Journal of Operations Management 33–34 (2015) 43–59

Contents lists available at ScienceDirect

Journal of Operations Management

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

Supply network disruption and resilience: A network structural perspective

Yusoon Kim[a,b,*], Yi-Su Chen[b,c], Kevin Linderman[b,d]

[a] College of Business, Oregon State University, Corvallis, OR 97331, United States
[b] Center for Supply Networks, Arizona State University, Phoenix, AZ 85004, United States
[c] Department of Management Studies, College of Business, University of Michigan—Dearborn, 19000 Hubbard Drive, FCS 184, Dearborn, MI 48126, United States
[d] Department of Supply Chain and Operations Management, Carlson School of Management, University of Minnesota, 321 19th Avenue South, Minneapolis, MN 54545, United States

ARTICLE INFO

Article history:
Received 10 January 2014
Received in revised form 1 August 2014
Accepted 16 October 2014
Available online 27 October 2014

Keywords:
Supply network disruption
Resilience
Graph theory
Complex networks
Network analysis

ABSTRACT

Increasingly, scholars recognize the importance of understanding *supply network disruptions*. However, the literature still lacks a clear conceptualization of a network-level understanding of supply disruptions. Not having a network level understanding of supply disruptions prevents firms from fully mitigating the negative effects of a supply disruption. Graph theory helps to conceptualize a supply network and differentiate between disruptions at the node/arc level vs. network level. The structure of a supply network consists of a collection of nodes (facilities) and the connecting arcs (transportation). From this perspective, small events that disrupt a node or arc in the network can have major consequences for the network. A failure in a node or arc can potentially stop the flow of material across network. This study conceptualizes supply network disruption and resilience by examining the structural relationships among entities in the network. We compare four fundamental supply network structures to help understand supply network disruption and resilience. The analysis shows that node/arc-level disruptions do not necessarily lead to network-level disruptions, and demonstrates the importance of differentiating a node/arc disruption vs. a network disruption. The results also indicate that network structure significantly determines the likelihood of disruption. In general, different structural relationships among network entities have different levels of resilience. More specifically, resilience improves when the structural relationships in a network follow the *power-law*. This paper not only offers a new perspective of supply network disruption, but also suggests a useful analytical approach to assessing supply network structures for resilience.

1. Introduction

Hendricks and Singhal (2005) found that an announcement of a supply disruption lowers a firm's stock returns on average by 20% six months after the announcement. Recent industry examples highlight the challenges that companies face in recovering from a disruption. For instance, Toyota had a supply network disruption in the aftermath of the 2011 tsunami in Japan. Six months later, Toyota had to idle some plants in North America due to shortage of parts (Ferreira, 2012). Some tsunami-stricken Japanese suppliers could no longer supply the North American plants, which shut them down. Several other examples have been documented, where supply disruptions in one part of the world created problems in another part of the world. One of the authors of this study worked with a multinational personal computer (PC) maker in the wake of the 2011 floods in Thailand, which then led to a disruption of the computer hard-disk industry. As the PC manufacturer executives were investigating their supply network, they became concerned about how a supplier "deep in the supply network" might disrupt their operations. In an increasingly globally connected world, managing supply disruptions involves more than just preventing disruptions at your facilities. It also requires a broader understanding of the overall structure of your supply network.

Many scholars have begun to study supply chain disruptions. These studies have largely focused on assessing vulnerabilities that firms face and/or capabilities they need to manage these vulnerabilities (Ellis et al., 2010; Sheffi, 2007). However, in many cases, supply disruptions (i.e., stoppages of material flows) do not originate from

* Corresponding author: College of Business, Oregon State University, Corvallis, OR 97331, United States. Tel.: +1 541 737 6066; fax: +1 541 737 4890..
E-mail addresses: yusoon.kim@bus.oregonstate.edu (Y. Kim), yisuchen@umich.edu (Y.-S. Chen), linde037@umn.edu (K. Linderman).

http://dx.doi.org/10.1016/j.jom.2014.10.006
0272-6963/© 2014 Elsevier B.V. All rights reserved.

a focal firm's facilities, but rather from its supply network. Also, disruptions at the local level do not necessarily lead to network-level disruptions. Consequently, a firm's failure to manage supply disruptions often stems from a lack of understanding of the supply network. Nonetheless, few studies to date have examined how the overall structure of a supply network can affect disruption risks. In addition, research has not offered a formal definition of a supply network disruption. As a result, empirical research cannot fully progress in this area. This study defines a supply network disruption and takes a network structural perspective to address the following questions: *how does the supply network structure influence disruptions, and how can one assess the resilience of supple network structure?*

From a structural perspective, a supply network can be viewed as a collection of nodes (facilities) and arcs (transportation linking facilities) (Borgatti and Li, 2009). A supply disruption thus depends on the structure of the nodes and arcs in the supply network. A disruption of a node or an arc sometimes has little overall effect, but other times can bring down the entire supply network—such as the Thailand floods did for the PC industry. Understanding the overall supply network structure and differentiating between node/arc-level and network-level disruptions can help better manage supply disruptions. Drawing on graph theory, this paper advances a more precise definition of supply network disruption. The definition has implications for how to understand and manage supply disruptions at the network level. An analysis of basic supply network structures demonstrates that the structure of the nodes and arcs in a supply network strongly determines its risk of disruption and resilience. In particular, a supply network will become more resilient when the overall structure of the nodes and arcs follow a *power-law* distribution. Consequently, firms will benefit from a deeper understanding of supply network structure and how it influences disruption risk and resilience at the network-level.

The rest of this article is organized as follows. Section 2 reviews the literature on supply network disruption and resilience. Section 3 draws on graph theory to conceptualize a supply network, disruption, and resilience. Section 4 develops the four basic supply network structures based on the literature and compares these structures on network resilience. Section 5 advances propositions about the connection between supply network structure and resilience. Finally, Section 6 discusses the implications of this study for research and practice.

2. Literature on supply network disruption and resilience

The literature has taken various perspectives on examining supply disruptions and resilience, including behavioral (e.g., Ellis et al., 2010; Wagner and Neshat, 2010), conceptual (e.g., Christopher and Peck, 2004; Kovács and Tatham, 2009; Tang, 2006), qualitative (e.g., Craighead et al., 2007; Jüttner et al., 2003; Sheffi and Rice, 2005), and simulation/modeling (e.g., Nair and Vidal, 2011; Wu et al., 2007; Zhao et al., 2011). For instance, Ellis et al. (2010) used a survey to study how firms make decisions in the face of supply disruptions. Christopher and Peck (2004) offered a conceptual model to classify some sources of supply chain risks and suggest how to overcome those risks. Craighead et al. (2007) employed structured interviews and critical incident technique to understand why disruption severity varies among supply chains. Wu et al. (2007) utilized a modeling approach to understand the propagation of disruptions across supply chain systems. In terms of the level of analysis, the literature also varies from the firm level, to the supply chain, to the supply network. Although this research has produced useful insights from a range of different perspectives, it has also led to confusion—especially when it comes to the level of analysis. Consequently, the literature uses different terms and concepts to define and assess supply network level disruptions and resilience.

In the literature, a supply network disruption is generally defined as an unplanned and unanticipated event that disrupts the normal flow of goods and materials in a supply network (Craighead et al., 2007; Hendricks and Singhal, 2003; Kleindorfer and Saad, 2005; Svensson, 2000), and viewed as a major source of firms' operational and financial risks (Stauffer, 2003). This definition, while offering a general description, does not clearly specify the level at which the disruption occurs and the scope of its effect. This becomes an important distinction since the cause and effect may occur at different levels. The Toyota example serves as a case in point—a disruption occurred in a component plant in Japan (a cause at the node-level), which led to a shutdown in their North American truck production (the effect at the supply network-level). Failure to make this distinction has implications for how we understand and manage disruptions.

The concept of network resilience also has important implications in understanding supply network disruptions (Sheffi, 2007). However, the literature gives no clear consensus on the definition of resilience in the context of supply network disruptions. Table 1 summarizes existing definitions, measures, and levels of analysis of the supply network disruption and resilience. The literature does not provide a clear formal definition of supply network resilience. Some define it as a property (Longo and Oren, 2008), while others describe it as a capability of the supply network (Christopher and Peck, 2004). Still others view resilience as both an inherent property (to absorb shock) and an ability to adapt to changes (Johnson et al., 2013). Furthermore, although scholars have treated the term "disruption" as a companion concept to resilience (Scholten et al., 2014), in many cases they do not formally define "disruption" and assume that it is clearly understood. Ambiguous definitions can lead to confusion and impede scholarly development (Wacker, 2004).

In addition, not clarifying the level of analysis when defining and theorizing about supply network disruptions exacerbates the problem. The literature shows inconsistencies and ambiguity when it comes to the level of analysis. This becomes problematic since the behavior of a network emerges from its elements. For example, Wu et al. (2007) described a supply chain disruption as a "disruption at a susceptible *location* in the supply chain" (p. 1677, emphasis added), which indicates a disruption as defined at the node level. The authors then took a network perspective in their analysis to show how far-reaching the effect of a disruption can propagate across a supply chain. Consequently, there is a disconnect between the conceptual definition (at the node level) and analysis (at the network level). Similarly, Craighead et al. (2007) defined supply chain disruptions as "unplanned and unanticipated events that disrupt the normal flow of goods and materials." Then, they proposed the *node criticality* notion to refer to the importance of a *node* within a supply chain and describe it as what eventually determines the severity of a supply chain-wide disruption. The assumption is that a disruption at a critical node invariably leads to a system-wide disruption via cumulating serious consequences across the entire supply chain. Their definition of supply chain disruption does not clarify or distinguish its cause and effect, leading to inconsistency in the level of focus between definition and analysis. Although these papers advanced our understanding of supply disruptions, at the same time, they lacked clarity.

According to Wacker (2004), a good (operational) definition should be "a concise, clear verbal expression of a unique concept that can be used for strict empirical testing" (p. 631). Nonetheless, few studies (except for Sheffi and Rice, 2005; Zhao et al., 2011) have offered a clear definition at the supply network level, let alone analytical measures. Further, much of the research is qualitative in nature, largely relying on event or case studies (with

Table 1
Existing research on supply network disruption and resilience.

References[a]	Definition		Level of definition and analysis	Methods/nature of study	Main findings
	Conceptual definition	Operational measures[b]			
Jüttner et al. (2003)	• Disruption (vulnerability) as "the propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse supply chain consequences"	• Disruption as possibility and effects of risks in supply chains (e.g., demand volatility, operational risks, human risks, market risks, political risks etc.)	• Unclear level of definition	• Literature review	• Identify an agenda for future research and provide working definitions of supply chain vulnerability and risk management based on the extant literature
	• Resilience not defined or discussed	• No operational measures for resilience	• Multi-level risk sources: firm, supply network, & environmental	• Qualitative (based on semi-structured interviews)	
Christopher and Peck (2004)	• Disruption as "an exposure to serious disturbance"	• No operational measures for disruption	• Network-level definition	• Conceptual	• Propose four principles (capabilities) to create a resilient supply chain: build-in resilience when designing a supply chain, collaboration across corporate entities, agility, and risk awareness culture
	• Resilience as the ability of a supply chain to return to its original state or move to a new, more desirable state after being disturbed	• Resilience as four mixed-level capabilities: supply chain (re)engineering, agility, collaboration, and risk awareness culture	• Unclear level of analysis	• Qualitative	
Sheffi and Rice (2005)	• Disruption not defined.	• No operational measures for disruption	• Node-level definition	• Qualitative	• Classify disruptions into random events or intentional disruption
	• Resilience as the ability of a company to bounce back from a disruption and can be achieved by either creating redundancy or increasing flexibility	• Resilience as competitive position, supply chain responsiveness	• Network-level analysis	• Interviews	• Propose a vulnerability framework and illustrate how to make use of it to identify potential disruptions
	• Firm-level resilience depends on network-level responsiveness				• Suggest creating redundancy and increasing flexibility as ways to build in resilience in a supply chain.
Tang (2006)	• Disruption not formally defined but just referred to as a major factor that has long-term negative effects on a firm's financial performance	• N.A. (operational measures for disruption or resilience not discussed)	• Unclear level of definition	• Conceptual	• Certain "robust" supply chain strategies are presented that are characterized as cost-effective and time-efficient, including postponement, strategic stock, flexible supply base, make-and-buy, economic supply incentives, flexible transportation, revenue management, dynamic assortment planning, silent product rollover
	• Resilience not formally defined, but just referred to as a situation where a firm can deploy the contingency plans efficiently/effectively when facing a disruption.		• Unclear level of analysis	• Qualitative (based on industry anecdotes)	
Craighead et al. (2007)	• Disruption as unplanned and unanticipated events that disrupt the normal flow of goods and materials within a supply chain (adapted from Kleindorfer and Saad, 2005, Stauffer, 2003, and Svensson, 2000)	• Disruption as the number of nodes in a supply network whose ability to ship and/or receive goods and materials (i.e., both outbound and inbound flow) has been hampered	• Node-level definition	• Qualitative	• Six propositions to prescribe relations among supply network properties, where severity of supply chain disruption is viewed as a function of supply chain density, supply chain complexity and node criticality
	• Resilience not defined, but referred to Sheffi & Rice (2005).	• No operational measures for resilience	• Unclear level of analysis: network-level of analysis often implied	• Multi-source, multi-method approach: single case study, structured interview with 9 firms, focus groups via critical incident technique	

Table 1 (*Continued*)

References[a]	Definition		Level of definition and analysis	Methods/nature of study	Main findings
	Conceptual definition	Operational measures[b]			
Wu et al. (2007)	• Disruption as unexpected events occurring in a supply chain	• N.A. (operational measures for disruption or resilience not discussed)	• Node-level definition (implied)	• Analytical	• Present a network-based approach to model supply chain systems to determine how changes/disruptions affect supply chains and how far the effects propagate in supply chains
	• Resilience not defined or discussed		• Network-level analysis (implied)	• Disruption Analysis Network by using Petri net-based modeling approach	• The network approach also embeds decision-making logic into the network
Longo and Oren (2008)	• Disruption not formally defined but just referred to as various firm-level disruptive events such as strike	• N.A. (operational measures for disruption or resilience not discussed)	• Supply chain- or network-level definition	• Qualitative	• Suggest four-stages supply chain resilience improvement scheme from a change management perspective: (1) identify strategic business decisions and effects of each decision on supply chain vulnerability; (2) identify actual guidelines; (3) categorize risks at each level; (4) map out a change process
	• Resilience as a property that allows a supply chain to react to internal/external risks/vulnerabilities, quickly recovering an equilibrium state capable of guarantying high performance/efficiency.		• Unclear level of analysis	• Literature review	
Kovács and Tatham (2009)	• Disruption defined as large-scale unpredictable events and a type of supply chain risks, different from operational vulnerabilities	• N.A. (operational measures for disruption or resilience not discussed)	• Unclear level of definition	• Conceptual	• Use resource-based view (RBV) as the theoretical lens
	• Supply chain risks consider all kinds of events from operational vulnerabilities to operational catastrophes disruptions. • Resilience not discussed.		• Level of analysis: ambiguous but network-level implied	• Literature review	• Focus on how configurations of military vs. humanitarian organizations in their dormant state to determine capabilities needed to respond to large-scale disruptions
Ponomarov and Holcomb (2009)	• Disruption not formally defined but sources of disruptions are discussed	• No operational measures for disruption.	• Network-level definition	• Qualitative	• Review the "resilience" concept from the ecological, psychological, organizational, as well as emerging interdisciplinary research streams, including emergency management and sustainable development perspective, and supply chain risk management perspective
	• Resilience as the adaptive capability of a supply chain to prepare for unexpected events, react to disruptions, and recover from them by maintaining continuity of operations and control over structure and function	• Resilience as logistics capability	• Unclear level of analysis	• Literature review	
Ellis et al. (2010)	• Disruption as unforeseen events that interfere with the normal flow of goods and/or materials within a supply chain [adapted from Craighead et al., 2007]	• Disruption as the overall disruption risk including the probability & magnitude of disruption	• Network-level definition	• Empirical	• Examine the effects of probability and magnitude of disruptions on overall perceived supply disruption risk, which in turn affects buyers' search for alternative suppliers
	• Resilience not discussed.	• No operational measures for resilience	• Unclear level of analysis	• Survey	

Table 1 (*Continued*)

References[a]	Definition		Level of definition and analysis	Methods/nature of study	Main findings
	Conceptual definition	Operational measures[b]			
Wagner and Neshat (2010)	• Disruption as "the trigger that leads to the occurrence of risk" (p. 122)	• Not operational measures for disruption discussed; but instead, supply chain vulnerability drivers categorized into demand side, supply side, and supply chain structure	• Unclear level of definition	• Empirical	• Propose a SCVI (supply chain vulnerability index) metric that can be used to assess the vulnerability of supply chains and compare vulnerabilities of supply chains across industries
	• A related concept, "vulnerability" is discussed • Resilience not discussed	• No operational measures for resilience	• Level of analysis: multiple & mixed (a firm, supply chain, industry, and entire economy)	• Survey	
Jüttner and Maklan (2011)	• Disruptions "imply a certain level of turbulence [Hamel and Valikangas, 2003] and uncertainty in the supply chain [van der Vorst and Beulens, 2002]" (p. 247)	• No operational measures for disruption	• Network-level definition	• Qualitative	• Suggest that supply chain risk and knowledge management enhance resilience by improving flexibility, visibility, velocity and collaboration capabilities at the supply chain/network level
	• Resilience defined by flexibility, velocity, visibility, and collaboration capabilities (adapted from Ponomarov and Holcomb, 2009)	• Resilience measured as flexibility capability, velocity capability, visibility capability, & collaboration capability	• Network-level analysis with emphasis on a focal firm	• Singe case study (a firm with its three supply chains)	
Nair and Vidal (2011)	• Disruption not formally defined	• Disruption as random failure and targeted attack on network nodes (firms) for their inventory levels, backorders, and total costs	• Network-level definition	• Analytical	• Certain established network characteristics (such as average path length, clustering coefficient, size of the largest connected component) are associated with the robustness of supply networks (to random failures/targeted attacks on demand and uptime of nodes)
	• Resilience (robustness) not formally defined	• Resilience (robustness) as multiple network attributes such as average path length, clustering coefficient, size of the largest connected component (LCC), and max. distance between nodes in the LCC	• Firm-level analysis	• Simulation (agent-based modeling)	
Zhao et al. (2011)	• Disruptions "affect the normal operations" (p. 1) and are either random or targeted	• No operational measures for disruption	• Network-level definition	• Analytical	• Suggest centrality as a measure for a node's importance.
	• Resilience as the ability to maintain operations and connectedness under the loss of some structures or functions (i.e., removal of nodes)	• Resilience as availability (percentage of demand nodes that have access to supplies), connectivity (size of the largest functional sub-network), and accessibility (average and max. supply path length)	• (Logistics) network-level analysis	• Simulation	• Rank network resilience in case of random disruptions: hierarchy > scale-free > DLA (degree and locality-based attachment) > random • Rank network resilience in case of targeted disruptions: random > DLA > scale-free > hierarchy
Johnson et al. (2013)	• Disruption not formally defined	• No operational measures for disruption	• Network-level definition	• Qualitative	• Argue that three dimensions of social capital enable and facilitate four formative capabilities of resilience identified by Jüttner and Maklan (2011)
	• Definition of resilience borrowed from Ponomarov and Holcomb (2009) • Acknowledge the dualism of resilience as the abilities to absorb shock and the ability to adapt to change	• Resilience as flexibility, velocity, visibility, collaboration (borrowed from Jüttner and Maklan (2011)	• Network-level of analysis with emphasis on a focal firm	• Single case study	• There social capital dimensions are structural (network ties, network configuration, appropriable organization), cognitive (shared codes/language, shared narratives), and relational (trust, norms, obligations, identification)

Table 1 (*Continued*)

References[a]	Definition		Level of definition and analysis	Methods/nature of study	Main findings
	Conceptual definition	Operational measures[b]			
Scholten et al. (2014)	• Borrowed from Craighead et al. (2007) definition of disruption	• No operational measures for disruption discussed	• Network level definition	• Qualitative	• Develop an integrated supply chain resilience framework by integrating the five capabilities (adapted from Christopher and Peck, 2004) and a four-phase disaster management process (mitigation, preparedness, response, and recovery)
	• Resilience in supply chain context, defined as an ability of supply chains to recover from inevitable and unexpected disruptions • Resilience in disaster management, defined as an ability of an individual, a household, a community, a country or a region to withstand, adapt, and quickly recover from stresses and shocks	• Resilience as adaptive capability to prepare for, respond to, and recover from disruption, including horizontal and vertical collaboration, supply chain (re)engineering, agility (flexibility), risk awareness, and knowledge management	• Network level of analysis with emphasis on a focal firm	• Single case study	• Knowledge management capability was added as a fifth formative resilience element

[a] References listed by year of publication.
[b] Measures used to operationalize supply chain/network disruption or resilience.

several exceptions including Ellis et al., 2010; Wagner and Neshat, 2010). This naturally constrains the research for its scope and level of analysis. In characterizing and assessing disruption and resilience, the research has largely overlooked the overall structure of a supply network, while its importance has been acknowledged (Christopher and Peck, 2004; Johnson et al., 2013). Consequently, the findings are insightful, whereas their generalizability and applicability become rather limited. This study aims to fill the observed gaps in the extant literature, and to that end, it is imperative to understand the basic components of a supply network structure. Adopting a network structural perspective, we propose a more precise, formal definition of supply network disruption and resilience, in which we clarify the nature of these network-level phenomena. This involves distinguishing between node/arc-level vs. network-level disruptions, which in turn helps clarify the definition of supply network resilience (Ponomarov and Holcomb, 2009).

3. Conceptualizing supply network disruption and resilience

3.1. Supply network from a graph-theoretic perspective

Graph theory provides a foundation for conceptualizing a supply network[1] (Diestel, 1991). Graph theory originated from Leonard Euler's famous Seven Bridges of Königsberg problem (Euler, 1741). The problem was to find a walk through the city that would cross each of the seven bridges once and only once (Gross and Yellen, 2006). Euler's Seven Bridges problem has structural similarities to moving physical goods across a supply network. This basic problem gave rise to an area of study called graph theory. A graph is a collection of nodes connected by arcs. The concept of a graph has been widely applied to various complex networks, which include the World Wide Web, power grids, and food webs (Gross and Yellen, 2006; Newman, 2010).

Scholars have begun to draw on graph theory to understand supply networks (e.g., Adhitya et al., 2007; Wagner and Neshat, 2010). Recently some have applied graph theory to examine supply chain risks and vulnerabilities (Thun et al., 2011; Wagner and Neshat, 2010), but there have been limited applications to theory development. For instance, Wagner and Neshat (2010) used graph theory to come up with a vulnerability index for individual nodes in a supply network. However, they did not distinguish a node-level disruption from a network-level disruption. Our study draws on graph theory to understand the difference between a node/arc-level disruption and a network-level disruption.

From a graph-theoretic perspective, a supply network can be characterized as a collection of nodes (facilities) and arcs connecting nodes (transportation). Understanding the basic elements (i.e., nodes and arcs) and their configuration in a supply network thus can help define and more precisely assess supply network disruption and resilience. Graph theory helps characterize the underlying structure of a supply network. As a result, graph theory helps to conceptualize supply network disruption and resilience, and understand how different supply network structures affect resilience. From this structural perspective, we examine the various network level metrics and basic supply network structures to understand network-level supply disruption and resilience.

In general, graph theory provides an analytical lens to characterize the structural relations among the nodes and arcs in a network (Gross and Yellen, 2006). Table 2 summarizes the terms used to describe a supply network from a graph-theoretic perspective. More formally, a graph, denoted as $G=(N, A)$, consists of two sets, where the elements in the set N and those in the set A are called *nodes* and *arcs*, respectively. Each *arc* in the set A connects two *nodes*, called endpoints. A directed graph or *digraph* is a graph with directed arcs, and each arc has one endpoint designated as *tail* and the other as *head*. This indicates the direction of flow of goods in the supply network. Fig. 1 illustrates a digraph of a supply

[1] Throughout the paper, the supply network refers to the physical supply network.

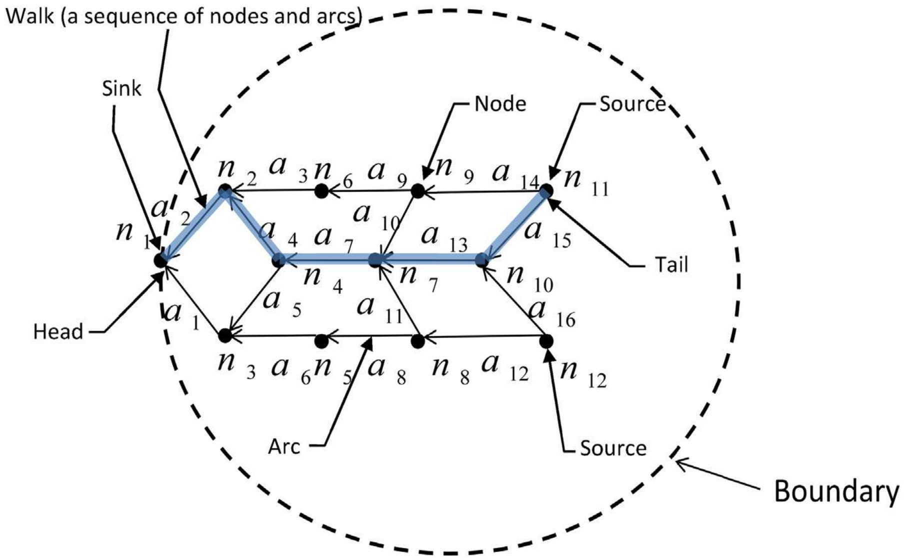


Fig. 1. Supply network.

network (SN) with the following structural relationships: SN = (N, A), where $N = \{n_1, \ldots, n_{12}\}$ and $A = \{a_1, \ldots, a_{16}\}$.

Some basic concepts in graph theory help understand the structure of a supply network, which leads to a definition of supply network disruption. The *degree* of a node is the number of arcs attached to the node. The *in-degree* is the number of arcs whose head connects to the node, and *out-degree* the number of arcs whose tail connects to the node. For instance, in Fig. 1 the node n_2 has out-degree, $Out\,(n_2)$ equal to 1 and in-degree, $In\,(n_2)$ equal to 2. That is, node n_2 receives physical supply from nodes n_4 and n_6 via the arcs a_4 and a_3, respectively, and supplies node n_1 via arc a_2. A *sink* node is a node with zero out-degree but positive in-degree, and a *source* node is a node with zero in-degree but positive out-degree. A *walk* in a digraph is an alternating sequence of nodes and arcs where two nodes are connected by the tail and head of an arc. In Fig. 1, $W = \{n_{11}, a_{14}, n_9, a_9, n_6, a_3, n_2, a_1, n_1\}$ is a walk from n_{11} (source) to n_1 (sink). The walk W gives one possible path where physical supply could start at node n_{11} (source) and traverse the supply network to end up at node n_1 (sink).

This study defines a *connected* supply network as a digraph, i.e., a network where there exists at least one walk between the source and the sink nodes[2]. In other words, in a connected supply network, it is possible to get physical supply from the source node(s) to the sink node. Consequently, we define *connectivity* of a supply network as the minimum number of nodes and/or arcs that can be removed from the network until it becomes disconnected (Gross and Yellen, 2006). For instance, the supply network in Fig. 1 has connectivity of 2. Disconnecting the network requires removing at least two elements, such as two arcs (a_1 and a_2), or one arc (a_2) and one node (n_3).

From a supply network perspective, nodes represent facilities such as factories, warehouses, depots, or retail outlets, where physical goods are stored. Arcs represent conveyance mechanisms between the nodes, such as air, ship, truck, rail transportation, where physical goods are in transit from one node to the next. Each arc has tail and head to indicate the direction of a physical flow. The in-degree and out-degree give the number of a given node's own suppliers and customers, respectively.

How one characterizes a supply network depends on whose perspective you take. Different participants in a supply network will have different perspectives of what the network looks like. For instance, in the automobile industry, the retailers, final assemblers, and part suppliers all have different perspectives of the supply network structure. Since everything is ultimately connected to everything else, a boundary helps establish the scope of analysis of supply networks. This study anchors its perspective of a supply network on a focal node, such as a final assembler in the automobile industry. That is, a supply network is bounded by a focal firm and various suppliers connected, either directly or indirectly, to the focal firm. The focal firm thus becomes the final destination of the physical flows, i.e., the sink node in the supply network, and the source node is where the raw material originates. Fig. 1 illustrates a supply network mapped from the perspective of the sink node n_1, along with the network boundary, delimited by a dotted line, in which there are two material sources, n_{11} and n_{12} and one sink, n_1.

3.2. Disruption and resilience in supply networks

3.2.1. Node and arc level disruptions

Disruptions are unplanned and unanticipated events that prevent the normal materials flow through a supply network (Svensson, 2000; Craighead et al., 2007). We argue that a clear distinction should be made between disruptions at the node/arc level vs. network level. From a graph-theoretic perspective, a disruption at the node/arc level occurs by removing a node or an arc from the supply network graph. That is, the node or the arc becomes inoperable and material no longer flows through the node or along the arc. Suppose, for example, the arc a_{14} in Fig. 2a was removed from the network. Namely, the conveyance mechanism between n_{11} and n_9 had an unplanned outage and no longer operates. From a graph-theoretic perspective, this induces a sub-graph (a graph resulting from removing nodes/arcs from the original graph). Fig. 2b shows a sub-graph induced by removing arc a_{14}, which is SN = (N, A) − a_{14}.

Notice that even without a_{14}, there still exist walks between the two sources (n_{11} and n_{12}) and the sink node (n_1). For instance, $W_1 = \{n_{11}, a_{15}, n_{10}, a_{13}, n_7, a_7, n_4, a_4, n_2, a_2, n_1\}$ is a walk from n_{11} to n_1 and $W_2 = \{n_{12}, a_{12}, n_8, a_8, n_5, a_6, n_3, a_1, n_1\}$ is a walk from n_{12} to n_1. As a result, even with an arc-level disruption (a_{14} removed), physical material can still flow across the network. Fig. 2c shows another

[2] Graph theory defines a connected graph in a slightly different way. In the theory, a graph is more generally defined as connected if for every pair of nodes u and v there is a walk from u and v (Gross and Yellen, 1998). In this paper, we adapt this definition to the supply network setting.

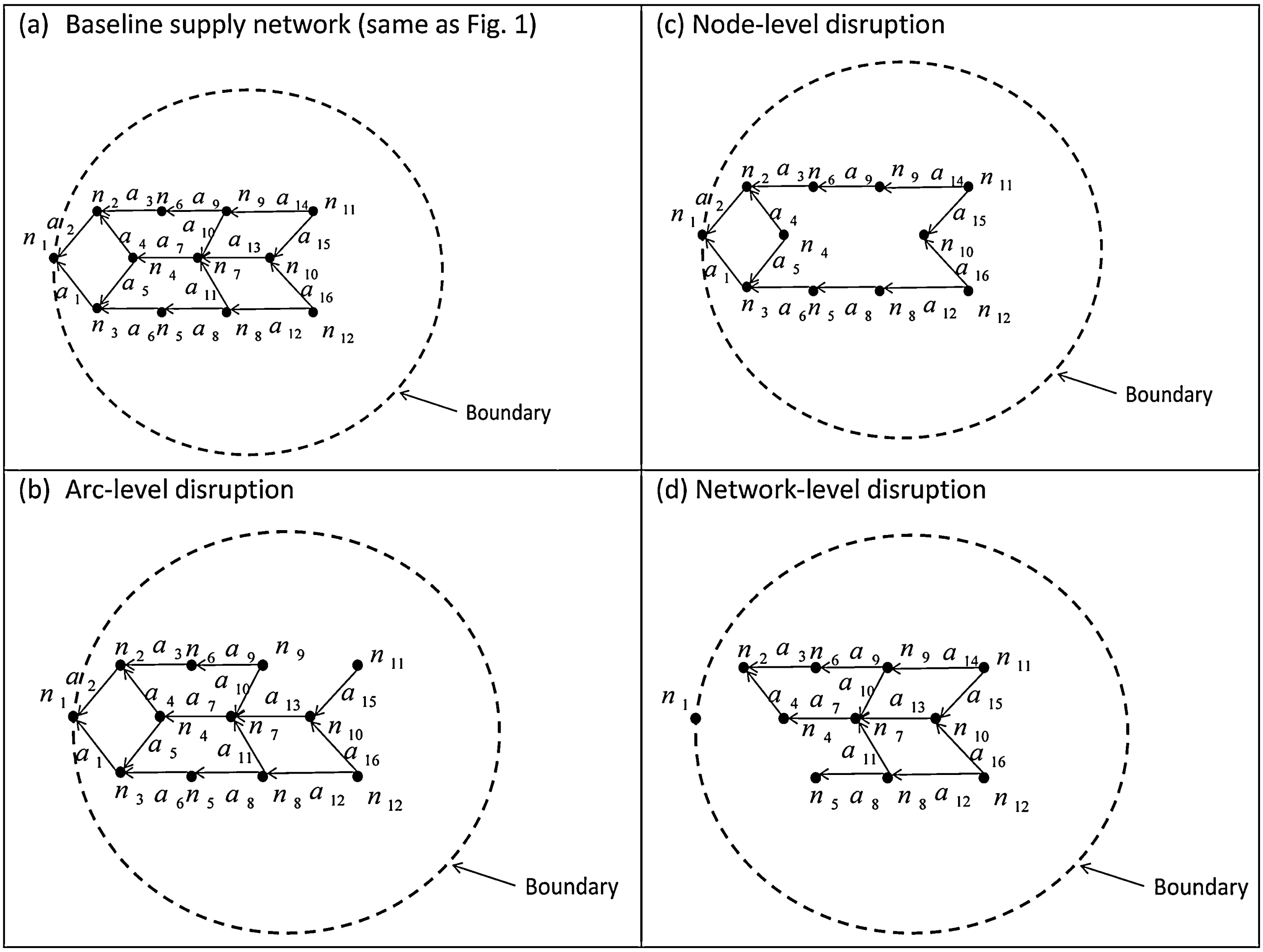


Fig. 2. Examples of supply disruptions at arc-, node-, and network-level.

sub-graph made by removing n_7, SN = $(N, A) - n_7$. Once n_7 becomes inoperable, then all the arcs attached to n_7 also become inoperable. Note, however, there still exist walks between the source nodes and the sink node; specifically $W_1 = \{n_{11}, a_{14}, n_9, a_9, n_6, a_3, n_2, a_1, n_1\}$ is a walk from n_{11} to n_1 and $W_2 = \{n_{12}, a_{12}, n_8, a_8, n_5, a_6, n_3, a_1, n_1\}$ is a walk from n_{12} to n_1. That is, despite the node-level disruption (n_7 removed), material can still flow through the network to the sink node.

In sum, the above examples illustrate that a disruption at either the node or arc level does not necessarily lead to a network-level disruption. Interestingly, one may consider the node n_7 critical to the network since it has the highest degree (in-degree plus out-degree) in the network. Nonetheless, the disruption of this node does not disrupt the entire supply network. This poses the question: *What kinds of disruption will lead to a disruption of the entire supply network?*

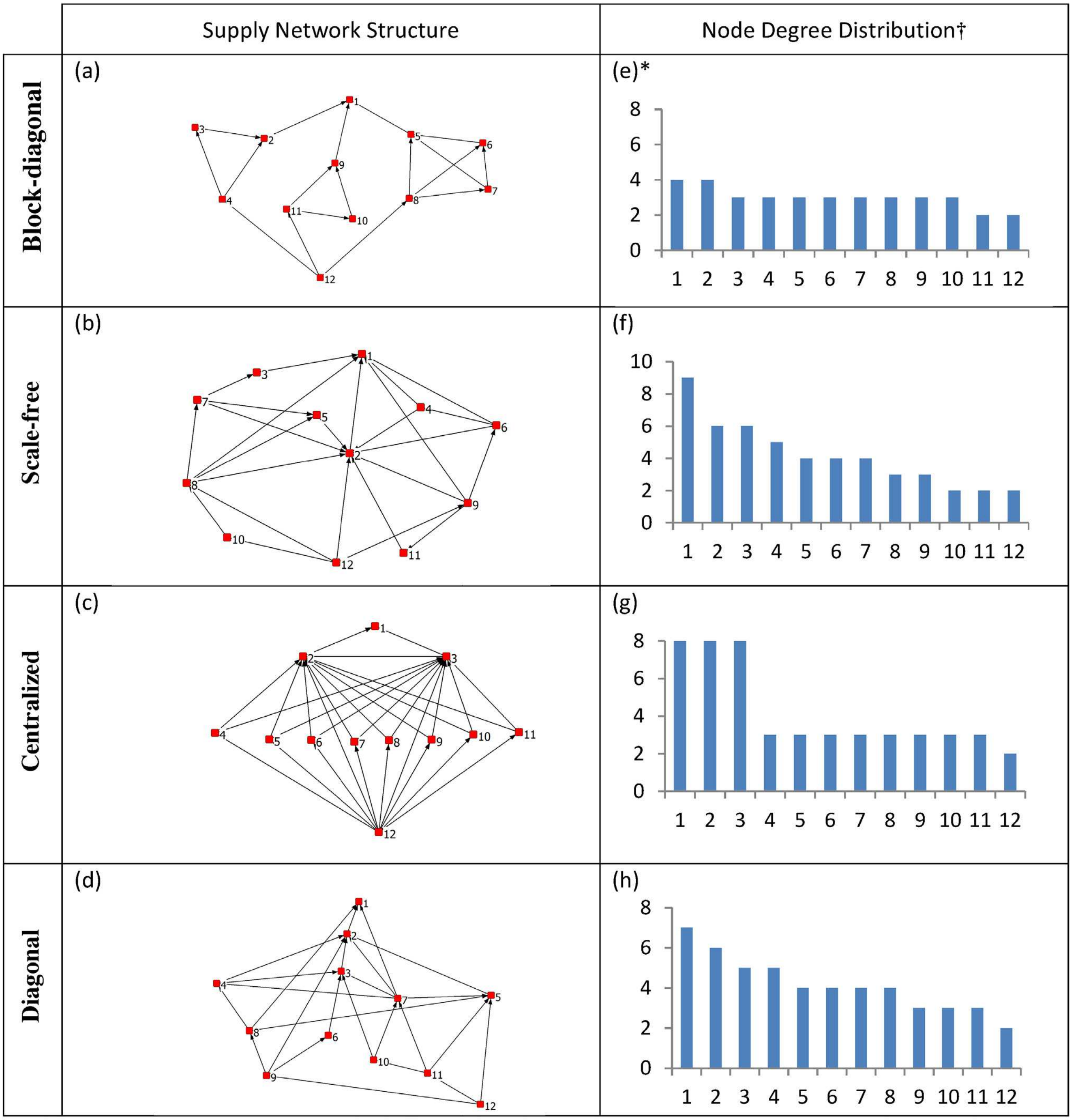
3.2.2. Network level disruption and resilience

We define a *supply network disruption* as a situation where there no longer exists a walk between the source(s) and sink node as a consequence of a disruption(s) in nodes or arcs. That is, the supply network becomes disconnected. However, as in the above examples, a disruption at a node (n_7) or arc level (a_{11}) may not lead to a disruption at the network level. Fig. 2d shows another situation, in which a disruption occurred with both the node n_3 and the arc a_2, SN = $(N, A) - n_3 - a_2$. As a consequence of removing the two elements, n_3 and a_2, from the supply network, there no longer exists a walk between the sources and sink node. This illustrates a situation where node/arc-level disruptions led to a network-level disruption. Here, one may conclude that a network-level disruption involves invariably more than one disruption in a node and/or arc. However, a disruption of a single node/single arc could also lead to a disruption of an entire network, which depends on the (relative) positions of nodes/arcs in the network and the overall network structure.

Taken together, the above illustrations point out the need to differentiate between a node/arc-level disruption and a network-level disruption. These illustrations also suggest that the positions, or structure, of nodes (facilities) and arcs (transportation) in a supply network affects its disruption risk. In other words, the overall configuration of the nodes/arcs in a network influences the extent to which the network stays connected or *resilient*. While network resilience can be defined in a number of ways (Newman, 2010), in keeping with our definition of a supply network disruption, we define *supply network resilience* as a network-level attribute to withstand disruptions that may be triggered at the node or arc level. Consequently, supply network resilience is an emergent structural property of a supply network. Therefore, different network structures will have different degrees of supply network resilience.

4. Supply network structures and resilience

Complex adaptive systems theory provides a useful theoretical framework for examining supply network structures (Langton, 1990; Kauffman, 1993). Based on this theory, researchers have developed analytic frameworks for studying the relations among



† The degree denotes the total degree, including both in-degree and out-degree for every node in the network.
* Horizontal axis rank-orders the 12 nodes by degree, and vertical axis denotes the corresponding node degree.

Fig. 3. Four basic supply network structures and the correspondent node degree distributions.

the elements of a system. In particular, the *NK* model helps understand complex systems (Kauffman and Levin, 1987; Kauffman, 1993). This model focuses on the interactions (or connections) of the elements in a system and their system-wide impact. This helps assess the structure of the supply network elements and the associated broad-scale impact on the overall supply network. Under the *NK* model, *N* refers to the number of elements (i.e., nodes) in a system and *K* refers to the degree of interaction among the elements (i.e., arcs). For instance, if $N = 10$ and $K = 2$, then there are 10 nodes and the average of 2 arcs per node (a total of 20 interactions [arcs]) in the network.

Scholars have identified some archetypes that can characterize basic network structures (Ghemawat and Levinthal, 2008; Rivkin, 2000; Rivkin and Siggelkow, 2003, 2007; Schilling and Phelps, 2007). They include: random, local, small-world, block-diagonal, scale-free, preferential-attachment, centralized, dependent, hierarchical, and diagonal. Rivkin and Siggelkow (2007) applied these structures to decision-making models, where they hold $N \times K$ (or *NK*) constant and investigate the effects of different structures at the same level of complexity. In this study, we adapt these fundamental structures to represent basic supply network structures. This analysis focuses on *four* basic network structures that

Table 2
Terminologies and definitions for supply network graphs.

Term	Definition	Denotation/example*
Graph	A structure defined by a set of nodes and a set of arcs which depicts a supply network	$G = (N, A)$/Fig. 1
Node	A point on a graph, which represents a physical location in a supply network (e.g. manufacturing facility, warehouse, retail store)	n_i, For $i = 1, \ldots, 12$
Arc	A line that connects to points in a graph, which represents a conveyance mechanism between two physical locations in a supply network (e.g. railroad shipping from a manufacture to a warehouse)	a_i, For $i = 1, \ldots, 12$
Digraph	A graph where all arcs have the head and tail, which gives a direction from one node to another node, whereby indicating the direction of the overall network flow. In a supply network, this represents the direction of the overall flow of physical goods (e.g. a railroad ships from the manufacture to the warehouse)	Fig. 1
Tail	One end of the arcs in a digraph, which indicates where the physical good originates	See Fig. 1
Head	One end of the arcs in a digraph, which indicates the destination of physical goods	See Fig. 1
In-degree	The number of heads connected to a node	$\text{In}(n_i)$(e.g., $\text{In}(n_2) = 2$)
Out-degree	The number of tails connected to a node	$\text{Out}(n_i)$(e.g., $\text{Out}(n_2) = 1$)
Source	A node that has a zero in-degree and positive out-degree. For example, a raw material supplier that does not receive any product, but only furnishes it	n_{11} and n_{12}
Sink	A node that has a zero out-degree and positive in-degree. For example, a supply network may end at a retailer where the physical good is not shipped anywhere else, but only receives it	n_1
Walk	A sequence of alternating nodes and arcs that originates from the source node(s) and ultimately ends at the sink node	$W = \{n_{11}, a_{15}, n_{10}, a_{13}, n_7, a_7, n_4, a_4, n_2, a_2, n_1\}$

[*] Based on a supply network illustrated in Fig. 1.

often occur in real-world supply chain management settings: *block-diagonal*, *scale-free*, *centralized*, and *diagonal* (see Fig. 3).

We exclude the other six structures from the analysis for the following reasons. The first three – random, local (a simple linear chain of nodes), and small-world (locally clustered nodes linked via a few long-distance bridging arcs) – are rarely found in practice. That is, in a physical supply network setting, it is hard to conceive of a practical situation where the nodes and arcs are determined by random assignment (*random*), where all the nodes and arcs are linearly aligned to form a single chain or walk (*local*), or where the network nodes are arranged into local, distantly separated clusters with only long, indirect links among them (*small-world*). Also, *preferential-attachment*, *dependent*, and *hierarchical* are structurally akin to the scale-free, centralized, and diagonal, respectively, where the latter three are viewed as relatively more realistic or basic in terms of physical supply network. We did analyze these "kin" structures, but they did not appreciably differ from the structures we discuss. Hence, we focus on the four fundamental structures and adapt them to the supply network context, where material flows from one node to another via a directed arc (digraph). Consequently, the complexity (*NK*) varies somewhat across these basic structures, but *NK* is kept as close to the same value as possible. To do this, we hold *N* (number of nodes) constant, and allow small deviations in *K* (number of arcs) to make each structure meaningful to the supply network setting. While we try to keep *K* similar across the four network structures, more focus is on making the patterns of connections correspond to the conceptual definition of each structure. This helps capture the essential differences of the basic structures. For instance, given the same *N*, the *block-diagonal* (disjointed multiple high-density clusters) and *centralized* (network connections concentrated on just a few nodes) patterns have different by but almost the same level of *K* (see Fig. 3). In addition, the analysis assumes that every node and arc in the supply networks has the same risk (or probability) of disruption, which further helps isolate the analysis to focus on structural differences.

Consistent with Rivkin and Siggelkow (2007), *N* is set to 12 for each supply network. Also, each network is assumed to have a single sink and a single source (Fig. 3), which reflects the most basic supply network structure and allows for more meaningful comparisons (Borgatti and Li, 2009). The nodes in the networks use the following labeling scheme—the sink node is labeled number 1, the source node 12, and the remaining nodes 2 to 11, where a lower number is given to a more downstream node (toward n_1) and a higher number to a more upstream node (toward n_{12}). The total number of arcs ranges from 18 (*block-diagonal*) to 29 (*centralized*) for each of the basic supply network structures.

A few extra constraints help make the structures more comparable. First, all nodes except the source and sink nodes, have both in-degree and out-degree greater than zero. In the supply network context, it makes no sense to examine nodes isolated from the network. Also, we arrange the network connections in such a way that physical flows always go from upstream to downstream. That is, there is no such a case where, for a given specific node, an incoming arc comes from a lower-numbered (downstream) node or an outgoing arc goes to a higher-numbered (upstream) node. This further helps keep the variation in complexity to a minimum across the four network structures and facilitate their structural comparisons on resilience. More detailed descriptions of the four basic supply network structures along with industry examples follow.

4.1. *Basic supply network structures*

4.1.1. *Block-diagonal*

This network structure (Fig. 3a) has clusters of nodes between the source and sink, where connections occur within clusters but not between clusters (Rivkin and Siggelkow, 2007). In general, this pattern relates to the notion of decomposability (Simon, 1962). In a supply network context, this characterizes a network that makes modular products (Starr, 1965; Sturgeon, 2002) such as personal computer (PC), bicycles, and financial services. For instance, consider a typical desktop PC supply chain. It comprises a final assembler and various module suppliers, each of which is fully responsible for designing and manufacturing the assigned module. To do so, each of these suppliers tightly coordinates its own cluster (block) of parts-suppliers or sub-assemblers (Baldwin and Clark, 1997). This basic supply network structure was adapted from Rivkin and Siggelkow (2007).

4.1.2. *Scale-free*

The *scale-free* network pattern captures "the rich-get-richer" dynamic (Barabási and Albert, 1999). In this network, a few nodes have disproportionately many connections, while most of the other nodes have only a few connections. The networking structure thus resembles the "hub-and-spoke" or "core-periphery" model (Borgatti and Everett, 1999). Consequently, the node degree distribution of the network appears as highly skewed and follows a *power-law* or Pareto distribution (Mitzenmacher, 2004). This network structure (Fig. 3b) is adapted from Rivkin and Siggelkow (2007). In the supply network context, this may reflect a situation where a small group of top-tier suppliers work closely together and collectively influence supply flows from upstream participants. This structure mirrors a keiretsu supply network such as Toyota city (Markusen, 1996), in which a small number of "core" firms (i.e., the focal manufacturer and its highly integrated top suppliers) jointly control and manage larger numbers of "peripheral" firms (Gerlach, 1992). The aerospace industry around the Seattle region offers another example of this network structure (Gray et al., 1996), where numerous suppliers cluster around a few core firms.

4.1.3. Centralized

The *centralized* network structure (Fig. 3c) takes the notion of highly central nodes to the extreme (Barabási, 2002). In this structure, a few nodes connect to (almost) all other nodes, while the other nodes link only to the few highly central nodes (Rivkin and Siggelkow, 2007). Barabási (2002: 103) describes this as a "winner-take-all" structure. In the supply network setting, this structure mirrors the situation where the source node directly connects to the few central nodes as well as to most of the nodes in-between. This type of supply network occurs in the Prato textile industrial district of Tuscany, Italy (Paniccia, 1998); the network revolves around a few coordinating agents called "impannatori." In the Prato textile industry, a few central brokers procure raw materials, allocate orders, give instructions to a number of small- to medium-sized specialist subcontractors (suppliers) in the region, and even market end-products to customer firms, and consequently exert a lot of clout in the supply network. Another real-world example comes from a field study experienced by one of the authors of this study, where one major automaker employs 'black-box sourcing' (Clark and Fujimoto, 1991) in producing navigation and stereo systems. That is, the top-tier suppliers assume complete responsibility for designing, engineering, and producing the entire systems on behalf of the customer firm, where they plan and manage all the necessary steps in the development process, even working directly with all the tertiary-level suppliers of the automaker.

4.1.4. Diagonal

This basic supply structure is based on the hierarchical interaction patterns. In this structure (Fig. 3d) connections occur sequentially, where every node takes supply from its lower-tier nodes, but not from the nodes above it (Rivkin and Siggelkow, 2007). This type of connection pattern embodies a multi-tiered supply network structure. In this structure, most of the nodes in between the source and sink can be partitioned into subsets of nodes that form tiers, in which the connections primarily occur across different tiers. Consequently, direct arcs to the sink node come only from top-tier nodes. Unlike in the "pure" hierarchical structure, however, in the diagonal structure not every higher-tier node takes delivery from all the nodes below it. This type of pattern typically occurs in military logistics networks (Zhao et al., 2011), where precedent activities have to be completed before the next activities can begin. Also, this may be the case for some OEMs in the automotive industry, in which they directly select and manage their 1st-tier suppliers and devolve on these suppliers the tasks of selecting and managing larger numbers of their own suppliers (i.e., the OEMs' 2nd-tier suppliers), and then the 1st-tier suppliers follow suit and so forth (Choi and Hong, 2002).

4.2. Resilience of basic supply networks

We evaluate the four basic supply network structures using several well-established network analysis metrics that may have implications for network resilience. In addition, we propose a new measure of supply network resilience that corresponds to our definition. The four basic network structures are compared on the various network metrics for their resilience and we determine how much the existing network metrics predict supply network resilience when compared to our measure of supply network resilience.

4.2.1. Network and resilience metrics

The network literature has identified several metrics for networks that may help understand supply network resilience. These metrics include: network density, average degree, walks, average walk length, maximum and minimum walk lengths, connectivity, betweenness centrality, and network centralization. *Network density* refers to a ratio of the number of total existing arcs to the total number of possible arcs in the network. The *average degree* is the average number of arcs across all the nodes in a network. The *average*, *maximum*, and *minimum walk lengths* refer to, respectively, the average length of the identified multiple walks, the length of the longest walk, and the length of the shortest walk for each basic supply network. The *connectivity* is the minimum number of nodes and/or arcs that must be removed to disconnect the network (Harary, 1969; Wasserman and Faust, 1994). *Betweenness centrality* is based on the node-level betweenness centrality $C_B(n_i)$ (Freeman, 1977) defined as follows:

$$C_B(n_i) = \sum_{j<k} \frac{g_{jk}(n_i)}{g_{jk}},$$

where g_{jk} is the total number of shortest paths between each pair of nodes, and $g_{jk}\ (n_i)$ is the number of those shortest paths that contain n_i. The each node's (n_i) betweenness is the probability that the node lies on shortest paths between other nodes. After calculating this metric for all the nodes in a network, the average of these values gives the network-level betweenness centrality. This metric assesses how often the nodes in a network lie on the shortest path between all combinations of pairs of other nodes in the network. The *centralization* (C) for each network is calculated using a definition for degree-based network centralization (Freeman, 1979):

$$C = \frac{\sum_{i=1}^{g} [C_D(n^*) - C_D(n_i)]}{\max \sum_{i=1}^{g} [C_D(n^*) - C_D(n_i)]},$$

where $C_D\ (n_i)$ is node-level degree centrality, and $C_D\ (n^*)$ is the maximum value in the network.

Finally, we use a simulation model to compute the *supply network resilience*. Recall, a *supply network disruption* occurs when the network no longer has a walk from the source to the sink node due to disruptions of nodes and arcs. Thus, to calculate supply network resilience, we estimate the likelihood that there exists at least one walk between the source and sink nodes with random removal of nodes and/or arcs in-between the two endpoints. That is, each simulation run determines if a network disruption occurs in the face of node/arc disruptions. More specifically, for each basic supply network, we calculated a ratio of the total number of combinations of node/arc removals that do not lead to a disruption of the network over the total number of possible combinations of node/arc removals (as determined by the total number of the given simulation runs), which may or may not lead to a network disruption. Formally,

Table 3
Network metrics and resilience for four basic supply network structures.

Network metrics	Block-diagonal	Scale-free	Centralized	Diagonal
Node/arcs	12/18	12/25	12/29	12/25
Network density	.14	.19	.22	.19
Average degree	1.50	2.08	2.42	2.08
Resilience	**.11**	**.30**	**.16**	**.13**
Walks	8	19	27	21
Average walk length	6.5	6.89	5.44	8.62
Max. walk length	9	11	7	13
Min. walk length	5	3	3	5
Connectivity	3	4	2	3
Betweenness centrality	1.33	1.67	.75	2.58
Centralization (%)	10.91	52.73	67.27	30.91

$$\text{Supply network resilience} = \frac{\text{total number of node/arc disruptions, which does not result in a supply network disruption}}{\text{total number of node/arc disruptions}}$$

We exclude the source and sink node in this calculation because this would automatically lead to a disruption, and because our focus is on understanding how the structure of relationships among the components in between the source and sink affects resilience at the network level. Nonetheless, including the two endpoints in the analysis would not change the metric too much even for moderately sized networks (such as ones under consideration in this study).

To assess this metric for the four basic network structures, we develop a simulation model using visual basic. In each simulation run, we randomly remove each of the nodes and arcs (between the source and sink) or their combinations with equal probability of failure. Then we determine if there exists at least a walk from the source to the sink node (i.e., the network was not disrupted). We ran this process with four different sample sizes (i.e., numbers of iteration) of 5000, 10,000, 15,000, and 30,000 times and then, for each sample size, computed the total number of times when the network was not disrupted over the total number of simulation runs (5000, 10,000, 15,000, or 30,000). This gives an estimate of the supply network resilience for each of the four basic supply network structures. The analysis gave very consistent results across the four different iterations of sample sizes. Table 3 reports the levels of supply network resilience based on 30,000 simulation runs, which is accurate to at least two decimal places (see authors for details of the visual basic software and simulation model).

For the analysis, we constructed a binary adjacency matrix or sociomatrix (Wasserman and Faust, 1994) for each basic network. The matrices were inputs to a simulation model that computes supply network resilience and the UCINET 6 social network software that analyzes the network data for the other network metrics (Borgatti et al., 2002). Table 3 gives these various metrics for the four supply network structures.

4.2.2. *Comparisons of supply networks on resilience*

The basic supply structures show different scores on the metrics, including the supply network resilience. Table 3 shows that the *scale-free* network structure has by far the highest resilience (.30), much higher than the *centralized* structure (.16), the next highest. Therefore, the results help show how well each of the network metrics can predict resilience. First, one might assume that a denser network (i.e., higher number of network arcs) tends to be more resilient. However, in terms of network density and average degree, the *centralized* structure has the highest values, due to its slightly higher total numbers of arcs. Also, intuition might suggest that more walks from the source to the sink would result in higher network resilience. Table 3 shows that the *centralized* structure again has the most walks (27), but it is not the most resilient. The *diagonal* structure has the second most walks (21), but with an even lower resilience score (.13). The average, maximum, and minimum walk lengths of each structure also did not predict network resilience. On these metrics, the *diagonal* structure has the highest scores.

The network-level metrics of *betweenness centrality* and *centralization* also did not correlate with resilience. One might assume that the more often the nodes bridge other nodes in a network or the more concentrated the network connections around a few nodes in a network, the more resilient the supply network will be to random failures. However, *diagonal* structure scores highest on the betweenness centrality metric but second lowest on resilience. The *centralized* structure scores highest on centralization, but again is not the most resilient. The *connectivity* metric appears to be more predictive of network resilience when compared with the other metrics. The *scale-free* structure has the highest connectivity (4). However, the *centralized* structure has the lowest connectivity (2), albeit the second most resilient. Further, the *diagonal* and *block-diagonal* structures tie for the connectivity at 3, while the former is relatively more resilient. This metric cannot distinguish among the three less resilient network structures. We also examined other network archetypes (after structural adaptations to the supply network context) and found similar results.

Taken together, the above results indicate that well established network metrics do not consistently nor reliably predict network resilience. Interestingly, denser or merely more complex networks do not necessarily have higher resilience. This implies that from a network perspective, redundancy may not always lead to higher resilience, which contradicts some of the conventional views on supply network resilience (see Sheffi, 2005). This also conflicts some research on supply network resilience that argues for the association between the well-established network metrics and resilience (e.g., Nair and Vidal, 2011). Overall, these results suggest that structure plays a significant role in supply network resilience. Researchers thus need to carefully consider their choices of metrics to assess resiliency. Taken-for-granted assumptions (e.g., that redundancy leads to higher resilience) may lead to an erroneous conclusion (e.g., that higher average degree will have higher resilience). Rather, there may be a non-linear relation between the existing metrics and resilience, which is contingent on network structure. Scholars conducting empirical research on supply network resilience need to be careful about how they conceptualize and use metrics. As such, network resilience represents an underexamined network property, and merits further research. As a step in this direction, we advance some propositions that link supply network structure to resilience.

5. Proposition development

The above comparisons demonstrate that network structure affects network resilience. A network-level disruption occurs with the removal of all possible walks between the source and sink. Removing nodes or arcs from a network potentially changes the number of walks, which may ultimately disrupt the entire network (Newman, 2003). Assuming that every node (facility) and arc (transportation) in a supply network has equal risk of failure, different configurations of the nodes and arcs will lead to different chances of reducing the number of walks in the face of node/arc disruptions, which determines the likelihood of network disruption.

In the literature on complex networks, many scholars have advocated examining network resilience from a structural perspective. Albert et al. (1999) studied the effect of node deletion on network resilience in the Internet and the World Wide Web. The same authors studied the attack- tolerance of complex networks

(Albert et al., 2000), and found that networks with a high level of centrality tend to be more robust to random removal of nodes/arcs. The social-ecological systems literature has also examined how network structure (of humans, communities, and organizations) affects an ability to adapt and withstand disruptions. For instance, Holme et al. (2002) studied vulnerability (measured by the average inverse shortest path length) of various virtual social networks with removal of both nodes and arcs. Adger et al. (2005), from a structural perspective, investigated social-ecological systems for their vulnerability to disasters and suggested that a multi-level structure can better cope with unexpected external shocks. The previous studies suggest that network structural properties, particularly connectedness and centrality, affect the resilience of complex networks (Albert et al., 2000; Dunne et al., 2004; Janssen et al., 2006). As a result, this study builds upon prior research by examining the network structure effect on supply disruption and resilience.

Our analysis provides further support for the significant link between network structure and network resilience, and supports this argument in the context of supply network. Each of the four structures reflects the unique archetype of supply network configuration. While they appear different from each other in form (Fig. 3), the four structures are analytically comparable. They were all adapted from the existing archetypes (in Rivkin and Siggelkow, 2007) to the supply network setting, so that they have similar levels of complexity (*NK*). However, the analysis demonstrates that these basic supply structures have different levels of network resilience. For instance, Table 3 shows that the *scale-free* structure has the highest resilience, but has relatively low scores on the density, average degree, number of walks, betweenness centrality, and network centralization metrics. We need to note that the number of arcs (i.e., inter-firm connections) itself may not be a reliable predictor of resilience, which contradicts some of the conventional views that promote redundancy in network elements to increase resilience (Sheffi, 2005). Apparently, there exist structural differences across the basic supply networks, that is, in the way that the nodes and arcs are configured in the network, which greatly affects the network disruption risk and resilience.

If we can observe much smaller differences in resilience between networks of similar structure than between dissimilar structures, this should further support the argument. In a post-hoc analysis, we adapt the preferential-attachment, dependent, and hierarchical structures based on Rivkin and Siggelkow (2007) and compare their resilience to their structural cousins, i.e., scale-free, centralized, and diagonal, respectively[3]. While we still find a difference in resilience level between each pair of structural cousins, the spread in each pair is much smaller compared with the differences between dissimilar structures. These observations thus lend support for our argument that the supply network structure significantly affects the degree of network resilience.

Proposition 1 (P1). Ceteris paribus, the structure of a supply network affects the resilience of the supply network.

What specific structural characteristic(s) affect the differences in resilience among the supply networks? The analysis and observations suggest that the overall arrangement of the nodes and arcs in a supply network influences the likelihood of network disruption. Namely, *degree distribution* of a supply network plays a critical role in determining its resilience.

The degree distribution (degree of a node equals the number of arcs attached to it) reflects the overall pattern of connectedness in a network (Strogatz, 2001). There are a variety of different ways in which nodes or arcs can be removed from a network. We assume, arguably, in a supply network, a node or arc disruption randomly occurs. That is, the individual nodes and arcs have approximately the same level of failure risk. Given such random failure nature of the network elements, configuring them in such a way that each of them carries the same weight (i.e., the same degree) in terms of connecting the supply network may not help mitigate supply disruption risk. Failure of any node (and subsequently a given number of arcs attached to it) will not only remove these elements from the network, but also cripple as many other nodes of the same importance by reducing their degree and removing paths between them, which can significantly disturb the material flows and disrupt the whole network. Drawing on complex systems theory, we propose that a network exhibit unique properties to failure when its (node) degree distribution follows a *power-law* (Newman, 2010). Network structures that follow a power-law feature skewed degree distributions (see Fig. 4).

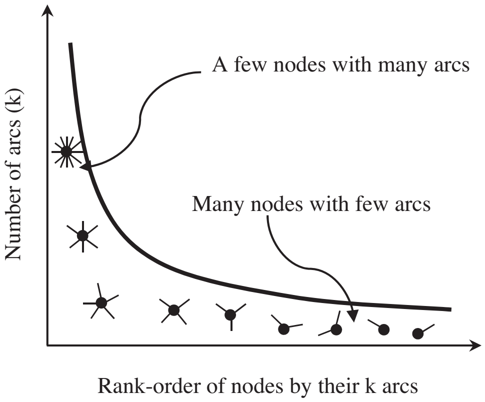

A few nodes with many arcs
Many nodes with few arcs
Number of arcs (k)
Rank-order of nodes by their k arcs

Fig. 4. Power-law distribution.

The power-law distribution, sometimes called scale-free (Barabási and Albert, 1999) or Pareto distribution (Newman, 2005), reflects a situation where a few nodes in a network have disproportionately high degree and many of the other nodes have low degree. This form of degree distribution has been recognized as a unique structural feature of many *attack-tolerant* complex networks. Albert et al. (2000) observe that some organic networks such as the Internet and the World Wide Web follow a power-law in their degree distributions. Furthermore, they found that the average path length between pairs of nodes in those networks was almost unaffected by random removal of nodes. Drawing on the same idea, Broder et al. (2000) argued that to destroy the connectedness in the World Wide Web, one would need to remove all nodes with degree greater than five. Given the highly skewed degree distribution of the Web, only a small proportion of all nodes have degree greater than five. These studies suggest that a skewed degree distribution can enhance the resilience of complex networks, especially to random shocks.

In networks that follow a power-law distribution, most of the nodes have low degree and therefore lie on few paths between others. Consequently, average path length would increase only marginally, if not at all, with random removal of node/arc from the network. In other words, random node/arc removal rarely affects the overall connectedness of a network with this structure. This has implications for reducing supply network disruptions. From the perspective of the focal firm of a supply network (e.g., OEMs in the automotive industry), if its key suppliers are closely connected to one another to the point where they even share preferred tertiary-level or raw-material suppliers, it is equivalent to the creation of potential alternative walks, which can make the supply system fairly robust to random failures that may occur even “deep in the supply network.” Toyota supply network provides a case in point in the Aisin fire case (Nishiguchi and Beaudet, 1998). A 1997 fire at a factory of Aisin Seiki, the main supplier of the brake valves to

[3] The additional analysis results are available upon request.

Toyota, threatened to halt Toyota's operations for weeks. However, the abrupt node-level failure, instead of leading to a network-level disaster, was averted due to the existence of alternative walks in the network. Toyota's top-tier suppliers shared the information and management of the upstream side of the network, which enabled them to set up alternative production capabilities outside of Aisin, and the whole process was orchestrated with very limited direct control from Toyota. Therefore, everything else being equal, a supply network structure with node degree distribution conforming to a power-law becomes less vulnerable to network-level disruptions, compared to networks with the distribution deviating from a power-law (Albert et al., 2000).

Our theoretical and computational analyses of the basic network structures support this argument. Fig. 3, panels e–h illustrates this point in the node-degree histogram plots for the four basic supply network structures. The horizontal axis on each histogram rank-orders 12 nodes by degree, and the vertical axis denote the node degree. Comparisons of the histograms show that the most resilient supply network, *scale-free*, most closely follows a power-law distribution. By definition, most of the nodes in the network have low degree, while just a few nodes have fairly high degree, which results in a long tail to the right of the histogram (Barabási, 2005). Observing the histograms, we can also notice that, next to the *scale-free*, the *centralized* structure appears to resemble a power-law pattern for its degree distribution. It is not surprising, thus, to see the structure having the second highest resilience level. Nonetheless, the *centralized* structure scores much lower (.16), compared to the *scale-free* (.30). The centralized pattern, as noted earlier, takes the notion of highly central nodes to the extreme, and so there are virtually no connections among the lower-degree nodes. This can translate into limited connectedness in the network (i.e., limited alternative paths to the central nodes as well as to the sink). Hence, the structure, despite its slightly more arcs (29) than *scale-free* (25), shows much lower resilience. Consequently, the degree distribution of a supply network influences its resilience to a greater extent, compared with other network-level metrics.

Proposition 2 (P2). The more closely a supply network follows a power-law for the degree distribution of the nodes, the more resilient the supply network will become.

6. Discussion and conclusion

Scholars have begun to study supply network disruption and resilience, but largely at the node level (Craighead et al., 2007). However, this can be misleading when looking at disruptions from a network perspective. Complexity theory argues that system behavior emerges from the actions or interactions of the components of a system. This paper develops a network perspective of disruptions and resilience to show how disruptions and resilience emerge from the network components. A network view alters how we manage and conduct research on supply network disruptions. Fig. 2 illustrates the importance of understanding the supply network as a whole. By looking at individual nodes in Fig. 2, some would consider node n_7 to be the most critical node due to its central location and high degree (Craighead et al., 2007). However, disrupting this node does not disrupt the network (see Fig. 2c). Without an understanding of the structure of the network, managers may unwittingly allocate resources only to increase the resilience of the wrong nodes in the network. Managers (and scholars) may be misled by looking at only the nodes of a supply network and not considering the overall structure.

This study makes the following contributions to the literature. First, it provides a formal definition of a supply network disruption by differentiating it from disruptions of nodes and arcs. Existing definitions of supply network disruption do not clearly specify the levels of effect and analysis, although node-level disruptions do not invariably lead to a disruption of a network. Our definition, however, distinguishes between node/arc-level vs. network-level disruptions. This distinction helps examine disruptions at the supply network level and highlight the importance of taking a network perspective to understand resilience. From this perspective, resilience at the node level is different than that at the network level, which affects how we study and manage supply network resilience. Second, we investigate the resilience of four basic supply network structures. These structures map onto prototypes of real-world supply networks. This gives fundamental insight into the effect of different supply network structures on resilience. Third, we develop a metric for supply network resilience that corresponds to our definition of supply network disruption, and compare it to some conventional network metrics. The standard network metrics do not reliably distinguish among different supply networks on resilience. Consequently, scholars should carefully define metrics when evaluating supply network resilience. For instance, Craighead et al. (2007) defines the term *node criticality* in terms of the importance of each node when viewed in isolation within the network. From a network perspective, our research shows that node criticality needs to be understood in terms of the overall network structure.

6.1. Implications for research

Failure to clarify the level of analysis in supply network disruptions can be problematic in a couple of ways. First, it risks committing the ecological fallacy (over-generalizing findings at a higher level to a lower level) or the atomistic fallacy (over-generalizing findings at a lower level to a higher level), both of which could lead to misleading conclusions. For instance, creating redundancy in nodes (i.e., redundant facilities) or arcs (i.e., alternate shipping channels) in the network may have no effect on overall resilience of the network. Although prior research (e.g., Sheffi and Rice, 2005) advocates redundancy as a strategy for mitigating supply network disruptions, the potential benefits need to be understood in the context of the whole supply network. Failure to clarify the level of analysis in prior research can diminish the applicability of the findings. By drawing on graph theory and formally defining a supply network in terms of the structural elements (i.e., nodes and arcs), we develop a more precise definition that differentiates a supply network disruption from a node/arc-level disruption, which clarifies the level of analysis and will increase the applicability of the findings.

Second, research on supply network resilience has not fully incorporated the role of network structure. Many studies (except for Sheffi, 2007 [cf. *The Resilient Enterprise*]) have approached the issue at an individual firm level, and do not fully consider the structure of supply networks. But, we show that network resilience is contingent on network structure. Managing supply disruptions by focusing on node-level risks gives only incomplete solutions for improving resilience. For example, some prior studies considered how facility location (node-level) decisions can improve supply chain resilience (Hale and Moberg, 2005; Reid and Sanders, 2010). However, a facility location decision can alter the overall structure of the supply network. Without incorporating the broader network implications, such node-level planning and decisions may be suboptimal.

This study also shows that established network analytic metrics do not precisely predict the resilience of supply networks. Although some researchers have argued, for instance, that high-degree nodes (Craighead et al., 2007) and short average path length (Nair and Vidal, 2011) play critical roles in network disruption, our analysis shows that node failure and average walk length are not necessarily related with a network disruption. Further, the results (in Table 3) show that there exist nonlinear relations between the conventional network metrics and the proposed network resilience metric. For instance, the *centralized* structure scores highest on the network density metric, but it is not the most resilient. Similarly, the *diagonal* structure scores highest on the betweenness centrality metric, but it is also not the most resilient. However, the *scale-free* has the highest level of resilience when compared to the other structures. Apparently, network resilience is a distinct property of a supply network, meriting further research.

In this regard, the concept of (structural) complexity in a network context merits further consideration. The literature on complex networks poses two competing arguments about the relation between complexity and resilience. Some studies argue for a positive relationship between more complex networks (i.e., greater network density) and resilience (Albert et al., 2000; Janssen et al., 2006), while others argue the opposite since "a complex supply chain would be more likely to be severe than the same... disruption occurring within a relatively less complex" supply network (Craighead et al., 2007: 141). The above nonlinear relationship suggests that either argument is only partially true––neither too little nor too much complexity is good for network resilience. This observation points out a need for further research to uncover optimal answers for increasing network resilience.

Finally, this study also has implications for empirical research. For instance, the existing empirical research on supply disruptions/risks has been discussing various capabilities that firms should develop for greater resilience or robustness, such as agility, collaboration capabilities, risk awareness (Christopher and Peck, 2004), production flexibility (Sheffi and Rice, 2005), and supply visibility/velocity (Jüttner and Maklan, 2011). However, do they represent node/arc-level or network-level capabilities? This study points out that empirical research should clarify the level at which it discusses resilience capabilities, because increases in node- or arc-level capabilities may not lead to an increase in network-level resilience. Acknowledging that much of the research has focused more on node/arc-level capabilities, now research needs to go beyond the local level to identify and suggest more of network-level capabilities for system-wide resilience.

6.2. Implications for practice

This study sheds light on how to manage supply network disruptions. Sheffi (2007) notes, "one of the most straightforward methods for creating resilience is building redundancy" (p. 275). However, this study shows that increasing redundancy by adding extra nodes or arcs may not improve the resilience of the network. Individual suppliers' relative positions and how they are linked up in the network should be given more careful consideration. Managers can improve the resilience of the supply network by managing network structure. This may entail mapping out the structure of the supply network to see if it follows a *scale-free* or Pareto distribution. As a practical matter, managers can apply the following rule of thumb, "Do 20% of the facilities (nodes) have transportation connections (arcs) with 80% of the other facilities (nodes) in the network?" If so, the network structure should lead to higher resilience since it follows the power-law distribution. Second, this research has implications for supplier selection and management practices. Often, companies focus on the internal qualities or capabilities when evaluating new and existing suppliers. However, this study suggests taking a broader view. A given supplier's role in network resilience depends, in part, on its position in the network. Fig. 2c shows that the most-connected supplier in the network may not be the most critical factor in terms of disrupting the network, which is contrary to conventional wisdom. Managers would need to identify all the linkages their individual suppliers have with the others in the supply network to precisely assess their impact on network resilience. Third, firms may need to update their method for classifying suppliers. The traditional focus in supplier classification has been on the importance of suppliers in their direct impact on the focal firm's profit and risk position (e.g., Kraljic, 1983). Thus, the immediate, top-tier suppliers are typical classification objects. However, our paper suggests a new category of potentially critical suppliers, different from the traditional "strategic" suppliers. This new category of suppliers becomes strategically important due to their positions and how they are linked up in the broader network. They serve as the "linchpin" of the supply network, and when removed, can disrupt the entire network.

6.3. Limitations and future research

This research has some conceptual and analytical limitations, which suggest avenues for future research. Conceptually, first we treat every node and arc as having equal probability of failure. In other words, in our theory and analysis, we did not consider varying importance of the nodes and arcs in the network, which may be less realistic. However, this helps isolate the analysis to network structural differences. In practice, the probably of failure may vary across different nodes and arcs in the supply network. Assigning different probabilities of failure for the elements in a supply network may have implications for network disruption and resilience. Also, in this paper, for the purpose of keeping the variation of complexity to a minimum, we imposed some constraints on our models, which might result in some practically important variables being excluded from our analysis. For instance, our analysis did not take into account the possible differential effects of different lead times due to different node-level (i.e., facilities) capabilities or different lengths of the arcs (i.e., transportation) in the network. Individual differences in lead-time at the nodes and along the arcs or collective differences along various walks in the network should determine the magnitude of a network-level disruption.

Further, this study takes a more static approach to supply network disruption. That is, in the analysis once a node or an arc is removed from a supply network, its function is removed altogether excluding the possibility of a substitution for this function. In practice, a focal firm may include by design a substitution capability into the supply system to reduce disruption risk. Future research may incorporate this into its research model to get more realistic results. However, this study has implications for dynamics in supply disruption and resilience. Every supply network should evolve in its structure over time toward more resilient structure. A supply network will become more resilient to node/arc disruptions if its structure follows a power-law pattern in the degree distribution. Finally, the size of the supply networks considered in this study might limit the reliability or generalizability of our findings. To ensure the validity of the basic supply networks, we adapted the network archetypes mapped in Rivkin and Siggelkow (2007), and as a result, the number of nodes in each basic supply network was set to 12. While this enabled meaningful comparisons of basic network archetypes, scaling up the network size would reflect greater structural complexity inherent in real-world supply networks. Future studies are encouraged to relax the constraints imposed in this research to further capture complexities and challenges of managing network disruption and resilience.

6.4. Conclusion

The emerging literature on supply network disruption and resilience has been confusing with respect to the conceptualization and level of analysis. We conceptualized supply network disruption and resilience from the network structural perspective by drawing on graph theory. This approach helps understand how network-level disruptions emerge from disruptions of the components of a supply network. Further, it clearly helps differentiate a node/arc disruption from a network disruption, which has been a point of confusion in the development of the literature. This research suggests theoretical and analytical approaches to understand and evaluate network level disruptions and resilience. Moreover, we hope that our summary observations, presented in the form of propositions, serve as a stepping-stone that stimulates more research to further understand supply network disruption and resilience.

References

Adger, W.N., Hughes, T.P., Folke, C., Carpenter, S.R., Rockstrom, J., 2005. Social–ecological resilience to coastal disasters. Science 309 (5737), 1036–1039.

Adhitya, A., Srinivasan, R., Karimi, I.A., 2007. A model-based rescheduling framework for managing abnormal supply chain events. Comput. Chem. Eng. 31 (5), 496–518.

Albert, R., Jeong, H., Barabási, A.-L., 1999. Diameter of the World Wide Web. Nature 401 (6749), 130–131.

Albert, R., Jeong, H., Barabási, A.-L., 2000. Error and attack tolerance of complex networks. Nature 406 (6794), 378–382.

Baldwin, C.Y., Clark, K.B., 1997. Managing in an age of modularity. Harv. Bus. Rev. 75 (5), 84–93.

Barabási, A.-L., 2002. Linked: The New Science of Networks. Perseus, Cambridge, MA.

Barabási, A.-L., 2005. The origin of bursts and heavy tails in human dynamics. Nature 435 (7039), 207–211.

Barabási, A.-L., Albert, R., 1999. Emergence of scaling in random networks. Science 286 (5439), 509–512.

Borgatti, S.P., Li, X., 2009. On social network analysis in a supply chain context. J. Supply Chain Manage. 45 (2), 5–22.

Borgatti, S., Everett, M., 1999. Models of core-periphery structures. Soc. Netw. 21 (4), 375–395.

Borgatti, S., Everett, M., Freeman, L., 2002. UCINET6 for Windows: Software for Social Network Analysis. Analytic Technologies, Inc., Natick, MA.

Broder, A., Kumar, R., Maghoul, F., Raghavan, P., Rajagopalan, S., Stata, R., Tomkins, A., Wiener, J., 2000. Graph structure in the web. Comput. Netw. 33 (1), 309–320.

Choi, T.Y., Hong, Y., 2002. Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler. J. Oper. Manage. 20 (5), 469–493.

Clark, L., Fujimoto, T., 1991. Product Development Performance: Strategy, Organization and Management in the World Auto Industries. Harvard Business School Press, Cambridge, MA.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. Int. J. Logist. Manage. 15 (2), 1–14.

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J., Handfield, R.B., 2007. The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decis. Sci. 38 (1), 131–156.

Diestel, R., 1991. Decomposing infinite graphs. Discrete Math. 95 (1), 69–89.

Dunne, J.A., Williams, R.J., Martinez, N.D., 2004. Network structure and robustness of marine food webs. Mar. Ecol.—Prog. Ser. 273, 291–302.

Ellis, S.C., Henry, R.M., Shockley, J., 2010. Buyer perceptions of supply disruption risk: a behavioral view and empirical assessment. J. Oper. Manage. 28 (1), 34–46.

Euler, L., 1741. Solutio problematis ad geometriam situs pertinentis. Commentarii academiae scientiarum imperialis Petropolitanae 8, 128–140.

Ferreira, G., 2012>. Toyota to Add Saturday Shifts at San Antonio Site to Ramp up Output, ⟨http://www.4wheelsnews.com/toyota-to-add-saturday-shifts-at-san-antonio-site-to-ramp-up-output/⟩.

Freeman, L.C., 1977. A set of measures of centrality based on betweenness. Sociometry 40 (1), 35–41.

Freeman, L.C., 1979. Centrality in social networks: conceptual clarification. Soc. Netw. 1 (3), 215–239.

Gerlach, J.M., 1992. The Japanese corporate network: a block model analysis. Adm. Sci. Q. 37 (1), 15–139.

Ghemawat, P., Levinthal, D., 2008. Choice interactions and business strategy. Manage. Sci. 54 (9), 1638–1651.

Gray, M., Golob, E., Markusen, A., 1996. Big firms, long arms, wide shoulders: the 'hub-and-spoke' industrial district in the Seattle region. Reg. Stud. 30 (7), 651–666.

Gross, J., Yellen, J., 1998. Graph Theory and its Applications. CRC Press, Boca Raton, FL.

Gross, J.L., Yellen, J., 2006. Graph Theory and its Applications. Macmillan Press Ltd, London.

Hale, T., Moberg, C.R., 2005. Improving supply chain disaster preparedness: a decision process for secure site location. Int. J. Phys. Distrib. Logist. Manage. 34 (3), 195–207.

Hamel, G., Valikangas, L., 2003. The quest for resilience. Harvard Bus. Rev. 81 (September&October)), 52–65.

Harary, F., 1969. Graph Theory. Addison-Wesley, Reading, MA.

Hendricks, K.B., Singhal, V.R., 2003. The effect of supply chain glitches on shareholder wealth. J. Oper. Manage. 21 (5), 501–522.

Hendricks, K.B., Singhal, V.R., 2005. An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. Prod. Oper. Manage. 14 (1), 35–52.

Holme, P., Kim, B.J., Yoon, C.N., Han, S.K., 2002. Attack vulnerability of complex networks. Phys. Rev. E: Stat. Nonlinear Soft Matter Phys. 65 (5), 056109.

Janssen, M.A., Bodin, Ö., Anderies, J.M., Elmqvist, T., Ernstson, H., McAllister, R.R.J., Olsson, P., Ryan, P., 2006. Toward a network perspective of the study of resilience in social-ecological systems. Ecol. Soc. 11 (1), 15.

Johnson, N., Elliott, D., Drake, P., 2013. Exploring the role of social capital in facilitating supply chain resilience. Supply Chain Manage.: Int. J. 18 (3), 324–336.

Jüttner, U., Peck, H., Christopher, M., 2003. Supply chain risk management: outlining an agenda for future research. Int. J. Logis.: Res. Appl. 6 (4), 197–210.

Jüttner, U., Maklan, S., 2011. Supply chain resilience in the global financial crisis: an empirical study. Supply Chain Manage.: Int. J. 16 (4), 246–259.

Kauffman, S.A., 1993. The Origins of Order: Self-organization and Selection in Evolution. Oxford University Press, New York, NY.

Kauffman, S.A., Levin, S., 1987. Toward a general theory of adaptive walks on rugged landscapes. J. Theor. Biol. 128 (1), 11–45.

Kleindorfer, P.R., Saad, G.H., 2005. Managing disruption risks in supply chains. Prod. Oper. Manage. 14 (1), 53–68.

Kovács, G., Tatham, P., 2009. Responding to disruptions in the supply network-from dormant to action. J. Bus. Logist. 30 (2), 215–229.

Kraljic, P., 1983. Purchasing must become supply management. Harv. Bus. Rev. 61 (5), 109–117.

Langton, C.G., 1990. Computation at the edge of chaos: phase transition and emergent computation. Physica D: Nonlinear Phenom. 42 (1), 12–37.

Longo, F., Oren, T., 2008. Supply chain vulnerability and resilience: a state of the art overview. In: Proceedings of the European Modeling and Simulation Symposium, Campora S. Giovanni (CS), Italy, pp. 17–19.

Markusen, A., 1996. Sticky places in slippery space: a typology of industrial districts. Econ. Geogr. 72 (3), 293–313.

Mitzenmacher, M., 2004. A brief history of generative models for power law and lognormal distributions. Internet Math. 1 (2), 226–251.

Nair, A., Vidal, J.M., 2011. Supply network topology and robustness against disruptions—an investigation using multi-agent model. Int. J. Prod. Res. 49 (5), 1391–1404.

Newman, M.E.J., 2003. The structure and function of complex networks. SIAM Rev. 45 (2), 167–256.

Newman, M.E.J., 2005. Power laws, Pareto distributions and Zipf's law. Contemp. Phys. 46 (5), 323–351.

Newman, M.E.J., 2010. Networks: An Introduction. Oxford University Press, New York, NY.

Nishiguchi, T., Beaudet, A., 1998. The Toyota group and the Aisin fire. MIT Sloan Manage. Rev. 40 (1), 49–59.

Paniccia, I., 1998. One, a hundred, thousands of industrial districts. Organizational variety in local networks of small and medium-sized enterprises. Organ. Stud. 4 (19), 667–699.

Ponomarov, S.Y., Holcomb, M.C., 2009. Understanding the concept of supply chain resilience. Int. J. Logist. Manage. 20 (1), 124–143.

Reid, R.D., Sanders, N.R., 2010. Operations Management: An Integrated Approach. Wiley, New York, NY.

Rivkin, J.W., 2000. Imitation of complex strategies. Manage. Sci. 46 (6), 824–844.

Rivkin, J.W., Siggelkow, N., 2003. Balancing search and stability: interdependencies among elements of organizational design. Manage. Sci. Manage. Sci. 49 (3), 290–311.

Rivkin, J.W., Siggelkow, N., 2007. Patterned interactions in complex systems: implications for exploration. Manage. Sci. 53 (7), 1068–1085.

Schilling, M.A., Phelps, C., 2007. Interfirm Collaboration Networks: the impact of large-scale network structure on firm innovation. Manage. Sci. 53 (7), 1113–1126.

Scholten, K., Scott, P.S., Fynes, B., 2014. Mitigation processes—antecedents for building supply chain resilience. Supply Chain Manage. 19 (2), 211–228.

Sheffi, Y., Rice, J., 2005. A supply chain view of the resilient enterprise. MIT Sloan Manage. Rev. 47 (1), 41–48.

Sheffi, Y., 2005. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. MIT Press Books.

Sheffi, Y., 2007. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. The MIT Press, Cambridge, MA.

Simon, H.A., 1962. The architecture of complexity. Proc. Am. Philos. Soc. 106 (6), 467–482.

Starr, M.K., 1965. Modular-production: A new concept. Harv. Bus. Rev. 46 (3), 131–142.

Stauffer, D., 2003. Risk: the weak link in your supply chain. Harv. Manage. Update 8 (3), 3–5.

Strogatz, S.H., 2001. Exploring complex networks. Nature 410 (6825), 268–276.

Sturgeon, T.J., 2002. Modular production networks: a new American model of industrial organization. Ind. Corp. Change 11 (1), 451–496.

Svensson, G., 2000. A conceptual framework for the analysis of vulnerability in supply chains. Int. J. Phys. Distrib. Logist. Manage. 30 (9), 731–749.

Tang, C.S., 2006. Robust strategies for mitigating supply chain disruptions. Int. J. Logist. Res. Appl. 9 (1), 33–45 (A Leading Journal of Supply Chain Management).

Thun, J.H., Drüke, M., Hoenig, D., 2011. Managing uncertainty—an empirical analysis of supply chain risk management in small and medium-sized enterprises. Int. J. Prod. Res. 49 (18), 5511–5525.

van der Vorst, J.G.A.J., Beulens, A.J.M., 2002. Identifying sources of uncertainty to generate supply chain redesign strategies. Int. J. Phys. Distrib. Logist. Manage. 32 (6), 409–430.

Wacker, J.G., 2004. A theory of formal conceptual definitions: developing theory building measurement instruments. J. Oper. Manage. 22 (6), 629–650.

Wagner, S.M., Neshat, N., 2010. Assessing the vulnerability of supply chains using graph theory. Int. J. Prod. Econ. 126 (1.), 121–129.

Wasserman, S., Faust, K., 1994. Social Network Analysis: Methods and Applications. Cambridge University Press, New York, NY.

Wu, T., Blackhurst, J., O'grady, P., 2007. Methodology for supply chain disruption analysis. Int. J. Prod. Res. 45 (7), 1665–1682.

Zhao, K., Kumar, A., Harrison, T.P., Yen, J., 2011. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. Sys. J., IEEE 5 (1), 28–39.