCNEWS*, 23 January, available at: http://www.nbcnews.com/id/34958965/ns/world_news-haiti/t/disaster-do-gooders-can-actually-hinder-help/#.V2wE6pErLct (accessed 23 June 2016).

Kang, Y. and Gershwin, S.B. (2005), “Information inaccuracy in inventory systems: stock loss and stockout”, *IIE Transactions*, Vol. 37, pp. 843–859.

Kerkkänen, A., Korpela, J. and Huiskonen, J. (2009), “Demand forecasting errors in industrial context: Measurement and impacts”, *International Journal of Production Economics*, Vol. 118, pp. 43–48.

Kim, Y., Chen, Y.-S. and Linderman, K. (2015), “Supply Network Disruption and Resilience: A Network Structural Perspective”, *Journal of Operations Management*, Vol. 33-34, pp. 43–59.

Kirilmaz, O. and Erol, S. (2015), “A proactive approach to supply chain risk management: Shifting orders among suppliers to mitigate the supply side risks”, *Journal of Purchasing and Supply Management*.

Kleindorfer, P.R. and Saad, G.H. (2005), “Managing Disruption Risks in Supply Chains”, *Production and Operations Management*, Vol. 14 No. 1, pp. 53–68.

Kwak, J.K. and Gavirneni, S. (2015), “Impact of information errors on supply chain performance”, *Journal of the Operational Research Society*, Vol. 66, pp. 288–298.

Landwehr, P.M. and Carley, K.M. (2014), “Social Media in Disaster Response”, *Data Mining and Knowledge Discovery for Big Data*, Springer Berlin Heidelberg, pp. 225–257.

Mazza, E. (2015), “Nepal Earthquake Happened Right On Schedule, Scientists Say”, *The Huffington Post*, available at: http://www.huffingtonpost.com/2015/04/27/nepal-earthquake-science_n_7149692.html (accessed 9 June 2015).

Oke, A. and Gopalakrishnan, M. (2009), “Managing disruptions in supply chains: A case study of a retail supply chain”, *International Journal of Production Economics*, Vol. 118, pp. 168–174.

Page, P. (2015), “Nepal Earthquake Response Challenges Logistics Experts”, *The Wall Street Journal*, p. 4.

Saghafian, S. and Van Oyen, M.P. (2012), “The value of flexible backup suppliers and disruption risk information: newsvendor analysis with recourse”, *IIE Transactions*, Vol. 44, pp. 834–867.

Sahin, E., Buzacott, J. and Dallery, Y. (2008), “Analysis of a newsvendor which has errors in inventory data records”, *European Journal of Operational Research*, Vol. 188, pp. 370–389.

Sahin, E. and Dallery, Y. (2009), “Assessing the impact of inventory inaccuracies within a Newsvendor framework”, *European Journal of Operational Research*, Vol. 197, pp. 1108–1118.

Sanders, N.R. (2014), *Big Data Driven Supply Chain Management: A Framework for Implementing Analytics and Turning Information Into Intelligence*, 1st ed., Pearson Education, Inc.

Simchi-Levi, D., Schmidt, W. and Wei, Y.H. (2014), "From Superstorms To Factory Fires Managing Unpredictable Supply-Chain Disruptions", *Harvard Business Review*, Vol. 92 No. 1-2, p. 96–+.

Tang, C. (2006), "Robust strategies for mitigating supply chain disruptions", *International Journal of Logistics*, Vol. 9, pp. 33–45.

Tomlin, B.T. and Snyder, L. V. (2006), *On the Value of a Threat Advisory System for Managing Supply Chain Disruptions*.

Wagner, S.M. and Bode, C. (2006), "An empirical investigation into supply chain vulnerability", *Journal of Purchasing and Supply Management*, Vol. 12 No. 6, pp. 301–312.

Yang, Z., Aydin, G., Babich, V. and Beil, D.R. (2008), "Supply Disruptions, Asymmetric Information, and a Backup Production Option", *Management Science*, Vol. 55, pp. 192–209.

Zhao, X. and Xie, J. (2002), "Forecasting errors and the value of information sharing in a supply chain", *International Journal of Production Research*, Vol. 40, pp. 311–335.

Appendix A

Proof of Property 1.

From Formula (4.3), when $\min\{\alpha,\theta\} \leq \pi$, $VOI_{\pi}(\theta) > 0$.

From Formula (4.2), when $\min\{\alpha,\theta\} > \pi$, $VOI_{\pi}(\theta) < 0 \equiv (r+h+p)\pi\text{-}(c_f+h)\min\{\alpha,\theta\} < 0$

So if $\alpha > \theta > \pi$, when $\pi < \frac{c_f+h}{r+h\text{-}c_f}\varepsilon$, $VOI_{\pi}(\theta) < 0$

if $\theta > \alpha > \pi$, when $\pi < \frac{c_f+h}{r+h+p}\alpha$, $VOI_{\pi}(\theta) < 0$

Proof of Property 2.

When $\varepsilon_1 > \varepsilon_2 \geq 0$, $q^*_{f1} = \min\{\alpha,\theta_1\}V$ and $q^*_{f2} = \min\{\alpha,\theta_2\}V$

Case 1: $\alpha > \theta_1 > \theta_2$, $q^*_{f1} = \theta_1 V$ and $q^*_{f2} = \theta_2 V$

$q'_s + q^*_{f1} = (1\text{-}\pi)V + (\pi+\varepsilon_1)V = (1+\varepsilon_1)V > V$

$q'_s + q^*_{f2} = (1\text{-}\pi)V + (\pi+\varepsilon_2)V = (1+\varepsilon_2)V > V$

Thus, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = \text{-}(c_f+h)(\varepsilon_1\text{-}\varepsilon_2)V \leq 0$

Case 2: $\theta_1 > \alpha > \theta_2$, $q^*_{f1} = Q = \alpha V$ and $q^*_{f2} = \theta_2 V$

As $q^*_{f1} > q^*_{f2}$, $q'_s + q^*_{f1} > q'_s + q^*_{f2} = (1+\varepsilon_2)V > V$

Thus, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = \text{-}(c_f+h)\left(q^*_{f1}\text{-}q^*_{f2}\right) \leq 0$

Case 3: $\theta_1 > \theta_2 > \alpha$, $q^*_{f1} = q^*_{f2} = Q = \alpha V$

Thus, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = 0$

In sum, when $\varepsilon_1 > \varepsilon_2 \geq 0$, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) \leq 0$, $VOI_{\pi}(\theta)$ is non-increasing with ε.

When $0 > \varepsilon_1 > \varepsilon_2$, $q^*_{f1} = \min\{\alpha,\theta_1\}V$ and $q^*_{f2} = \min\{\alpha,\theta_2\}V$

Case 1: $\alpha > \theta_1 > \theta_2$, $q^*_{f1} = \theta_1 V$ and $q^*_{f2} = \theta_2 V$

$q'_s + q^*_{f1} = (1\text{-}\pi)V + (\pi+\varepsilon_1)V = (1+\varepsilon_1)V < V$

$q'_s + q^*_{f2} = (1\text{-}\pi)V + (\pi+\varepsilon_2)V = (1+\varepsilon_2)V < V$

Thus, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = (r+p\text{-}c_f)(q^*_{f1}\text{-}q^*_{f2}) > 0$

Case 2: $\theta_1 > \alpha > \theta_2$, $q^*_{f1} = Q = \alpha V$ and $q^*_{f2} = \theta_2 V$

$VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = (r+p\text{-}c_f)\left(q^*_{f1}\text{-}q^*_{f2}\right) \geq 0$

Case 3: $\theta_1 > \theta_2 > \alpha$, $q^*_{f1} = q^*_{f2} = Q = \alpha V$

Thus, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) = 0$

In sum, when $0 > \varepsilon_1 > \varepsilon_2$, $VOI_{\pi}(\theta_1)\text{-}VOI_{\pi}(\theta_2) \geq 0$, $VOI_{\pi}(\theta)$ is non-decreasing with ε.

Proof of Property 3.

When $\alpha \leq \theta$, $q_f^* = \min\{\alpha, \theta\} V = Q = \alpha V$

if $q_s^{'} + q_f^* > V \Rightarrow (1\text{-}\pi)V + \alpha V > V \Rightarrow \alpha > \pi$,

$VOI_\pi(\theta) = (r + h + p)\pi V\text{-}(c_f + h)Q$

$\frac{dVOI_\pi(\theta)}{dQ} = \text{-}(c_f + h) < 0$

if $q_s^{'} + q_f^* \leq V \Rightarrow (1\text{-}\pi)V + \alpha V \leq V \Rightarrow \alpha \leq \pi$

$VOI_\pi(\theta) = (r + h\text{-}c_f)Q$

$\frac{dVOI_\pi(\theta)}{dQ} = (r + h\text{-}c_f) > 0$

When $\alpha > \theta$, $q_f^* = \theta V$, so $VOI_\pi(\theta)$ is independent of Q.

Proof of Property 4.

When $q_s^{'} + q_f^* > V$, $\frac{dVOI_\pi(\theta)}{dr} = \frac{dVOI_\pi(\theta)}{dp} = \pi V \geq 0$, $\frac{dVOI_\pi(\theta)}{dc_f} = \text{-}q_f^* \geq 0$, $\frac{dVOI_\pi(\theta)}{dh} = \pi V\text{-}q_f^* < 0$,

When $q_s^{'} + q_f^* \leq V$, $\frac{dVOI_\pi(\theta)}{dr} = \frac{dVOI_\pi(\theta)}{dp} = q_f^* \geq 0$, $\frac{dVOI_\pi(\theta)}{dc_f} = \text{-}q_f^* \geq 0$, $\frac{dVOI_\pi(\theta)}{dh} = 0$.

Chapter 3: Quantifying Supply Chain Network Resilience: A Dynamic Approach

3.1 Introduction

Responding to the challenges of global sourcing, localized assortment, and cross-channel marketing, the supply chain networks of many companies are becoming increasingly complex and intricate, and are thus more vulnerable to disruptions. Studies show that supply chain complexity can both increase the frequency of supply chain disruptions (Bode & Wagner 2015) and the severity of the disruptions (Craighead et al. 2007). These disruptions can be further exacerbated by risk diffusion – poor performance of one supplier can cause financial loss to a company, and eventually may affect other companies in the network. Understanding supply chain health, especially on a quantitative level, can support practitioners in comparing different disruption mitigation and recovery strategies, and it can assist with decision making.

Supply chain resilience is a holistic measure of supply chain health (Ponomarov and Holcomb 2009; Christopher and Peck 2004). This concept is based on the idea that supply chain disruption is unavoidable (Ponomarov and Holcomb 2009; Pettit, Croxton, and Fiksel 2013), therefore a supply chain should not only reduce disruption risks but also be well prepared to quickly respond and recover from disruptions. Previous studies have proposed an integrated quantitative measure of disruption risk, disruption severity and disruption recoverability (Falasca, Zobel, and Cook 2008; Zobel 2011; Zobel and Khansa 2014; Tierney and Bruneau 2007). These approaches, however, only consider disruptions occurring at a specific node in the network.

There are compelling needs to investigate *network* level resilience, which incorporates the risk diffusion process and looks into both network robustness and recoverability. Firstly, studying network resilience is practically needed. A recent study shows that 42% of disruptions originated below the tier one supplier (Business Continuity Institute 2013), and these disruptions can easily spread to the whole supply network through risk diffusion. Secondly, looking at network level resilience can fill the current literature gap. Existing quantitative studies on supply chain performance against disruptions offer two approaches, with one focusing on network tolerance to disruptions (Zhao et al. 2011; Thadakamalla et al. 2004; Nair and Vidal 2011; Kim, Chen, and Linderman 2015), and the other on network impact on the risk diffusion process (Basole and

Bellamy 2014a). Although each approach provides important insights, neither considers both the disruption severity and recoverability at the same time. Thirdly, considering only one aspect of the resilience can have misleading results, as trade-offs might exist between robustness and recoverability. For example, a scale free network is robust in terms of random disruptions (Nair and Vidal 2011; Zhao et al. 2011), but it can accelerate risk propagation and hence lead to lower recoverability (Basole and Bellamy 2014a).

Therefore, in this study we build an analytical framework to quantify supply chain network resilience in the presence of risk diffusion, with both robustness and recoverability accounted for. We also perform in-depth analysis to show how the proposed resilience measure can help people better understand the network, and support decision making against disruptions. The study is expected to contribute to the literature both theoretically and practically.

Theoretically, this study will enrich the supply chain network resilience literature by providing a multi-dimensional framework. Conceptually, supply chain resilience is a holistic measure of supply chain health, although recent quantitative studies tend to focus only on robustness, or the ability to withstand the initial impact of a disruption (Thadakamalla et al. 2004; Zhao et al. 2011; Kim, Chen, and Linderman 2015), and not on other important aspects of the network's behavior. Providing a multi-dimensional framework can narrow the gap between qualitative study and quantitative study.

This study also contributes to the limited quantitative research on dynamic supply chain network resilience (Basole and Bellamy 2014a). A disruption that happens to a network may propagate and amplify its impact, even if it is just a few nodes in the network that are initially disrupted; recovery may therefore take a long time. In order to characterize this recovery behavior, as a part of overall resilience, it is important to adopt a dynamic approach.

Finally, this study enhances our understanding of the impact of network structure and other factors on different aspects of supply chain resilience. Current studies show that network structure greatly impacts the supply chain robustness and risk diffusion process. However, the impacts are not complementary. For example, a scale-free network is especially robust to disruption severity (Nair and Vidal 2011; Zhao et al. 2011; Kim, Chen, and Linderman 2015), but it can also accelerate the risk diffusion process and lead to a lower health level (Basole & Bellamy, 2014). Thus, a comprehensive understanding of these effects can lead to a better understanding of the significance of network structure and other factors.

Practically, this study can help practitioners better understand the health status of the supply chain network, which will allow them to develop better strategies. The health of the supply chain network can greatly influence the health level of each node within the network. Understanding this network health can help practitioners formulate proper sourcing, production and marketing strategies to gain competitive advantage. Besides, this work can allow practitioners to evaluate the impacts of different network configurations, and node recovery and risk diffusion rates, on network resilience, and thus it can assist their managerial decision making with respect to disruption mitigation and recovery.

The remainder of the paper is organized as follows: Section 2 provides a review of the literature. Section 3 proposes an analytical network resilience framework. In Section 4, we provide an in-depth analysis on how different impact factors influence different aspects of network resilience, and we derive practical implications based on the analytical results. Then, in Section 5, we use a case study to show how this framework can help supply chain managers in understanding their supply chain network. Finally, we conclude with a brief summary in Section 6.

3.2 Background

3.2.1. Supply Chain Resilience

The study of supply chain disruptions has experienced a recent explosion of interest both from academics (Snyder et al. 2012; Fahimnia et al. 2015) and from practitioners in the past decade. This sharp increase in interest is due to several reasons. First, high-profile disaster events, such as Hurricane Sandy in 2012 and the Tohoku Earthquake in 2011, have brought disruptions into public attention (Snyder et al. 2012); secondly, global supply chains are becoming more complex and thus more vulnerable to disruptions (Craighead et al. 2007; Bode and Wagner 2015); thirdly, the development of new techniques, such as big data analysis and social media analysis (Landwehr and Carley 2014), and sustainability risk analysis (Fahimnia et al. 2015), has sparked new research interest in this area. The concept of supply chain resilience has emerged from this background.

Supply chain resilience, as a distinct topic, is quickly evolving within the supply chain risk management (SCRM) field (Ponomarov and Holcomb 2009; Christopher and Peck 2004). Traditional SCRM covers a wide topic of risk identification (Wagner and Bode 2006; Kleindorfer and Saad 2005), risk mitigation (Tomlin 2006; Tang 2006; Craighead et al. 2007; Blackhurst et al. 2005; Oke and Gopalakrishnan 2009) and supply chain recoverability (Tomlin and Snyder 2006; Kleindorfer and Saad 2005; Tomlin 2006). Comparatively, supply chain resilience focuses on the capability of a company to prepare for, to respond, and to recover from a disruption (Pettit, Fiksel, and Croxton 2010; Falasca, Zobel, and Cook 2008; Ponomarov and Holcomb 2009; Jüttner and Maklan 2011). The fundamental difference between them is that SCRM focuses on risk control, while supply chain resilience also emphasizes the system capability to be well prepared for, to quickly respond to, and to recover from disruptions. The idea of supply chain resilience is thus based on the understanding that some disruptions are unavoidable.

Compared with qualitative studies of supply chain resilience, there are relatively few quantitative studies on supply chain resilience, and they tend to focus on specific dimensions of resilience, and thus are less integrated. Besides the traditional emphasis on supply chain robustness (Zhao et al. 2011; Zhao, Kumar, and Yen 2011; Nair and Vidal 2011; Kim, Chen, and Linderman 2015), researchers recently have looked into an integrated measure of the disruption's severity and the ability to recover from it (Falasca, Zobel, and Cook 2008; Zobel 2011; Zobel and Khansa 2014). However, to our best knowledge, no existing quantitative research provides a truly holistic view of supply chain resilience, as do the more conceptual research efforts; we therefore are motivated to develop a resilience framework to narrow the gap between qualitative studies and quantitative studies.

We will take a network perspective of the supply chain resilience, as it is well recognized that a supply chain is a complex network (Carter, Rogers, and Choi 2015). Studies of supply chain resilience are either from the node view that considers the influence of disruptions on a specific node (Pettit et al., 2013; Pettit et al., 2010; Zobel & Khansa, 2014; Zobel, 2014), or from the network view that focuses on the influences of disruption on the whole network (Zhao et al. 2011; Kim, Chen, and Linderman 2015).

3.2.2. Risk Diffusion

Supply chains are complex networks with firms as the nodes and their interactions as the arcs. With industry globalization and regional specification, current supply chains are becoming more complex, hence more vulnerable to disruptions.

These disruptions can be further exacerbated by risk diffusion – a sudden disruption at one node in a company's supply chain network can spread to other nodes in the same network, and may adversely impact other companies as well. For example, in the aftermath of the Thailand floods from July 2011 to January 2012, although the disruption happened locally, the consequences of the flood were global. As Thailand is the world's second largest producer of hard disk drives

(HDD), this flood severely hurt the consumer electronics industry. For its fiscal quarter including December 2011, HDD manufacturer Western Digital, with local factories in Thailand, suffered a 50% slump in sales volume of HDD units and incurred costs of $199 million related to the flooding; computer producer Hewlett Packard then reported a 7% drop in its revenue and blamed the HDD shortage for more than half of the decline; and microprocessor maker Intel posted a revenue of $13.9 billion, $0.8 billion lower than its previous forecast as a result of lower demand following the flood.

As this example illustrates, the risk diffusion mechanism of a network can significantly influence supply chain recoverability, and thus supply chain resilience. Ignoring this effect will result in an underestimation of the systemic risk and hence a decreased profit. As an indicator of its importance, studies on risk diffusion are rich in the business literature. There are empirical studies that examine the wealth effects of financial distress along the supply chain (Hertzel et al. 2008), and conceptual studies that consider the ripple effect in supply chains (Ivanov, Sokolov, and Dolgui 2014; Koh, Gunasekaran, and Tseng 2012). Quantitative studies are also presented to investigate the mechanisms of bankruptcy propagation in large-scale supply chain networks (Battiston et al. 2007; Basole and Bellamy 2014a) or complex financial networks (Gai and Kapadia 2010). No such work has yet been done, however, within the context of supply chain resilience. By incorporating the risk diffusion effect into the resilience framework, our study is expected to contribute to the quantitative literature in this important area.

3.2.3. Network Structure

Network structure has been well recognized as a determining factor for supply chain performance against disruptions (Snyder et al. 2012). Studies of network structure in terms of their ability to resist disruptions mainly follow two research streams: traditional optimization approaches (Nagurney 2010; Eskandarpour et al. 2015; Wang, Lai, and Shi 2011) and high level approaches focusing on comparing the relative performance of different network types (Kim, Chen, and Linderman 2015; Nair and Vidal 2011; Zhao et al. 2011; Thadakamalla et al. 2004). We discuss each of these in more detail below.

In terms of the global complex supply chain network, traditional optimization approaches are especially difficult to perform, and they tend to be ineffective. Supply chain network structure has been extensively studied from the classical optimization perspective, from which the authors construct a network from available nodes and arcs to maximize the supply chain performance against disruptions (Snyder et al. 2012). This approach works well under the assumption of static and relatively small size networks, but not for a large scale and dynamic network, which are the main characteristics of the current global supply chain networks. For example, with over 75,000 direct suppliers worldwide (P&G News 2015) and complex relationships among these suppliers, it is impossible for Procter & Gamble to enumerate all relationships, especially since these suppliers are dynamically changing with the global economy.

Accordingly, researchers started to investigate high level questions that compare different network structures with respect to their ability to tolerate disruptions. Current research shows that the structure of a supply chain network has great impact on the robustness (Zhao et al. 2011; Thadakamalla et al. 2004; Nair and Vidal 2011; Kim, Chen, and Linderman 2015), and on risk propagation (Basole and Bellamy 2014a), and hence on recoverability. These studies, however, show that there might be a trade-off between robustness and recoverability. For example, a scale-free network is especially robust against random disruptions (Nair and Vidal 2011; Zhao et al. 2011; Kim, Chen, and Linderman 2015). Comparatively, Basole and Bellamy (2014a) shows that a scale-free network can accelerate risk diffusion, resulting in lower recoverability.

Looking into the network types also has practical implications. By comparing the real supply network with the simulated network, Basole and Bellamy (2014a) illustrate that the electronics industry supply network is more of a small-world type of network, and the automotive industry is more of a scale-free type of network. Therefore, understanding how network types influence supply chain resilience can let practitioners better estimate the disruption influence, and it can assist managerial decisions about disruption mitigation and recovery.

3.3 Resilience Modelling Framework

3.3.1. Disruption Profile and Resilience Framework

In terms of the impact on company performance, which can be measured by sales, production level, customer service or any other relevant metric, a typical disruption profile includes eight phases, including preparation, the disruptive event, first response, initial impact, full impact, recovery preparations, recovery and long-term impact. (Sheffi and Rice Jr. 2005). As the nature of the disruption and the dynamics of a supply chain network’s response resembles a company’s, we adopt the concept of the disruption profile in our network context to propose a quantitative network resilience framework. This framework includes three dimensions: robustness, recoverability and resilience, which are explained below in detail. Figure 1 illustrates this reformed disruption profile, and Table 1 summarizes this quantitative framework.

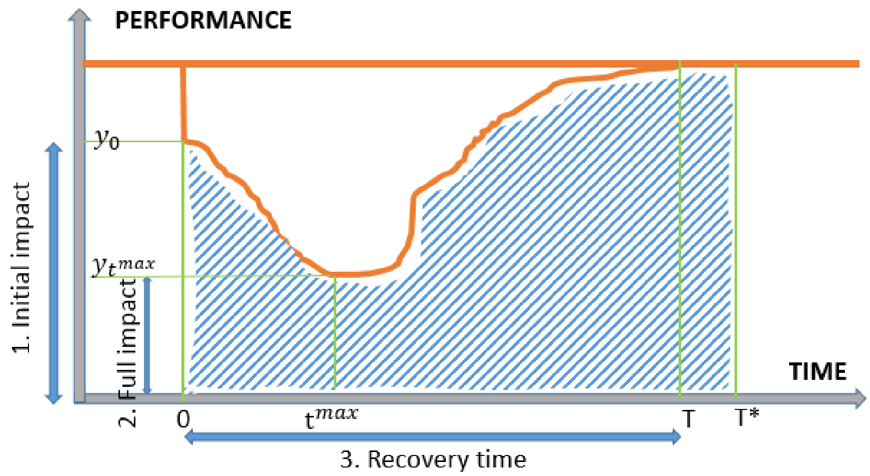


Fig. 1. Disruption profile.

Table 1

Quantitative Network Resilience Framework

Dimension	Measures
Robustness	Initial impact, Full impact
Recoverability	Recovery time
Resilience	Overall resilience

3.3.1.1. Robustness

Supply chain robustness, or disruption absorptive capacity, measures the system's capability to maintain functionality under a disruption, or to absorb the disruption impact and minimize consequences (Tierney and Bruneau 2007; Vugrin, Warren, and Ehlen 2011). Based on this definition, a system that has higher robustness tends to perform better right after the disruption, or to have a higher functionality when the full impact of the disruption is realized. We therefore use the functionality at *initial impact* and at *full impact* to measure supply chain network robustness, a bigger value represents a higher network robustness. To make different systems comparable, this functionality is measured as the percentage to the full operation level.

Specifically, the *initial impact* measures the network functionality right after the disruption, and *full impact* measures the network functionality when the maximum impact happens. If we set t as the time, and y_t as the performance at time t, then assuming the disruption happens at time $t = 0$ and the full impact occurs at time t^{max}, the two robustness measures are:

$$Robustness_{initial-impact} = y_0$$

$$Robustness_{full-impact} = y_{t^{max}}$$

3.3.1.2. Recoverability

System recoverability, or restorative capacity, normally connects with a system's capacity to restore full functionality in a timely manner (Tierney and Bruneau 2007; Vugrin, Warren, and Ehlen 2011). Here we use the total *recovery time* to measure the system recoverability, where a higher recovery time represents a lower recoverability. The recoverability measure is thus:

$$\text{recovery time} = T$$

3.3.1.3. Resilience

Although there is no commonly agreed upon definition of resilience, resilience is consistently viewed as a dynamic process in a certain period of time (Ponomarov and Holcomb 2009; Tierney and Bruneau 2007; Sheffi and Rice Jr. 2005). To measure supply chain network resilience, we adopt the resilience triangle proposed by Tierney & Bruneau (2007), and then greatly extended by Zobel & Khansa (2012, 2014) and Zobel (2011, 2014). From this perspective, resilience is calculated as the percentage area under the performance curve over the total area in a specific time period, which represents the system's overall performance, or operation capacity, within the given timeline. In Figure 1, for example, the area under the performance curve from time zero to time T^* is $\int_0^{T^*} y_t dt$, here y_t is the performance curve function. In reality, supply chain performance is often recorded at distinct points in time, rather than continuously, thus a discrete version $\sum_0^{t=T^*} y_t dt$ may be more adaptable to practical usage.

For the following analyses and case study, we therefore define resilience as the percentage of the (discretized) shaded area over the total area for the given period. Specifically, the resilience function is:

$$\text{Resilience} = \frac{1}{T^*} \sum_0^{t=T^*} y_t dt.$$

From the resilience function, we know that the value of resilience is dependent on the selection of T^* (Zobel 2014), which is based on a decision maker's requirements. For example, if a decision maker cares about short term resilience, he might choose a smaller T^*. However, as long as the T^* is chosen to be bigger than the *recovery time*, then the actual value chosen for T^* is less significant, since the relative ranking of resilience values then will not change for different T^* (Zobel 2014). In order to measure long time average performance consistently across different networks, we therefore select $T^* > t^*$ in the following analysis.

3.3.1.4. Performance Measures

As mentioned before, a performance measure can be any quantitative metric related to network performance. Previous studies have used different measures to measure network performance against disruptions. In Table 2, we list these performance measures and their measurement scope, as used in recent quantitative studies.

Table 2

Resilience measures of current quantitative studies.

Reference	**Performance Measures**	**Measurement Scope**				**Static/ Dynamic**
		Robustness --Initial impact	**Robustness --Full impact**	**Recoverability**	**Resilience**	
Nair & Vidal (2011)	Inventory level, Backorders Total costs	Y				Static
Thadakamalla et al. (2004) Zhao et al., (2011)	Size of LCC Average path length in LCC Max. path length in LCC	Y				Static
Kim et al., (2015)	$\frac{\text{Total number of node or arc disruptions that does not result a network disruption}}{\text{total number of node or arc disruptions}}$	Y				Static
Basole & Bellamy, (2014)	Change of healthy nodes		Y			Dynamic

All of these performance measures have their advantages and disadvantages. The performance measures chosen by Nair & Vidal (2011), for example, are easy to understand, but calculating them requires lots of assumptions and this approach only fits one product situation. Measures used by Thadakamalla et al. (2004), Zhao et al. (2011) and Kim et al. (2015) are easier to calculate and can be adapt to multi-products situations, but these measures are abstract, and less interpretable to practitioners.

Different performance measures also represent different angles by which to look at network tolerance. For example, *total costs* describe how a disruption influences operations (Nair and Vidal 2011), *size of LCC* describes the network connectivity and *average path length in LCC* and *Max. path length in LCC* describe network accessibility (Thadakamalla et al. 2004; Zhao et al. 2011). The calculated measure from Kim et al. (2015) represents the likelihood of a network level disruption.

For demonstration reasons, we carefully select three performance measures to show the corresponding results when they are incorporated into the network resilience calculation. We need to be aware that other performance measures can also be used to calculate the corresponding resilience. The selected performance measures are:

Number of healthy nodes: this measure is the number of healthy nodes in the network, which is used by Basole and Bellamy (2014) to measure the network risk propagation. As the health of a supply chain network is largely dependent on the health of each entity within the network, this measure represents the health status of a network.

Size of LCC: this measure is the number of healthy nodes in the largest connected component(s) (LCC) of the network. When a disruption happens, the network may disconnect and separate to pieces. LCC is the largest connected piece that represents the well-functioning part of the network. A larger LCC means better network performance against the disruption (Thadakamalla et al. 2004; Zhao et al. 2011). The difference between the size of the LCC and the number of healthy nodes is the total healthy nodes outside of the LCC. Although these "external" nodes are isolated, once the path resumes the network can quickly recover. In this sense, the number of healthy nodes and the size of the LCC provide different, but complementary perspectives to look at network performance against disruptions.

Size of LCC/Average path length of LCC: Average path length (APL) is also a common measure of supply chain efficiency after disruption. A shorter APL means more efficient flow in the network (Albet, Jeong, and Barabasi 2000; Thadakamalla et al. 2004; Zhao et al. 2011) However, the average path length is highly correlated with the size of the network in that a bigger size LCC tends to have a larger APL. Thus, to incorporate this efficiency into our resilience measure, we use the size of LCC/APL as one of the performance measures.

3.3.2. Model Assumptions: Network risk diffusion and recovery

Once a disruption happens in a supply chain network, the disruption risk can disperse to the direct suppliers and customers of the disrupted nodes. For example, in the 2011 Thailand floods, the flood severely hurt the local HDD manufacturer and Western Digital consequently suffered a 50% slump in sales volume of HDD units and incurred costs of $199 million. Its customer, computer producer Hewlett Packard, subsequently reported a 7% drop in its revenue and blamed the HDD shortage for more than half of the decline. HP's supplier, Intel, also posted revenues of $800 million lower than forecast as a result of lower demand following the flood.

At the same time, the disrupted companies seek resources to restore their operations, and they have a probability of recovering from the disruption during a given time period. Once a node recovers from a disruption, we consider that this node has become immune against this specific instance of risk. For example, the 2011 Tohoku earthquake and tsunami severely impacted Japan as a vital supplier of parts and equipment for automobiles. This earthquake caused many automobile plants to be closed, with restart dates uncertain. However, once these companies successively restored their operations, they remained operational afterwards.

In the context of our modeling approach, we use a constant risk diffusion probability and a constant recovery probability in order to illustrate this recovery process within the supply chain network resilience measurement framework. Basically, we adopt the assumptions below:

- In a supply chain network, one node represents one company and the disruptions happen at the node level.
- There are two statuses of a node: disrupted and healthy. A healthy node can be susceptible or immune. A node is immune once it recovers from a disruption.
- There is a constant risk diffusion probability $p_{risk\_diffusion}$ and a constant recovery probability $p_{recovery}$.
- The network is undirected, with respect to risk propagation, as the risk can disperse in either direction.

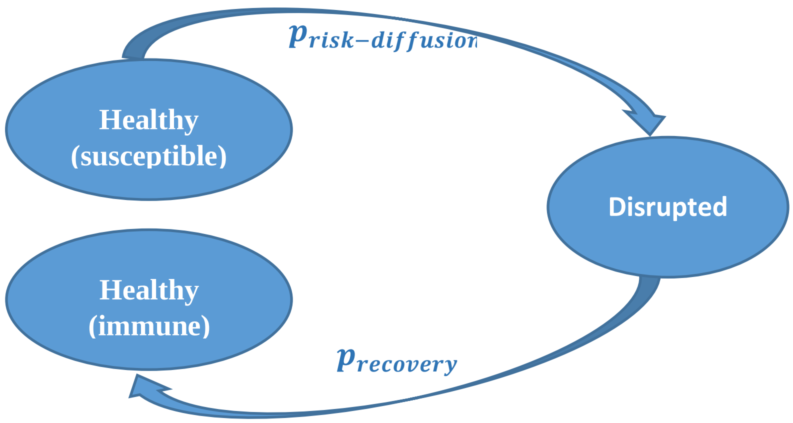


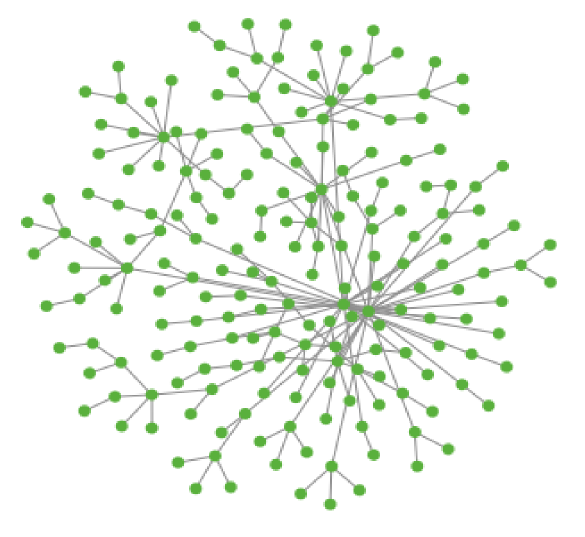
Fig. 2. Node status transition.

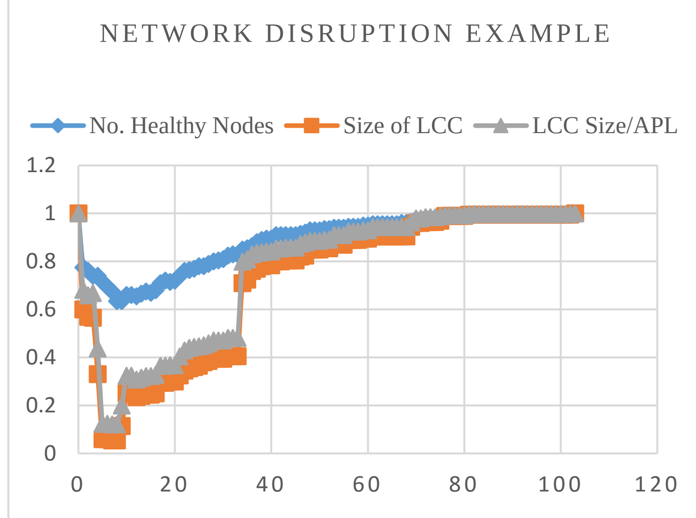
3.3.3. Calculation Illustrations

Here we use a simulated network to illustrate the calculation of supply chain network robustness, recoverability, and resilience. The NetLogo 5.3 modeling platform (Wilensky 1999) is the simulation tool that is used. We record the three different performance measures at each time point, and calculate the network robustness, recoverability, and resilience for a given time period.

The simulated network is a scale free network with 200 nodes. Initially we shut down 30 nodes randomly, which is 15% of the total number of nodes. We further assume that each individual node has the same recovery rate of 5%, and that this disruption risk can be spread to neighbors at a probability rate of 10%. Once a node has recovered from the disruption, this node has immunity to this specific disruption risk and cannot be reinfected.

Under the above setting, this simulated disruption takes 103 steps to total recovery. Figure 3 shows the exemplified network and one run of the simulated disruption and recovery process across different resilience measures. Table 3 then shows the calculated robustness, recoverability and resilience measures. To reflect the short time and the long time overall performance, we use $T^* = 30$ and $T^* = 120$ to calculate partial resilience and full resilience scores.





Network Type: Scale Free No. nodes: 200 No. links: 200	Disruption Severity: 15% (30 nodes) Recovery rate: 5% Risk diffusion rate: 10%

Fig. 3. Calculation illustration.

Table 3

Illustrative results.

	Robustness		Recoverability (steps)	Resilience	
	Initial Impact	Full Impact		$T^* = 30$	$T^* = 120$
No. Healthy nodes	0.755	0.635	103	0.723	0.902
Size of LCC	0.600	0.055	103	0.300	0.761
Size of LCC/APL	0.682	0.122	103	0.378	0.798

3.4 Network Resilience Analysis

In this section we provide a preliminary illustration of the value of the new framework by examining how network structure and other parameters influence robustness, recoverability and resilience, and by analyzing some of the intricate relationships between these three output measures. These analyses can give us an integral knowledge of how different factors influence different aspects of network resilience and help us understand the tradeoffs among different measures, thus supporting more informed decision making to improve supply chain resilience.

3.4.1. Experimental Design

To discover the relationships between network parameters and resilience, and to review the associations among the different aspects of resilience, we design an experiment accordingly. The parameter settings of the experimental design are motivated by previous work, and Table 4 reports the details.

3.4.1.1. Control Variables

We select network size (or number of nodes) and disruption severity as the control variables in our experiment, as the settings of these two variables are beyond the control of the decision makers (single company in a network or supply chain managers), yet they may play an important role in network resilience.

Network size, together with the number of links, defines a network's complexity (Choi and Krause 2006), which is conceptualized in three dimensions: network size (number of nodes), the in-degree and out-degree of suppliers, and inter-relationships among the suppliers. Studies on network size have generated different results from different perspectives. Bode and Wagner (2015), for example, conclude that supply chain complexity, defined by number of suppliers in horizontal, vertical and spatial aspects, increases the frequency of disruptions. Craighead et al. (2007) believe that supply chain complexity is positively correlated with disruption severity as a more complex network would likely have more nodes affected than a less complex network. Albet, Jeong, and Barabasi (2000) discuss the result that network robustness, specifically average path length, is independent of the network size, apart from a logarithmic size correction.

Disruption severity, in turn, is the number of nodes (or companies) impacted at the beginning of a disruption. Although a company owner or supply chain manager can often invest in mitigation practices to reduce the local impact of a disruption once it occurs, they generally cannot predict or prevent the disruption, or affect its initial intensity, particularly if they are not directly responsible for the portion of the network that is impacted. As with network size, this is thus a factor that is out of the decision maker's control.

The settings for network size used in the following analysis range from 100 to 500, which represents a moderate size supply chain network (Basole and Bellamy 2014b). The disruption severity levels are set to vary from 10% to 70%, in order to provide a range of values from low initial risk to high initial risk.

3.4.1.2. Independent Variables

Our analysis focuses on four independent variables: network type, average degree, recovery rate and risk diffusion rate. Among them, network type and average degree are in the scope of network structure, while recovery rate and risk diffusion rate are in the scope of system adaptivity and flexibility.

Previous studies show that network structure influences network performance against disruptions, and these studies mainly take a network-level perspective (Thadakamalla et al. 2004; Zhao et al. 2011; Kim, Chen, and Linderman 2015; Nair and Vidal 2011). The most frequently studied supply chain network types are scale-free, small-world, and random, because scale-free and small-world resemble real supply chain networks (Basole and Bellamy 2014a) and the random type of network is used as a benchmark for comparison (Nair and Vidal 2011). For this reason, we also use these three network types to conduct the analysis.

To make the different network types comparable, we examine their performance based on the same settings for both network size (as discussed above) and average degree (number of links). The average degree of the network ranges from 2 to 8 to reflect prior parameter considerations and to represent moderate size actual supply chain networks (Basole and Bellamy 2014b). For example, Zhao et al. (2011) measure supply chain resilience for a network with average degree 3.6. Basole and Bellamy (2014a) study the risk diffusion process using an average degree ranging from 2 to 20.

Understanding the association between network structure and network resilience can be very important to supply chain managers in that by better understanding the risk level of the system, even if it is outside of their control, they can be better prepared for future disruptions. They may also, however, be able to improve at least a portion of the network structure to enhance network resilience. For example, as the total number of links represents the collaboration among nodes in a network, supply chain managers can increase or decrease these links to achieve better performance.

For both the recovery rate and the risk diffusion rate, we chose values between 20% and 80% in order to represent a wide range of network behaviors. Practitioners can potentially improve these rates by investing in resources such as extra stock, backup suppliers, IT functionality, or emergency planning. Gaining more insights into the relationship between the two rate variables and the network resilience metrics can therefore support more informed decision making with respect to the relative value of the related investments.

Table 4

Experimental Design.

Parameters	Settings
Control Variables	
Network Size	(100, 300, 500)
Disruption Severity	(10%, 30%, 50%, 70%)
Independent Variables	
Network Types	(Scale-free, Small-world, Random)
Average Degree	(2,4,6,8)
Recovery Rate	(20%, 40%, 50%, 80%)
Risk Diffusion Rate	(20%, 40%, 50%, 80%)
Total observations: $3 * 3 * 4 * 4 * 4 * 4 = 2304$	

3.4.1.3. Dependent Variables and Models

As mentioned above, we conduct two analyses: the first is intended to help uncover the relationships between the independent variables and resilience metrics, and the second is to explore the association between the different dimensions of resilience.

For the first analysis, the dependent variables are the output measures within our proposed resilience framework, specifically robustness (initial impact, full impact), recoverability and resilience. For each of the dependent variables, we use an OLS regression model to test the impact of the independent variable on these dependent variables. The output of these regression models is reflected in Models (2)-(5) in Tables 5, 6, and 7.

For the second analysis, we use the overall resilience, as calculated from each of the performance measures, as the unique dependent variable, while adding robustness and recoverability, together with the other variables, into the explanation part of the function. As there are two measures for the robustness, we add each one separately. The results are reflected in Models (6) and (7) in Tables 5-7. The overall resilience, based on our quantitative definition, is a measure of the overall average performance within a certain period. Assuming, for example, that the chosen performance measure is total sales, resilience is thus the normalized average loss of sales across the total number of time periods being considered. In comparison, robustness is the initial level of sales after the disruption (for initial impact robustness), or the minimum level of sales during the disruption (for full impact robustness). Recoverability is the total recovery time needed for the system to return to a completely healthy state. By examining the influences of different levels of both robustness and recoverability on the resilience behavior, we can thus review the interconnections among them.

3.4.2. Data collection and analyses

To generate the data for analysis, we simulate each scenario in Table 3, using NetLogo as the simulation platform. Each observation result is the mean of 30 replications to average out the stochastic effects. For the three types of network, we use the network generation algorithms described in Appendix B.

The total period chosen for resilience calculation is $T^*=50$, which is larger than the maximum recovery time of any of the replications. Although the selection of total period influences the resilience calculation, it does not influence the relative ranking of our testing results since the selected period is larger than the maximum recovery time. To verify this, we compared the results for different total period values of 50, 60, and 100 and reached the same conclusion as below.

We present the OLS regression results for the different performance measures in this section. Tables 5-7 display the results of the number of healthy nodes, the size of LCC, and the size of LCC/average path length of LCC, respectively. All of these analyses are run in STATA Version 14.1.

Table 5

Number of Healthy Nodes.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	Resilience	Initial-Impact	Full-Impact	Recovery-steps	Resilience	Resilience	Resilience
	b/se	b/se	b/se	b/se	b/se	b/se	b/se
Controls							
Num_nodes	0.0000	-0.0000	0.0000	0.0087***	0.0000	0.0000***	0.0000***
	(0.000)	(.)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Disruption_size	-0.0003***	-0.0100	-0.0080***	-0.0175***	-0.0003***	-0.0004***	-0.0000
	(0.000)	(.)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Direct effect							
Scale-free		-0.0000	0.0010	-0.0973	0.0002	-0.0001	-0.0001
		(.)	(0.004)	(0.178)	(0.001)	(0.000)	(0.000)
Small-world		-0.0000	-0.0011	0.0601	-0.0002	0.0000	0.0000
		(.)	(0.004)	(0.178)	(0.001)	(0.000)	(0.000)
Num_neighbors		0.0000	-0.0133***	0.0784*	-0.0012***	-0.0010***	-0.0005***
		(.)	(0.001)	(0.032)	(0.000)	(0.000)	(0.000)
Recovery_rate		-0.0000	0.0032***	-0.3881***	0.0011***	0.0000*	0.0000
		(.)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Riskdiffuse_rate		0.0000	-0.0012***	-0.0074*	-0.0001***	-0.0001***	-0.0000***
		(.)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Robustness and recoverability effect							
Initial-Impact						0.0000	
						(.)	
Full-Impact							0.0416***
							(0.002)
Recovery-steps						-0.0028***	-0.0025***
						(0.000)	(0.000)
Constant	0.9754***	1.0000	0.8133***	30.8560***	0.9280***	1.0158***	0.9720***
	(0.002)	(.)	(0.008)	(0.359)	(0.001)	(0.001)	(0.002)
Number of observations	2304	2304	2304	2304	2304	2304	2304
R-squared	0.05	1.00	0.87	0.87	0.84	0.95	0.96
adjusted R-squared	0.05	1.00	0.87	0.87	0.84	0.95	0.96
F statistic	66.55	.	2242.78	2109.13	1698.13	5947.99	6869.93

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6

Size of the LCC.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	Resilience	Initial-Impact	Full-Impact	Recovery-steps	Resilience	Resilience	Resilience
	b/se	b/se	b/se	b/se	b/se	b/se	b/se
Controls							
Num_nodes	-0.0000***	-0.0001***	-0.0000*	0.0087***	-0.0000***	0.0000***	0.0000***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Disruption_size	-0.0004***	-0.0110***	-0.0084***	-0.0175***	-0.0004***	0.0011***	0.0000
	(0.000)	(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Direct effect							
Scale-free		0.0136**	0.0006	-0.0973	0.0028	0.0005	0.0024*
		(0.005)	(0.006)	(0.178)	(0.001)	(0.001)	(0.001)
Small-world		-0.0183***	-0.0073	0.0601	-0.0050***	-0.0022*	-0.0043***
		(0.005)	(0.006)	(0.178)	(0.001)	(0.001)	(0.001)
Num_neighbors		0.0566***	0.0485***	0.0784*	0.0079***	0.0006	0.0056***
		(0.001)	(0.001)	(0.032)	(0.000)	(0.000)	(0.000)
Recovery_rate		-0.0000	0.0041***	-0.3881***	0.0017***	0.0000	0.0000
		(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Riskdiffuse_rate		-0.0000	-0.0014***	-0.0074*	-0.0001***	-0.0001***	-0.0000
		(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Robustness and recoverability effect							
Initial-Impact						0.1361***	
						(0.004)	
Full-Impact							0.0539***
							(0.004)
Recovery-steps						-0.0043***	-0.0037***
						(0.000)	(0.000)
Constant	0.9640***	0.6500***	0.3512***	30.8560***	0.8457***	0.8891***	0.9401***
	(0.003)	(0.010)	(0.013)	(0.359)	(0.003)	(0.005)	(0.005)
Number of observations	2304	2304	2304	2304	2304	2304	2304
R-squared	0.02	0.89	0.79	0.87	0.70	0.84	0.79
adjusted R-squared	0.02	0.89	0.79	0.87	0.70	0.84	0.79
F statistic	30.33	2641.77	1228.55	2109.13	753.98	1358.71	957.92

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 7

Size of LCC/APL.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	Resilience	Initial-Impact	Full-Impact	Recovery-steps	Resilience	Resilience	Resilience
	b/se	b/se	b/se	b/se	b/se	b/se	b/se
Controls							
Num_nodes	-0.0000***	-0.0001***	-0.0001***	0.0087***	-0.0000***	0.0000***	0.0000***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Disruption_size	-0.0003***	-0.0114***	-0.0081***	-0.0175***	-0.0003***	0.0003***	-0.0003***
	(0.000)	(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Direct effect							
Scale-free		0.0244***	0.0057	-0.0973	0.0037***	0.0017**	0.0032***
		(0.003)	(0.005)	(0.178)	(0.001)	(0.001)	(0.001)
Small-world		0.0086**	0.0213***	0.0601	0.0002	-0.0001	0.0002
		(0.003)	(0.005)	(0.178)	(0.001)	(0.001)	(0.001)
Num_neighbors		0.0271***	0.0170***	0.0784*	0.0040***	0.0026***	0.0041***
		(0.001)	(0.001)	(0.032)	(0.000)	(0.000)	(0.000)
Recovery_rate		0.0000	0.0042***	-0.3881***	0.0017***	0.0000	0.0000
		(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Riskdiffuse_rate		-0.0000	-0.0013***	-0.0074*	-0.0001***	-0.0001***	-0.0001***
		(0.000)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)
Robustness and recoverability effect							
Initial-Impact						0.0653***	
						(0.004)	
Full-Impact							0.0113***
							(0.002)
Recovery-steps						-0.0044***	-0.0042***
						(0.000)	(0.000)
Constant	0.9628***	0.7992***	0.4787***	30.8560***	0.8586***	0.9416***	0.9841***
	(0.003)	(0.006)	(0.011)	(0.359)	(0.002)	(0.004)	(0.003)
Number of observations	2304	2304	2304	2304	2304	2304	2304
R-squared	0.03	0.95	0.81	0.87	0.82	0.94	0.93
adjusted R-squared	0.03	0.95	0.81	0.87	0.82	0.94	0.93
F statistic	2046.21	6025.48	1394.28	2109.13	1474.26	3782.34	3367.10

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the results from Table 5 to Table 7, we summarize the direct impact of independent variables in Table 8.

Table 8

Direct impact of independent variables.

<table>
<tr><td colspan="2" rowspan="2"></td><td rowspan="2"></td><td colspan="2">Robustness</td><td rowspan="2">Recoverability*</td><td rowspan="2">Resilience</td></tr>
<tr><td>Initial Impact</td><td>Full Impact</td></tr>
<tr><td rowspan="9">Network Structure</td><td rowspan="3">Scale-free</td><td>No. healthy nodes</td><td></td><td>No</td><td>No</td><td>No</td></tr>
<tr><td>Size of LCC</td><td>+</td><td>No</td><td>No</td><td>No</td></tr>
<tr><td>Size of LCC/APL</td><td>+</td><td>No</td><td>No</td><td>+</td></tr>
<tr><td rowspan="3">Small-world</td><td>No. healthy nodes</td><td></td><td>No</td><td>No</td><td>No</td></tr>
<tr><td>Size of LCC</td><td>-</td><td>No</td><td>No</td><td>-</td></tr>
<tr><td>Size of LCC/APL</td><td>+</td><td>+</td><td>No</td><td>No</td></tr>
<tr><td rowspan="3">Average degree</td><td>No. healthy nodes</td><td></td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Size of LCC</td><td>+</td><td>+</td><td>-</td><td>+</td></tr>
<tr><td>Size of LCC/APL</td><td>+</td><td>+</td><td>-</td><td>+</td></tr>
<tr><td rowspan="6">Other</td><td rowspan="3">Recovery rate</td><td>No. healthy nodes</td><td></td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Size of LCC</td><td>No</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Size of LCC/APL</td><td>No</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td rowspan="3">Risk-diffuse rate</td><td>No. healthy nodes</td><td></td><td>-</td><td>+</td><td>-</td></tr>
<tr><td>Size of LCC</td><td>No</td><td>-</td><td>+</td><td>-</td></tr>
<tr><td>Size of LCC/APL</td><td>No</td><td>-</td><td>+</td><td>-</td></tr>
</table>

* a positive recoverability means variables negatively influence total recovery time
\+ means there is significant positive relationship
\- means there is significant negative relationship
No means there is no significant relationship
The shaded grid means the situation is not suitable for the association calculation. This is because initial impact is the same as the disruption severity in terms of the number of healthy nodes.

3.4.2.1. Direct Impact of network structure

Obviously from Table 8, the network types mainly influence the robustness at the initial impact, much less so the robustness at full impact and the overall resilience, and they have no impact on recoverability.

The scale-free network, which characteristically has an exponential degree distribution, is the most widely studied network type in the supply chain field (Zhao et al. 2011; Basole and Bellamy 2014a; Nair and Vidal 2011; Kim, Chen, and Linderman 2015). This is because it resembles some realistic networks, for example, the automotive industry network (Basole and Bellamy 2014a) and the case example used in Section 5 of this study. Our analysis reinforces the previous finding that a scale-free network is particularly robust at initial impact, compared with a random network, in terms of measuring the size of LCC and the size of LCC/APL (Thadakamalla et al. 2004; Albet, Jeong, and Barabasi 2000; Zhao et al. 2011).

With the existence of risk diffusion and node recovery, scale-free network behavior becomes more complex and unpredictable. In contrast to Basole and Bellamy's (2014a) statement that supply networks with scale-free characteristics will accelerate risk propagation and result in less favorable network health, our results show that the existence of a scale-free network does not have a significant impact on full impact robustness or on recoverability. This might be because of our differing assumptions about immunity. Basole and Bellamy (2014a) assume that nodes do *not* gain immunity after recovery, and thus that the risk can further propogate to previously recovered nodes. Comparatively, under the assumption of node immunity, although the scale-free network can accelerate the risk diffusion process, the network will gain robustness again once the hub nodes gain immunity and hamper the risk diffusion process afterwards, thus offsetting the initial negative impact.

The small-world network is a type of network in which most interactions are local, and few links exist between a node and another distant node. This is the network type that lies between regular lattice and random network. Watts and Strogatz (1998) showed that a small-world network has a clustering coefficient that is close to that of a regular lattice network, which is much higher than that of a pure random network, while at the same time keeping its average path length similar to that of a random network. These properties make the network easier to navigate (Kleinberg 2000) and synchronize (Barahona and Pecora 2002). The small-world phenomenon has been documented in different real-world settings, including the ownership structure of German firms, academic collaboration networks, firm alliance networks, and electronic industry supply networks (Rivkin and Siggelkow 2007; Basole and Bellamy 2014a; Kim, Chen, and Linderman 2015).

For this type of network, the robustness at the initial impact is different for different measures. Our results are consistent with a previous study that shows that a small-world network has a lower size of LCC compared to that of a random network after disruption (Thadakamalla et al. 2004). However, the small-world type of network has positive robustness of Size of LCC/APL because of the increased level of "small-worldness" after the disruption (Jalili 2011). Small-worldness is a measure of the degree of the small-world pattern by comparing the average path length and clustering coefficient of a random network. This increase in small-worldness means that a small world network tends to have a smaller average path length and a bigger clustering coefficient when more nodes are removed. The small-world network type also does not have a significant impact on recoverability, and we believe that this is for the same reason as with the scale-free network type.

Along with the two different network types, we also consider the average degree of the network with respect to its impact on the resilience-related measures. Average degree describes the total number of links in a network. It represents the connectedness and clustering of the network, and it is a linear function of the total number of links for a given network size: $\boldsymbol{k} = \frac{\mathbf{2}*\boldsymbol{N}\text{um\_}\boldsymbol{links}}{\boldsymbol{Num\_nodes}}$. A higher average degree means more links in a network, and hence more complexity. Our results show that it negatively influences recoverability.

The average degree of the network also influences robustness and resilience differently for various performance measures. For the number of healthy nodes performance measure, the average degree negatively influences robustness and resilience, while for the size of LCC and size of LCC/APL measures, it has a positive relationship with robustness and resilience. Practitioners should be aware of this conflict in network performance, in that investing to improve the network connectivity might lead to more nodes in a network being exposed to disruption risk.

3.4.2.2. Direct Impact of recovery and risk diffusion rate

Both the recovery rate and the risk diffusion rate have significant impacts on the robustness at full impact, as well as on recoverability and resilience, but not on robustness at initial impact. This is because the influence on recovery and risk diffusion is through the risk propagation period.

Recovery rate represents individual nodes' capability to recover from a disruption. In reality, a company or a facility, which is a node in a supply chain network, can increase its recovery rate by having backup suppliers implement techniques such as efficient risk mitigation methods. These activities can decrease loss and improve recovery time locally, and can have a big impact on the network as a whole if many nodes adopt them. Thus, unsurprisingly, our results show that recovery rate is positively associated with robustness at full impact, with recoverability, and with overall resilience.

A company can decrease its risk diffusion rate by having a multi-supplier procurement strategy, increasing stock level to enhance its capability to protect against a disruption, and hence lower the probability of infection. On the contrary, increasing the diffusion rate will make a company suffer bigger losses, which is supported by our results that risk diffusion rate is negatively associated with robustness at full impact.

We also find that risk diffusion rate positively impacts recoverability, in other words, negatively influences the total recovery time. This is because of our assumption of immunity. In the extreme case, if the risk diffusion rate is very high, then all nodes will be disrupted in the second time period, and the following time periods will involve only recovery. Under this situation, the total recovery time is normally shorter than a process that experiences a longer risk propagation period and then recover. Although the risk diffusion rate influences robustness and recoverability differently, its integrated impact on network performance-resilience is positive.

3.4.2.3. Robustness, Recoverability and Resilience

The behavior of a complex system like a supply chain network is nonlinear and unpredictable (Basole and Bellamy 2014a; Choi, Dooley, and Rungtusanatham 2001), since a change of given magnitude of input may not result in a linear corresponding change of output (Choi et al 2001). For example, a severe disruption may be recovered from very quickly, whereas a small initial impact may propagate to the whole system and lead to devastating impacts (Choi, Dooley, and Rungtusanatham 2001). This second phenomenon is called the “butterfly effect” or “cascade effect”. One recent example of the “butterfly effect” in supply chain management is General Mills' recall of nearly 10 million pounds of flour because of possible E. coli contamination (Beach 2016). This nonlinear behavior leads to the question of whether robustness, the ability to withstand a disruption's initial impact on the supply chain network, can predict the performance of resilience, the overall system performance in a certain period.

Although in the conceptual literature both robustness and recoverability are well recognized as aspects of resilience (Pettit, Croxton, and Fiksel 2013; Ponomarov and Holcomb 2009), robustness in particular is widely believed to be an important indicator of resilience and it is extensively used as a direct proxy for resilience in qualitative studies (Zhao et al. 2011; Kim, Chen, and Linderman 2015). Our analysis above supports this practice in that both robustness and recoverability are indeed positively correlated with resilience for all three different performance measures. This result can be used to support a better understanding of the network's general health status when only partial information is given, i.e. in the case of when only robustness or recovery information exists, we can use them as a measure to replace resilience.

We also notice from the results in Table 8 that different measures are explained by different variables. Specifically, the robustness at initial impact is affected by network structure and the initial disruption severity, while the robustness at full impact and the recoverability are not only influenced by initial disruption severity and network structure, but also influenced by recovery rate and risk diffusion rate. The resilience in our measurement framework, which represents the network's integrated capability to against and recover from a disruption, can be explained, at least in part, by robustness and recoverability, together with other control variables.

3.4.3. Practical Implications

3.4.3.1. Implication of network structure

Network structure is the pattern of connections in a network. Network type, network complexity, and network characteristics are all ways to describe the network structure. In this study context, we only focus on network type and network complexity.

Our results show that network type mainly influences robustness at initial impact of a disruption, but not much with respect to robustness at full impact, recoverability and resilience. This means that with the existence of risk diffusion and node recovery, the connection pattern has less control of the network performance later on, hence less influence on robustness at full impact, total recovery time, and the overall resilience. However, there is an exception that the small-world type of network has a negative effect on resilience when measuring the size of LCC, and has a positive effect on robustness at full impact when measuring the size of LCC/APL. We think that this simply implies that network types are too general to study their impact on network resilience. Thus, we propose that **looking at a more detailed level, for example, network characteristics or different combinations of network characteristics, may lead to a more concrete understanding about how network interconnections influence network resilience.**

Network complexity is also an important aspect of network structure. We follow the network complexity definition by Choi and Krause (2006) that it is conceptualized in three dimensions: network size (number of nodes), the in-degree and out-degree of suppliers, and inter-relationships among suppliers. Specifically, network complexity can be measured by the number of nodes and number of links within a given supply chain (Craighead et al. 2007). Our results show that network size has a negative direct effect on robustness, recoverability, and overall resilience. Comparatively, the average degree has a positive impact on robustness and resilience when measuring the size of LCC and the size of LCC/APL, but has a negative impact when measuring number of healthy nodes. This means **in general the influence of network complexity is complex and one needs to be careful when interpreting its influence on network resilience**.

We also need to be aware that **even though the network size has a statistically significant impact on the network resilience metric, this influence is too small to consider practically** by looking at the coefficients. For example, in the case of recoverability, an increase of 100 nodes in network size only increases recovery time by 0.87 steps. Thus, we can conclude that network size does not influence resilience to a large extent, which is consistent with the statement by Albet, Jeong, and Barabasi (2000) that network robustness is independent of the system size. This finding actually allows us to directly compare the performance of systems with different size.

3.4.3.2. Implication of tradeoff between robustness and recoverability

An ideal investment in network resilience would be to increase both robustness and recoverability simultaneously. However, in some cases increasing one of these measures might sacrifice the other. Our results prove that the tradeoff between robustness and recoverability exists. Specifically, increasing the average degree of the network will increase network robustness, but it will also decrease network recoverability in terms of the size of LCC and the size of LCC/APL. Similarly, decreasing the risk diffusion rate will increase network robustness but decrease network recoverability for all three performance measures.

These tradeoffs tell us that **when making an investment decision, practitioners should evaluate its overall effect, hence achieving an integrated acceptable health status.**

3.4.3.3. Implication of tradeoff between different performance measures

This study selects three different performance measures for the purposes of demonstration, each providing a different angle for describing network performance. As the results above demonstrate, different performance measures may provide different results. For example, compared with a random network, a small-world network is no different in terms of robustness when measuring the number of healthy nodes, it is less robust when measuring the size of LCC, and it is more robust when measuring the size of LCC/APL. Also, increasing the average degree in the network will decrease robustness at full impact when measuring the number of healthy nodes, but it will increase robustness when considering the other two performance measures.

Therefore, in future studies on network resilience, **it is important to clearly specify which aspect or aspects of the system are exhibiting the resilient behavior, as different performance measures may lead to different outcomes**. For practitioners, they **not only need to evaluate benefit of one performance measure, but also need to assess the counter effects of other**

performance measures. Systems and networks may be resilient in different ways under different circumstances and the decision to make an investment in improving resilience should be based on a comprehensive understanding of the ways in which the system will actually be impacted by that investment.

3.4.3.4. Implication of resilience framework

Network resilience is a relatively new area of study, especially in the context of quantitative studies. Compared with previous work, the network resilience framework presented above provides a more comprehensive understanding of network resilience in several different aspects, and it helps to fill the literature gap between qualitative studies and quantitative studies.

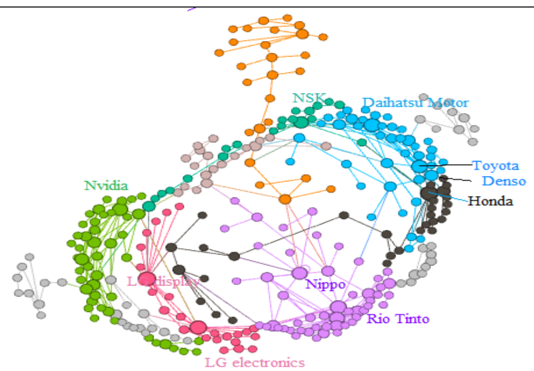
The study of network resilience is also evolving quickly, and we expect this framework to help with building a solid foundation for future work. The framework can be expanded in several ways in the future. To begin with, additional output measures related to robustness, recoverability and resilience can be added, depending on the type of decisions that will be made. For example, the length of time between when the disruption happens and the full impact is realized can also provide an additional measure of recoverability, capturing how quickly the system can start to recover. Another example is that for overall resilience calculation, different time periods could be used to calculate short time resilience, mid-term resilience or long-term resilience. In addition, the framework easily could be expanded by adding additional performance measures, for example, from a practical perspective, it could focus on total sales, total customer satisfaction, etc., as those performance measures change over time after a disruption.

3.5 Case Example – Japanese Auto Industry Network

Our proposed quantitative resilience framework can help supply chain managers grasp the resilience status of their supply chain network in different situations, and hence help them better prepare for recovery after a disruption. In this section, we use a real supply chain network - the Japanese auto supply chain network – to demonstrate the use of the resilience framework. The auto industry is one of the most popular supply chains studied in the supply chain risk management field, as it is exposed to a variety of risks, and supply chain management is one of the core elements influencing its success (Xia and Tang 2011). Current studies look into the structure of the auto industry and its relationship with supply chain performance (Bode and Wagner 2015; Kim et al.

2011). However, none of them shows a complete picture of the supply network and provide a comprehensive network risk analysis.

We construct a model of the Japanese Auto supply network using the Bloomberg SPLC database, based on the theory that the supply chain is bounded by the visible horizon of the focal agents (Carter, Rogers, and Choi 2015). We select Honda and Toyota as the focal firms because these two are the largest auto makers in Japan, occupying global market shares of 11.6% and 5.9%, respectively, as of August 2014 (Statista 2014). Then we derive the first tier and second tier suppliers of these two focal firms. Among each of these suppliers and connections, we select only COGS (Cost Of Goods Sold) relationships where the percentage of COGS is over 1%, in order to get the most significant material flows. This gives us a network with 302 nodes and 404 links. Figure 8 illustrates the detail of this network, using Gephi (Bastian, Heymann, and Jacomy 2009) as the visualization tool.



Parameters of this network

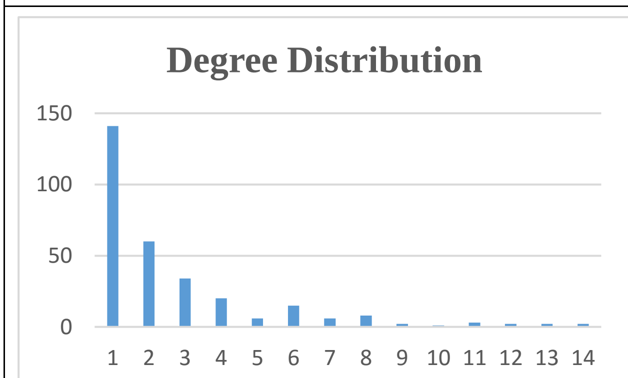
No. Nodes: 302

No. Links: 404

Average path length: 7.1731

Mean clustering coefficient: 0.02

Average degree: 2.675



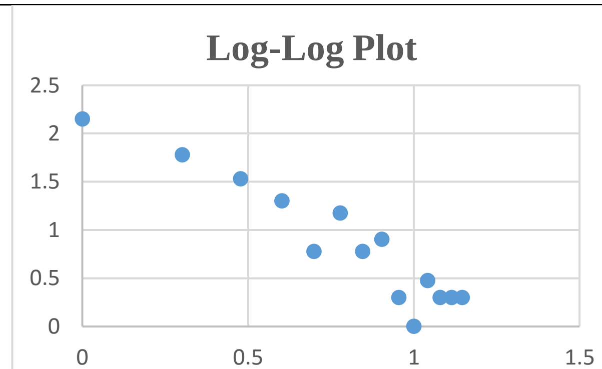


Fig. 8. Japanese Auto Industry Network.

Based on the network characteristics, especially the log-log plot, this is more or less a scale-free type of network, which is consistent with the findings of Basole and Bellamy (2014a) from using the SDC Platinum database.

We use our resilience framework to understand the behavior of this specific network and to evaluate its health status across different disruption levels (specifically, from 5% to 60% with all disruptions impacting nodes randomly). We set the recovery rate at 5% and the risk diffusion rate to 10% in order to simulate a quick risk diffusion process, similar to how the 2012 Japan earthquake and tsunami impacted the Japanese auto industry. The actual settings for the recovery rate and the risk diffusion rate are somewhat arbitrary, as both rates are tightly connected with the length of time represented by a single period in the model. For example, if one period represents a week, then the recovery rate is 5%; and if it represents one month, the recovery rate will be approximately 20%. Hence, the difference between these rates is more important than their absolute values.

Below are the detailed analyses of the different output measures, where each data point is the average of 100 replications.

3.5.1. Robustness

We display the robustness of initial impact and full impact, respectively, in Figure 6. As expected, both the robustness at initial impact and that at full impact are decreasing with the disruption severity. However, the influence of disruption severity is more significant at the initial impact than at the full impact, as the robustness at full impact decreases more slowly, especially when we measure the size of LCC and size of LCC/APL. This tells us that compared to at the initial impact, robustness at full impact fluctuates less and we can use the simulated data (or historical record) to more accurately estimate the full impact of a disruption. In our example, the robustness at full impact lies within a small range from 0.12 to 0.10 for disruptions that range from 15% to 50% for the size of LCC performance measure. This means that the size of LCC ranges from 36 to 30.

With the increase of disruption severity, the gap between the robustness at initial impact and that at full impact is also decreasing. For example, when the disruption severity is 5%, the robustness at initial impact is 95% and the robustness at full impact is 69.9% in terms of the count of healthy nodes. Comparatively, when the disruption severity is at 40%, the two robustness values are 40% and 35.5%, respectively. This tells us that in the case of quick risk diffusion, it is better for the supply chain manager to prepare for the worst-case situation, especially when the disruption severity is small.

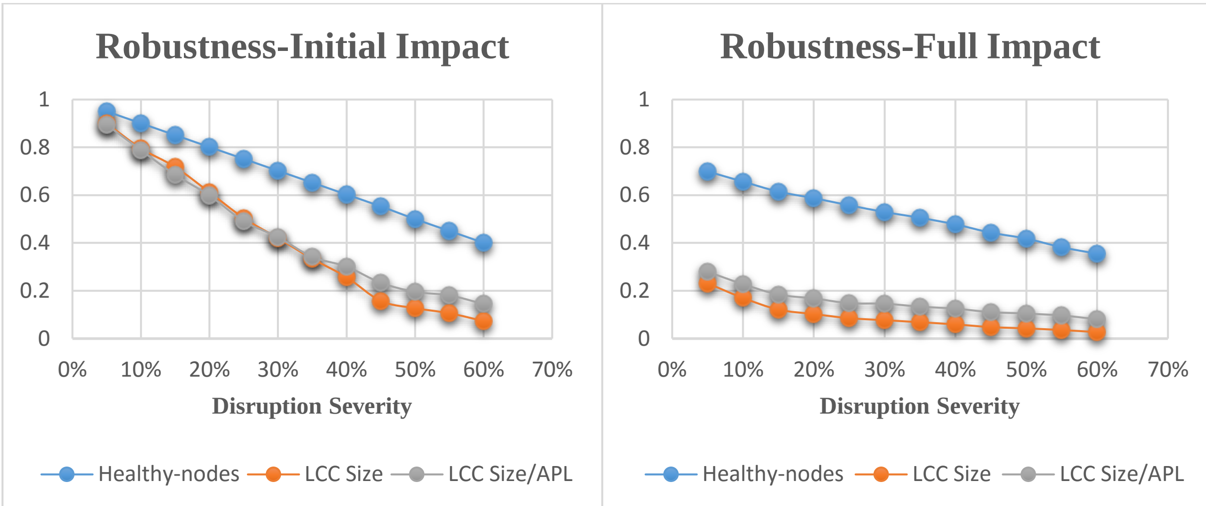


Fig. 9. Robustness of the Japanese auto network.

3.5.2. Recoverability

To assess recoverability, we create the plot of the total recovery period, along with the plot of the full impact period. The total recovery period displays the total periods need for a full recovery, while the full impact period illustrates the time until the full impact is realized, which is also the point at which the network system starts to recover. Properly estimating the full impact period can allow practitioners to understand the trend of the disruption, and hence help them to prepare for the worst situation and the recovery.

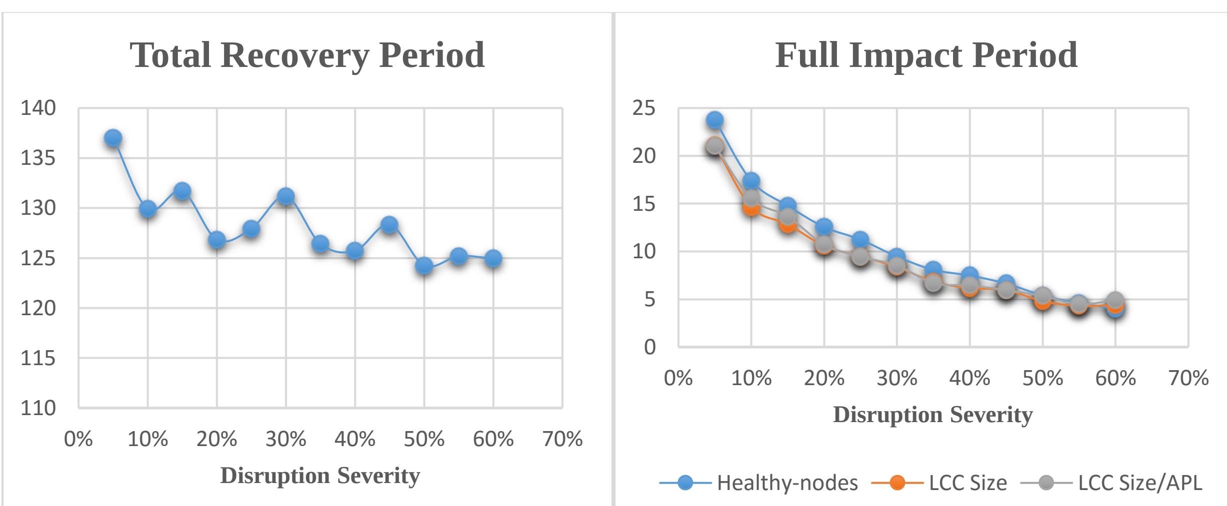


Fig. 10. Recoverability of the Japanese auto network.

Although the trend of the total recovery period is decreasing with fluctuations, the range of a full recovery is from 124 to 131 periods for a disruption severity from 10% to 60%, which only has a difference of 7 periods. This means that in a quick risk diffusion situation, the difference between total recovery periods is relatively small. This therefore supports companies in making a more accurate estimate of the business impact of a disruption.

The trend of the full impact period is monotonically decreasing with the disruption severity, which means that a small scale disruption normally has a longer risk diffusion time than does a larger disruption. The plot in Figure 10 also shows that the impact in the healthy nodes case is higher than that for size of LCC. This tells us that the most severe situation in the connection-focused measures (size of LCC, and size of LCC/APL) generally happens a little earlier than the in the case of measuring the total number of healthy nodes.

3.5.3. Resilience

We calculate the overall resilience at period 20 (resilience-20) and at period 150 (resilience-150) to illustrate network behavior in both the short term and the long term. Each measure represents the average performance (i.e., the remaining functionality) of the network during the given time period.

As illustrated in Figure 11, the value for resilience-20 is clearly decreasing with disruption severity, which means that the disruption severity influences the short term network performance more obviously than it does the long term performance. In contrast, the value for resilience-150 changes very little across the different disruption severity levels, although it does decrease very slightly along with the disruption severity. This is still significant, however, since a minor change in resilience may correspond to a significant financial loss in reality. For example, Toyota ranked No. 9 in the 2014 Fortune 500 list, with revenues of $256 billion and profits of $18 billion. Even a slight improvement in resilience indicates improved performance after a disruption, and this can have a significant impact on a company's revenues.

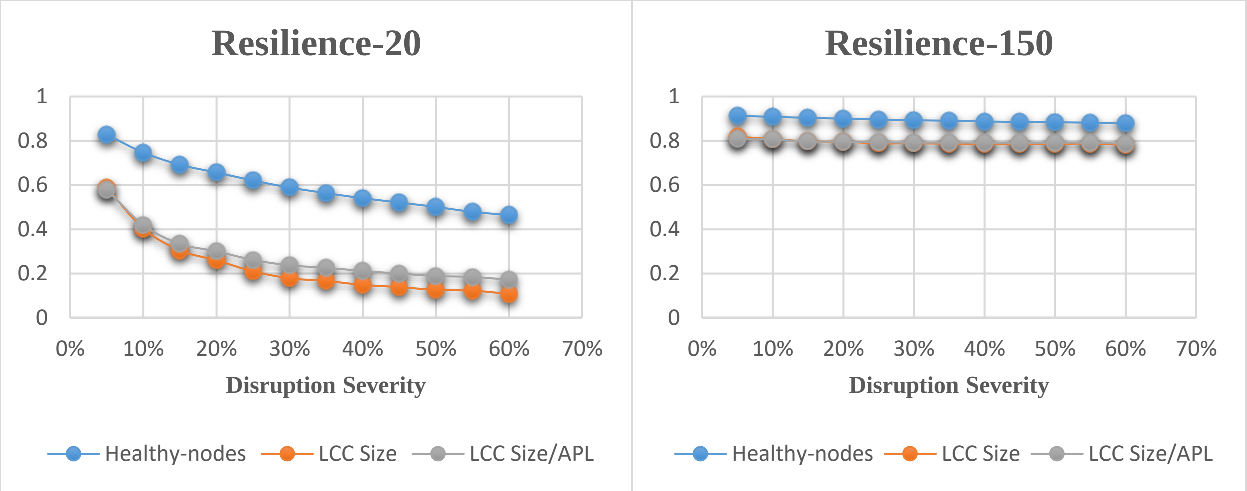


Fig. 11. Resilience of the Japanese auto network.

3.6 Conclusion

In this study, we have proposed an analytical framework to quantify supply chain network resilience in the presence of risk diffusion. This framework adopts a multi-dimensional view of resilience by measuring overall resilience as well as robustness and recoverability, based on various performance measures. Through a series of in-depth analyses, we have shown how different factors influence the proposed resilience metrics, and we have discussed important practical implications. We also have provided a case study to show how this framework can help practitioners better understand their own supply chain network, and hence how it can support related decision making efforts. We hope that this work will provide a solid basis for measuring, understanding, and improving network resilience moving forward.

References

Albet, R, N Jeong, and A L Barabasi. 2000. “Error and Attack Tolerance of Complex Networks (vol 406, Pg 378, 2000).” *Nature* 406 (6794): 378–82.

Barahona, Mauricio, and Louis M. Pecora. 2002. “Synchronization in Small-World Systems.” *Physical Review Letters* 89 (5): 054101. doi:10.1103/PhysRevLett.89.054101.

Basole, Rahul C, and Marcus A Bellamy. 2014a. “Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach.” *Decision Sciences* 45 (4): 1–49.

Basole, Rahul C., and Marcus A. Bellamy. 2014b. “Visual Analysis of Supply Network Risks: Insights from the Electronics Industry.” *Decision Support Systems* 67: 109–20. doi:10.1016/j.dss.2014.08.008.

Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy. 2009. “Gephi: An Open Source Software for Exploring and Manipulating Networks.” *Third International AAAI Conference on Weblogs and Social Media*, 361–62. doi:10.1136/qshc.2004.010033.

Battiston, Stefano, Domenico Delli Gatti, Mauro Gallegati, Bruce Greenwald, and Joseph E. Stiglitz. 2007. “Credit Chains and Bankruptcy Propagation in Production Networks.” *Journal of Economic Dynamics and Control* 31 (6): 2061–84.

Beach, Coral. 2016. “UPDATED: General Mills Recalls Flour because of E. Coli Outbreak.” *Food Safety News*, May 31. http://www.foodsafetynews.com/2016/05/general-mills-recalls-flour-because-of-e-coli-20-state-outbreak/#.V3bSCpErLct.

Blackhurst, J., C. W. Craighead, D. Elkins, and R. B. Handfield. 2005. “An Empirically Derived Agenda of Critical Research Issues for Managing Supply-Chain Disruptions.” *International Journal of Production Research*.

Bode, Christoph, and Stephan M. Wagner. 2015. “Dimensions of Supply Chain Complexity and Their Effects on the Frequency of Supply Chain Disruptions.” *Journal of Operations Management* 36. Elsevier B.V.: 215–28.

Business Continuity Institute. 2013. “Supply Chain Resilience 2013 Annual Survey.” http://www.zurich.com/internet/main/sitecollectiondocuments/insight/Supply-Chain-Resilience-2013.pdf.

Carter, Craig R., Dale S. Rogers, and Thomas Y. Choi. 2015. “Toward the Theory of the Supply Chain.” *Journal of Supply Chain Management* 51 (2): 89–97. doi:10.1111/jscm.12073.

Choi, Thomas Y., Kevin J. Dooley, and Manus Rungtusanatham. 2001. “Supply Networks and Complex Adaptive Systems: Control versus Emergence.” *Journal of Operations Management* 19 (3): 351–66.

Choi, Thomas Y., and Daniel R. Krause. 2006. “The Supply Base and Its Complexity: Implications for Transaction Costs, Risks, Responsiveness, and Innovation.” *Journal of Operations Management* 24

(5): 637–52. doi:10.1016/j.jom.2005.07.002.

Christopher, Martin, and Helen Peck. 2004. “Building the Resilient Supply Chain.” 15 (2): 1–13.

Craighead, Christopher W., Jennifer Blackhurst, M. Johnny Rungtusanatham, and Robert B. Handfield. 2007. “The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities.” *Decision Sciences* 38: 131–56.

Eskandarpour, Majid, Pierre Dejax, Joe Miemczyk, and Olivier Péton. 2015. “Sustainable Supply Chain Network Design: An Optimization-Oriented Review.” *Omega* 54: 11–32.

Fahimnia, Behnam, Christopher S. Tang, Hoda Davarzani, and Joseph Sarkis. 2015. “Quantitative Models for Managing Supply Chain Risks: A Review.” *European Journal of Operational Research* 247 (1). Elsevier Ltd.: 1–15.

Falasca, Mauro, Christopher W Zobel, and Deborah Cook. 2008. “A Decision Support Framework to Assess Supply Chain Resilience.” In *Framework,* Proceeding:596–605.

Gai, P., and S. Kapadia. 2010. “Contagion in Financial Networks.” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* 466 (2120): 2401.

Hertzel, M, Z Li, M Officer, and K Rodgers. 2008. “Inter-Firm Linkages and the Wealth Effects of Financial Distress along the Supply Chain.” *Journal of Financial Economics* 87 (2): 374–87.

Ivanov, D.a, B.b Sokolov, and A.c Dolgui. 2014. “The Ripple Effect in Supply Chains: Trade-off ‘Efficiency-Flexibility- Resilience’ in Disruption Management.” *International Journal of Production Research* 52 (7): 2154–72.

Jalili, Mahdi. 2011. “Error and Attack Tolerance of Small-Worldness in Complex Networks.” *Journal of Informetrics* 5 (3): 422–30. doi:10.1016/j.joi.2011.03.002.

Jüttner, U, and S Maklan. 2011. “Supply Chain Resilience in the Global Financial Crisis: An Empirical Study.” *Supply Chain Management* 16 (4): 246–59.

Kim, Yusoon, Yi-Su Chen, and Kevin Linderman. 2015. “Supply Network Disruption and Resilience: A Network Structural Perspective.” *Journal of Operations Management* 33-34: 43–59.

Kim, Yusoon, Thomas Y. Choi, Tingting Yan, and Kevin Dooley. 2011. “Structural Investigation of Supply Networks: A Social Network Analysis Approach.” *Journal of Operations Management* 29 (3): 194–211. doi:10.1016/j.jom.2010.11.001.

Kleinberg, Jon M. 2000. “Navigation in a Small World.” *Nature* 406 (6798): 845. doi:10.1038/35022643.

Kleindorfer, Paul R., and Germaine H. Saad. 2005. “Managing Disruption Risks in Supply Chains.” *Production and Operations Management* 14 (1): 53–68.

Koh, S C L, A Gunasekaran, and C S Tseng. 2012. “Cross-Tier Ripple and Indirect Effects of Directives WEEE and RoHS on Greening a Supply Chain.” *International Journal of Production Economics* 140 (1): 305–17.

Landwehr, Peter M., and Kathleen M. Carley. 2014. "Social Media in Disaster Response." In *Data Mining and Knowledge Discovery for Big Data*, 225–57. Springer Berlin Heidelberg.

Nagurney, Anna. 2010. "Optimal Supply Chain Network Design and Redesign at Minimal Total Cost and with Demand Satisfaction." In *International Journal of Production Economics*, 128:200–208.

Nair, Anand, and José M. Vidal. 2011. "Supply Network Topology and Robustness against Disruptions – an Investigation Using Multi-Agent Model." *International Journal of Production Research*.

Oke, Adegoke, and Mohan Gopalakrishnan. 2009. "Managing Disruptions in Supply Chains: A Case Study of a Retail Supply Chain." *International Journal of Production Economics* 118: 168–74.

P&G News. 2015. "P&G Recognizes Top Performing Global Partners." http://news.pg.com/press-release/pg-corporate-announcements/pg-recognizes-top-performing-global-partners-0.

Pettit, Timothy J, Joseph Fiksel, and Keely L Croxton. 2010. "Ensuring Supply Chain Resilience: Development of a Conceptual Framework." *Journal of Business Logistics* 31 (1): 1–21.

Pettit, Timothy J., Keely L. Croxton, and Joseph Fiksel. 2013. "Ensuring Supply Chain Resilience: Development and Implementation of an Assessment Tool." *Journal of Business Logistics* 34 (1): 46–76.

Ponomarov, Serhiy Y., and Mary C. Holcomb. 2009. "Understanding the Concept of Supply Chain Resilience." *The International Journal of Logistics Management*.

Rivkin, Jan W., and Nicolaj Siggelkow. 2007. "Patterned Interactions in Complex Systems: Implications for Exploration." *Management Science* 53 (7): 1068–85. doi:10.1287/mnsc.1060.0626.

Sheffi, Yossi, and James B Rice Jr. 2005. "A Supply Chain View of the Resilient Enterprise." *MIT Sloan Management Review* 47 (1): 41–48.

Snyder, Lawrence V, and Burcu Atan, Zumbul; Peng, Peng; Rong, Ying; Schmitt, Amanda J; Sinsoysal. 2012. "OR / MS Models for Supply Chain Disruptions : A Review."

Statista. 2014. "Global Market Share of the World's Largest Automobile OEMs as of August 30, 2014." *Statista.com*. http://www.statista.com/statistics/316786/global-market-share-of-the-leading-automakers/.

Tang, Christopher. 2006. "Robust Strategies for Mitigating Supply Chain Disruptions." *International Journal of Logistics* 9: 33–45.

Thadakamalla, Hari Prasad, Usha Nandini Raghavan, Soundar Kumara, and Réka Albert. 2004. "Survivability of Multiagent-Based Supply Networks: A Topological Perspective." *IEEE Intelligent Systems* 19 (5): 24–31.

Tierney, Kathleen, and Michel Bruneau. 2007. *Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction*. *TR News*.

Tomlin, Brian. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply

Chain Disruption Risks." *Management Science*.

Tomlin, Brian T, and Lawrence V Snyder. 2006. "On the Value of a Threat Advisory System for Managing Supply Chain Disruptions."

Vugrin, Eric D., Drake E. Warren, and Mark A. Ehlen. 2011. "A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane." *Process Safety Progress* 30 (3): 280–90. doi:10.1002/prs.10437.

Wagner, Stephan M., and Christoph Bode. 2006. "An Empirical Investigation into Supply Chain Vulnerability." *Journal of Purchasing and Supply Management* 12 (6): 301–12.

Wang, Fan, Xiaofan Lai, and Ning Shi. 2011. "A Multi-Objective Optimization for Green Supply Chain Network Design." *Decision Support Systems* 51 (2): 262–69.

Watts, Duncan J., and Steven H. Strogatz. 1998. "Collective Dynamics of 'small-World' Networks." *Nature* 393 (6684): 440–42. doi:10.1038/30918.

Wilensky, U. 1999. "NetLogo." *Center for Connected Learning and ComputerBased Modeling Northwestern University Evanston IL*. http://ccl.northwestern.edu/netlogo/.

Xia, Yu, and Thomas Li-Ping Tang. 2011. "Sustainability in Supply Chain Management: Suggestions for the Auto Industry." *Management Decision* 49 (4): 495–512. doi:10.1108/00251741111126459.

Zhao, Kang, Akhil Kumar, Terry P. Harrison, and John Yen. 2011. "Analyzing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions." *IEEE Systems Journal*.

Zhao, Kang, Akhil Kumar, and John Yen. 2011. "Achieving High Robustness in Supply Distribution Networks by Rewiring." *IEEE Transactions on Engineering Management* 58 (2): 347–62.

Zobel, Christopher W. 2011. "Representing Perceived Tradeoffs in Defining Disaster Resilience." *Decision Support Systems* 50 (2): 394–403.

———. 2014. "Quantitatively Representing Nonlinear Disaster Recovery." *Decision Sciences* 45 (6): 1053–82.

Zobel, Christopher W., and Lara Khansa. 2012. "Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks." *Decision Sciences* 43 (4): 687–710.

———. 2014. "Characterizing Multi-Event Disaster Resilience." *Computers and Operations Research* 42: 83–94.

Appendix B: Network Generation Algorithm

Scale-free Network

We use preferential attachment model to build the scale-free network. The model starts with (m+1) nodes in the initial fully connected network, at every time step a new node is introduced, and connects with (m/2) of the already existing nodes with a probability that is proportional to the number of links that the existing nodes already have. This method can generate a fully connected scale-free network with n nodes and m average degree (or average number of neighbors).

$$average\ degree = \frac{2 * \#\ of\ links}{\#\ of\ nodes}$$

$$\#\ of\ links = 0.5 * n * m$$

Small World network

We use the Watts-Strogatz model to generate a full connected small world network. We first construct a regular ring lattice network with n nodes, each node is connected to m/2 nearest neighbors. Thus, we have a regular network with n nodes and nm/2 edges. For each edge, rewire one node with a certain rewire probability and the new edge cannot duplicate and self-looped. After rewire each edge, we get a small world network. In our example, we use the rewire probability equals to 0.5.

Random network

To generate a fully connected random network, we start with 2 initial connected nodes, then at each time step introduce a new node, which connects with an already existing nodes with equal probability. At this stage, we get a network with n nodes and (n-1) edges. Then we randomly select two nodes and connect them if no link exists between them. We repeat this process until the total number of links is equal to nm/2. Finally, we have a fully connected random network with n nodes and nm/2 edges.

Chapter 4: Network Characteristics and Supply Chain Disruption Resilience

4.1 Introduction

Supply Chains are complex networks of firms that are engaged in material and service exchange activities. Together with industry globalization and regional specialization, supply chain networks are becoming more complex and thus more vulnerable to disruptions (Bode and Wagner, 2015).

Supply chain resilience is a holistic measure of supply chain health (Pettit, Fiksel, and Croxton 2010; Ponomarov and Holcomb 2009), and the interest in it is accelerating in this background. Compared with traditional supply chain risk management that focuses on risk control, supply chain resilience emphasizes the supply chain's adaptability, flexibility and recoverability against disruptions, which is based on the idea that not all disruptions are avoidable (Pettit, Croxton, and Fiksel, 2013; Ponomarov & Holcomb, 2009, Marchese & Paramasivam, 2013). In this sense, a supply chain should not only be able to reduce disruption risks but also be well prepared to quickly respond and recover from disruptions.

Network structure is well recognized as an important determinant of supply chain health, hence it is an important strategic factor in managing disruptions (Snyder et al., 2012). Network structure influences supply chain health in two different ways. One way is to influence the network tolerance against disruptions. The network flow changes immediately as nodes and arcs are disrupted, and certain types of network perform better than others. For example, Thadakamalla et al. (2004) and Zhao et al. (2011) show that a scale free network has better performance against random disruptions. The other way that network structure influences supply chain health is in its effect on network recoverability. A disruption at one node in a supply chain network can spread to other nodes in the same network, hence the network structure affects the network recoverability through influencing the risk diffusion process. Basole & Bellamy (2014) prove that scale free networks accelerate risk propagation, thus resulting in a less favorable network health status.

Current research on network structure against disruptions has been performed by primarily considering the network type. The most frequently studied network types are scale free network, small world network and random network (Basole and Bellamy, 2014; Kim et al., 2015; Nair and Vidal, 2011; Zhao et al., 2011). Although such studies provide valuable insights, using network types as the research objects has its limitations by nature. This is because this approach ignores that many real supply chain networks do not belong to a certain type of network, and it fails to provide a prescription for improving the network structure because a single company in a complex supply network almost has no power to change the whole network type.

To address these limitations, therefore, this current study focuses instead on network characteristics. A network characteristic describes one particular facet of the network structure. For example, the clustering coefficient measures the degree to which nodes in a network tend to cluster together, and the average path length depicts the average of the shortest path length between any pair of nodes. A certain type of network can always be described by a group of network characteristics. In this sense, we believe that the set of network characteristics as a whole can describe a realistic supply network better than the network type can. Furthermore, one company in a complex network, although it has no control over the network type, is able to change the supply network characteristics to some extent through activities like selecting suppliers, decisions about self-production or outsourcing, and managing suppliers' relationship.

In this study, we want to investigate the relationships between network characteristics and supply chain resilience. Specifically, we expect to answer the questions below:

- Can network characteristics provide a better understanding of supply chain resilience than network types can?
- Among all network characteristics, which characteristics are the key influential factors that determine supply chain network resilience?
- How do these key influential characteristics affect the supply chain resilience?
- How can understanding these effects support more effective decision making?

In summary, this study is expected to enrich the limited research on network characteristics and supply chain resilience, and to provide an easy tool to understand supply chain resilience and to support decision making.

4.2 Background

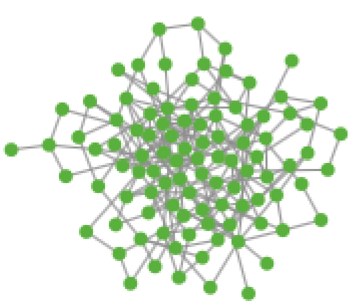
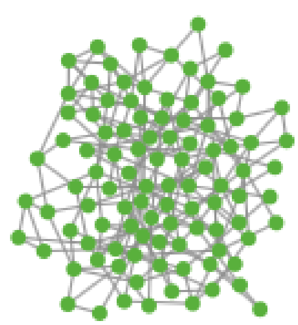
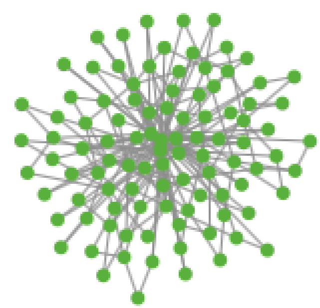
4.2.1 Network types and Network characteristics

Supply chain network structure has been extensively studied with respect to its performance against disruptions. Traditional approaches follow an optimization framework in which decision makers choose nodes and edges to construct a network in order to maximize supply chain performance (Snyder et al., 2012). With supply chain networks becoming more complex and dynamic, however, researchers have begun to study high level questions about how network structure influences the supply chain performance against disruptions (Basole and Bellamy, 2014; Kim et al., 2015; Nair and Vidal, 2011; Zhao et al., 2011).

The network type and network characteristics are two common ways to describe the structure of a network. In graph theory, network types are simple categorizations of complex networks that possess certain characteristics and can be described mathematically. Different from network types, network characteristics only describe one aspect of the network. For example, the degree distribution of a network is the probability distribution of the nodes' degrees, and average path length is the average distance between any pair of nodes.

Obviously, we can describe a certain network type by a group of network characteristics, and Table 1 thus shows examples of network types and their corresponding network characteristics. All three networks are generated using NetLogo (Wilensky, 1999). To compare different network types, the network examples we generated have the same number of nodes and links. In Table 1, we focus on a subset of five specific network characteristics to illustrate their relationships.

Table 1: Network type vs. network characteristics.

Network Type	Random network 	Small-world network 	Scale free network 
Network Characteristics	No. of nodes: 100 Max degree: 10 Average degree: 4 Average path length: 3.416 Average clustering coefficient: 0.0413	No. of nodes: 100 Max degree: 8 Average degree: 4 Average path length: 3.53 Average clustering coefficient: 0.065	No. of nodes: 100 Max degree: 27 Average degree: 4 Average path length: 2.90 Average clustering coefficient: 0.194

Studying network types has practical importance. In the supply chain risk management field, the most commonly studied network types are scale free network, small world network and random network (Basole and Bellamy, 2014; Kim et al., 2015; Nair and Vidal, 2011; Zhao et al., 2011). A scale free network has a power-law degree distribution, and is characterized by many nodes with only a few links and a few nodes with a large number of links. These highly connected nodes are known as hubs. A small world network has the property that most nodes are not neighbors of one another, and yet most nodes can be reached from other nodes by a small number of steps. Meanwhile, a random network serves as a benchmark to compare the performance of other network types. Basole & Bellamy (2014) show that the electronics industry supply network is more of a small world type, and the automotive industry supply network is more of a scale free type through comparing real supply networks and simulated networks.

Using network types as the research objects, however, also has its limitations by nature. First of all, many real supply chain networks do not belong to a certain type, thus taking this approach restricts any analysis only to networks with certain types. Second, this approach might fail to provide a realistic prescription for improving the network structure. This is because in a complex supply network, one node, which represents one company, almost has no power to change the whole network type.

With this in mind, therefore, we want to examine how network characteristics, especially the combinations of characteristics, influence supply chain resilience. We expect to contribute the following aspects. Firstly, this study will fill the current literature gap that only Nair & Vidal (2011) has studied the influence of network characteristics, although they only focus on several network characteristics. Secondly, the combinations of network characteristics can better describe a real supply chain network than can network types, especially a special network that doesn’t belong to any specific type. Thus, results of this study can adapt to more general situations. Thirdly, comparatively, the results of studying network characteristics can apply to the real world more easily. Although one company has limited control over the network type, it can change its local supply network characteristics to some extent through activities like selecting suppliers, decisions on self-production or outsourcing and managing suppliers’ relationships.

4.2.2 Supply Chain Resilience

Supply chain resilience is the performance measure used in this study. Although there is no generally acknowledged definition of supply chain resilience, it is well accepted that robustness and recoverability (Tierney and Bruneau, 2007; Zobel and Khansa, 2012; Zobel, 2011, 2014) are two of the most important aspects of resilience. Robustness measures a system's ability to withstand a disaster and recoverability measures a system's recovery speed after a disruption happens. Supply chain resilience can be measured at different levels, i.e. at the firm level, at the supply chain network level, at the industry level, or at the entire economy level (Wagner and Neshat, 2010). We will focus on network level supply chain resilience in this study.

Current quantitative research on supply chain network topologies and supply chain resilience tends to focus either on network robustness (Kim, Chen, & Linderman, 2015; Nair & Vidal, 2011; Thadakamalla et al., 2004; Zhao et al., 2011), or on network recoverability (Basole and Bellamy, 2014). These existing studies provide important insights on how network structure influences supply chain resilience. Interestingly, these results also show that there can be trade-offs between robustness and recoverability. For example, in terms of random disruptions, although a scale-free network is especially robust (Kim et al., 2015; Nair & Vidal, 2011; Zhao et al., 2011), Basole & Bellamy (2014) also show that scale-free networks accelerate risk propagation in the network and thus can result in less favorable network health over time.

To investigate the relationships between network characteristics and supply chain resilience, we conduct an experimental design in the following section, following the work in Chapter 2, in which the resilience measurement approach that we use considers both the network robustness and network recoverability.

4.3 Experimental Design

We take a quantitative approach to investigating the relationships between network characteristics and supply chain resilience. To begin, we generate a large number of various networks and calculate their network characteristics. Then we simulate a disruption process and calculate network resilience measures for each network, and thus for each set of corresponding characteristics. We then combine the data of network characteristics and network resilience measures and analyze them to examine the relationships between network characteristics and resilience measures.

In the next section, we explain in detail the rule for generating the different networks, and discuss the approaches for deriving the network characteristics and calculating the disruption resilience measures.

4.3.1 Network Sample Rule

As the basis for our analysis, we focus on small-world, scale-free, regular, and random networks because they are the most extensively studied network types in business organizations (Basole and Bellamy, 2014; Rivkin and Siggelkow, 2007). Since a real supply chain network may not belong to any specific network type, however, and may indeed have characteristics from different network types, we also create hybrid networks by combining the scale-free type and other network types to get a large range of different network types.

For each specific network type that we create, we randomly generate 50 different sample networks. These networks have same network size, 250 nodes, which is determined as a balance of representing real networks and for computational convenience. The set of average degree settings for the random, lattice, small-world and scale-free networks is {2, 4, 6, 8}, and the set of average degree settings for hybrid networks is {4, 6, 8}, since we are unable to generate a connected hybrid network when the average degree is too small. In total, our sample of networks includes 1750 different network instances. Table 2 shows the detail of the network samples.

We use the Python Networkx package (Hagberg et al., 2008) to create the set of networks. All generated networks are connected, because a supply chain network is functional only if it is connected. The hybrid network creation process is as follows: To begin, we create two different types of network with same number of nodes and links. We then create a network with same number of nodes and randomly select r percent links from one network, and (1-r) percent links from the other network. Next, we check to see if the new network is connected. If the network is connected, we report this as the hybrid network; if not, we repeat step 2 until we find a connected network. In our case, we set the hybrid ratio r=50%.

Table 2: Network Sample

Network Type	Samples	Parameter configuration
Random	50 * 4	Average degree = 2, 4, 6, 8
Small-world	150 *4	p=0.25, 0.5, 0.75 (rewire probability) Average degree = 2, 4, 6, 8
Scale-free	50 *4	Average degree = 2, 4, 6, 8
Hybrid-Random/Scale-free	50 *3	r=0.5 (hybrid ratio) Average degree = 4, 6, 8
Hybrid-Lattice/Scale-free	50 *3	r=0.5 (hybrid ratio) Average degree = 4, 6, 8
Hybrid-SmallWorld(0.25)/Scale-free	50 *3	r=0.5 (hybrid ratio); p=0.25; Average degree = 4, 6, 8
Hybrid-SmallWorld(0.50)/Scale-free	50 *3	r=0.5 (hybrid ratio); p=0.5; Average degree = 4, 6, 8
Hybrid-SmallWorld(0.75)/Scale-free	50 *3	r=0.5 (hybrid ratio); p=0.75; Average degree = 4, 6, 8

4.3.2 Network Characteristics

To calculate the network characteristics for each created network instance, we consider 32 network characteristic metrics that are widely used in the social and physical sciences. These network characteristics are selected from the eight different perspectives of network centralization. The concept of centrality is based at the node level, and captures the extent to which the overall connectedness is organized around a particular node in a network. To capture the network level characteristics, we choose the min, max, mean and standard deviation of the set of individual node centrality measures to describe the network level features (Airoldi et al., 2011). We select these eight centrality measures because the network level characteristics represented by them cover all commonly used network characteristics. For example, mean of degree centrality is equivalent to average degree, mean of betweenness centrality is equivalent to average path length, and maximum of eccentricity is the network diameter, etc. To eliminate the influence of network size, all our calculations of characteristics are normalized by network size. Below is the detailed description of these characteristics.

3.2.1 Degree Centrality

Degree centrality (Freeman, 1978) measures the number of direct neighbors a node has. The degree centrality $\mathrm{DC}(v_i)$ of a node v_i in a unidirectional network thus is defined as $\mathrm{DC}(v_i) = \sum_{i \neq j} e_{ij}$, where e_{ij} is binary, and $e_{ij} = 1$ if there is a link between node v_i and node v_j and $e_{ij} = 0$

otherwise. In a supply chain network, a node with high degree centrality normally plays an important role in material distribution, thus disruption in this node will significantly impact the network performance. Comparatively, disruption in a node with low degree centrality has a minor effect on the network.

To account for the influence of network size, degree centrality is normalized by dividing by the maximum possible degree (n-1), where n is the number of nodes in the network. The normalized degree centrality is thus: $\mathrm{DC}'(v_i) = \frac{\mathrm{DC}(v_i)}{n-1}$.

Degree centrality is calculated from the node perspective. To capture the corresponding network level characteristics, we use four different degree centrality measures: Min(DC), Max(DC), Mean(DC), and Std(DC). Min(DC) is the minimum degree centrality across all nodes in the network. Since the network is connected, $Min(\mathrm{DC}) \geq 1$. Max(DC) is the maximum degree centrality across all nodes in the network, which represents the largest number of direct neighbors that a node has. $Mean(\mathrm{DC})$ is the average degree of the network, which describes the overall connectiveness of the network. The network is more connected with higher $Mean(\mathrm{DC})$. $Std(\mathrm{DC})$ is the standard deviation of the degree centrality across all nodes in the network. Bigger $Std(\mathrm{DC})$ means that nodes' centrality has a lot of variability. For example, a scale-free network normally has a bigger $Std(\mathrm{DC})$ than does a small-world network.

3.2.2 Betweenness Centrality

Betweenness centrality (Freeman, 1978) measures the extent to which a node lies on geodesic paths between other nodes. A geodesic path is the shortest path through a network between two vertices. In a supply chain network, a node with higher betweenness centrality is considered to have more control over the material passing through. Thus, if a disruption happens in such a node, the network will be greatly influenced. Mathematically, if t_{jk} is the total number of shortest paths between node v_j and v_k, where $t_{jk}(v_i)$ is the number of shortest paths passing node v_i, then the betweenness centrality of node v_i can be expressed as (Freeman, 1977): $\mathrm{BC}(v_i) = \sum_{j<k} \frac{t_{jk}(v_i)}{t_{jk}}$.

The maximum betweenness centrality is reached when a node is on all geodesics, in which case $\mathrm{BC}(v_i) = \sum_{j<k} 1 = \frac{(n-1)(n-2)}{2}$. To normalize the impact of network size, the normalized betweenness centrality can be expressed by: $\mathrm{BC}'(v_i) = \frac{\mathrm{BC}(v_i)}{(n-1)(n-2)/2}$.

Similar to degree centrality, we use four measures to represent network level betweenness centrality: Min(BC), Max(BC), Mean(BC) and Std(BC). Min(BC) is the minimum betweenness centrality across all nodes in the network. If there are nodes that only have one neighbor in a network, then the minimum betweenness centrality is zero. Max(BC) is the maximum betweenness centrality across all nodes. Mean(BC) is the average betweenness centrality of all nodes, which is equivalent to the measure of average path length (Gago et al., 2014). Std(BC) is the standard deviation of betweenness centrality. A scale free network with many nodes that have betweenness centrality zero and several hub nodes that have high betweenness centrality tends to have a higher standard deviation of betweenness centrality.

3.2.3 Closeness Centrality

Closeness centrality (Freeman, 1978) measures the degree to which a node is close to all other nodes in a network, and it is calculated as the reciprocal of the mean distance from a node to other nodes. The mathematical expression is $\mathrm{CC}(v_i) = \frac{1}{\sum_j g_{ij}}$, where g_{ij} is the shortest path, or geodesic, from node v_i to node v_j. A node with high closeness centrality tends to have low distance to all other nodes. In a supply chain network, if a disruption happens in such a node, the average path length of the network may become bigger after the disruption, thus the material flow efficiency will be greatly impacted.

As the maximum $\mathrm{CC}(v_i) = 1/(n-1)$ when the node is connected with all other nodes, the measure can be normalized by multiplying by (n-1). The normalized closeness centrality is therefore $\mathrm{CC}'(v_i) = \frac{n-1}{\sum_j g_{ij}}$.

For network level closeness centrality, we use $\mathrm{Min(CC)}$, $\mathrm{Max(CC)}$, $\mathrm{Mean(CC)}$ and $\mathrm{Std(CC)}$ to represent the minimum, maximum, average and standard deviation of closeness centrality across all nodes in the network. Max(CC) reflects the degree of closeness for the most influential node on the network, and Mean(CC) implies the overall closeness of the entire network.

3.2.4 Eigenvector Centrality

Eigenvector centrality (Ruhnau, 2000) is a measure of the influence of a node in a network. It assigns relative scores to all nodes in the network based on the concept that connections to high-scoring nodes contribute more to the centrality score of the node than connections to low-scoring nodes. Thus, eigenvector centrality considers a node highly important if many other highly important nodes link to it. In a supply chain, if disruption happens in a node with high eigenvector centrality, this disruption risk may quickly diffuse to other important nodes, and hence it can influence the network severely.

Let $A = (a_{i,j})$ be the adjacency matrix where $a_{i,j} = 1$ when node v_i links with node v_j, otherwise $a_{i,j} = 0$. The eigenvector centrality of node v_i is the value of λ that satisfies $\mathrm{EC}(v_i) = \frac{\sum_j a_{ij} * EC(v_j)}{\lambda}$, where λ is a non-zero constant.

For network level eigenvector centrality, we use Min(EC), Max(EC), Mean(EC) and Std(EC) to represent the minimum, maximum, average and standard deviation of eigenvector centrality across all nodes in the network.

3.2.5 Clustering Coefficient

The clustering coefficient (Watts and Strogatz, 1998) is a measure of the degree to which nodes tend to cluster together. The clustering of a node is the fraction of possible triangles through that node that exist, which can be expressed as: $\mathrm{Clustering}(v_i) = \frac{2T(v_i)}{\deg(v_i)(\deg(v_i)-1)}$. Here $T(v_i)$ is the number of triangles through node v_i, and $\deg(v_i)$ is the degree of v_i. A network with high clustering coefficient tends to cluster tightly. When a disruption happens in such a network, this network normally maintains good functionality as nodes can still connect with each other because of the high clustering nature, but this network can also accelerate the risk diffusion process because nodes are tightly clustered together.

For network level clustering coefficient, we use Min(Clust), Max(Clust), Mean(Clust) and Std(Clust) to represent minimum, maximum, average and standard deviation of clustering coefficient across all nodes in the network.

3.2.6 Eccentricity

The eccentricity (Dankelmann et al., 2004) of a node v_i is the maximum geodesic distance from v_i to all other nodes in the network. In some literature, eccentricity is called node levels (Airoldi et al., 2011). Same with above, we use Min(Eccentr), Max(Eccentr), Mean(Eccentr) and Std(Eccentr) to represent minimum, maximum, average and standard deviation of eccentricity across all nodes in the network. Obviously, the Min(Eccentr) is the network radius, and the Max(Eccentr) is the network diameter.

3.2.7 Information Centrality

Information centrality (Estrada and Hatano, 2010; Stephenson and Zelen, 1989) is a variant of closeness centrality. It is assumed that information can be transmitted through any two nodes in a connected network. The information between v_i and v_j is defined as: $I_{ij} = 1/g_{ij}$, and $I_{ii} = \infty$. The information centrality of node v_i is then given by: $\mathrm{IC}(v_i) = [\frac{1}{n} * \sum_j \frac{1}{I_{ij}}]^{-1}$.

From the network level, we use Min(IC), Max(IC), Mean(IC) and Std(IC) to represent minimum, maximum, average and standard deviation of information centrality across all nodes in the network.

3.2.8 Communicability

Communicability (Estrada and Hatano, 2008) measures the generalized shortest path between two pairs of nodes. This generalization not only considers the shortest paths, but also consider all other walks between these two nodes. Here, communicability between two nodes is calculated as the sum of closed walks of different lengths between two nodes.

From the network level, we use Min(Commu), Max(Commu), Mean(Commu) and Std(Commu) to represent minimum, maximum, average and standard deviation of communicability between all pairs of nodes in the network.

4.3.3 Supply Chain Network Resilience

Supply chain network resilience measures the network's capability to maintain operationality and recover from a disruption. We adopt the resilience measures in Chapter 2 and select four commonly used indicators, including three robustness measures and one recoverability measure. The criteria for selecting these particular indicators is based on the analysis in chapter 2 that resilience can be characterized by both robustness and recovery time, and also based on their popularity in resilience studies. Below we will describe these four measures in detail.

Figure 1 displays the disruption profile. y_0 is the level of performance at initial impact, which describes the network's functionality immediately after the disruption. $t^{max}$is the time point that when performance measures reaches the worst situation. $y_{t^{max}}$ is the value of the performance measure at the worst situation, and T is the total recovery time for the disruption.

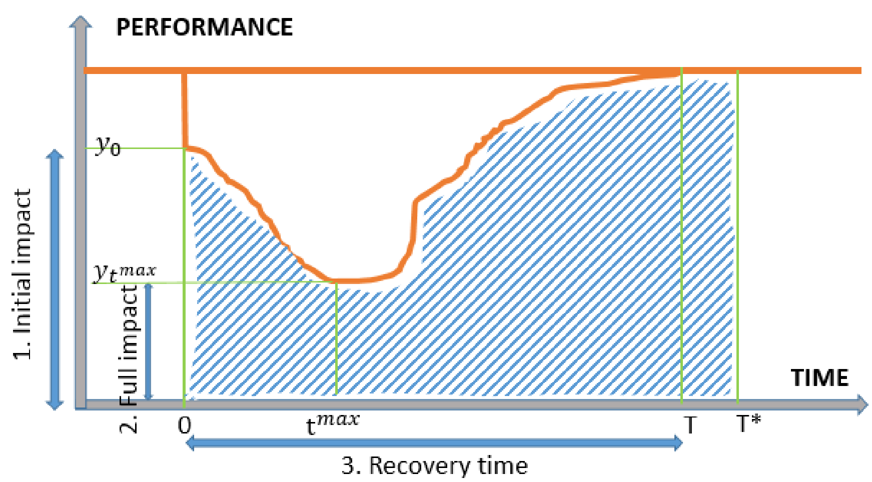


Figure 1: Disruption Profile (adopt from chapter 2)

Number of healthy nodes at full impact (NH_FI): measures the number of healthy nodes at the worst situation during the whole disruption period, which is the number of healthy nodes at t^{max}. Number of healthy nodes can describe the system performance at each time point in that a higher number of healthy nodes means better system robustness (Basole and Bellamy, 2014). In our calculation, we normalize this measure by network size, so that the measure can describe the percentage of healthy nodes. NH_FI measures the network functionality at the worst situation, and represents the network robustness against disruptions. We explicitly chose not to include the number of healthy nodes at initial impact (NH-II) in our set of resilience measures because NH-II is equivalent to disruption severity, which is totally independent of network structure and the risk diffusion process.

$$NH\_FI = \frac{(number\ of\ healthy\ nodes)_{t^{max}}}{network\ size} = \frac{min_{0\le t\le T}(number\ of\ healthy\ nodes)}{network\ size}$$

Size of the LCC at initial impact (LCC_II): measures the size of the LCC immediately after the disruption. LCC is the largest connected component, and size of the LCC is the number of nodes of the largest connected component. When a disruption happens, the network can become disconnected, and the connected part of the network is the actual functioning part. In general, the bigger the size of the LCC, the more resilient the network is (Zhao et al., 2011). LCC-II thus measures the robustness of the network right after the disruption. For the calculation of LCC_II, we normalize it by network size, so LCC_II can describe the percentage of functionality right after the disruption.

$$LCC\_II = \frac{(size\ of\ the\ LCC)_0}{network\ size}$$

Size of the LCC at full impact (LCC_FI): measures the smallest size of the LCC during the whole disruption period. LCC_FI is also a robustness measure of the network, and it is the percentage of functionality at the worst situation.

$$LCC\_FI = \frac{(size\ of\ LCC)_{t^{max}}}{network\ size} = \frac{min_{0\le t\le T}(size\ of\ LCC)}{network\ size}$$

Recovery Time (RT): measures the total recovery time of a disruption. In general, a network is more resilient to a given disruption when the recovery time is smaller. Thus, recovery time can measure the network recoverability.

$$RT = T$$

4.3.4 Disruption and Risk Diffusion Setting

Since, in reality, disruptions in a supply chain network typically start from a localized area within the network and then spread to other nodes in the network, we set the initial disruption severity equal to 10% of the network size to represent a relatively small initial disruption. For example, both the 2011 Thailand flood affected the electronics industry and the 2012 Japan earthquake influenced the global auto industry start from a small fraction of the supply chain network.

For the risk diffusion process, we use three settings to represent various risk diffusion processes in reality. First is 5% recovery rate and 10% risk diffusion rate to represent a quick risk diffusion process. Second is 5% recovery rate and 5% risk diffusion rate to represent a benchmark process for comparison. The third is 10% recovery rate and 5% risk diffusion rate to represent a quick recovery process.

4.4 Data Collection and Analysis

We collect data based on the experimental design given in Section 3. As discussed previously, we use the Python Networkx package to generate the set of different networks and to calculate the corresponding network characteristics. All the created networks are connected networks, as only connected supply chain networks can function well in reality.

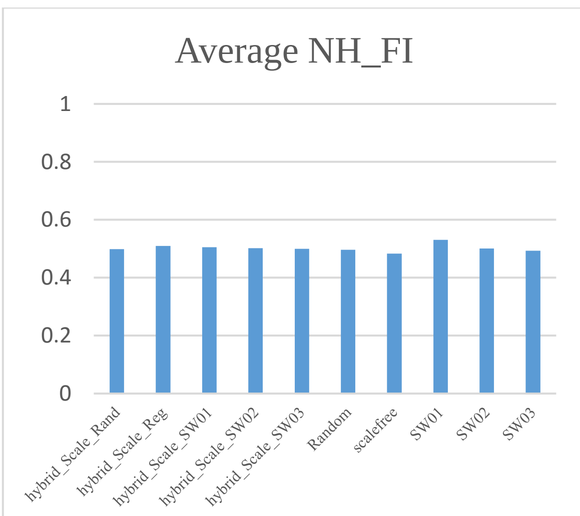
For each generated network, we use NetLogo to simulate the initial disruption and the risk propagation process. We then calculate resilience scores based on the disruption process. To eliminate the random error, we simulate each individual process 30 times and use the average resilience scores for each network.

In this section, we show the detailed data analysis.

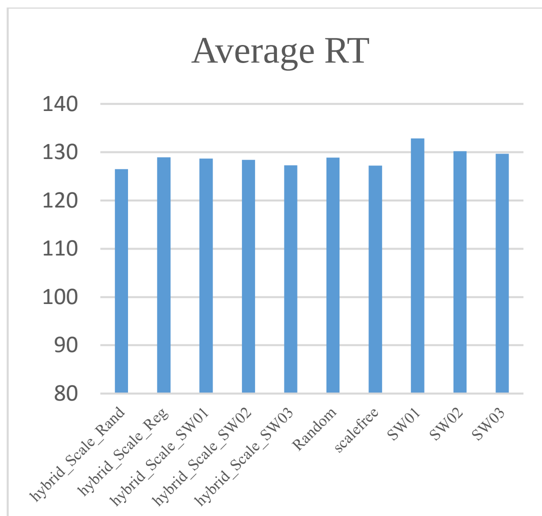
4.4.1 Data Summary

We first compare the network resilience of different network types. To make these different types of network comparable, we select only the network types with average degree 4 and with the quick risk diffusion disruption process, which has a 10% initial disruption severity, a 5% recovery rate and a 10% risk diffusion rate. The results are plotted in Figure 2. In these charts, SW01 refers to a small-world network with rewire probability 0.25, SW02 refers to a small-world network with rewire probability 0.5, and SW03 refers to the small-world network with rewire probability 0.75. Hybrid_*NetworkType1_NetworkType2* is then the hybrid network created from networks of type *NetworkType1* and *NetworkType2*. For example, Hybrid_Scale_Rand is hybrid network of scale-free and random network.

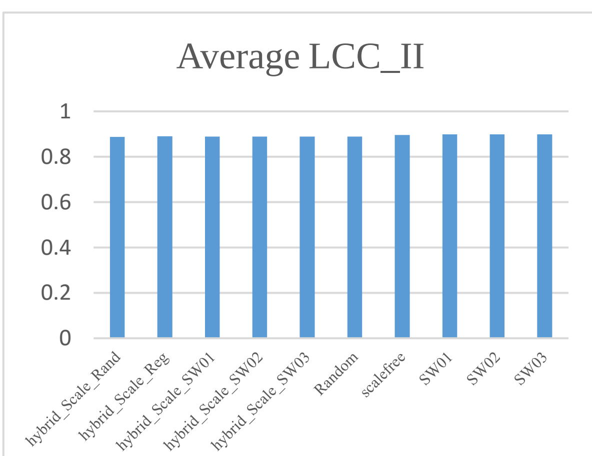
We compare three different network types: scale-free, small-world (rewire probability = 0.5) and random network in Chapter 2, from which we conclude that network types do not have a significant impact on robustness at full impact and recoverability, specifically NH_FI, LCC_FI and RT in this context. This is supported by our observation from Figure 2 that the differences of NH_FI, LCC_FI and RT among various network types are small. Although Chapter 2 states that a scale free network has significantly higher LCC_II than a random network and a small world network has significantly lower LCC_II than a random network, it is hard to visually observe this difference in Figure 2(c). Therefore, the resilience patterns are not obvious for different types of network, and looking at network characteristics may provide better understanding of network resilience.

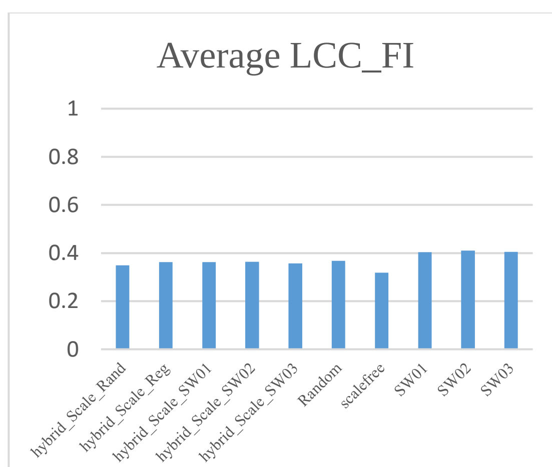


(a)



(b)





(c) (d)

Figure 2. Disruption Resilience

To investigate the relationships between network characteristics and supply chain resilience, we first look at these selected characteristics. We find that there are strong correlations among network characteristics. Obviously, correlation exists among different characteristics within the same centrality measure. For example, if the gap between minimum and maximum of one centrality measure is bigger, standard deviation of this measure is in general larger. Strong correlation also exists among different centrality measures. Table 3 is the correlation table of the mean centrality measures.

Table 3. Correlation of network characteristics

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Mean(DC)	(1)	1.000							
Mean(BC)	(2)	-0.655	1.000						
Mean(CC)	(3)	0.886	-0.894	1.000					
Mean(EC)	(4)	0.733	-0.785	0.770	1.000				
Mean(Clust)	(5)	0.377	-0.321	0.275	0.466	1.000			
Mean(Eccentr)	(6)	-0.651	0.998	-0.887	-0.789	-0.328	1.000		
Mean(IC)	(7)	0.992	-0.663	0.877	0.780	0.369	-0.660	1.000	
Mean(Commu)	(8)	0.267	-0.114	0.249	0.024	0.089	-0.112	0.209	1.000

From Table 3, strong correlation exists among mean of betweenness centrality, mean of eigenvector centrality, mean of closeness centrality, mean of eccentricity and mean of information centrality. Their strong collinearity implies that redundant information exists in these characteristics, thus identifying the key influential factors has both practical and academic importance. We will discuss the key influential factors in section 4.3.

4.4.2 Comparison of Goodness of Fit

In this study, we want to show that looking into network characteristics can provide a better understanding of supply chain network resilience than can simply using network types. Thus, in this section, we test this hypothesis by comparing the impact on supply chain resilience of network type against the corresponding impact on resilience of the network characteristics.

Models 4.2.1-4.2.3 exhibit three high-level regression models of supply chain network resilience. As the disruption process is exogenous, we first set it as a control variable. Model 4.2.1 specifically tests the influence of this control variable on supply chain resilience. As discussed above, there are three different disruption process, including quick risk diffusion process, benchmark process and quick recovery process.

The second model, Model 4.2.2, is the simple linear regression model of network structure & average degree on supply chain resilience. The third model, Model 4.2.3, is the simple linear regression model of network characteristics on supply chain resilience, in which we include all 32 network characteristics discussed above. Since network type and average degree are used to randomly generate the different networks in our data set, the characteristics of these networks implicitly embed the information of both network type and average degree. Furthermore, because the type of disruption process can also influence a supply chain's resilience, we also consider the disruption process as a control variable in each of these regression models. Thus, comparing the goodness of fit of Model 4.2.2 and Model 4.2.3 can help us to know if network characteristics can better explain the variance of supply chain resilience.

Table 4 displays the comparative results for the three models in terms of the R-Square and adjusted R-Square values. The corresponding detailed regression results are listed in Appendix C.

$$resilience = f(disruption\ process) \qquad \text{Model 4.2.1}$$

$$resilience = f(network\ type, average\ degree, disruption\ process) \qquad \text{Model 4.2.2}$$

$$resilience = f(network\ characteristics, disruption\ process) \qquad \text{Model 4.2.3}$$

Table 4: Comparison of Goodness of Fit

		NH_FI	**LCC_II**	**LCC_FI**	**RT**
Model 4.2.1	RSquare	0.5107	0.0000	0.6274	0.9047
	RSquare Adj	0.5105	0.0000	0.6273	0.9047
Model 4.2.2	RSquare	0.9425	0.4787	0.6578	0.9078
	RSquare Adj	0.9424	0.4777	0.6570	0.9076
Model 4.2.3	RSquare	0.9551	0.9938	0.9346	0.9553
	RSquare Adj	0.9548	0.9937	0.9341	0.9550

Table 4 clearly shows that the network characteristics models have a better goodness of fit than the network type and average degree models in general, in terms of their ability to explain the different aspects of supply chain network resilience. This shows that looking into network characteristics can potentially give us a better understanding of network resilience, which can then better support decision making. The R Square difference between Model 4.2.2/Model 4.2.3 and Model 4.2.1 is the pure influence of network type & average degree/network characteristics on supply chain resilience. The R-square values of zero for Model 4.2.1 on LCC_II imply that the disruption process has no impact on LCC_II, which makes sense because LCC at initial impact is not influenced by the risk diffusion rate and recovery rate. Comparatively, LCC_FI is greatly impacted by the disruption process.

4.4.3 Key Influential Characteristics

As strong correlations exist among network characteristics, there is a lot of redundant information in the 32 specified network characteristics. Thus, identifying the key characteristics that can represent network structure influence on network resilience has both research and practical importance. Selecting the key influential characteristics can eliminate redundant information caused by collinearity, allowing both the researcher and the practitioner to focus on several important characteristics. The fewer the number of key characteristics that we select, the easier these key characteristics can be understood and utilized in practice.

We use stepwise regression to select the key influential factors for each of the resilience measures. Stepwise regression is a simple and widely used variable selection method to identify a useful subset of predictors. In each step, a variable will be added or deleted from the set of explanatory variables based on certain criteria. Based on the options for adding or deleting variables, stepwise regression has three main different approaches: forward selection, backward elimination and bidirectional elimination. In our example, we use the forward selection approach. As average degree is one of the criteria we used to produce all the networks, we mandatorily add mean degree centrality, which is equivalent to average degree, in the fitted model. In each subsequent step, we then add another variable whose inclusion results in the most significant increase of the fitness of the model. This process is repeated until the single-step improvement of the R-square value is smaller than 0.005. Table 5 displays the resulting key influential characteristics that were thus derived for each resilience measure. In summary, the selected key influential factors that result from generating the stepwise regression model are degree centrality (Mean, Max), betweenness centrality (Max, Std) and closeness centrality (Mean, Max).

Table 5: Key Influential Characteristics

	NH_FI	**LCC_II**	**LCC_FI**	**RT**
Key influential characteristic	Mean(DC) Mean(CC)	Mean(DC) Std(BC) Max(CC)	Mean(DC) Max(DC) Max(BC) Std(BC)	Mean(DC) Max(BC) Std(BC)

For each of the resilience measures, we fit a linear regression model using the identified key influential characteristics together with the control variable representing the disruption process. Table 6 displays the results, which shows that these selected key influential characteristics are indeed statistically significant in terms of explaining the variance of the different supply chain resilience measures.

To illustrate the relative performance of the key influential characteristics, we plot the R-square value comparison in Figure 3. CT represents the control variable for disruption type, KIC represents the key influential characteristics, FLC represents the full list of characteristics, and NT/AD is network type & average degree. Clearly from this chart, these key influential characteristics almost have no difference with the full list of characteristics on their ability to explain the variance of supply chain resilience. This implies that during analysis and decision making, we need only consider these key characteristics and do not need to worry about all other characteristics.

Table 6

	(1)	(2)	(3)	(4)
	NH_FI	**LCC_II**	**LCC_FI**	**RT**
	b/se	b/se	b/se	b/se
Quick Risk Diffusion Process	-0.1528***	0.0001	-0.1973***	-8.0345***
	(0.001)	(0.001)	(0.002)	(0.206)
Quick Recovery Process	0.1727***	-0.0000	0.1962***	-60.3441***
	(0.001)	(0.001)	(0.002)	(0.206)
Mean(DC)	-9.7606***	-4.0198***	-14.6906***	-727.0269***
	(0.147)	(0.059)	(0.170)	(15.461)
Max(DC)			0.5906***	
			(0.022)	
Max(BC)			-0.6533***	-19.4906***
			(0.013)	(1.046)
Std(BC)		-4.2799***	-1.2245***	-149.8168***
		(0.014)	(0.061)	(5.352)
Mean(CC)	-0.5357***			
	(0.014)			
Max(CC)		0.3827***		
		(0.005)		
Constant	0.9577***	0.8948***	0.9049***	156.7715***
	(0.002)	(0.002)	(0.004)	(0.450)
Number of observations	5220	5220	5220	5220
R-squared	0.9531	0.9837	0.9243	0.9532
adjusted R-squared	0.9531	0.9837	0.9242	0.9531
F statistic	26523.92	63081.87	10610.56	21225.86

All models are significant with $p < 0.0001$
Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

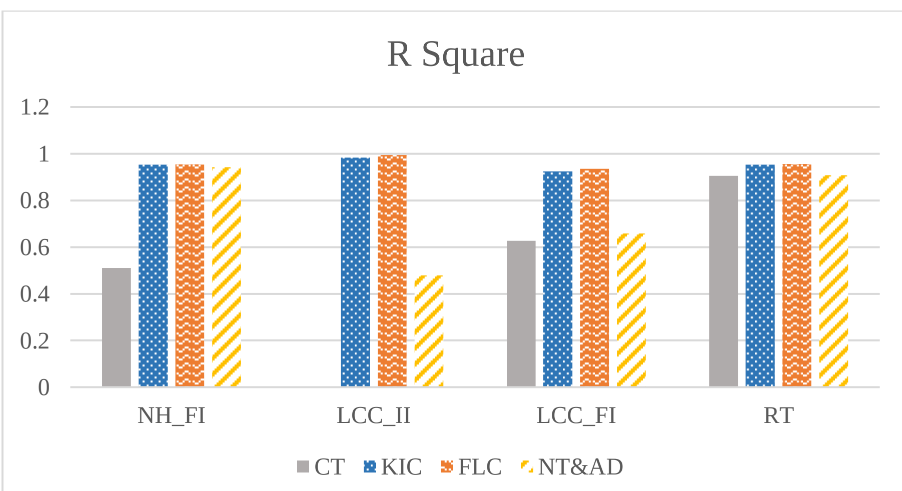


Figure 3: R Square Comparison

In Table 6, Mean(DC) is negatively related to LCC_II and LCC_FI, while in Chapter 2 we found that average degree is positively related to LCC_II and LCC_FI. This inconsistency comes from the strong collinearity among network characteristics, thus the positive side of Mean(DC) is represented by other characteristics and the Mean(DC) becomes negative. This phenomenon makes interpreting the influence of characteristics difficult. Therefore, in the following section we will discuss in detail how we interpret our results and how our results can support better understanding of the supply chain resilience.

4.4.4 Results Interpretation and Discussion

Interpreting resilience results using the regression models developed above may be misleading given the existence of collinearity. For example, as discussed above, the negative parameters of network characteristics in Table 6 do not necessarily indicate that these characteristics are negatively associated with supply chain resilience. To better interpret the results, therefore, we need to be aware of the following points when attempting to understand them.

1. **Interpreting the relationship between individual network characteristics and supply chain resilience should be done with care and should consider the impact of collinearity.**

In Section 4.3, we claim that interpreting the relationship between individual network characteristics and supply chain resilience using the parameters of the regression model may be misleading because strong correlations exist among network characteristics. With the existence of collinearity, the parameters of the regression models may significantly change when introducing or deleting a variable. In our case, although Mean(DC) is positively related to LCC_FI, the parameter of Mean(DC) in Table 6 is negative since the positive portion of Mean(DC) is represented by other variables in the model because of the strong collinearity.

Although we select the key influential characteristics and eliminate collinearity by excluding many characteristics from the model, there is still redundant information in these key influential characteristics. Appendix D shows the correlation table of these key influential characteristics. Clearly, strong collinearity exists among these characteristics, especially among Max(BC), Std(BC), Max(CC) and Mean(CC).

The collinearity phenomenon also reflects the fact that varying one characteristic to improve the supply chain resilience will almost always result in changing other characteristics. Thus, it is critical to evaluate the overall impact of network characteristic combinations on supply chain resilience. Simply looking at the parameter value of a particular characteristic can be misleading.

2. **Non-key influential characteristics may also have a significant impact on supply chain resilience, but including them in the models will not greatly improve the fitness of models.**

We select key influential characteristics based on the rule that the combination of these characteristics can best capture the network structure's influence on supply chain resilience. Other non-key influential characteristics also may have a significant impact on supply chain resilience, but this influence simply can be represented by the key influential characteristics. In other words, non-key influential characteristics do not provide substantial additional information in terms of explaining supply chain resilience, which is clearly supported by Figure 3 in that the R-Square value for the key influential characteristics is close to the R-Square value for the full list of these 32 characteristics.

The key influential characteristics that we selected above are the combination that **BEST** represent the influence of network structure on supply chain resilience with **FEWER** network characteristics. Some other combinations of network characteristics may also capture the influence of network structure, but they are not as good as the one we have in terms of using fewer characteristics to fit best.

In practice, therefore, to understand supply chain resilience, we only need to consider these key influential characteristics, and do not need to worry about other characteristics.

3. **Both network characteristics and the disruption process have a significant influence on the resilience measures at full impact, specifically HN-FI and LCC-FI.**

When a disruption reaches full impact, it normally takes a period of risk diffusion time. Thus, resilience measures at full impact are the results of both network structure and the risk propagation process. This is supported by results in Figure 3. In Figure 3, CT represents the control variable disruption process, and the gray bar of CT is the percentage of variance explained by disruption process. The blue bar of KIC is the percentage of variance explained by both disruption process and key influential characteristics. Thus, the difference between the blue bar and the grey bar is the percentage of variance explained purely by the key influential characteristics, or the supply chain network structure. Our data shows that the disruption process contributes 51% of the variance of NH_FI and 63% of the variance of LCC_FI, while the key influential characteristics contribute 44% of the variance of NH_FI and 30% variance of the variance of LCC-FI.

This result implies that for understanding resilience behaviors at full impact, researchers and practitioners should not only look into the network structure, but should have a good understanding of the disruption nature and the possible risk propagation process.

4. **Network characteristics contribute limited variance for the recovery time.**

From Figure 3, we can observe that the difference between CT and KIC of RT is small, which indicates that the disruption process has a great impact on recovery time and network structure only contributes very little to the variance of RT. Our data in Table 4 and Table 6 shows that the disruption process explains 90% of the variance of RT and that network characteristics explain an additional 4.8% of the variation in recovery time. As the disruption process is independent of network characteristics, we can always use the total R-Square value of network characteristics and disruption process minus the R-Square value of the disruption process to get the R-Square value for pure network characteristics.

To show more detail about how the disruption process influences RT, we plot the distribution table of RT for different disruption processes in Figure 8. Disruption process A is the quick risk diffusion process with recovery rate 5% and risk diffusion rate 10%; disruption process B is the benchmark process with recovery rate 5% and risk diffusion rate 5%; and disruption process C is the quick recovery process with recovery rate 10% and risk diffusion rate 5%.

Clearly from Figure 4, the recovery time of quick recovery process is significantly lower than that of quick risk diffusion process, which is lower than that of the benchmark process. This result indicates that the disruption process has a significant impact on RT. To predict the total recovery time, therefore, we need to emphasize the risk propagation and recovery process more than the network structure.

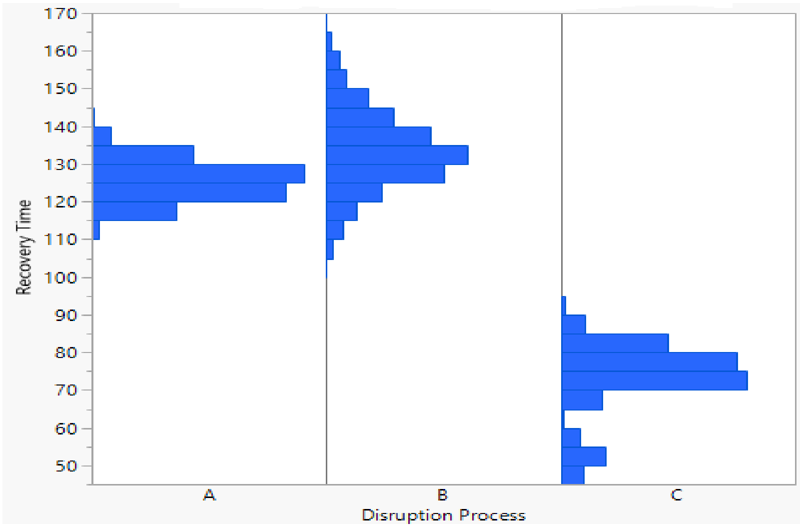


Figure 4: Recovery time distribution vs. Disruption process

5. **The better performance of network characteristics compared to network type & average degree is obvious at explaining the variance of LCC and RT, but not of NH.**

The difference between KIC and NT&AD in Figure 3 is effectively the additional explanatory power that the key influential characteristics have over network type & average degree in explaining the variance of supply chain resilience. Thus, the bigger the gap between KIC and NT&AD, the better the performance of KIC than NT&AD.

Clearly from Figure 3, the gap between KIC and NT&AD is big for LCC_II and LCC_FI, and is almost invisible for NH_FI. This result indicates that the better performance of network characteristics mainly serves to explain the variance of network connectivity (LCC), but not number of healthy nodes.

For RT, the R Square of CT is almost the same as the R Square of NT&AD, which indicates that network type and average degree almost contribute nothing to the variance of recovery time. This is supported by our findings in Chapter 2 that network type is insignificant for recovery time, and decreasing one average degree of network can only decrease recovery time by 0.08 period, which is practically insignificant.

4.5 Decision Tree models

Section 4 displays the linear relationships between key network characteristics and supply chain resilience measures. Using these fitted linear regression models, we can estimate the supply chain resilience using key network characteristics for different disruption processes.

In practice, however, estimation by regression models is restricted by the model accuracy and the knowledge of the user. More difficult models in general are more accurate, but less easy to interpret. Considering that supply chain managers may have different backgrounds, we want to provide a model with balanced accuracy and interpretability. This leads us to consider applying a decision tree model, which is an easy-to-use tool to estimate network resilience, especially for people who have a limited mathematical background.

In order to illustrate the associated advantages of using decision trees in this context, we create the decision tree charts of each network resilience measure for the quick risk diffusion process in Figure 5 – 8. We also create the decision tree charts of the benchmark process and quick recovery process in Appendix E. We set the total splits of the decision trees to four, so that the models have a balance of accuracy and interpretability. As the disruption process does not have significant impact on LCC_II, the decision tree of LCC_II can be used across any disruption process. For example, as given by Figure 5, if a network has Mean(DC)=0.0122 and Mean(CC)=0.2142, then we can estimate that the resilience value for the Number of Healthy Nodes at Full Impact is 0.7165 for the quick risk diffusion process.

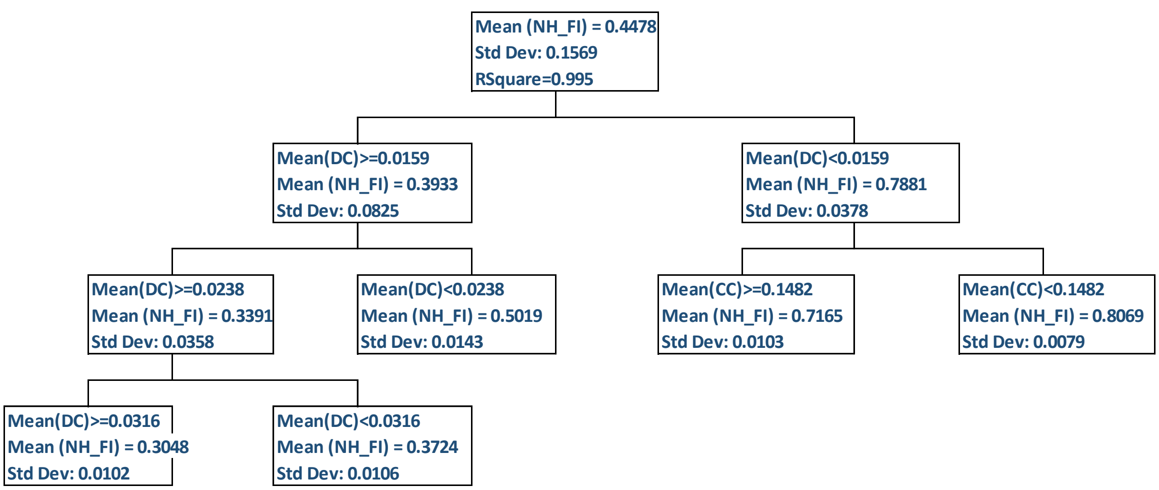


Figure 5: HN-FI Decision Tree

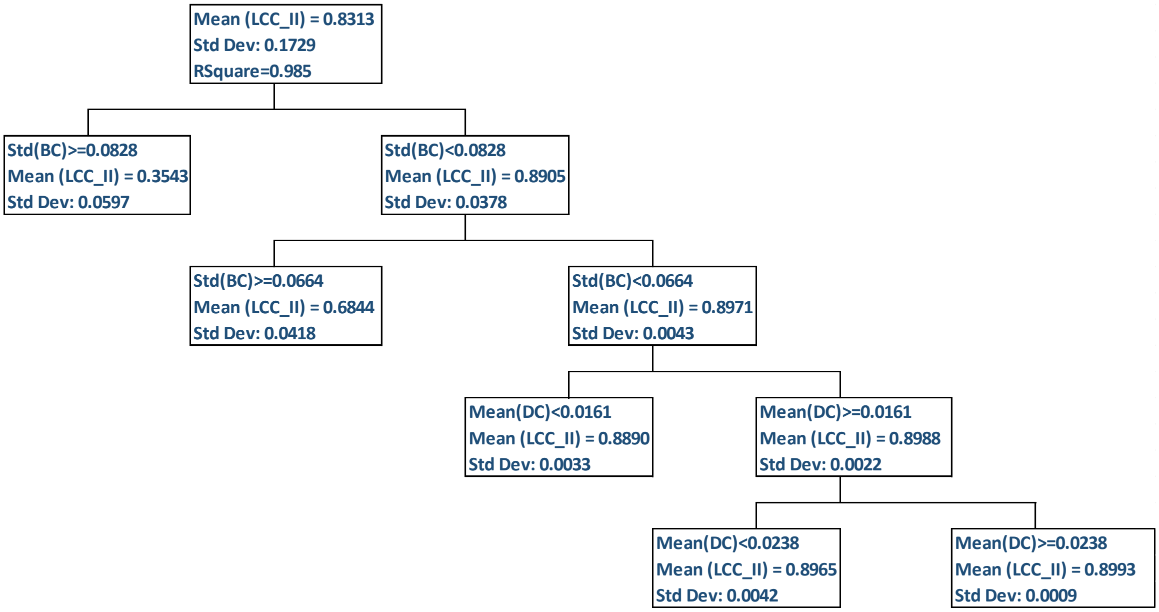


Figure 6: LCC_II Decision Tree

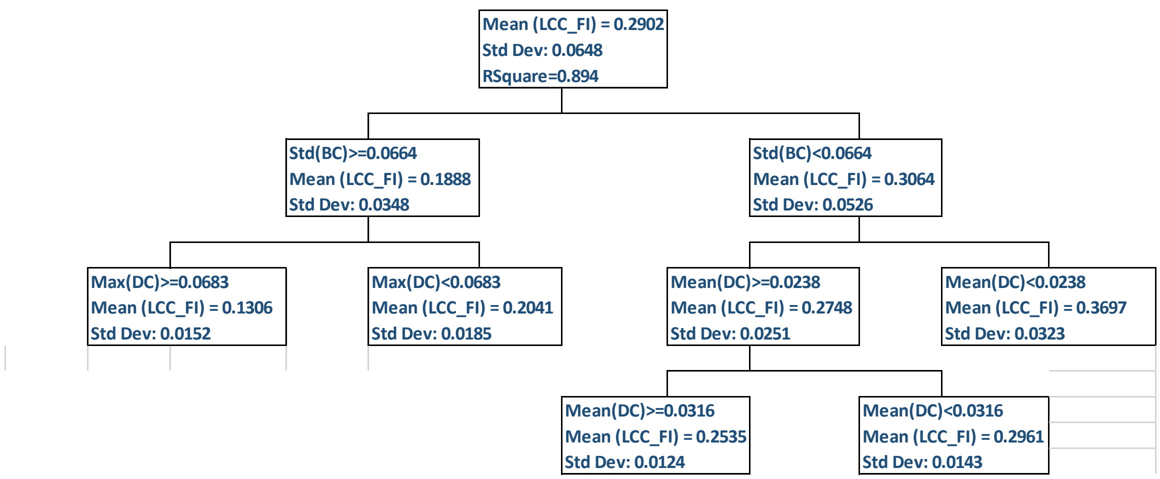


Figure 7: LCC_FI Decision Tree

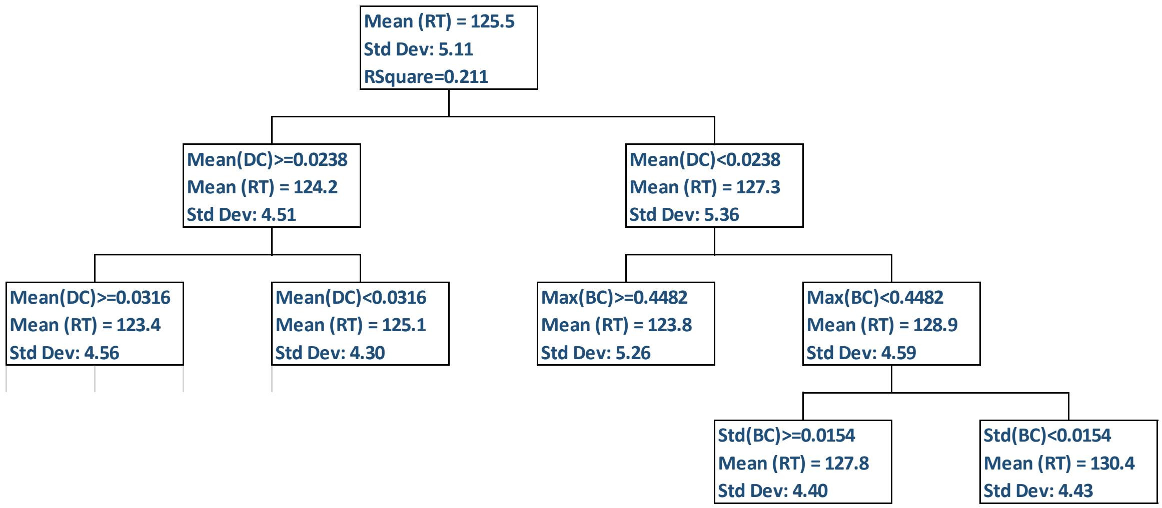


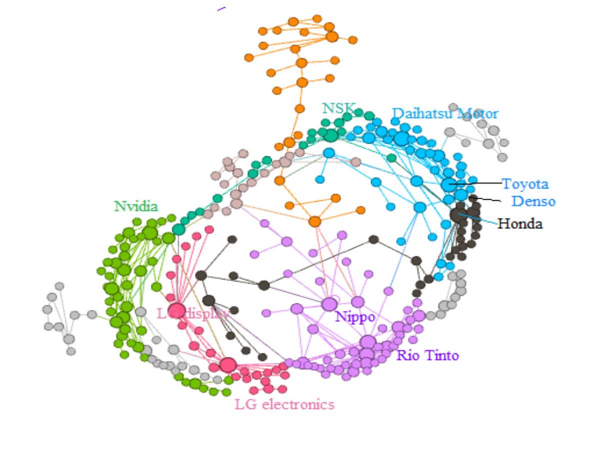
Figure 8: RT Decision Tree

From Figure 5-8, we can observe some general rules of network characteristics. For example, Figure 4 shows that higher Mean(DC) has lower NH_FI, and given Mean(DC)<0.0159, higher Mean(CC) has lower NH_FI. Figure 5 shows that higher Std(BC) tends to have smaller LCC_II, and if Std(BC)<0.0664, then a bigger Mean(DC) tends to have higher LCC_II. Figure 6 shows that higher Std(BC) tends to have smaller LCC_FI, and for given Std(BC), LCC_FI is decreasing with Mean(DC). And Figure 7 shows that smaller Mean(DC) tends to have higher RT.

We thus can estimate supply chain resilience for different disruption processes based on both the linear regression models and the decision tree models. In next section, we use a case study to evaluate these different models.

4.6 Case Example

All of our analyses in section 4 and 5 are based on simulated data. To examine if these results can be applied to real supply chain network, we conduct a case study in this section. We use the Japan auto supply chain network discussed in Chapter 2, and calculate its key influential characteristics. Figure 9 displays the Japan auto network and the values for its key influential characteristics.



Key Network Characteristics:

No. Nodes: 302   No. Links: 404

Mean (DC)=0.00889

Max (DC)=0.0465

Max (BC)=0.2333

Std (BC)=0.04024

Mean (CC)=0.1441

Max (CC)= 0.2001

Figure 9: Japan auto network (adopted from Chapter 2) and key influential characteristics

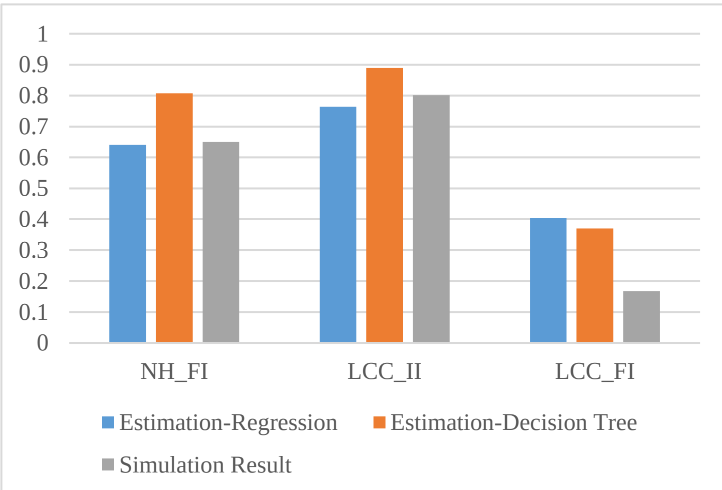
As all key influential characteristics are normalized by network size and Chapter 2 demonstrates that network size does not have a practical significant influence on network resilience, we can simply use the regression and decision tree models in Section 4.4 to estimate the supply chain network resilience. Based on Table 6, therefore, we calculate the estimated resilience associated with each of these regression models. Furthermore, based on the decision trees given in Figures 4-7, we calculate the estimated resilience as assessed by the decision tree models. To evaluate the relative accuracy of each of these models, we compare the estimated resilience measures against the actual resilience, which is the average resilience of the simulated results.

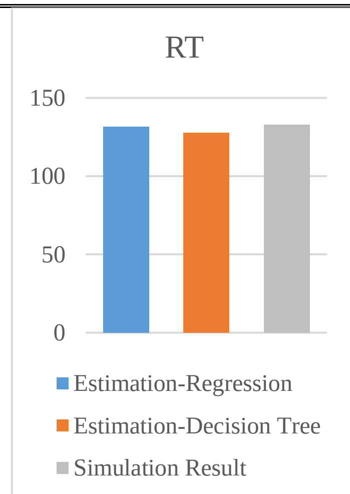
We conduct the simulation with respect to the same three different disruption processes discussed above, with 10% disruption severity: the quick risk diffusion process, the benchmark process and the quick recovery process. Then we compare the estimated resilience measures with the simulated resilience at each disruption process scenario. Table 7 displays these results.

Table 7: Resilience measure comparison

Quick Risk Diffusion Process

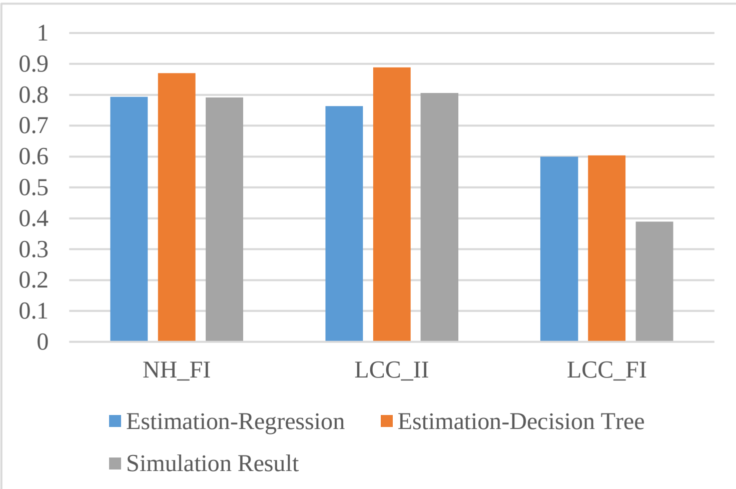
	NH_FI	LCC_II	LCC_FI	RT
Estimation-Regression	0.6409	0.7635	0.4028	131.7
Estimation-Decision Tree	0.8069	0.8890	0.3697	127.8
Simulation Result	0.6494	0.8015	0.1675	132.9

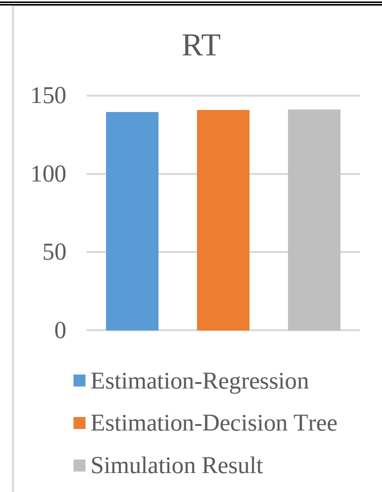




Benchmark Process

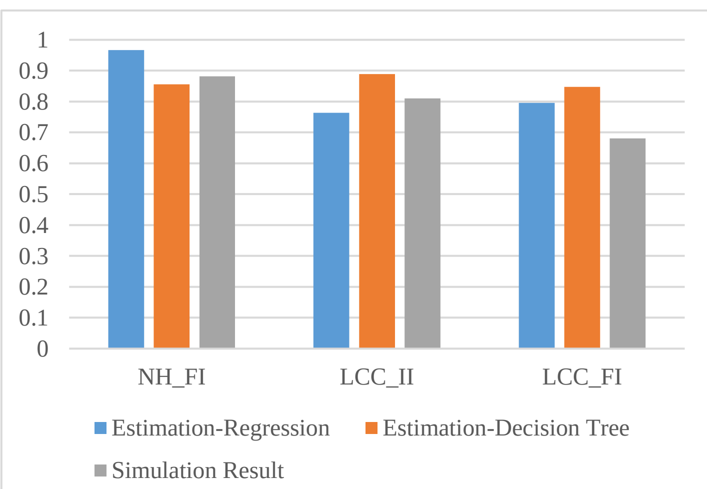
	NH_FI	LCC_II	LCC_FI	RT
Estimation-Regression	0.7937	0.7634	0.6001	139.7
Estimation-Decision Tree	0.8701	0.8890	0.6040	140.7
Simulation Result	0.7914	0.8056	0.3894	141.2

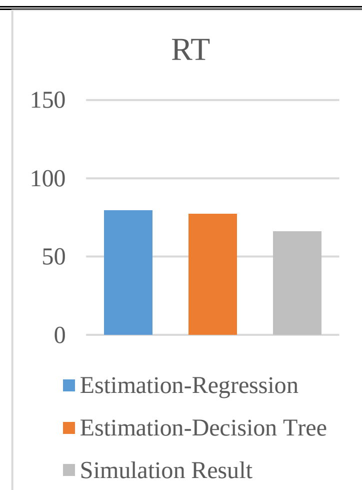




Quick Recovery Process

	NH_FI	LCC_II	LCC_FI	RT
Estimation-Regression	0.9664	0.7634	0.79627	79.4
Estimation-Decision Tree	0.8564	0.889	0.8475	77.3
Simulation Result	0.882	0.8103	0.6811	66.1





From Table 7, we have the following results. First, in general, for predicting the robustness component of resilience, such as NH_FI, LCC_II and LCC_FI, regression models tend to be more accurate than decision tree models. The only exception is the estimation of NH_FI for the quick recovery process. The model accuracy is measured by the difference between the estimated resilience and the simulation results, where a small difference between these values means that the estimation is more accurate.

Second, among all resilience measures, recovery time has the best estimation performance by both regression models and decision tree models; regression models perform better than decision tree models at estimating NH_FI and LCC_II; and both regression models and decision tree models overestimate the LCC_FI. Thus, when we estimate the largest connected component at full impact, we may need to be aware that real situation may be much worse than expected and we need to prepare more resources for recovery.

Third, although in general regression models are more accurate than decision tree models, their estimations are close. As the decision tree models are easy to implement and interpret, these decision tree models can be used as a quick tool for assessing network resilience.

At the end, except for in the case of LCC_II, other resilience measures vary for different disruption processes. In general, NH_FI and LCC_FI are higher for the quick recovery process than for the benchmark process, following the quick risk diffusion process. This indicates that recovery rate has a positive impact on the resilience measures at full impact, while the risk diffusion rate has a negative impact on the resilience measures at full impact. For RT, the RT value in the case of the quick risk diffusion process is slightly lower than that of the benchmark process, and both of them are much bigger than that of the quick recovery process. Thus, recovery rate greatly negatively impacts the RT, and risk diffusion rate slightly positively impacts RT. As the real disruption process is very complex in reality, we could use these rules to get a rule of thumb knowledge about resilient network behaviors.

4.7 Conclusion

This study investigates the relationships between network characteristics and supply chain resilience through a quantitative approach. At the start, we prove that network characteristics perform better than network types in terms of understanding network resilience behaviors. Then we select key influential characteristics that can best represent network structure in terms of their influence on supply chain resilience. Later we construct the regression and decision tree models for assessing supply chain resilience. At the end, we use a case study to compare different estimation models.

The main findings of this study are following. First, in terms of explaining the variance of supply chain resilience, network characteristics perform better than just the combination of network types & average degree. The improved performance of the network characteristics is obvious at explaining the variance of size of the largest connected component (LCC) and recovery time (RT), but not as much at explaining the variance of the number of healthy nodes (NH).

Second, as strong collinearity exists among network characteristics, we select key influential characteristics that can best represent the network structure information. Different resilience measures have different key influential characteristics. For example, Mean(DC) and Mean(CC) are key characteristics for NH_FI; Mean(DC), Std(BC) and Max(CC) are key characteristics for LCC_II; Mean(DC), Max(DC), Max(BC) and Std(BC) are key characteristics for LCC_FI; and Mean(DC), Max(BC), and Std(BC) are key characteristics for RT.

Finally, understanding the impacts of these key influential characteristics on network behavior can support decision making. First, both the regression models and the decision tree models can help assessing the impact of key influential characteristics. When interpreting the effects, we need to aware that changing one characteristic may always result in changing other characteristics because of the existence of strong collinearity. Thus, we should always consider the integrated impact of all key influential characteristics. Second, our study also shows that both network characteristics and the disruption process have a significant influence on the resilience measures at full impact, specifically HN-FI and LCC-FI. Thus, to gain a better understanding of resilience behavior at full impact, we need also to investigate the effects of different disruption processes. Third, the variance of RT is mainly explained by the disruption processes and much less by the network characteristics. Thus in practice, to estimate the total recovery time, we should focus on investigating different disruption and risk diffusion processes, and not focus so much on the network structure side.

In summary, this study is expected to contribute to the literature in both a theoretical and a practical sense. Theoretically, our study will fill the literature gap that the academic literature rarely investigates the relationship between network characteristics and supply chain resilience, and it will contribute to the growing body of literature that focuses on quantitatively studying supply chain resilience. Practically, this study is expected to provide implementable suggestions to support decision making, as supply chain managers attempt to improve the resilience of their networks in the face of the growing likelihood of disruptive events..

References

Airoldi, E.M., Bai, X. and Carley, K.M. (2011), “Network sampling and classification: An investigation of network model representations”, *Decision Support Systems*, Vol. 51 No. 3, pp. 506–518.

Basole, R.C. and Bellamy, M.A. (2014), “Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach”, *Decision Sciences*, Vol. 45 No. 4, pp. 1–49.

Bode, C. and Wagner, S.M. (2015), “Dimensions of supply chain complexity and their effects on the frequency of supply chain disruptions”, *Journal of Operations Management*, Elsevier B.V., Vol. 36, pp. 215–228.

Dankelmann, P., Goddard, W. and Swart, C.S. (2004), “The Average Eccentricity of a Graph and its Subgraphs”, *Util. Math*, Vol. 65, pp. 41–51.

Estrada, E. and Hatano, N. (2008), “Communicability in complex networks”, *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, Vol. 77 No. 3, available at:http://doi.org/10.1103/PhysRevE.77.036111.

Estrada, E. and Hatano, N. (2010), “Resistance distance, information centrality, node vulnerability and vibrations in complex networks”, *Network Science: Complexity in Nature and Technology*, pp. 13–29.

Freeman, L.C. (1977), “A Set of Measures of Centrality Based on Betweenness”, *Sociometry*.

Freeman, L.C. (1978), “Centrality in social networks conceptual clarification”, *Social Networks*, Vol. 1 No. 3, pp. 215–239.

Gago, S., Coroničová Hurajová, J. and Tomáš, M. (2014), “Betweenness Centrality in Graph”, in Dehmer, D. and Emmert-Streib, F. (Eds.), *Quantitative Graph Theory: Mathematical Foundations and Applications*, p. 233.

Hagberg, A. a., Schult, D. a. and Swart, P.J. (2008), “Exploring network structure, dynamics, and function using NetworkX”, *Proceedings of the 7th Python in Science Conference (SciPy2008)*, Vol. 836, pp. 11–15.

Kim, Y., Chen, Y.-S. and Linderman, K. (2015), “Supply Network Disruption and Resilience: A Network Structural Perspective”, *Journal of Operations Management*, Vol. 33-34, pp. 43–59.

Nair, A. and Vidal, J.M. (2011), “Supply network topology and robustness against disruptions – an investigation using multi-agent model”, *International Journal of Production Research*.

Pettit, T.J., Croxton, K.L. and Fiksel, J. (2013), “Ensuring supply chain resilience: Development and implementation of an assessment tool”, *Journal of Business Logistics*, Vol. 34 No. 1, pp. 46–76.

Pettit, T.J., Fiksel, J. and Croxton, K.L. (2010), “Ensuring Supply Chain Resilience: Development of a Conceptual Framework”, *Journal of Business Logistics*, Vol. 31 No. 1, pp. 1–21.

Ponomarov, S.Y. and Holcomb, M.C. (2009), “Understanding the concept of supply chain resilience”, *The International Journal of Logistics Management*.

Rivkin, J.W. and Siggelkow, N. (2007), “Patterned Interactions in Complex Systems: Implications for Exploration”, *Management Science*, Vol. 53 No. 7, pp. 1068–1085.

Ruhnau, B. (2000), “Eigenvector-centrality — a node-centrality?”, *Social Networks*, Vol. 22, pp. 357–365.

Snyder, L. V and Atan, Zumbul; Peng, Peng; Rong, Ying; Schmitt, Amanda J; Sinsoysal, B. (2012), *OR / MS Models for Supply Chain Disruptions : A Review*.

Stephenson, K. and Zelen, M. (1989), “Rethinking centrality: Methods and examples”, *Social Networks*, Vol. 11 No. 1, pp. 1–37.

Thadakamalla, H.P., Raghavan, U.N., Kumara, S. and Albert, R. (2004), “Survivability of multiagent-based supply networks: A topological perspective”, *IEEE Intelligent Systems*, Vol. 19 No. 5, pp. 24–31.

Tierney, K. and Bruneau, M. (2007), *Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction, TR News*.

Wagner, S.M. and Neshat, N. (2010), “Assessing the vulnerability of supply chains using graph theory”, *International Journal of Production Economics*, Vol. 126 No. 1, pp. 121–129.

Watts, D.J. and Strogatz, S.H. (1998), “Collective dynamics of ‘small-world’ networks”, *Nature*, Vol. 393 No. 6684, pp. 440–442.

Wilensky, U. (1999), “NetLogo”, *Center for Connected Learning and ComputerBased Modeling Northwestern University Evanston IL*.

Zhao, K., Kumar, A., Harrison, T.P. and Yen, J. (2011), “Analyzing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions”, *IEEE Systems Journal*.

Zobel, C.W. (2011), “Representing perceived tradeoffs in defining disaster resilience”, *Decision Support Systems*, Vol. 50 No. 2, pp. 394–403.

Zobel, C.W. (2014), “Quantitatively Representing Nonlinear Disaster Recovery”, *Decision Sciences*, Vol. 45 No. 6, pp. 1053–1082.

Zobel, C.W. and Khansa, L. (2012), “Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks”, *Decision Sciences*, Vol. 43 No. 4, pp. 687–710.

Appendix C

Table 1

	(1)	(2)	(3)	(4)
	NH_FI	LCC-II	LCC-FI	RT
	b/se	b/se	b/se	b/se
Disruption Process A	-0.1528***	0.0001	-0.1973***	-8.0345***
	(0.004)	(0.006)	(0.004)	(0.294)
Disruption Process C	0.1727***	-0.0000	0.1962***	-60.3441***
	(0.004)	(0.006)	(0.004)	(0.294)
Constant	0.6006***	0.8313***	0.4875***	133.5429***
	(0.003)	(0.004)	(0.003)	(0.208)
Number of observations	5220	5220	5220	5220
R-squared	0.5107	0.0000	0.6274	0.9047
adjusted R-squared	0.5105	0.0000	0.6273	0.9047
F statistic	2722.77	0.00	4392.95	24777.84

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 2

	(1)	(2)	(3)	(4)
	NH_FI	LCC_II	LCC_FI	RT
	b/se	b/se	b/se	b/se
Disruption Process A	-0.1528***	0.0001	-0.1973***	-8.0345***
	(0.002)	(0.004)	(0.004)	(0.290)
Disruption Process C	0.1727***	-0.0000	0.1962***	-60.3441***
	(0.002)	(0.004)	(0.004)	(0.290)
Networktype =SW01	0.0168***	-0.0153*	0.0124	1.7205***
	(0.003)	(0.007)	(0.007)	(0.497)
Networktype =SW02	0.0031	0.0005	0.0159*	1.4604**
	(0.003)	(0.007)	(0.007)	(0.497)
Networktype =SW03	-0.0003	0.0020	0.0120	0.8346
	(0.003)	(0.007)	(0.007)	(0.496)
Networktype =hybrid_Scale_Rand	-0.0142***	0.0766***	0.0449***	1.8265***
	(0.003)	(0.008)	(0.007)	(0.537)
Networktype =hybrid_Scale_Reg	-0.0059*	0.0781***	0.0572***	2.4750***
	(0.003)	(0.008)	(0.007)	(0.537)
Networktype =hybrid_Scale_SW01	-0.0107***	0.0778***	0.0542***	2.4800***
	(0.003)	(0.008)	(0.007)	(0.537)
Networktype =hybrid_Scale_SW02	-0.0131***	0.0776***	0.0518***	2.5932***
	(0.003)	(0.008)	(0.007)	(0.537)
Networktype =hybrid_Scale_SW03	-0.0139***	0.0775***	0.0502***	2.3578***
	(0.003)	(0.008)	(0.007)	(0.537)
Networktype =scalefree	-0.0203***	0.0791***	-0.0407***	-1.7870***
	(0.003)	(0.007)	(0.007)	(0.495)
Mean (DC)	-14.7653***	12.9534***	1.5910***	68.7889***
	(0.078)	(0.218)	(0.207)	(14.885)
Constant	0.9272***	0.5081***	0.4307***	130.7840***
	(0.003)	(0.007)	(0.007)	(0.491)
Number of observations	5220	5220	5220	5220
R-squared	0.9425	0.4787	0.6578	0.9078
adjusted R-squared	0.9424	0.4775	0.6570	0.9076

F statistic	7112.34	398.48	833.96	4272.33

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 3

	(1) NH_FI b/se	(2) LCC_II b/se	(3) LCC_FI b/se	(4) RT b/se
Disruption Process A	-0.1528***	0.0001	-0.1973***	-8.0345***
	(0.001)	(0.000)	(0.002)	(0.202)
Disruption Process C	0.1727***	-0.0000	0.1962***	-60.3441***
	(0.001)	(0.000)	(0.002)	(0.202)
Max(DC)	-0.0602	0.2623***	0.8431***	36.7437**
	(0.080)	(0.028)	(0.105)	(12.029)
Min(DC)	1.5715	2.5886***	1.7783	134.1151
	(1.124)	(0.388)	(1.478)	(169.555)
Mean(DC)	-16.4836***	-14.8040***	11.6105**	-1296.3930**
	(3.240)	(1.120)	(4.263)	(488.939)
Std(DC)	3.4427**	-5.8128***	-12.7097***	-615.2130***
	(1.052)	(0.364)	(1.384)	(158.727)
Max(BC)	0.0133	-0.2099***	-0.5547***	-24.8636***
	(0.021)	(0.007)	(0.028)	(3.217)
Min(BC)	-1.5366	1.6265	1.4595	-262.0954
	(3.036)	(1.049)	(3.994)	(458.109)
Mean(BC)	0.0208	-3.3285***	-1.3678*	-150.8193
	(0.517)	(0.179)	(0.680)	(78.040)
Std(BC)	-0.3102	-0.8382***	-1.5393***	-41.3026
	(0.177)	(0.061)	(0.232)	(26.657)
Max(CC)	0.0051	0.1317***	0.9474***	24.5105
	(0.101)	(0.035)	(0.133)	(15.253)
Min(CC)	0.0760	0.1144***	0.1032	-3.2671
	(0.087)	(0.030)	(0.115)	(13.171)
Mean(CC)	-1.4407***	0.4993***	-1.5235***	-31.4379
	(0.208)	(0.072)	(0.273)	(31.347)
Std(CC)	2.3487***	2.7162***	-1.8872*	-64.0366
	(0.601)	(0.208)	(0.791)	(90.747)
Max(EC)	0.0408	0.1020***	-0.0051	4.0196
	(0.023)	(0.008)	(0.030)	(3.395)
Min(EC)	0.0588	0.2251	-0.1465	77.0832
	(0.333)	(0.115)	(0.438)	(50.251)
Mean(EC)	1.8130**	5.2513***	3.3019***	345.6268***
	(0.694)	(0.240)	(0.913)	(104.765)
Std(EC)	0.4565	2.6310***	3.3338***	205.0945*
	(0.661)	(0.228)	(0.869)	(99.714)
Max(clust)	-0.0013	0.0008	-0.0124**	0.0288
	(0.003)	(0.001)	(0.004)	(0.505)
Min(clust)	0.0634	0.0178	0.0903	-4.3567
	(0.140)	(0.048)	(0.184)	(21.072)
Mean(clust)	-0.0435	0.1604***	-0.4670***	8.9665
	(0.043)	(0.015)	(0.057)	(6.522)
Std(clust)	0.0394	0.0967***	0.6027***	9.4693
	(0.036)	(0.012)	(0.047)	(5.388)
Max(eccentr)	-0.0008	-0.0038***	-0.0034*	-0.1400
	(0.001)	(0.000)	(0.002)	(0.182)
Min(eccentr)	0.0007	-0.0038***	-0.0055**	-0.4401
	(0.002)	(0.001)	(0.002)	(0.242)
Mean(eccentr)	0.0002	0.0086***	0.0090***	0.5835*

	(0.002)	(0.001)	(0.003)	(0.296)
Std(eccentr)	0.0004	0.0101***	0.0065	0.4339
	(0.004)	(0.001)	(0.005)	(0.563)
Max(IC)	-2.3657	-4.7519***	-9.8125**	75.6078
	(2.624)	(0.907)	(3.453)	(396.006)
Min(IC)	-4.6477	-6.4919***	0.5786	-132.2856
	(2.885)	(0.997)	(3.796)	(435.364)
Mean(IC)	28.2155***	25.0694***	-25.6923*	624.7027
	(7.611)	(2.631)	(10.014)	(1148.495)
Std(IC)	-2.4227	19.5466***	11.1658	4415.2818*
	(12.936)	(4.472)	(17.020)	(1951.994)
Max(commu)	0.0000	0.0000***	-0.0000	0.0001
	(0.000)	(0.000)	(0.000)	(0.000)
Min(commu)	-0.0001	-0.0001**	-0.0001	-0.0160
	(0.000)	(0.000)	(0.000)	(0.024)
Mean(commu)	0.0000*	0.0001***	0.0000	0.0069*
	(0.000)	(0.000)	(0.000)	(0.003)
Std(commu)	-0.0000*	-0.0000***	-0.0000	-0.0028*
	(0.000)	(0.000)	(0.000)	(0.001)
Constant	0.9645***	0.4665***	0.5087***	135.2301***
	(0.069)	(0.024)	(0.091)	(10.438)
Number of observations	5220	5220	5220	5220
R-squared	0.9551	0.9938	0.9346	0.9553
adjusted R-squared	0.9548	0.9937	0.9342	0.9550
F statistic	3242.52	24375.03	2178.73	3255.46

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

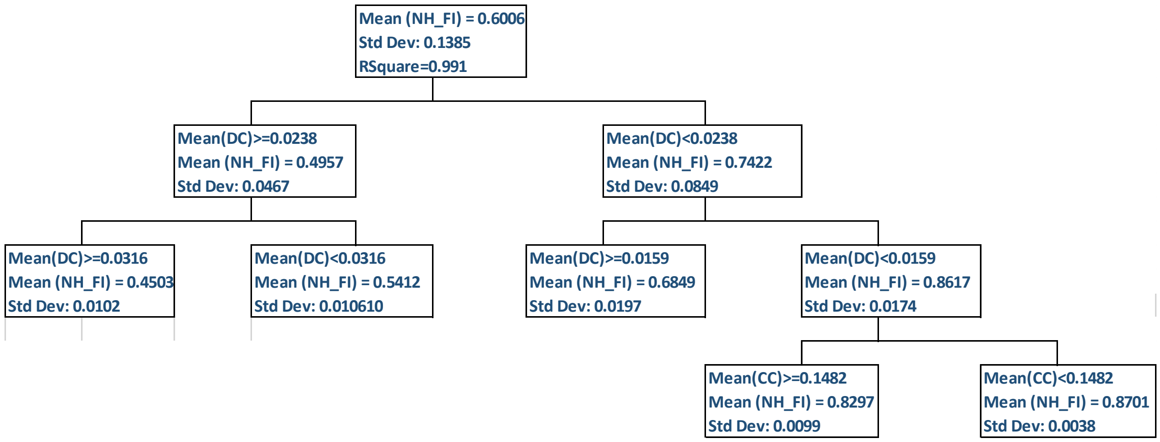
Appendix D

Correlation table of key influential characteristics

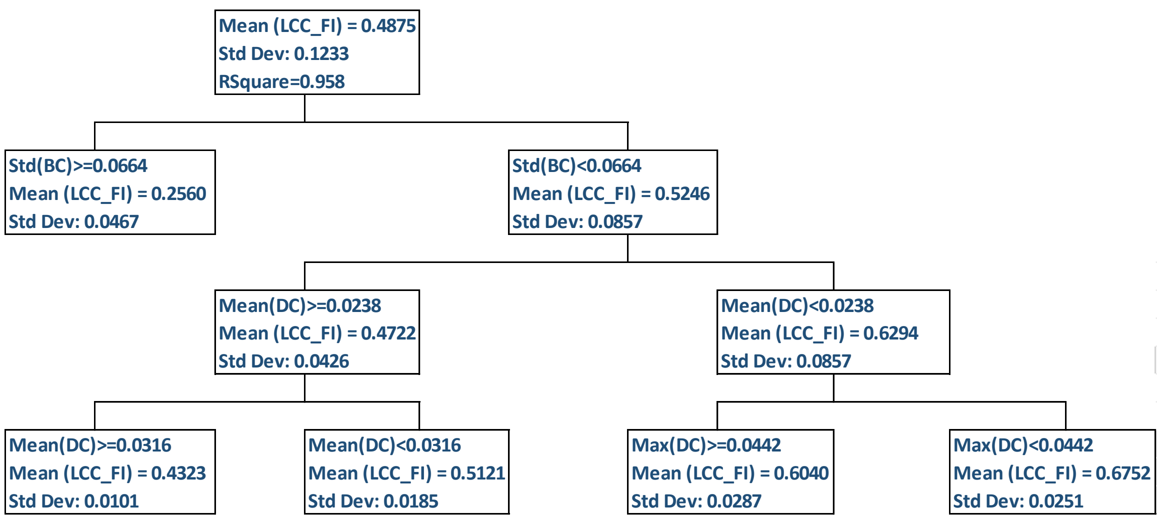
		(1)	(2)	(3)	(4)	(5)	(6)
Max(DC)	(1)	1					
Mean(DC)	(2)	0.404	1				
Max(BC)	(3)	-0.062	-0.737	1			
Std(BC)	(4)	-0.306	-0.710	0.901	1		
Max (CC)	(5)	0.590	0.886	-0.775	-0.884	1	
Mean(CC)	(6)	0.802	0.749	-0.580	-0.777	0.942	1

Appendix E

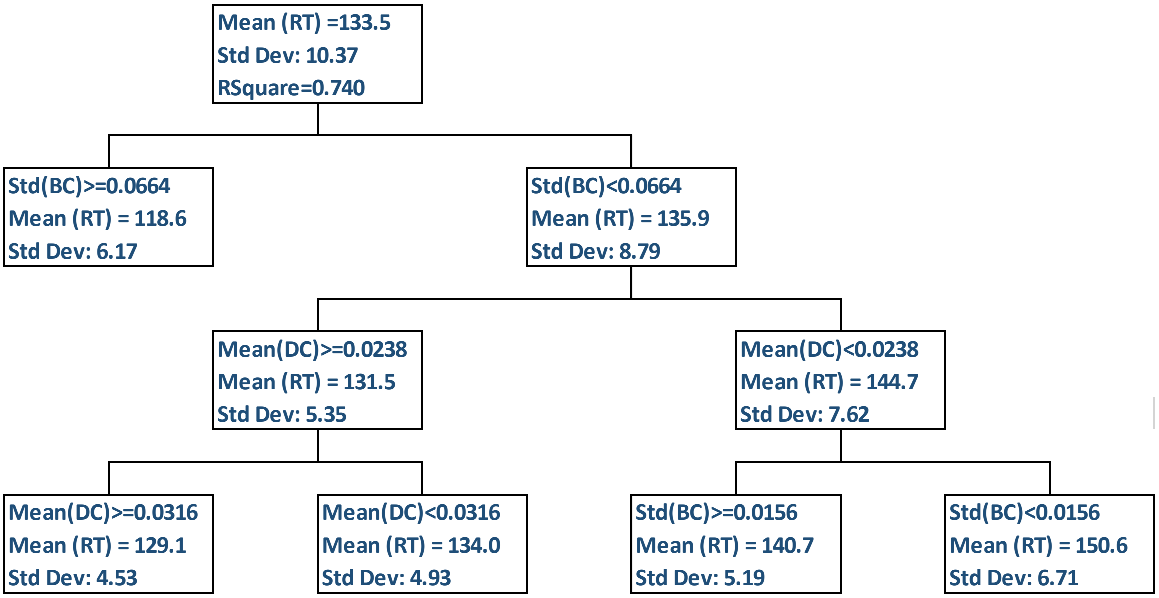
Decision Tree for Benchmark Process



NH_FI

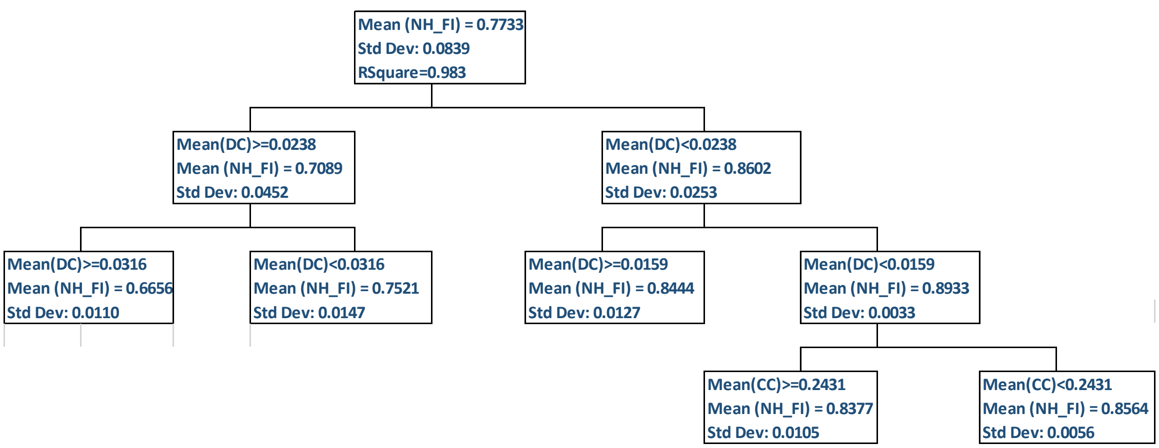


LCC_FI

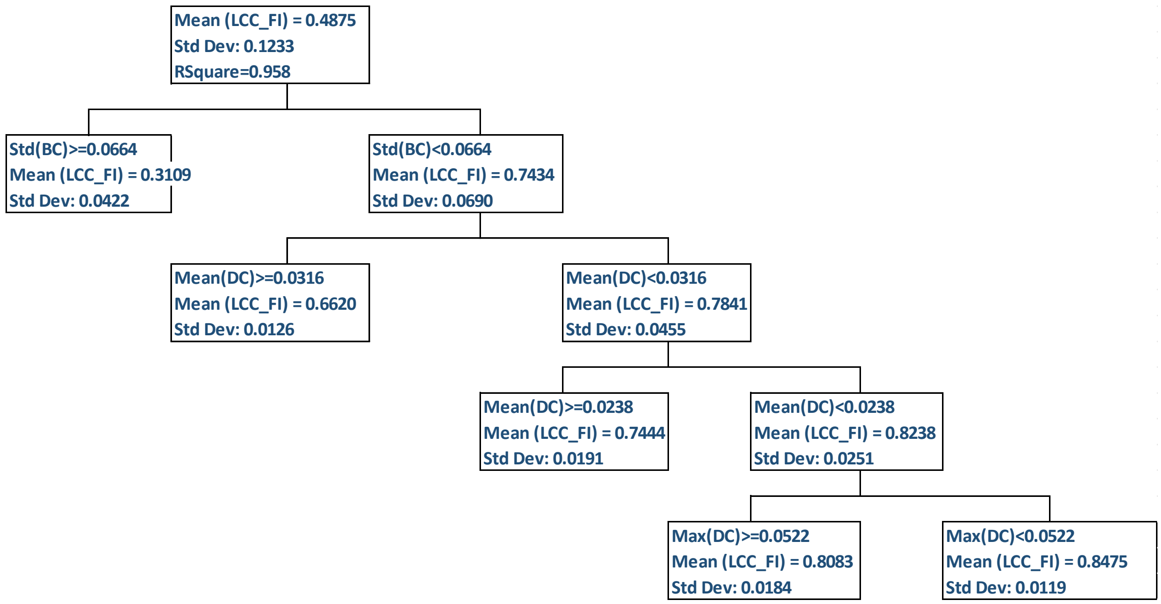


RT

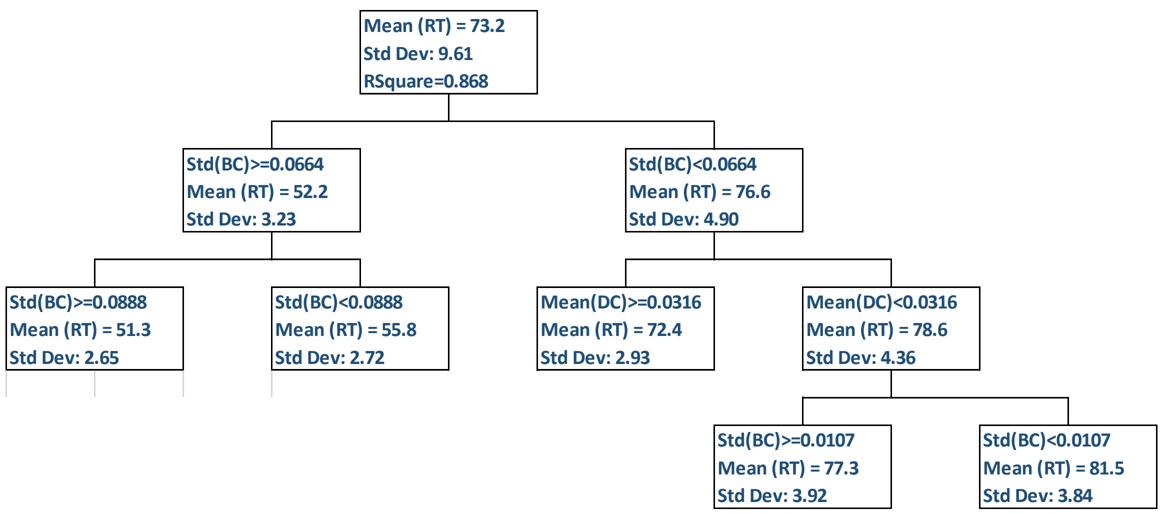
Decision Tree for Quick Recovery Process



NH_FI


Mean (LCC_FI) = 0.4875
Std Dev: 0.1233
RSquare=0.958
Std(BC)>=0.0664
Mean (LCC_FI) = 0.3109
Std Dev: 0.0422
Std(BC)<0.0664
Mean (LCC_FI) = 0.7434
Std Dev: 0.0690
Mean(DC)>=0.0316
Mean (LCC_FI) = 0.6620
Std Dev: 0.0126
Mean(DC)<0.0316
Mean (LCC_FI) = 0.7841
Std Dev: 0.0455
Mean(DC)>=0.0238
Mean (LCC_FI) = 0.7444
Std Dev: 0.0191
Mean(DC)<0.0238
Mean (LCC_FI) = 0.8238
Std Dev: 0.0251
Max(DC)>=0.0522
Mean (LCC_FI) = 0.8083
Std Dev: 0.0184
Max(DC)<0.0522
Mean (LCC_FI) = 0.8475
Std Dev: 0.0119

LCC_FI


Mean (RT) = 73.2
Std Dev: 9.61
RSquare=0.868
Std(BC)>=0.0664
Mean (RT) = 52.2
Std Dev: 3.23
Std(BC)<0.0664
Mean (RT) = 76.6
Std Dev: 4.90
Std(BC)>=0.0888
Mean (RT) = 51.3
Std Dev: 2.65
Std(BC)<0.0888
Mean (RT) = 55.8
Std Dev: 2.72
Mean(DC)>=0.0316
Mean (RT) = 72.4
Std Dev: 2.93
Mean(DC)<0.0316
Mean (RT) = 78.6
Std Dev: 4.36
Std(BC)>=0.0107
Mean (RT) = 77.3
Std Dev: 3.92
Std(BC)<0.0107
Mean (RT) = 81.5
Std Dev: 3.84

RT