Achieving High Robustness in Supply Distribution Networks by Rewiring

Kang Zhao, *Member, IEEE*, Akhil Kumar, *Member, IEEE*, and John Yen, *Fellow, IEEE*

***Abstract*—In this paper, we propose a new rewiring approach for distribution networks called *randomized local rewiring* (RLR). We evaluate the robustness of original and rewired distribution networks using new metrics and show that the choice of a network topology can affect its robustness considerably. Some supply and distribution networks exhibit characteristics similar to those of scale-free networks. Simulation results show that applying RLR to such distribution networks can improve the network robustness on the supply availability and network connectivity metrics when both random and targeted disruptions are likely to occur. A unique feature of our model is a tunable rewiring parameter, which makes it possible to design networks with the same performance on the supply availability, network connectivity, and average delivery efficiency metrics in the presence of both types of disruptions. This paper will describe the robustness metrics and the new approach, illustrate the experimental results in the context of a military logistic and a retailer's distribution network, and discuss the insights gained about choosing the right topology for achieving higher robustness.**

***Index Terms*—Complex network, disruption, rewiring, robustness, supply distribution network, topology.**

I. Introduction

OUR daily lives rely heavily on the distribution of goods and services, such as groceries, water, and electricity, through supply chains. With globalization and the development of information technology, supply-chain systems are becoming more complex and dynamic. Today's supply-chain systems often feature a network of interacting entities of different types, such as suppliers, manufacturers, retailers, and customers. Supply chains, which represented linear flows of goods from suppliers to customers, are evolving into supply networks [1]. Since entities may take different forms in various application domains, we refer to them simply as *nodes* in a network. Here, we consider a supply network as a graph of nodes, where the nodes are generally of two types: *supply* (or *supplier*) and *demand* (or *requester*) nodes. In this sense, these networks have *heterogeneous* nodes as opposed to conventional networks, where all nodes are of one type, and hence, homogeneous. Most research in the area of complex networks has focused on homogeneous networks. However, it is important to note that notions of network connectedness are different in these two types of networks. Therefore, metrics of connectedness, such as *path length and the size of the largest component, may mean something different in a heterogeneous supply network* than they do in a homogeneous network. Whereas connectedness in a homogeneous network is measured by how a given node is connected to other nodes, in a supply network, connectedness should focus on how a demand node is connected to any supply node. For instance, if a demand node is connected to other demand nodes only but isolated from a supply node, then it should not be considered as connected because no supplies can reach the demand node.

Moreover, large global supply chains or networks are often embedded in dynamic environments and may face disruptions, such as natural disasters, economic recessions, unexpected accidents, or terrorist attacks. A disruption may initially affect or disable only one or a few entities in the system, but its impact may propagate, sometimes even with amplifications [2], among interconnected entities. Such cascading disruptions will thus affect the normal operations of many other entities. Occasionally, failures in a small portion of the system may cause the catastrophic failure of the whole system [3]. Those events may seriously disrupt or delay the flow of people, goods, information, and funds, leading to higher costs or reduced sales [4] and affecting a company's long-term stock performance [5]. Therefore, designing supply chains that are robust against disruptions is a high priority concern, and it has drawn a lot of attention from managers, shareholders, and researchers [6], [7].

Traditional research on supply-chain disruptions often adopts the risk management perspective and focuses on strategies and technologies to identify, assess, and mitigate risks and problems caused by disruptions [4], [6], [7]. However, even though research has revealed that the topology of a supply network will affect its robustness [8], subsequent research in this direction is lacking.

In this paper, we will adopt the complex-network view of supply chains and study the robustness of heterogeneous distribution networks, i.e., the downstream part of a supply network whose main goal is to distribute goods or services, from a topological perspective. In particular, we are interested in understanding how the network topology affects various metrics of connectedness in a distribution network in the presence of both *random* and *targeted* disruptions. In addition to developing new metrics for supply networks, another goal in this research is to

Manuscript received December 2, 2009; revised May 16, 2010, September 15, 2010, and October 31, 2010; accepted November 15, 2010. Date of publication December 30, 2010; date of current version April 20, 2011. The work of K. Zhao was supported in part by the Network Science Exploration Research Grant from the Pennsylvania State University. The work of A. Kumar was supported in part by the Smeal College of Business, Pennsylvania State University.

K. Zhao and J. Yen are with the College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802 USA (e-mail: kangzhao@psu.edu).

A. Kumar is with the Smeal College of Business, The Pennsylvania State University, University Park, PA 16802 USA (e-mail: akhilkumar@psu.edu; jyen@ist.psu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2010.2095503

find a network design that can perform well under both random and targeted disruptions.

A "full-spectrum" supply network is a large "ecosystem" with many actors, such as raw material providers, manufacturers, warehouses, distribution centers (DCs), and retailers. In this research, we will focus mainly on the distribution network in which manufacturers, distributors, and retailers have close interaction with each another. Thus, the managers of these organizations often have good knowledge of, as well as control over, the network's structure. Therefore, compared with the network from other parts of a supply network such as the procurement network, it is easier to change the topology of this part of an existing network or implement another network design.

We believe that the topological perspective can help managers quickly evaluate the effectiveness of strategies to build a resilient[1] distribution network. While building a new distribution network from scratch is often a response to major disruptions [9], such as the Haiti earthquake and Hurricane Katrina, an organization may also take initiatives in rebuilding its supply network because today's corporations have to respond to very dynamic global markets. In order to be competitive, they may need to "burn themselves down every few years and rebuild their strategies, roles, and practices" [10]. This includes rebuilding the corporation's supply network [11]. Such active rebuilding of supply networks has been found in online retailers, chain retail stores, apparel manufactures, etc. [12]–[14]. The overhaul often aims at saving cost, improving responsiveness, raising customer satisfaction level, and so on.

The remainder of the paper is organized as follows. We first briefly review related research on the robustness of complex networks and distribution networks. Section III first proposes a new set of robustness metrics for heterogeneous distribution networks. This section will also introduce a new rewiring approach for distribution networks called randomized local rewiring (RLR). Through computational simulations of a military logistic network and a retailer's distribution network, we evaluate how our new model can help to improve the robustness of a distribution network in Sections IV and V. The paper will conclude with directions of future research.

II. Related Work

First we briefly review related research on complex networks. Complex networks are defined as networks whose "*physical or logical structure is irregular, complex, and dynamically evolving in time*" [15]. Research on complex networks has drawn growing interest during the past decades [16]–[18]. Researchers found that real-world networks, such as online social networks, the World Wide Web, and biological cellular networks, often have nontrivial and complex topologies that are different from lattice or random graph structures (with a Poisson degree distribution). *Scale-free* [19] and *small-world* [20] are two well-known network structures that were proposed to represent the topologies of many real-world complex networks. Moreover, some supply networks also show characteristics similar to those of a scale-free network [21], [22]. Thus, in this paper, we will study whether our new model can improve the robustness of distribution networks with the two types of topologies.

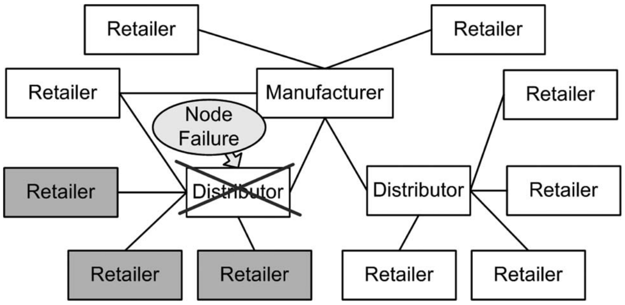


Fig. 1. Hierarchical distribution network.

Specifically, the robustness of complex network topologies against normal failures and attacks has been analyzed. It has been found that scale-free networks, which are a kind of complex networks where the degree distribution follows a power law, have very high tolerance against random failures, but are fragile to disruptions that target the most connected nodes [23], [24]. Compared with scale-free networks, random networks [25] are less robust against random disruptions, but often have better performance when important nodes fail. Grubesic *et al.* [26] provided a review of approaches to assess network vulnerability and robustness.

The research of Thadakamalla *et al.* [8] introduced the *topological perspective* into the study of the robustness of distribution networks. The research argued that traditional supply chains with hierarchical topologies are subject to disruptions. For example, in the hierarchical distribution network in Fig. 1, *the failure of a single distributor disconnects about 25% of the retailers from supplies*. Using a military logistic network as an example, the study compared the performance of distribution networks with various complex network topologies in two types of node-removal attack scenarios. The simulation results showed that the survivability of distribution networks is improved by concentrating on the network topology. However, the new network design proposed in this research is an *ad hoc* model for military logistic networks only. Our research will further extend this study and try to find a general design to improve the robustness of distribution networks.

III. Proposed Approach

In this section, we first present the new taxonomy of robustness metrics for distribution networks. It includes system- and topology-level metrics, which reflect the heterogeneous roles of different types of entities in distribution networks. Then, we introduce a parameterized model that generates new distribution network topologies by rewiring an existing one and evaluate multiple distribution networks' performance against disruptions using our new metrics.

[1] Note that the terms *resilience* and *robustness* are used interchangeably in this paper. We do not distinguish between them.

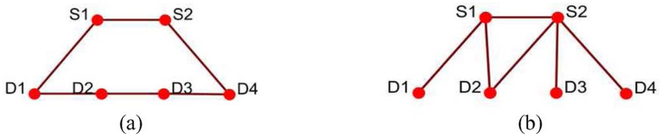


Fig. 2. (a) and (b) Two sample distribution networks with the same number of supply (S) and demand (D) nodes and edges. Network in (a) can maintain flow of supplies better than the network in (b).

A. New Robustness Metrics

Robustness of a network is its ability to maintain operations and connectedness when some structures or functions are lost [27]. A robust distribution network, whose main function is to deliver supplies in response to demands, should be able to maintain the flow of these supplies despite disruptions. Take the two illustrative networks in Fig. 2 as examples. There are two supply nodes, four demand nodes, and six edges in both networks. A demand node can get supplies from either supply node. However, the two networks have different robustness against disruptions. For instance, if a supply node, say S2, fails because of disruptions, all demand nodes in the network shown in Fig. 2(a) can still access supplies from S1. Meanwhile, in the network shown in Fig. 2(a), the failure of S2 will interrupt the delivery of supplies to demand nodes D3 and D4.

To measure the robustness of a complex network, we must first develop appropriate metrics. In most earlier research on the robustness of complex networks and supply networks, the evaluation of robustness often focuses on the largest connected component (LCC) in which there is a path between any pair of nodes [8], [23]. Most of the existing network metrics are standard topological metrics from graph theory, including *characteristic path length*, *size of the LCC*, *average path length in the LCC*, and *the maximum path length in the LCC*. Costa *et al.* provided a comprehensive survey of existing measurements for complex network [28]. Table I explains some of the commonly used metrics.

These metrics assume that entities in a distribution network perform homogeneous roles or functions. However, in real-world distribution networks, different types of entities play different roles in the system. Often times, the normal functioning of *downstream* entities may be highly dependent on the operations of *upstream* entities. As mentioned earlier, one of the fundamental purposes of a distribution network is to deliver supplies from the supplier to the consumer. This type of "Supply–Demand" connection is the prerequisite for the flow of goods and services, and is critical for maintaining the operation of the distribution network.

Take the military logistic network in [8] as an example. The network consists of battalions and support units, including *forward support battalions* (FSBs) and *main support battalions* (MSB). Support units play a different role from battalions in this network. Naturally, battalions cannot perform their military duties for long without receiving supplies from support units. Thus, a large connected component, in which there is no support unit, or even where battalions are far from support units, should not be considered robust, as there is none or limited supply flow in such a subnetwork. Similarly, the distance between battalion and support units is generally more important for a robust distribution network than the distance among battalion units. Therefore, the heterogeneous roles (as supply and demand nodes) of different types of entities in a distribution network must be recognized when evaluating the robustness of the distribution network. Although Albert *et al.* considered the roles of power plants and substations in a power-grid network when defining their connectivity metric [29], more systematic formalization and analysis are still needed to find metrics to reflect the robustness of distribution networks from more than one perspective. Also, in their research, only the robustness of a power grid was analyzed without offering any remedies.

The proposed taxonomy consists of system- and topology-level metrics. Neely *et al.* proposed to use quality, flexibility, time, and cost as four major performance metrics for supply chains [30]. Although relying on topological measures, our metrics can also reflect some aspects of those four performance metrics.

First, we introduce *supply availability* as a critical robustness metric for distribution networks because it shows whether entities in the network can get its requisite supplies to maintain normal operations. The inability to deliver goods to those who need them is a failure, which will affect the quality of the distribution network [31]. At the topological level, availability can also be interpreted as supply availability rate, which is the percentage of demand nodes that have access to supply nodes through the network.

Consider a supply network as an undirected, unweighted graph $G(V, E)$ with node set V and edge set E, where $e_{i,j} \in E$ denotes an edge between nodes $v_i, v_j \in V$. As shown in (1), V is the union of two nonoverlapping subsets of demand and supply nodes (sets V_D, V_S), assuming a node cannot play both roles in the supply distribution network. Then, (2) defines the set of demand nodes that have access to supply nodes in the network, where $\text{path}_{i,j}$ denotes a path between nodes v_i and v_j. Thus V'_D is the set of demand nodes that have access to supply nodes through the supply network. Consequently, the supply availability AV for a distribution network is the ratio between the cardinalities of sets V'_D and V_D [see (3)]

$$V = V_D \cup V_S, \qquad \text{where } V_D \cap V_S = \phi \tag{1}$$

$$V'_D = \{v_i \in V_D \mid \exists \quad v_j \in V_S : \exists \quad \text{path}_{i,j}\} \tag{2}$$

$$\text{AV} = \frac{|V'_D|}{|V_D|}. \tag{3}$$

The second metric we introduce is *network connectivity*. Clearly, the connectivity of the whole network is very important. On one hand, a well-connected network provides better access flexibility [32] because there are more options for routing, or rerouting, the delivery of goods to more customers, if supply or demand patterns change or unexpected events occur. On the other hand, flows of goods or services are often limited and less fluid in networks that are partitioned into small components. In complex network research, *network connectivity* is usually measured by the size of the LCC in which there is a path between every pair of nodes. Here, we incorporate the idea of availability

TABLE I
SOME STANDARD METRICS FOR NETWORK ROBUSTNESS

Name of the metric	**Brief explanations of the metric (based on graph theory)**
Characteristic path length	The average of the shortest path length between any two nodes.
Size of the largest connected component of a network	The number of nodes in the largest connected component of a network.
Average path length in the largest connected component	The average of the shortest path length between any two nodes in the largest connected component of a network.
Maximum path length in the largest connected component	The maximum path length between any two nodes in the largest connected component of a network.

into this metric and use the size of the largest *functional* subnetwork instead of the size of the LCC. For the supply network $G(V, E)$, its largest functional subnetwork is defined as the node set V_{sub}. Nodes in the largest functional subnetwork satisfy the following two requirements

$$\forall v_i, v_j \in V_{\text{sub}} : \exists\ \text{path}_{i,j} \text{ and } \exists\ v_k \in V_{\text{sub}} : v_k \in V_s. \qquad (4)$$

The difference between the old and the new metrics is that there must be at least one supply node in the largest functional subnetwork. A subnetwork of a distribution network cannot function or maintain the supply flow without a supply node in it. When nodes fail during disruptions, a distribution network that features a larger functional subnetwork can maintain a higher level of connectivity, and is considered more robust.

The third and fourth new metrics are both related to *delivery efficiency*. While availability describes whether supplies can be delivered to a demand node from a supply node, it does not measure how "efficient" the delivery is, in terms of lead time and transportation cost. One way to measure delivery efficiency is by the distance between supply and demand nodes. Intuitively, a shorter distance often means that goods can be delivered faster and cheaper, and thus, the network is more efficient. For networks with homogeneous nodes, Latora and Marchiori [33] proposed the network-efficiency metric that is based on characteristic path length. However, in a heterogeneous distribution network, the distance between demand nodes is not as important as *the distance between supply nodes and demand nodes*.

Consequently, we propose two new delivery-efficiency metrics, which are based only on *supply-path lengths*, rather than *all* path lengths as in [33]. In a distribution network, *a supply path for a demand node refers to the path between this demand node and a supply node*. Then, the average (across all demand nodes) of a demand node's shortest supply-path length to its nearest supply node, defined as AVG_DIST in (5), is a measure of how fast supplies can be delivered to demand nodes across the distribution network. We use the reciprocal of the average as a metric for efficiency [defined as BEST_DEF in (6)] so that a higher value corresponds to supplies being nearer and the network being more efficient.

$$\text{AVG\_DIST} = \frac{1}{|V'_D|}\sum_{i=1}^{|V'_D|}\min\{\text{distance}(v_i, v_j), \forall v_j \in V_S\},$$
$$\text{where } v_i \in V'_D \qquad (5)$$

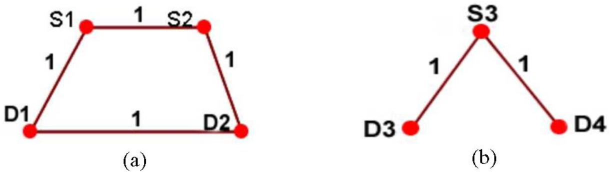


Fig. 3. (a) and (b) Two simple supply networks with supply nodes (denoted with S) and demand nodes (denoted with D). Each edge represents a distance of 1.

$$\begin{aligned}\text{BEST\_DEF} &= \frac{1}{\text{AVG\_DIST}}\\ &= \frac{|V'_D|}{\sum_{i=1}^{|V'_D|}\min\{\text{distance}(v_i, v_j), \forall v_j \in V_S\}},\\ &\qquad \text{where } v_i \in V'_D. \qquad (6)\end{aligned}$$

Efficiency BEST_DEF answers the question "how far away are the nearest supply nodes from demand nodes in the network?" This is essentially the best case scenario for a demand node to access supplies. What about the average case, since all demand will clearly not be filled by the nearest source of supply? Perhaps, one might be tempted to consider the average of shortest supply-path lengths between all pairs of connected demand nodes and supply nodes. However, such an average fails to capture the number of supply nodes that are accessible from a demand node. In fact, with this average, demand nodes that can access more supply nodes often look worse than those that can access fewer supply nodes, as illustrated in the following example.

Fig. 3 shows two simple distribution networks. In the network shown in Fig. 3(a), demand node D1 has access to two supply nodes S1 and S2, with supply-path length of 1 and 2, respectively. D2 is in the same situation. In the network shown in Fig. 3(b), both demand nodes D3 and D4 can access only one supply node S3 with supply-path length of 1. There are four demand–supply pairs in the network shown in Fig. 3(a), namely, D1–S1, D1–S2, D2–S1, and D2–S2. The average shortest supply-path length is $(1 + 2 + 2 + 1)/4 = 1.5$. In the network shown in Fig. 3(b), there are two such pairs, D3–S3 and D4–S3, with an average shortest supply-path length of 1. Although the network shown in Fig. 3(a) has a longer average supply-path length, its supplies are often considered more "accessible," because if a demand node is able to access more supply nodes, it clearly suggests that average delivery efficiency

TABLE II
TAXONOMY OF THE NEW ROBUSTNESS METRICS FOR DISTRIBUTION NETWORKS

System-level metric	**Topology-level metric**	**Brief explanations of topology-level metrics**
Supply Availability	Supply availability rate	The percentage of demand nodes that have access to supplies from at least one supply node.
Network Connectivity	Size of the largest functional sub-network	The number of nodes in the largest functional sub-network, in which there is a path between any pair of nodes and there exists at least one supply node.
Best Delivery Efficiency	Inverse of average minimum supply path length across all demand nodes	The reciprocal of the average of each demand node's shortest supply path length to its nearest supply node.
Average Delivery Efficiency	Adjusted average inverse supply path length across all (supply, demand) path pairs	The average inverse supply path length for all possible demand-supply node pairs, adjusted by a weighting factor for each path.

is greater. Of course, there is a tradeoff between having access to two supply nodes, each at a distance of 10 (or 100), versus one supply node at a distance of 1.

Thus, we introduce a new metric called *average delivery efficiency* that combines both the number of supply nodes that can be accessed by a demand node and also the distance at which each supply node is located. It is based on inverse supply-path length calculation. For demand node D_i, its average delivery efficiency $\mathrm{AVG\_DEF}_{D_i}$ is defined in (7), where k is the total number of supply nodes that D_i can access. The supply nodes are sorted based on their shortest distance to the demand node, ties being broken arbitrarily. Thus, $\mathrm{dist}_{i,j}$ represents the shortest path length from D_i to its jth nearest supply node. For example, $\mathrm{dist}_{i,2}$ is the shortest supply-path length from demand node D_i to its second nearest supply node. The exponent $f(j)$ is a weighting factor to specify the relative importance of shortest supply paths j among the k shortest supply paths to k supply nodes

$$\mathrm{AVG\_DEF}_{D_i} = \sum_{j=1}^{k}\left[\left(\frac{1}{\mathrm{dist}_{i,j}}\right)^{1/f(j)}\right]. \tag{7}$$

While one could define a weighting factor $f(j)$ in many ways, it is reasonable to argue that $f(j)$ should be *a nonincreasing function of* j, because the distance to a nearer supply node is often considered more important than that to a farther supply node. As $1/\mathrm{dist}_{i,j} \leq 1 \,\forall i, j$, the lower the exponent $f(j)$ is, the lower the $(1/\mathrm{dist}_{i,j})^{1/f(j)}$ is. For example, if $f(1) = f(2) = 1$, then equal importance is assigned to both the first and second shortest supply paths. However, if $f(2)$ is reduced to 0.5 and $f(1)$ is kept as 1, then it suggests that the weighting factor for the second path is lower, reflecting the lesser importance of the second shortest path as compared to the shortest one. In general, different $f(j)$ may be customized for different supply networks in various domains. For example, the function $f(j)$ may vary from an exponential to a linear or sublinear decreasing function. (see Appendix A for desirable properties of a metric like AVG_DEF.)

Consequently, the *average delivery efficiency* for the whole distribution network, defined as AVG_DEF in (8), is the average of $\mathrm{AVG\_DEF}_{D_i}$ over all demand nodes in the network. Naturally, a higher AVG_DEF value corresponds to greater efficiency.

$$\mathrm{AVG\_DEF} = \frac{1}{|V_D|}\sum_{i=1}^{|V_D|}\mathrm{AVG\_DEF}_{D_i}. \tag{8}$$

Here, we show how AVG_DEF is calculated for the network in Fig. 3(a). We use $f(j) = 1/j$, thus $f(1) = 1$ and $f(2) = 0.5$. Then, $\mathrm{AVG\_DEF} = (1 + 0.5^2 + 1 + 0.5^2)/2 = 1.25$.

Overall, these metrics reflect the heterogeneous roles of different types of entities in distribution networks and improve our ability to measure supply network robustness. Thus, we believe the new taxonomy is more systematic and realistic as compared to the metrics used in [8]. Table II summarizes our new metrics.

One might also combine these metrics into a single objective function in order to optimize the overall performance of a network, if the context in which a specific distribution network operates is known. For instance, a weighted linear combination of the four metrics may serve as an overall robustness metric. However, we decided to use multiple separate metrics instead of a single composite one so as to gain a better understanding of a supply network's performance from different perspectives.

B. New Rewiring Approach for Distribution Networks (RLR)

Different ways to connect nodes in a network (often called network growth in the literature) will lead to different network topologies [34]. For example, preferential attachment of new nodes with an existing node generates the scale-free topology [19]. Connecting any two randomly chosen nodes in the network with a predefined probability will create an Erdos–Renyi random (ER-random) network [25]. Thadakamalla *et al.*, also presented a military logistic network model that uses arbitrary numbers of edges and *ad hoc* attachment rules for battalions and support units [8].

Our new model, based on the rewiring of a distribution network, is called *RLR*. To rewire a distribution network using

```
Given a supply distribution network $G(V,E)$;
Given a rewiring probability $p_r$ and a re-wiring radius $d_{max}$.
foreach (edge $e_i \in E$) {
        $rnd = Random(0,1)$; //generate a random number $rnd$
        If ($rnd < p_r$ ) {
                $v_i^1$ = endpoint 1 of edge $e_i$ ($v_i^1 \in V$);
                $v_i^2$ = endpoint 2 of edge $e_i$ ($v_i^2 \in V$);
                Case Switch{ //rewire an edge
                        degree($v_i^1$) $>$ degree($v_i^2$):
                                Rewire($e_i$, $v_i^1$, $v_i^2$);
                        degree($v_i^1$) $<$ degree($v_i^2$):
                                Rewire($e_i$, $v_i^2$, $v_i^1$);
                        degree($v_i^1$) $==$ degree($v_i^2$):
                                Rewire($e_i$, $v_i^1$, $v_i^2$) or Rewire($e_i$, $v_i^2$, $v_i^1$);
                }
        }
}
Function Rewire ($e_{rewire}$, $v_{toDisconnect}$, $v_{toKeep}$){
        $E = E - \{e_{rewire}\}$
        Identify $V_r \subset V$, such that $\forall v_j \in V_r$, 0<distance($v_{toKeep}$,$v_j$)$\leq d_{max}$;
        $v_{new}$ = Random($v_j \in V_r$);
        If ($v_{new} \neq v_{toKeep}$ and $v_{new} \notin$ direct neighbors of $v_{toKeep}$){
                $e_{rewire}$ = Connect($v_{toKeep}$,$v_{new}$);
                $E = E + \{e_{rewire}\}$;
        }
}
```

Fig. 4. Pseudocode for the algorithm to generate the RLR network topology.

RLR, we iterate through all edges, and consider the pairs of nodes at both ends of an edge. With a predetermined rewiring probability p_r, an edge will disconnect from one of its two endpoints—the one with higher degree. Then, the other endpoint of the rewired edge will rewire the edge to connect with a randomly chosen node within a radius of $d_{\max}$. Unlike the Thadakamalla model [8], this model does not require special attachment rules for different types of military units and may be applied to existing distribution networks with various topologies.

The rewiring probability p_r essentially determines how much rewiring will occur. On one hand, if $p_r = 0$, no rewiring will take place and the network remains unchanged. On the other hand, if $p_r = 1$, all edges will go through this random rewiring process. The other parameter, maximum rewiring radius $d_{\max}$, imposes a practical constraint for rewiring. In the context of a distribution network, a node may not be able to connect to any randomly selected node at will because the establishment of a connection between two nodes is often associated with cost. Connecting two nodes that are closer to each other is generally more economical. Thus, the upper limit on the rewiring radius reflects this preference on locality. When implementing the algorithm, the radius can be either physical distance (say, in miles), or topological distance (in number of hops/edges).

In general, the rewiring process aims at adding randomness in a controlled way to a distribution network. A higher p_r value will lead to more rewiring, and thus, introduce more randomness, while a lower $d_{\max}$ will impose more control over rewiring. Fig. 4 shows the pseudocode for rewiring a network with RLR. It uses a function called "*Rewire*" that disconnects an edge from an existing node, and reconnects the remaining node (v_{toKeep}) of the edge to a new node (v_{new}) chosen at random, provided v_{new} is not a direct neighbor of v_{toKeep}.

C. Simulation-Based Approach

Lacking access to a large real-world distribution network that can be rewired and disrupted at will for experiments, we must rely on computational simulations. The simulation enables us to generate different distribution networks with various topologies and configurations and to apply the RLR approach to various network topologies to see whether rewiring can help to improve the robustness of distribution networks.

We also need a model to simulate disruptions. In the literature on network robustness, two types of disruption scenarios based on node removal are commonly studied: *random* and *targeted*. In random disruptions, each node has the same probability of failure. This scenario often corresponds to accidents (e.g., fires and power outrage), and unexpected economic events (e.g., recessions and bankruptcy). To simulate random disruptions, we randomly remove nodes from the network. Edges that are connected to them are also removed.

On the other hand, in targeted disruptions, important nodes are more likely to be disrupted than unimportant ones. Examples of targeted disruptions include terrorist and military attacks, which often target critical entities in the system such as network hubs. Among many metrics to measure a node's importance in a network, we chose the widely used *degree centrality* in line with the earlier research [8] [23]. In other words, we assume that the higher the node degree is, the more important it is. The reason for picking degree as the indicator of importance is that node degree is easier for attackers to find. High-degree nodes are often more visible because they are in contact with many other nodes [35]. Other centrality measures, such as *closeness*, *betweenness*, and *eigenvector centrality* [36], require knowledge of the network topology, which is usually difficult for attackers to obtain. To simulate targeted disruptions, we remove nodes in the order of decreasing node degree. In addition, because the removal of one node will affect the degree of some other, we recalculate the degrees of remaining nodes after each node removal. This dynamic update ensures the removal of the node with the highest degree in the remaining network.

Note that the focus of our study is the robustness of distribution networks, and hence, we only consider disruptions at the supply nodes, or supply disruptions. Disruptions at demand nodes are not relevant for our purposes.

IV. Experiment for a Military Logistic Network

In this section, we analyze how a RLR rewiring affects the robustness of distribution networks with the well-known, scale-free, and small-world topologies. Using an experiment for a military logistic network, we describe our method for evaluating and comparing the robustness of different military logistic network topologies using simulations. The results will be illustrated and discussed.

A. RLR Scale-Free Networks

1) Simulation Setup: The simulation scenario is based on the military logistic network example in [8]. In this network,

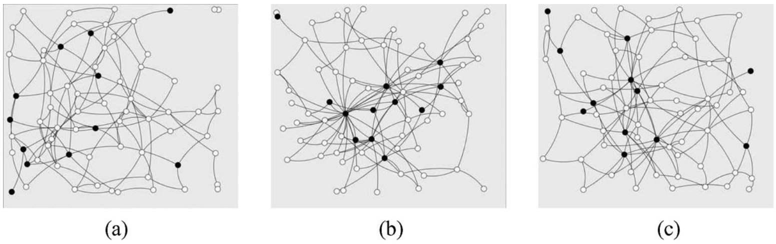


Fig. 5. Snapshots of simulated 70-node, 120-edge supply networks with various topologies. (Supply nodes are denoted in black and demand nodes are in white.) (a) ER-random supply network. (b) Scale-free supply network. (c) RLR scale-free supply network ($p_r = 0.25$).

demand nodes are battalions. We also consider MSBs and FSBs as supply nodes for simplicity. The supply network consists of 1000 nodes, including 166 supply and 834 demand nodes. The supply–demand ratio was estimated from a real-world military logistic system [8]. RLR rewiring is performed with different probabilities and the robustness of the so called *RLR scale-free networks* is analyzed. To better illustrate the robustness of different distribution networks, we will also include an ER-random network in the comparison. For each supply network topology, we will first construct the network using the military logistic network configuration. Then, we will simulate disruptions to those networks and observe their responses on our aforementioned robustness metrics.

We did not include the Thadakamalla model [8] in the comparison because it often makes battalions the network hubs, i.e., nodes with very high degrees, in the resulting supply network. This is not desirable because although a battalion can occasionally forward supplies to other battalions, it is not the primary task of a battalion, and a battalion should not forward supplies more than MSBs and FSBs do. Thus, we expect such a configuration to be rarely used in real-world military logistic systems.

When RLR rewiring the military logistic network, we assume that all the military units are deployed in a battlefield and close to each other. Thus, when generating a RLR scale-free network, the distance between units is not a significant factor for selecting nodes as rewiring destinations. In other words, we set the maximum rewiring radius in the RLR approach to infinity ($d_{\max} = \infty$) so that a rewired edge can randomly select a new destination node among all other nodes.

For illustrative purposes, we show the snapshots of three 70-node, 120-edge military logistic networks with ER-random, scale-free, and RLR scale-free (with $p_r = 0.25$) topologies in Fig. 5(a)–(c). Fig. 6 illustrates the Ln–Ln degree distributions of the three networks.

In our simulation, we remove eight nodes, about 5% of all the supply nodes, between successive observations. Because most attacks in a real-world network will disrupt only a relatively small number of nodes, we simulate disruption scenarios, where the percentage of supply nodes removed lies in the 0%–20% range. During the process of node removal, we track the robustness metrics for each network topology. When evaluating the average delivery efficiency of supply networks, we use $f(j) = 1$ for (7), i.e., assigning equal importance to all supply paths. This experiment is repeated for various topologies in order to facilitate a comparison among them. To ensure a fair comparison, each network topology will have the same number of nodes and edges. The average degree is kept at 3.6 edges per node in our simulations so as to correspond with the military supply network in [8].

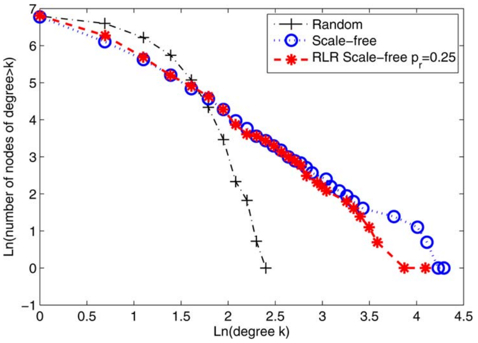
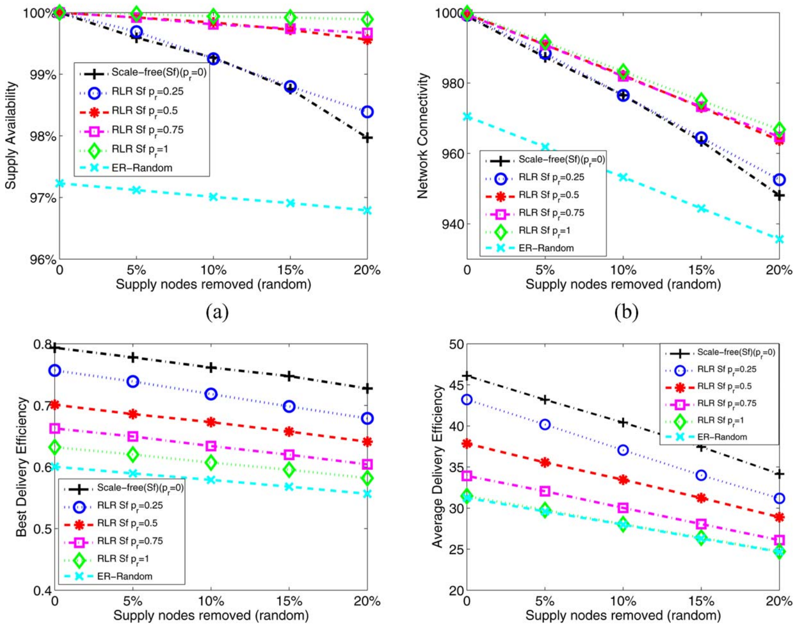


Fig. 6. Distribution of the three simulated supply distribution networks with 1000 nodes each.

2) Simulation Results for Random Supply Disruptions: Fig. 7 shows the responses to random disruptions of six network topologies, including scale-free, ER-random, and four RLR scale-free networks with various p_r. The horizontal axes denote the percentage of supply nodes removed, while the vertical axes are values of the topology-level robustness metrics proposed earlier in this paper. As one would expect intuitively, the performance of all networks decreases when nodes are removed from the network. The ER-random has the least value for all four metrics, with small slopes and lower initial values. The scale-free supply network excels in delivery efficiency (both, best and average). Higher rewiring probabilities for RLR scale-free networks lead to better availability and connectivity, but at the cost of delivery efficiency.

Surprisingly, we find very good performance from the totally rewired scale-free network, i.e., RLR scale-free with $p_r = 1$, which incorporates some level of random attachment in all its edges. Fig. 7(a) and (b) reveals that random disruptions to 20% of its supply nodes have negligible impact on its supply availability, which hardly decreases even 1%. Network connectivity is also well preserved as almost all the remaining nodes are still connected in one functional subnetwork.

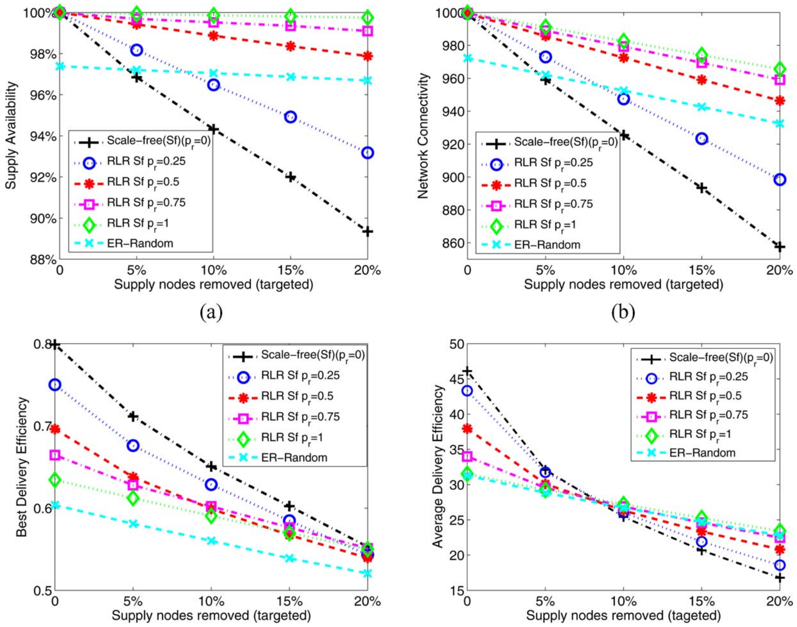
3) Simulation Results for Targeted Supply Disruptions: Arguably, robustness against targeted disruptions is more important than against random disruptions because targeted disruptions are usually more damaging than random ones. Also,



(a) (b)

(c) (d)

Fig. 7. Various military logistic networks' responses to random supply disruptions. Average of 20 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.



(a) (b)

(c) (d)

Fig. 8. Various military logistic networks' responses to targeted supply disruptions. Average of 20 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.

military logistic networks often face more targeted than random attacks from opponents. Fig. 8 shows the responses of the six network topologies to targeted disruptions. Similar to Fig. 7, the horizontal axes denote the percentage of supply-node removal, while the vertical axes are the topology-level robustness metrics. As expected, robustness of all the four supply networks suffers different levels of deterioration when compared with the case of random disruptions.

For the scale-free network, its supply availability and network connectivity deteriorate very rapidly. Although the scale-free network still maintains the highest efficiency at the early stage of disruptions, the deterioration rates on the two efficiency metrics are higher than for the other topologies. For example, scale-free networks have the highest average delivery efficiency when no disruption occurs, 47% higher than that of the ER-random network. However, as supply nodes are removed, the

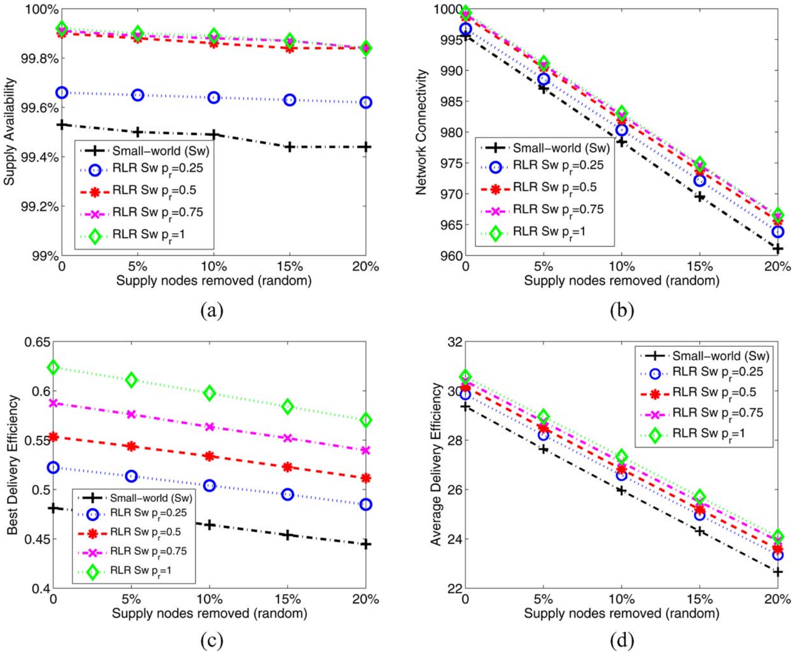


Fig. 9. Various military logistic networks' responses to random supply disruptions. Average of 20 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.

average delivery efficiency falls the fastest for scale-free, which is a major drawback. When 10% of the supply nodes are removed, scale-free already has lower average delivery efficiency than ER-random. An additional 10% removal will make the average delivery efficiency of scale-free 27% lower than that of ER-random. Generally, the performance of scale-free seems to confirm earlier research that it is very fragile to targeted disruptions [23].

At the other end of the spectrum, the ER-random network deteriorates slowly with increasing failure rate on all the four metrics, but it still suffers from poor initial values. For instance, even though its rate of decrease in best delivery efficiency is much lower than for the scale-free and several RLR scale-free networks, 20% supply node removal is still not enough for the ER-random to catch up with the other topologies on the delivery-efficiency metrics.

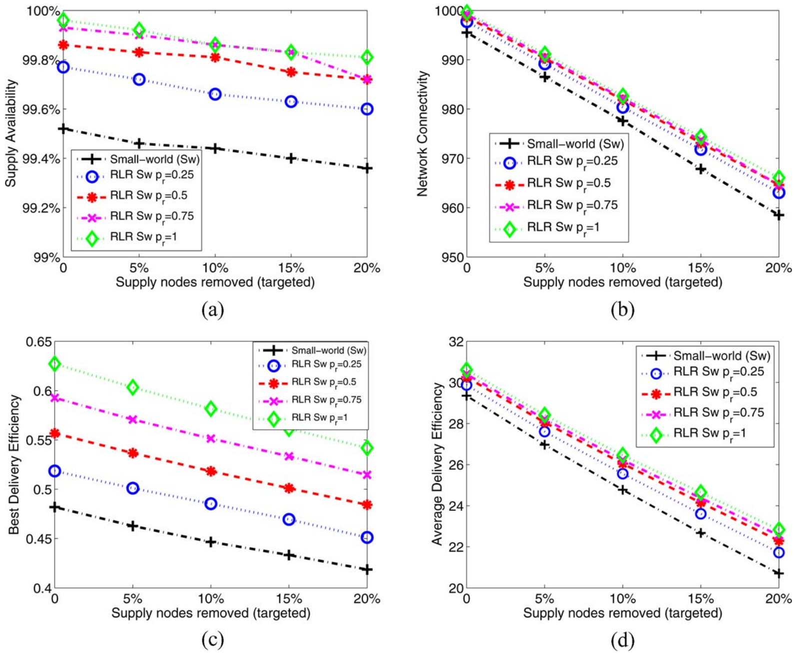
As for the RLR scale-free supply network, it still offers better availability and connectivity than scale-free. Its availability and connectivity also increase when using higher rewiring probability p_r. The supply availability and network connectivity of the RLR scale-free network with $p_r \geq 0.5$ are also higher than ER-random when 0%–20% of the supply nodes are removed. In terms of the efficiency metrics, its performance generally lies in between the scale-free and the ER-random, although the RLR scale-free with $p_r = 1$ slightly outperforms the ER-random in average delivery efficiency. Although higher p_r leads to a lower initial delivery efficiency values, it helps to slow deterioration rates. Take average delivery efficiency as an example. At the very beginning, the scale-free ($p_r = 0$) has the highest average delivery efficiency and the ER-random the least. Most RLR scale-free networks fall between the two, and rewired scale-free with higher p_r have better initial efficiency than those with lower p_r. As supply nodes are removed, the gaps in average delivery efficiency get smaller. After 10% of supply-node removal, the RLR scale-free with $p_r = 1$ actually has the best average delivery efficiency, better than the scale-free, the ER-random, and other rewired scale-free with lower p_r.

B. *Rewiring Small-World Networks With RLR*

As we mentioned earlier, besides the scale-free topology, another popular complex network topology is the small-world [20], which features high clustering coefficients and low characteristic path length. The degree distribution of a small-world network is also more uniform than the highly skewed power law distribution. Adopting the simulation settings in Section 4-A1, we generate a small-world military logistic network using the model proposed in [20], apply RLR to the small-world network, and compare the robustness of the original small-world logistic network with that of the rewired ones (referred to as *RLR small-world networks*).

Fig. 9 illustrates the robustness of the military logistic network with the small-world topology and RLR small-world networks with various p_r when random disruptions occur. RLR small-world networks dominate the original small-world networks on all four metrics. Higher rewiring probability p_r generally leads to better performance. The advantage of RLR small-world networks mainly lies in their good initial performance, especially on the metric of best delivery efficiency. In terms of the rates of performance deterioration when supply nodes are removed, RLR small-world networks are only slightly slower than the small-world network on the metrics of network connectivity and average delivery efficiency.

The five networks' robustness against targeted disruptions (shown in Fig. 10) is similar to that against random disruptions. Although the performance of all the distribution networks



(a)

(b)

(c)

(d)

Fig. 10. Various military logistic networks' responses to targeted supply disruptions. Average of 20 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.

deteriorates slightly faster than in random disruptions, more rewiring still helps RLR small-world to become more robust than small-world.

C. Discussion

According to our simulation study, rewiring a distribution network with RLR will affect its robustness in different ways. We first discuss the case when RLR is applied to a military logistic network with the scale-free topology. Comparing the scale-free distribution network with rewired RLR scale-free networks, we found that *there is no optimal network topology* that dominates all others on every metric in both supply disruption scenarios. Some earlier conclusions about the robustness of scale-free networks still hold in our heterogeneous military logistic networks. For example, while a scale-free network is able to maintain good average delivery efficiency in random disruptions, its robustness against targeted disruptions is unacceptable with low supply availability and network connectivity. Although its initial delivery efficiency values are better than other topologies, they deteriorate rapidly when high-degree supply nodes are disrupted.

Now, we turn to RLR scale-free networks. Recall that the rewiring probability p_r is tunable: a lower p_r will retain more aspects of the original topology, while higher p_r will add greater randomness. One advantage of RLR scale-free with high p_r, say 0.75 or 1, is that very high supply availability and network connectivity are maintained in both random and targeted disruptions (even as high as 20%). However, its delivery efficiency is often not as good as for the other topologies, even with a low rewiring probability, in both disruption scenarios. While topologies such as scale-free and ER-random are usually robust against one type of disruption but fragile to another type, *RLR scale-free networks have the unique property that their behaviors on all four metrics are relatively consistent in both types of disruptions*, which gives rewired scale-free balanced robustness against both types of supply disruptions.

In addition, for RLR scale-free networks, better performance on availability and connectivity is often gained at the cost of delivery efficiency. This tradeoff, together with the tunable rewiring probability, provides another way to balance a distribution network's robustness. If availability or connectivity is more important than delivery efficiency for a distribution network, an RLR scale-free distribution network with high rewiring probability will be preferred. Conversely, for networks in which delivery efficiency is critical, an RLR scale-free distribution network with low rewiring probability may offer a better choice.

Another interesting issue pertains to the RLR scale-free network with $p_r = 1$. Since it randomly rewires every edge in the scale-free network, one might expect it to approach a random network. However, the ER-random network, which is constructed in a purely random manner, does not demonstrate its well-known robustness against targeted disruptions in our heterogeneous distribution networks. Although the ER-random network generally features low performance deterioration rates when supply nodes are removed (in both random and targeted disruptions), it is outperformed by the RLR scale-free network with $p_r = 1$.

Then, what are the differences between the two supply network topologies? The experimental results suggest that the advantage of RLR scale-free with $p_r = 1$ mainly lies in its initial performance. In an ER-random network, edges between any pair of nodes are established based on a predetermined probability. We fear this growth model may leave some nodes with no connection at all.

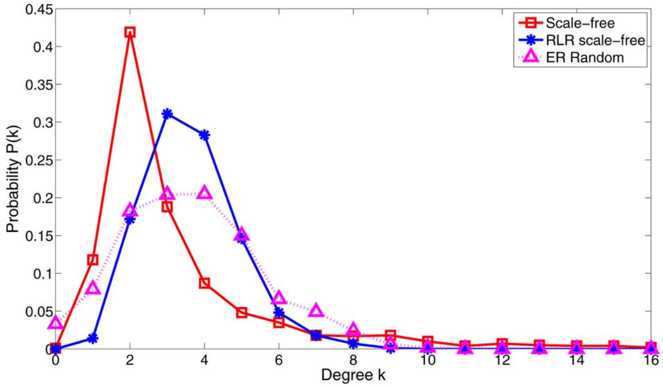


Fig. 11. Degree distributions of simulated supply distribution networks ($p_r = 1$ for the RLR scale-free supply network. All networks have 1000 nodes and 1815 edges).

To confirm our conjecture, we drew the degree distributions of simulated ER-random, scale-free, and RLR scale-free with $p_r = 1$ networks in Fig. 11. All three simulated networks have 1000 nodes and 1815 edges. The horizontal axes denote the degree of nodes, while the vertical axes reflect the probability of finding a node with a given degree. One might observe in Fig. 10 that some nodes have degree 0 and are thus isolated from other nodes in the ER-random network. Such isolation directly affects its initial values on the metrics. As a comparison, the simulated scale-free network has almost no zero-degree node, but features few nodes with very high degrees. The RLR scale-free network takes some advantage of the scale-free network's good initial performance by using a scale-free network as the basis for rewring. As a result, the RLR scale-free has few, or none, disconnected nodes.

Moreover, the degree distributions of simulated RLR scale-free networks are in accord with our theoretical analysis in Appendix B. Compared with the simplified RLR scale-free network with $p_r = 1$ in Appendix B, the simulated rewired one with $p_r = 1$ in Fig. 11 has a much shorter right tail and exhibits a near-Poisson degree distribution. The degree distribution of the simulated RLR scale-free supply network and its performance in the simulations also validate our earlier hypothesis regarding its networks' topology and robustness. In addition, some may notice that the degree distribution of the scale-free network in Fig. 11 features fewer 1-degree nodes than 2-degree nodes. This is different from the monotonically decreasing distribution of the scale-free network in Appendix B. The low probability for 1-degree nodes can be explained by the simulation setting: each new node initiates an average of 1.8 edges in the simulation, and thus, very few nodes have only one edge in the resulting network.

In contrast with the tradeoffs between scale-free and RLR scale-free, when RLR rewiring is applied to a military logistic network with small-world topology, its impact is very positive. RLR small-world networks can help to improve the original network's robustness against both random and targeted disruptions, reflected by their very good performance on all four robustness metrics. Meanwhile, similar to RLR scale-free, the performance of RLR small-world distribution networks is also consistent in random and targeted disruptions.

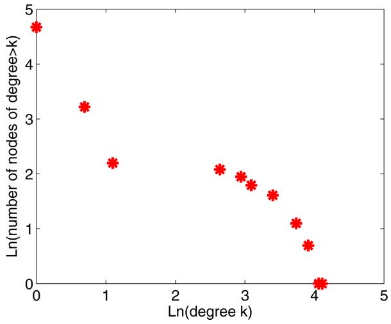


Fig. 12. Ln–Ln degree distribution of the retailer's distribution network in California. It has two scale-free parts. Hence, we call it quasi-scale-free.

In sum, when applied to scale-free networks, RLR rewiring is able to represent both the preferential and random attachment networks at the extreme rewiring probabilities $p_r = 0$ and $p_r = 1$, respectively. Varying p_r between 0 and 1 generates intermediate supply networks that can balance the robustness between scale-free and random distribution networks. When applied to small-world distribution networks, RLR can improve the robustness against both random and targeted disruptions, with higher p_r leading to better performance.

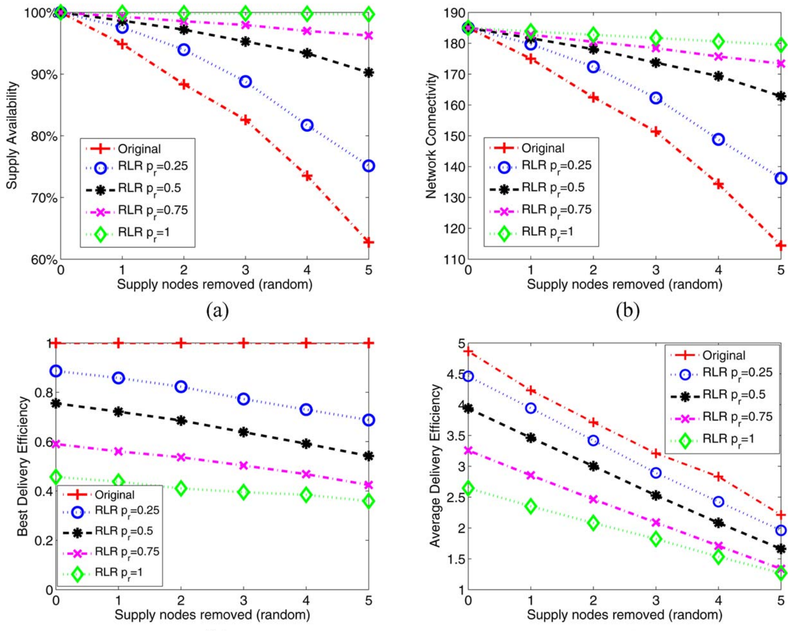
V. Experiment for a Retailer's Distribution Network

To further evaluate the performance of the RLR approach, we conducted another experiment and applied the model to a commercial distribution network—a leading retailer's distribution network in the state of California. Different from the synthesized scale-free or small-world military logistic networks, the retailer's distribution network does not conform to any established complex network topology, and thus, provides a more realistic test bed for RLR.

A. Simulation Setting

The distribution network consists of 185 nodes, including 2 warehouses (both are located in southern California), 7 DCs, and 176 stores. We also have the address of each node, and are able to calculate the physical distance between any two nodes. As this three-level structure is also quite similar to the military logistic network in the earlier experiment, we consider warehouses and DCs as supply nodes, and stores as demand nodes. On the basis of the retailer's rule of building a distribution network, we are able to generate a distribution network with the following realistic configuration: 1) the two warehouses are connected; 2) each DC randomly connects to one or two warehouses and two other DCs; 3) each store uses preferential attachment to connect to a one or two DCs within a radius of 300 miles. Ten percent of all stores are able to connect directly to a warehouse.

The degree distribution of the retailer's distribution network (shown in Fig. 12) is a combination of two power laws. This is because the roles of nodes in the somewhat hierarchical distribution network polarize the node degrees. Lower in the hierarchy, stores' degrees are in the range of 1–3, and follow the power law distribution (on the left), while DCs and warehouses gen-



(a)

(b)

(c)

(d)

Fig. 13. Various retail distribution networks' responses to random supply disruptions. Average of 30 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.

erally have degrees higher than 12, and their node degrees are reflected in the power law distribution on the right. Even though this network is not a scale-free or small-world network, we can still apply the RLR approach and rewire it.

As California is very large and the retailer's facilities are located all across the state, our RLR approach in this experiment will consider the radius limit when rewiring edges. While robustness is important, the cost to operate the distribution network is also a major concern for the retailer. It is expensive to rewire an edge and connect a store in southern California, an area with several DCs, to a DC in northern California 600 miles away. In this experiment, we set the maximum rewiring radius $d_{\max} = 300$ miles so that an edge's rewiring destination must be within a physical distance of 300 miles from the node that the edge currently attaches to.

In the experiment, we also consider both random and targeted disruptions to the distribution network. While random disruptions can happen in any distribution network, this retailer's distribution network may also face targeted disruptions. As a major retailer with hundreds of billions of annual sale around the world, the company is a strategic target for terrorist attacks and cyber attacks [37], which tend to aim at warehouses and DCs that play more important roles in the network. Also, some of the retailer's highly connected warehouses and DCs are located near the coast of southern California, an area that is more subject to earthquakes and tsunamis than other areas in the state.

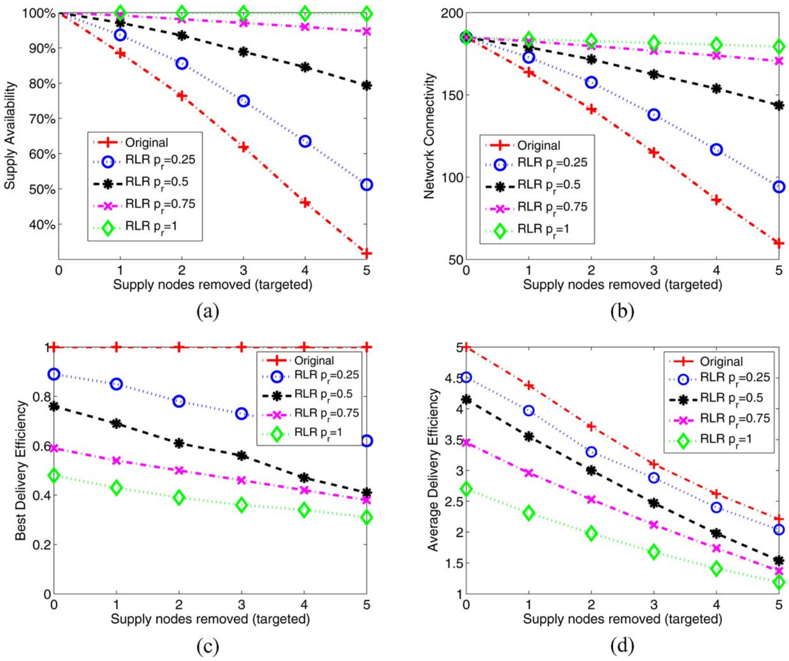
In our simulation, we removed five supply nodes (out of nine)—one at a time between successive observations. During the process of node removal, we track the robustness metrics for each network topology. While evaluating the supply networks, we also set $f(j) = 1$ in (7) for average delivery efficiency. We apply the RLR approach with four different rewiring probabilities ($p_r = 0.25, 0.5, 0.75,$ and 1) to the original network ($p_r = 0$) and compare the robustness of rewired networks (referred to as *RLR retail networks*) with the original one.

B. *Experimental Results*

Figs. 13 and 14 show the performance of the five distribution networks against random and targeted disruptions, respectively. The horizontal axes denote the number of supply nodes that have been removed, and the vertical axes are the topology-level supply-network robustness metrics. As one can see, the results are similar to those for the military logistic network.

The original distribution network is able to maintain very good delivery efficiency in both types of disruptions. Its delivery efficiency does not change when supply nodes are removed because, as noted earlier, nodes in the network generally follow a hierarchical structure. Stores only connect to DCs or warehouses, but do not connect to other stores. Thus, if a store can still access a DC or a warehouse after disruptions, the closest DC or warehouse is always the store's immediate neighbor. However, when disruptions happen, the network is fragmented easily and many stores lose access to DCs or warehouses, as shown by its very fast deterioration in network connectivity and supply availability, especially in targeted disruptions.

In summary, the experiment on the retailer's distribution network also reveals that no network topology can dominate all others on every metric, but it is important to understand the tradeoffs that are involved. The experiment also validates the advantage of RLR retail networks on supply availability and network connectivity, as well as its stable performance in both random and targeted disruptions.



(a)

(b)

(c)

(d)

Fig. 14. Various retail distribution networks' responses to targeted supply disruptions. Average of 30 runs. (a) Supply availability. (b) Network connectivity. (c) Best delivery efficiency. (d) Average delivery efficiency.

As mentioned earlier, some retailers may adjust or rebuild their distribution networks to adapt to the changing market conditions. Our approach offers a simple yet effective heuristic strategy to improve the distribution network's robustness on supply availability and network connectivity. A manager of the distribution network can add some controlled randomness into the existing network by rewiring edges. The manager can select new destination of a rewired edge among nodes that are not too far away from the remained node of the edge. The tunable rewring probability and the maximum rewiring distance also allow the retailer to balance the distribution network's availability/connectivity and delivery efficiency on the basis of robustness requirements and the operation budget.

VI. Conclusion and Future Work

In this paper, we study the robustness of heterogeneous distribution networks against supply disruptions from the perspective of complex network topologies. We first propose the new taxonomy of distribution-network robustness metrics to reflect the fact that nodes play heterogeneous roles in a distribution network, which is not the case for many other networks. Hence, the notions of robustness change. The taxonomy consists of system-level metrics, including supply availability, network connectivity and delivery efficiency, and corresponding topology-level metrics. The second contribution of this paper is the new RLR approach, which is based on probabilistic and localized rewiring of a distribution network. Such rewired distribution networks rewired with the RLR approach with various rewiring probabilities have some nice robustness properties under both random and targeted supply disruptions. In our experiments, we apply the model to military logistic networks with scale-free and small-world topologies and the retailer's distribution networks to compare the robustness of original and rewired networks in detail using computational simulations. The results suggest that the rewired distribution networks generally have stable robustness against both types of disruptions.

We found that the choice of distribution network topology affects its robustness, and the proposed RLR approach can improve the robustness of a distribution network in supply availability and network connectivity, and is a good option in situations where both random and targeted disruptions can occur. We also compared the effect of varying the rewiring probability p_r on the performance. Increasing p_r, i.e., bringing more controlled randomness into the network, generally leads to better supply availability and network connectivity, but at the cost of delivery efficiency, if the original network has a nonuniform or skewed degree distribution. This is intuitively meaningful. To decide the optimal value for p_r, a designer or manager should consider the tradeoff between the higher costs of accessing supply nodes because of longer distances when p_r is high versus the cost of stock outs, if some nodes cannot obtain supplies when p_r is low.

Although we use a military logistic network and a retailer's distribution network as two case studies from different industries, the taxonomy of robustness metrics and the RLR approach may also provide insights to the study and design of robust distribution networks in other domains or industries. Specifically, our approach provides a simple strategy for supply-chain designers or managers to adjust or fine-tune existing distribution networks and get balanced robustness on the four new metrics when both random and targeted disruptions are likely to happen. Our simulation platform also provides the basis for the future development of a decision support tool. Such a tool will help managers to: 1) evaluate the robustness of an existing supply network; 2) assess how possible rebuilding strategies affect the resulting network's robustness; and 3) quickly make rewiring decisions when disruptions occur. In addition, the research may also be applicable in other complex networks whose operations rely on the delivery of people, information, goods, or services between entities with heterogeneous roles. Example networks with similar features may include communication networks such as the Internet (with servers and clients), and infrastructure networks such as power grids.

There are several areas that we would like to address in future. First, in our simulation of disruptions, we only consider the removal of nodes, which corresponds to the failures of entities in a supply network. Actually, a real-world supply network may also face disruptions of connections, e.g., a road block may force a manufacturer to find an alternative path to deliver the goods. Thus, it would be useful to study the removal of edges from the supply network. Second, our analysis of robustness in this paper is only on the topological level. Nevertheless, the design of supply networks in the real world needs to consider more operational level factors and constraints, such as the capacities of supply nodes, the needs of demand nodes, and the cost of transportation. Thus, we also plan to apply network optimization techniques to robustness analysis so that this research can provide better decision support.

Third, as suggested in earlier research [38], we would also like to study the effect of adaptive behavior, such as increased capacity and new delivery routes, on the distribution network robustness in the presence of disruptions. Fourth, this research classifies nodes in a distribution network into two roles: supply and demand nodes. While this classification is simple and straightforward, it may overlook the diversity of node roles in a supply network. By incorporating more heterogeneous roles into this research, we will be able to improve the validity of our conclusion. Other possible research directions include a more analytical study of the robustness of networks rewired with RLR, and the cascading failures of nodes caused by load redistribution [39].

Appendix A

Properties of a Good Metric for Average Delivery Efficiency

The *average delivery efficiency* metric must integrate in the evaluation *both the number of accessible supply nodes* and *the length of supply paths to those supply nodes*. For demand node D_i, its average delivery efficiency AVG_DEF_{D_i} must satisfy the following three requirements (under the reasonable assumption that higher average delivery efficiency is better).

1) If two demand nodes can access the same number of supply nodes, the metric should favor the one with shorter supply-path length. For example, given two demand nodes $D_p, D_q \in V_D$, both nodes can access m supply nodes $S_1, S_2, \ldots, S_m \in V_S$ with shortest supply-path lengths $l_{p,1}, l_{p,2}, \ldots, l_{p,m}$ and $l_{q,1}, l_{q,2}, \ldots, l_{q,m}$, respectively. Then, the average delivery efficiency value of the two demand nodes must satisfy the following equation:

$$\text{If } \forall i \in [1, m], l_{p,i} \le l_{q,i}, \quad \text{then } \text{AVG\_DEF}_{D_p} \le \text{AVG\_DEF}_{D_q}. \tag{9}$$

2) The metric should provide some reward to a demand node that can access more supply nodes. For instance, demand node $D_p \in V_D$ can only access supply nodes $S_1, S_2, \ldots, S_m \in V_S$ with shortest supply-path lengths $l_{p,1}, l_{p,2}, \ldots, l_{p,m}$. Demand node $D_q \in V_D$ can also access these m supply nodes, with shortest supply-path lengths $l_{q,1}, l_{q,2}, \ldots, l_{q,m}$, respectively. However, D_q can also access k, where $k \ge 1$, additional supply nodes $S_{m+1}, \ldots, S_{m+k} \in V_S$ with shortest supply-path lengths $l_{p,m+1}, \ldots, l_{p,m+k}$. Then, the following equation must hold:

$$\text{If } \forall i \in [1, m] : l_{p,i} = l_{q,i}, \quad \text{then } \text{AVG\_DEF}_{D_p} < \text{AVG\_DEF}_{D_q}. \tag{10}$$

3) The metric must be able to handle the situation when a demand node is not connected to any supply node, i.e., its shortest supply-path length to any supply node is infinity. If demand node $D_p \in V_D$ cannot access any supply node, then $\text{AVG\_DEF}_{D_p} = 0$.

Appendix B

Theoretical Analysis of the Degree Distribution for Simplified RLR Scale-free Networks

In networks with homogeneous nodes, degree distribution is often closely related to the network's robustness [23]. Now, let us briefly look at the degree distribution $P_{\text{RL}}(k)$ of a simplified RLR scale-free network with n nodes and m edges. Assume $P(k_0) = k_0^{-r}$ is the degree distribution of the scale-free network generated with the preferential attachment model [19]. The maximum node degree is D and the rewiring probability is p_r. Then, we have (11), where $P_{\text{discon}}(x, k_0)$ is the probability that x edges are disconnected from a node with degree k_0; $P_{\text{new}}(k - k_0 + x, mp_r)$ is the probability that among all the mp_r edges to be rewired, $k - k_0 + x$ connect to the same node. Both probabilities are based on binomial distributions

$$P_{\text{RL}}(k) = \sum_{k_0=0}^{D} P(k_0) \left[\sum_{x=0}^{k_0} P_{\text{discon}}(x, k_0) P_{\text{new}}(k - k_0 + x, mp_r) \right]. \tag{11}$$

For the purpose of simplicity, we assume that when rewiring an edge, we randomly choose one end to disconnect and set $d_{\max} = \infty$. Using this simplified rewiring, we have

$$P_{\text{discon}}(x, k_0) = \binom{k_0}{x} \left(\frac{p_r}{2}\right)^x \left(1 - \frac{p_r}{2}\right)^{k_0 - x} \tag{12}$$

$$P_{\text{new}}(k - k_0 + x, mp_r) = \begin{cases} \binom{mp_r}{k - k_0 + x} \left(\frac{1}{n-2}\right)^{k-k_0+x} \left(1 - \frac{1}{n-2}\right)^{mp_r - k + k_o - x}, & \text{if } k - k_0 + x \ge 0 \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

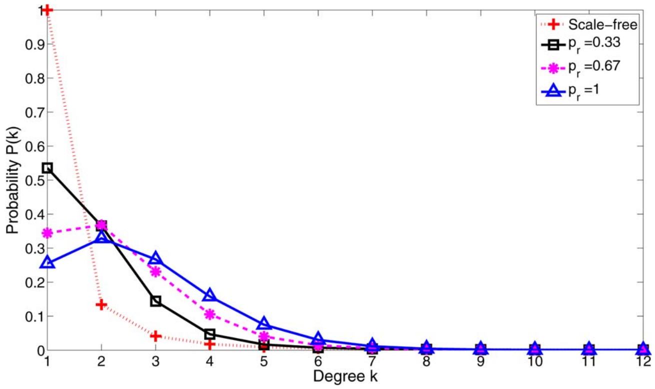


Fig. 15. Inferred degree distributions of scale-free and three simplified RLR rewired scale-free networks.

The expected value of $P_{\mathrm{discon}}(x, k_0)$ is $E(P_{\mathrm{discon}}(x, k_0)) = k_0 p_r/2$. This means that a node with degree k_0 in the scale-free network will on average lose $k_0 p_r/2$ edges in the rewiring process. The expected value of $P_{\mathrm{new}}(k - k_0 + x, m p_r)$ is $E(P_{\mathrm{new}}(k - k_0 + x, m p_r)) = m p_r/(n - 2)$. As $n \gg 2$, $E(P_{\mathrm{new}}(k - k_0 + x, m p_r)) \approx m p_r/n$, where $m/n = \langle k_0 \rangle$ is the average degree in the network. We can then infer that a node in the original scale-free network will, on average, get $\langle k_0 \rangle p_r$ new edges in the rewiring process. As a result, a node with original degree k_0 will on average have degree $k_0 + \langle k_0 \rangle p_r - k_0 p_r/2$ after rewiring. In the rewired network, a node with original degree $k_0 > 2\langle k_0 \rangle$ will most likely have lower degree, while a node with original degree $k_0 < 2\langle k_0 \rangle$ will generally get higher degree.

Using (11)–(13), we can infer the degree distributions of simplified rewired networks. In Fig. 15, we draw the inferred degree distributions of three simplified rewired networks, each with different rewiring probabilities. The horizontal axes denote the degree of nodes; the vertical axes reflect the probability that a node has a given degree. As a comparison, we also include the scale-free network with degree distribution $P(k) = k^{-2.9}$ [19]. Each network has 1000 nodes and 1815 edges. The maximum node degree D is set to 70, but Fig. 15 only shows probabilities for node degrees up to 12, because the probabilities for still higher degrees nodes is very small. As the figure shows, a higher rewiring probability for the simplified rewired network will lead to fewer high-degree nodes and more nodes with low and medium degrees. The degree distributions of rewired networks generally become less skewed than that of the scale-free network. As the rewiring probability increases, the degree distribution of a simplified rewired scale-free network gradually approaches a Poisson distribution.

Recall that in the RLR approach, instead of randomly choosing which node to disconnect, we actually disconnect an edge from the node with higher degree, which means high-degree nodes would lose and low-degree nodes would gain more edges in the rewiring process. As a result, the degree distribution of a RLR scale-free network should be more homogeneous than that of a simplified rewired network with the same rewiring probability, which means a RLR scale-free network will have many nodes with medium degrees and few nodes with high or low degrees. Earlier research on networks revealed that robustness in the presence of targeted failures increases when nodes have similar degrees [23]. Thus, we hypothesize that RLR scale-free should have better robustness than scale-free networks in targeted supply disruptions. We will validate this hypothesis with our simulations of specific distribution networks.

ACKNOWLEDGMENT

The authors would like to thank the Associate Editor and the Reviewers for their valuable comments and insights that helped to improve the paper. They also thank Dr. Robert Novack for sharing his knowledge about supply networks with them.

REFERENCES

[1] A. Surana, S. Kumara, M. Greaves, and U. N. Raghavan, “Supply-chain networks: a complex adaptive systems perspective,” *Int. J. Prod. Res.*, vol. 43, no. 20, pp. 4235–4265, 2005.

[2] H. L. Lee, V. Padmanabhan, and S. Whang, “The bullwhip effect in supply chains,” *Sloan Manag. Rev.*, vol. 38, no. 3, pp. 93–102, 1997.

[3] J. Rice and F. Caniato, “Building a secure and resilient supply network,” *Supply Chain Manag. Rev.*, vol. 7, no. 5, pp. 22–30, 2003.

[4] S. Chopra and M. S. Sodhi, “Managing risk to avoid supply-chain breakdown,” *MIT Sloan Manag. Rev.*, vol. 46, no. 1, pp. 53–61, 2004.

[5] K. B. Hendricks and V. R. Singhal, “An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm,” *Prod. Oper. Manag.*, vol. 14, no. 1, pp. 35–52, 2005.

[6] P. R. Kleindorfer and G. H. Saad, “Managing disruption risks in supply chains,” *Prod. Oper. Manag.*, vol. 14, no. 1, pp. 53–68, 2005.

[7] T. Wu, J. Blackhurst, and P. O’Grady, “Methodology for supply chain disruption analysis,” *Int. J. Prod. Res.*, vol. 45, no. 7, pp. 1665–1682, 2007.

[8] H. P. Thadakamalla, U. N. Raghavan, S. Kumara, and R. Albert, “Survivability of multiagent-based supply networks: A topological perspective,” *IEEE Intelligent Systems*, vol. 19, no. 5, pp. 24–31, Sep./Oct. 2004.

[9] B. M. Beamon, “Humanitarian relief chains: issues and challenges,” in *Proc. 34th Int. Conf. Comput. Ind. Eng.*, 2004, pp. 77–82.

[10] R. Martin, “Changing the mind of the corporation,” *Harvard Bus. Rev.*, vol. 71, no. 6, pp. 81–94, Nov./Dec. 1993.

[11] E. D. Fassoula, “Transforming the supply chain,” *J. Manuf. Technol. Manag.*, vol. 17, no. 6, pp. 848–860, 2006.

[12] G. H. Subramanian and A. C. Iyigungor, “Information systems in supply chain management: a comparative case study of three organisations,” *Int. J. Bus. Inf. Syst.*, vol. 1, no. 4, pp. 370–386, 2006.

[13] G. Lao and L.Xing, “Supply chain system integration in retailing: A case study of LianHua,” in Research and Practical Issues of Enterprise Information Systems II, L. Xu, A. Tjoa, and S. Chaudhry, Eds., Boston: Springer-Verlag, 2008, vol. 254, pp. 519–528.

[14] “BaselineMagazine, “The limited designs supply chain to begin and end with the customer,” *Baseline*, Apr. 3, 2006.

[15] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, “Complex networks: Structure and dynamics,” *Physics Reports*, vol. 424, no. 4–5, pp. 175–308, 2006. DOI: 10.1016/j.physrep.2005.10.009.

[16] K. Zhao, J. Yen, C. Maitland, A. Tapia, and L.-M. N. Tchouakeu, “A formal model for emerging coalitions under network influence in humanitarian relief coordination,” presented at the 2009 Spring Simul. Conf., San Diego, CA, 2009.

[17] R. M. Anderson and R. M. May, *Infectious Diseases of Humans: Dynamics and Control*. London, U.K.: Oxford Univ. Press, 2002.

[18] J. Leskovec, L. A. Adamic, and B. A. Huberman, “The dynamics of viral marketing,” *ACM Trans. Web*, vol. 1, no. 1, art. 5, 2007.

[19] A. L. Barabasi and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[20] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks,” *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[21] H. Sun and J. Wu, “Scale-free characteristics of supply chain distribution networks,” *Modern Phys. Lett. B*, vol. 19, no. 17, pp. 841–848, 2005.

[22] K. Wang, Z. Zeng, and D. Sun, “Structure analysis of supply chain networks based on complex network theory,” in *Proc. 2008 4th Int. Conf. Semant., Knowl. Grid*, 2008, pp. 493–494.

[23] R. Albert, H. Jeong, and A. L. Barabasi, “Error and attack tolerance of complex networks,” *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[24] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, “Attack vulnerability of complex networks,” *Phys. Rev. E*, vol. 65, no. 5, pp. 056109-1–056109-14, 2002.

[25] P. Erdos and A. Renyi, “On random graphs,” *Publicationes Mathematicae.*, vol. 6, pp. 290–297, 1959.

[26] T. H. Grubesic, T. C. Matisziw, A. T. Murray, and D. Snediker, “Comparative approaches for assessing network vulnerability,” *Int. Regional Sci. Rev.*, vol. 31, no. 1, pp. 88–112, 2008.

[27] G. W. Klau and R. Weiskircher, *Robustness and Resilience*. Berlin/Heidelberg, Germany: Springer-Verlag, 2005, pp. 417–437.

[28] L. d. F. Costa, F. A. Rodrigues, G. Travieso, and P. R. V. Boas, “Characterization of complex networks: A survey of measurements,” *Adv. Phys.*, vol. 56, no. 1, pp. 167–242, 2007.

[29] R. Albert, I. Albert, and G. L. Nakarado, “Structural vulnerability of the north american power grid,” *Phys. Rev. E*, vol. 69, no. 2, pp. 025103(R)-1–025103(R)-4, 2004.

[30] A. Neely, M. Gregory, and K. Platts, “Performance measurement system design: A literature review and research agenda,” *Int. J. Oper. Prod. Manag.*, vol. 15, no. 4, pp. 80–166, 1995.

[31] A. Feigenbaum, *Total Quality Control*. New York: McGraw-Hill, 1961.

[32] S. Vickery, R. Calantone, and C. Dröge, “Supply chain flexibility: an empirical study,” *J. Supply Chain Manag.*, vol. 35, no. 3, pp. 16–24, 1999.

[33] V. Latora and M. Marchiori, “Efficient behavior of small-world networks,” *Phys. Rev. Lett.*, vol. 87, no. 19, pp. 198701-1–198701-4, 2001.

[34] R. Albert and A. L. Barabasi, “Statistical mechanics of complex networks,” *Rev. Modern Phys.*, vol. 74, no. 1, pp. 47–97, 2002.

[35] V. Latora and M. Marchiori, “Vulnerability and protection of infrastructure networks,” *Phys. Rev. E*, vol. 71, no. 1, pp. 015103(R)-1–015103(R)-4, 2005.

[36] M. E. J. Newman, *Mathematics of Networks*, 2nd ed. Basingstoke, U.K.: Palgrave Macmillan, 2008.

[37] M. Warren and W. Hutchinson, “Cyber attacks against supply chain management systems: A short note,” *Int. J. Phys. Distrib. Logist. Manag.*, vol. 30, no. 7–8, pp. 710–716, 2000.

[38] T. Y. Choi, K. J. Dooley, and M. Rungtusanatham, “Supply networks and complex adaptive systems: Control versus emergence,” *J. Oper. Manag.*, vol. 19, no. 3, pp. 351–366, 2001.

[39] P. Crucitti, V. Latora, and M. Marchiori, “Model for cascading failures in complex networks,” *Phys. Rev. E*, vol. 69, no. 4, pp. 045104-1–045104-4, 2004.

Kang Zhao received the M.S. degree in computer science from Eastern Michigan University, Ypsilanti, and the B.E. degree in electrical engineering from Beijing Institute of Technology, Beijing, China. He is currently working toward the Ph.D. degree at the College of Information Sciences and Technology, the Pennsylvania State University, University Park.

His current research interests include the simulation and analysis of complex networks (including social, interorganizational and supply-chain networks), social computing, agent-based models, and complex systems.

Mr. Zhao was the recipient of the R.W. Graham Endowed Graduate Fellowship and the 2010 Network Science Exploration Research Grant at The Pennsylvania State University.

Akhil Kumar received the Ph.D. degree from the University of California, Berkeley.

Previously, he was on the faculties at Cornell University and University of Colorado. He is currently a Professor of information systems at the Smeal College of Business, The Pennsylvania State University, University Park. He has authored or coauthored more than 80 scientific papers in academic journals and international conferences, and also held many editorial positions. He has done pioneering work in data replication and XML-based workflows. His research interests include workflow systems, e-services, distributed information systems, and intelligent systems.

John Yen (F'00) received the B.S. degree in electrical engineering from National Taiwan University, Taiwan, the M.S. degree in computer science from Santa Clara University, Santa Clara, CA, and the Ph.D. degree in computer science from the University of California, Berkeley.

He is currently the University Professor and the Director for Strategic Initiatives at the College of Information Sciences and Technology, The Pennsylvania State University, University Park. He His research interests include intelligent agents, decision supports, and social network analysis, especially within the context of extreme events and social dynamic modeling.

Dr. Yen received the National Science Foundation (NSF) Young Investigator Award in 1992.