Transportation Research Part E 145 (2021) 102166

Contents lists available at ScienceDirect

Transportation Research Part E

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

The impact of congestion on protection decisions in supply networks under disruptions☆

Anubhuti Parajuli [a], Onur Kuzgunkaya [a,*], Navneet Vidyarthi [b]

[a] Department of Mechanical Industrial and Aerospace Engineering, Gina Cody School of Engineering and Computer Science, Concordia University, Montreal, QC H3G 1M8, Canada

[b] Department of Supply Chain and Business Technology Management, John Molson School of Business, Concordia University, Montreal, QC H3G 1M8, Canada

ARTICLE INFO

Keywords:
Contingent capacity planning
Interdiction
Disruption
Congestion
Fortification
Trilevel optimization

ABSTRACT

We analyze the impact of congestion on the protection decisions of supply networks for mitigating major disruption. We present a tri-level mixed integer programming model to identify critical facilities to secure and backup plans with appropriate capacity levels and response speeds during disruption. The congestion arising at the facilities as a result of flow reallocation from the disrupted facilities is modelled as a convex cost function. We present an implicit enumeration algorithm to solve the tri-level model. The computational results demonstrate the efficiency of the solution method. Our analysis depicts that a decentralized protection strategy is recommended under congestion.

1. Introduction

The protection planning of supply networks has become increasingly important amidst the risks of catastrophic disruptions. The global trends in outsourcing, globalization, shorter product life cycles, just in time delivery and other lean practices have increased vulnerability of supply chains to disruptions while lowering its operational costs. In the short term, disruptions lead to increased transportation costs, order delays and lost sales but also affect market share with long term implications. Catastrophic events (e.g., earthquakes, floods, terrorist attacks, hurricanes) causing disruption in the upstream supply chain have been reported to affect wider supply chain operations due to its ripple effect downstream (Ivanov and Dolgui 2014, Dolgui et al. 2018). Despite numerous supply-chain upheavals inflicted by disasters in the last decade — including the eruption of a volcano in Iceland, the Japanese earthquake and tsunami, Thailand floods, and Hurricanes Maria and Harvey — most companies still found themselves vulnerable to the recent coronavirus (COVID 19/SARS-CoV-2) pandemic (Choi, 2020). Ivanov (2020) demonstrates the impact of epidemic propagation on supply chain performance. For example, due to the pandemic, many companies have reported severe supply disruptions as they rely on a fewer number of suppliers (often single or dual suppliers) rather than a large and diversified supply base, making it impossible for them to meet downstream demand in case of supply disruptions. Furthermore, many supply chains have reported that their capacity have been impacted in three primary ways: (1) factory closures or manufacturing slowdowns, (2) limited access to employees due to quarantines, and (3) limited access to logistics (e.g. transportation, warehousing) due to closures or slowdowns. Thus, the recent

☆ This paper is a part of the PhD dissertation of the first author.

* Corresponding author.
E-mail addresses: a_paraju@encs.concordia.ca (A. Parajuli), onurk@encs.concordia.ca (O. Kuzgunkaya), n.vidyarthi@concordia.ca (N. Vidyarthi).

https://doi.org/10.1016/j.tre.2020.102166
Received 28 February 2020; Received in revised form 30 September 2020; Accepted 8 November 2020
Available online 8 December 2020

coronavirus pandemic has highlighted the vulnerability of global supply chains to worst case conditions (Fortune, 2020). Protection of critical network components and maintaining effective recourse actions are crucial measures to avoid major losses from disruptions.

The strategies for disruption risk mitigation can broadly be viewed as "preventive strategy" and "recovery strategy". While preventive strategies are driven by system security concerns, they are similar to increasing the mean time to failure (*MTTF*) of the infrastructure systems. The recovery strategies, on the other hand, are driven by resiliency concerns and can be compared to reducing the mean time to repair (*MTTR*). Preventive risk management strategies follow practices of protecting supply flows through proactive redundancy measures such as acquiring redundant suppliers, inventory backup or protection (hardening) of supply facilities. Redundancy measures build supply chain capability towards risk mitigation, but these measures alone may not be enough under a major disruption. For example, inventory can be effective under minor disruptions such as due to machine failures or routine maintenance but under major disruptions, holding inventory leads to higher costs.

Recovery strategies for disruption risk mitigation rely on reactive measures for a quick recovery from disruptions (Ivanov et al. 2018, Pavlov et al. 2017). Contingent capacity/production backup can be considered a recovery strategy since it focuses on recovering lost flows through a backup production. Such a strategy does not lead to the accumulation of inventory as backup production can only be initiated after disaster occurrence and therefore is more cost effective under a major disruption. Capacity of a production facility can be contingently adjusted (ramped up) to partially recover the lost capacities due to disruptions or to partially/completely meet the re-routed demands from the failed facilities. This is especially facilitated in modern flexible or reconfigurable manufacturing systems which can make quick capacity change-over to adapt to fluctuating demands (Wang and Koren 2012, Putnik et al. 2013). A major consideration for these systems is how fast the desired level of backup production can be made available. This response time is dependent on the manufacturing system structure of a backup production facility. A scalable facility can quickly ramp up capacities in small increments, whereas a facility relying on dedicated equipment to reduce production cost will have a slower response time (Ebrahim Nejad et al., 2014). Response speed is related to response time and determines how fast a facility can reach its desired level of production. Hence, response speed and back up capacity volumes are critical parameters for efficient design of a backup resource for contingent recovery actions.

Congestion of facilities from demand overloads during disruption periods will affect the recovery actions by lowering throughput and causing supply delays. This can create a short-term sales loss and long-term demand forfeitures, especially when customer demand is sensitive to availability. The production capability of a manufacturing system is overestimated when congestion is ignored, leading to an inappropriate selection of backup capacities for recovery and a suboptimal supply network performance. The impact of facility congestion on supply and service level and the importance of considering this effect in decision analysis have been emphasized in several relevant and recent articles (Zhang et al. 2011, Aboolian et al. 2012, An et al. 2015, Kian and Kargar 2016, Marufuzzaman and Eskioglu 2017, Alumur et al. 2018, Azizi et al. 2018, Berman and Krass 2019, Poudel et al. 2019, Alkaabneh et al. 2019). It is often possible to manage congestion through backup capacity expansion, however under a limited protection budget, only a finite capacity expansion is possible which warrants the need to analyze the impacts of congestion in proper planning of such backup capacity.

In this paper, we investigate the congestion impacts driving the operational costs of a supply network subject to major disruption risks and develop robust and cost-effective protection solution to cope with such occurrences. The congestion cost is modeled as a flow dependent power law convex function. A major disruption is modeled utilizing attacker as an agent that can create maximum loss through intelligently targeted facility attacks. Countering this type of disruption and the resulting system loss poses significant challenge, as attackers tend to moderate attacks by observing the state of the system. The protection problem is therefore posed in a game theoretic framework of attack and defense resulting in a tri-level *MIP* optimization model. This modeling approach is commonly applied for infrastructure vulnerability assessment and protection and known in the literature as interdiction and fortification models (Cappanera and Scaparra, 2011; Church and Scaparra, 2007; Losada et al., 2012). A binary search tree algorithm is utilized to solve the developed tri-level optimization problem in which protection strategies are implicitly enumerated, following sequential attack and protection decisions.

The contribution of this article is the integration of congestion effects in a supply network protection model for disruption risk mitigation. Varying congestion profiles have been considered to understand the supply network performance under different congestion levels and its influence on the protection design decisions. The study has enhanced the scope and applicability of the interdiction-fortification modeling framework and its solution methodology, while delivering valuable managerial insights for key protection design decisions influencing backup capability of the supply system. One major finding in the study suggests that a centralized protection with high volume backup production with faster response speeds are generally not desirable when congestion impacts are considered, and risk aversion is a decision priority. When congestion related costs are significant, a decentralized strategy that distributes smaller protection budget over a larger number of facilities lead to a better supply network performance due to flow distribution. This finding is in line with recent discussions with post COVID-19 era supply chain strategies of decentralization of manufacturing capabilities (The World Economic Forum COVID Action Platform, 2020).

The remainder of the sections are organized as follows. Section 2 provides a brief review of the literature. Section 3 provides the problem statement and model formulation. The linearization of the congestion cost function is also described in Section 3. In Section 4, the solution methodology to solve the resulting tri-level defender-attacker-defender model is presented. The numerical results are presented in Section 5 and Section 6 concludes with future research directions.

2. Literature review

The literature relevant to supply chain disruption risk mitigation and management have increased in the recent years, highlighting the importance of advanced protection planning and resilient design of logistics and supply networks (Bier et al. 2020, Xu et al. 2020).

Table 1
Classification of relevant literature on features of risk and mitigation policy.

Articles	Risk Feature		Mitigation Feature	
	Risk averse	Risk neutral	Preventive	Recovery
Church and Scaparra (2007)	√		√	
Berman et al. (2007)		√	√	
Scaparra and Church (2008a, 2008b)	√		√	
Aksen et al. (2010)	√		√	
Cui et al. (2010)		√	√	
Lim et al. (2010)		√	√	
Qi et al. (2010)		√	√	
Li and Ouyang (2010)		√	√	
Liberatore et al. (2011)	√		√	
Liberatore and Scaparra (2011)	√		√	
Aksen and Aras (2012)	√		√	
Liberatore et al. (2012)	√		√	
Losada et al. (2012)		√	√	
Losada et al. (2012)	√			√
Scaparra and Church (2012)	√		√	
Li et al. (2013)		√	√	
Parajuli et al. (2017)	√		√	√
Azad and Hassini (2019)		√		√
Jalali et al. (2018)	√		√	
Forghani et al. (2020)	√		√	
Bao et al. (2019)	√		√	√
Goldbeck et al. (2020)		√	√	√

The mathematical models of protection in the literature can be categorized into two groups on the basis of underlying risk consideration: (1) risk neutral models and (2) risk averse models. Further, based on the mitigation strategy, the models can be grouped as (1) preventive mitigation strategies, (2) recovery mitigation strategies.

The risk neutral models to handle disruptions have most commonly been developed to contain supply or demand uncertainties, such as demand fluctuations, machine breakdowns and temporary production shutdowns. Their mathematical formulations rely on optimizing an expected value of a given performance measure e.g. minimize expected costs, maximize expected profits, taking a stochastic modeling approach with probability estimates of disruption occurrences. However, under major disruptions such as terror attacks or catastrophic disasters such as earthquakes, hurricanes, these models are ill suited for two reasons: (1) it is difficult to obtain historical data for probability estimates since such events are rare and less frequent; (2) their solutions are not reliable in a worst case or extreme loss possibility. Risk averse models that optimize protection against a worst-case disruption scenario have subsequently been developed.

The risk averse models are designed to control the maximum or worst-case losses that the system may suffer due to major disruptions. These models do not require disruption probability estimates but provide robust solutions for planning protection against random catastrophic disruptions such as due to the natural disasters, (earthquakes, hurricanes, etc). Planning protection against intentional attacks, however, the models need to properly reflect the behavior of the attacker creating disruptions, which may not be random. Protection models in this category find their roots in interdiction and fortification planning literature. The interdiction models have been utilized to assess supply and infrastructure system vulnerability against worst case attacks from an adversary. The readers are referred to Churchet al. (2004) for a survey of such models. The fortification models build on the interdiction models by including protection decisions. These models are used to identify critical facilities, whose protection would prevent against the worst- case interdiction of such facilities. In most of the fortification models, the interdictor is assumed to be an intelligent adversary (e.g., an attacker) capable of utilizing resources in an intelligent manner so as to create maximum damage to the targeted system. Therefore, fortification models are commonly developed in a game theoretic mathematical framework of attack and defense, in order to capture the underlying relationship of attack and defense. Fortification has mostly been defined in the literature as some form of facility hardening, structural reinforcement, redundant suppliers, inventory, etc., which represent some investments that a defender of the system makes to prevent against disruptions (Scaparra and Church 2008a, 2008b, Liberatore and Scaparra 2011, Aksen and Aras 2012). Such preventive measures however, do not explicitly consider the optimization of recovery or contingency mechanisms in the post disruption recourse. Additionally, the models ignore the congestion effects that may arise as a result of demand overflow during such recovery or contingent actions.

The relevant literature on the features of risk tolerance (i.e., risk neutral or risk averse) and underlying mitigation strategy, (i.e., preventive or recovery) are summarized in Table 1. It is observed that most of the risk neutral models have a preventive risk mitigation focus (Berman et al., 2007; Cui et al., 2010; Li et al., 2013; Li and Ouyang, 2010; Lim et al., 2010; Losada et al., 2012; Qi et al., 2010). Preventive risk mitigation is implied in these models as their decisions involve facility location or facility location with some redundancy placement decisions e.g., inventory, backup supplier, etc. so that the supply network is inherently reliable to operate under major disruptions. A majority of risk averse models also have preventive mitigation focus involving decisions on which of the existing facilities to protect or fortify (Aksen et al., 2010; Aksen and Aras, 2012; Church and Scaparra, 2007; Forghani et al., 2020; Liberatore et al., 2011, 2012; Liberatore and Scaparra, 2011; Losada et al., 2012; Scaparra and Church, 2008, 2012). As these models are

developed for protection of existing networks, they do not involve facility location decisions. Jalali et al. (2018) however, consider a risk averse model with simultaneous decisions of facility location and protection, so that the supply network is inherently more robust to major disruptions. While the risk averse models considered in these articles are more effective than risk neutral models for handling major disruptions, the models do not explicitly optimize recovery period of disruption. Losada et al. (2012) were the first to introduce fortification model with recovery time optimization. The protection is implied as a decision to allocate available budget into facilities for reducing their recovery times following disruption. A drawback of this model is that it does not examine contingency strategies for disruption recovery, other than deciding where to invest for enhancing recovery. Parajuli et al. (2017) address this issue by developing a model involving multiperiod recovery process and a contingency strategy involving gradual backup production. The protection budget allocation decisions are made to appropriately select contingent backup capacity and their response speeds of production.

Contingency strategies for disruption recovery have been dealt more recently in Azad and Hassimi (2018), Bao et al. (2019) and Goldbeck et al. (2020). Azad and Hassimi (2018) utilize a risk neutral modeling approach through scenario-based uncertainty considerations in both the facility capacity availability and recovery periods from disruptions. Optimal recovery is achieved through post disruption decisions involving dynamic pricing, inventory transshipment and outsourcing over the disruption time horizon. Goldbeck et al. (2020) also utilize a risk neutral approach to investigate the problem of procuring repair resources to speed up recovery process. They develop a stochastic multi time horizon model, involving both pre disruption decisions of investments in repair capabilities and the post disruption decisions of contingent resource allocation and repair tasks scheduling. Bao et al (2020) develop a risk averse model to handle disruptions from attack on facilities in which recovery strategy is achieved through capacity expansion and repair of a disrupted facility. The time and cost dimensions for facility repair are considered while the model does not take account of time dimension of capacity expansion.

Contingency strategies involving disruption recovery have been addressed in most papers related to production and logistics, which do not necessarily make supply network and facility related decisions. Hopp and Yin (2006), Tomlin (2006), and Schmitt (2011) consider mitigation of major disruptions through flexible backup supply where the full backup is available only after a response time and no supply is available until the response time. Additionally, Ebrahim Nejad et al. (2014) and Niroomand et al. (2012) consider response time with gradual capacity availability at a backup supplier during the disruption of a primary supplier. Klibi and Martel (2012) develop a discrete stepwise function to represent gradual capacity availability based on disruption intensity and recovery time. It is observed that apart from Ebrahim Nejad et al. (2014), none of these articles consider congestion impacts during flow recovery, despite the fact that disruption can create congestion at facility due to demand shifts which may adversely affect capacity availability and influence protection decisions.

Congestion models have mostly been studied within the traffic and transportation domains. Facility congestion models are limited and most have been developed using queueing theory approach. Bitran and Tirupati (1989) developed a capacity planning model using GI/G/m queueing system in which facility congestion was handled with a constraint limiting the work in progress (WIP) to a target value. Marianov and Serra (2003) applied the similar approach in a hub and spoke network topology where the hubs are modeled as M/D/c queueing system and congestion is captured using a probabilistic capacity constraint limiting the queue length at hub facilities. Both of these approaches can be considered as implicit formulations as congestion terms do not appear in the objective functions of the optimization models. Explicit formulations have included congestion terms in the objective function of the optimization model. Clearing function is utilized to model congestion effects on available capacity (throughput) in a few articles. Clearing function is introduced by Karmakar (1989) and provide throughput as a function of WIP and the service rates at facilities. Kim (2013) utilizes this function to estimate the capacity levels of facilities under congestion. The WIP is computed by considering facilities as GI/G/1 queueing models. The model involves facility location problem which simultaneously minimizes the order waiting cost due to congestion, the fixed costs and transportation costs. Ebrahim Nejad et al. (2014) also utilize clearing function to model congestion in a responsive contingency planning problem involving a backup supplier. The WIP for the clearing function is derived using a M/G/1 queueing system. The appropriate level of capacity of a backup supplier is estimated using this clearing function.

Alternative approaches have modeled congestion as an increasing function of flows from facilities, without resorting to queueing approaches. Elhedhli and Hu (2005) apply a convex congestion cost function that increases according to a power law as more flows are routed to the facilities (hubs). Camargo et al. (2009) propose a generalized convex cost function to model congestion under a deterministic demand at the hubs. In a closely related article involving competitive facility location in a distribution network, Konur and Geunes (2011,2012) also introduce convex cost functions in the objective function of their model to capture traffic congestion cost on the distribution link.

From this literature review, it can be observed that most of the research in supply chain network design and risk management is focused on preventive or pre-disruption mitigation strategy. The recovery strategy and contingency mechanisms involving the flow recovery process have not been dealt adequately and congestion impact on recovery and mitigation is largely ignored. Furthermore, most of the approaches are based on optimizing the system for its expected performance (risk neutral), whereas major disruptions tend to create significant short and long term economic losses and warrant a risk averse decision approach. In this paper, we have incorporated congestion effects while developing a risk averse model for contingency planning that hedges against the worst-case loss from a major disruption. This model developed on an interdiction-fortification framework, provides solutions for optimal protection and recovery of supply networks subject to major disruptions and congestion of facilities.

3. Problem description and model formulation

The supply network is represented with a set of production facilities (J) supplying a set of customer zones (I) with finite demands h_{it} each time period t in the planning horizon T. Every facility j has a finite production/supply capacity, which is lost completely if it is

attacked, i.e complete interdiction. A limited protection budget B can be applied to secure critical facilities with a backup production capability so as to meet additional demands shifted from disrupted facilities. The production capability of the backup production is contingent upon the selected production volume and response speeds. The levels of protection are defined with respect to the nominal volume and response speeds for backup production, with each level involving a finite cost and therefore using a certain amount of the protection budget.

The congestion at a facility increases with increasing flows from the facility. The congestion cost is represented by a non-linear and convex power law cost function. In addition to the congestion costs, supplying each unit of demand i from a facility j involves unit transportation costs, which is surrogate to distance d_{ij} between the customer zone and the facility. Note that this assumption does not consider the economies of scale in transportation costs, however it is an approach followed in most classical facility location models for its simplicity. Supply chain faces a major loss through the loss of its customers while demands cannot be fulfilled and this cost is an important consideration in resilient design of supply chains (Ni, Howell, and Sharkey 2018). The unmet demands are accounted by applying a lost sales cost or penalty for each unit of unmet demand. The decisions therefore involve identification of critical facilities to secure and determination of their backup production capability within the available budget, so that worst case network costs (transportation, cost of lost sales, congestion) due to attacks can be minimized.

3.1. Model formulation

The protection problem is formulated as a tri-level nested optimization problem involving optimization between two players at system user level(defender), attacker level and the defender level. Interdiction-protection design modeling framework used in this paper follows a common set of key assumptions regarding the game being examined (Smith and Song 2020):

- All problem information is known to both the defender and the attacker.
- The attacker is certain of the effect that its interdiction actions have on the defender's problem.
- The attacker and defender play a zero-sum game in the sense that the value of the game is given by the defender's objective, with the attacker seeking to maximize the minimum value that the defender can achieve via constrained optimization.
- In each round of the interdiction game, the attacker and defender each make one set of decisions, with the attacker making all of its decisions before the defender makes its set of decisions.
- Only one round of the game is played.

We first define the mathematical notations used as follows:

Sets and Parameters:	
I	set of customers (indexed by i)
J	set of facilities (indexed by j)
T	time period t
B	total fortification budget
L	set of protection levels (indexed by l)
S	set of attacked facilities (indexed by s)
Z	set of protected facilities (indexed by z)
X	set of all served demands
U	set of all unserved demands
c_{jl}	cost of protection of facility j at level l
m_{tl}	the proportion of extra capacity available each time period during the response time and after, based on selected response speeds of facilities
d_{ij}	distance (proxy to unit transport cost) from customer i to facility j
h_{it}	demand of customer i in time period t
v_{jt}	base supply capacity of facility j in time period t
a_{jl}	maximum additional capacity that can be added at facility j for corresponding fortification level l
β_i	unit cost of lost sales for unmet demand from customer i
r	number of (facility) interdictions/attacks
w/q	non linear congestion profile parameters
Decision variables:	
x_{ijt}	Units of demand from customer zone i served by facility j in time period t
s_j	1 if facility j is interdicted and 0 otherwise
z_{jl}	1 if facility j is fortified with capacity backups at level l, 0 otherwise
u_{it}	total unmet demand of customer i in time period t

In this formulation, the user level problem corresponds to finding a best recourse action in a post disruption scenario. The system user can therefore be considered as a defender of the network with a cost minimization objective. This level involves making allocation decisions to solve the underlying cost minimization problem when both attacked facility set (s) and protected facility set (z) are known. The cost minimization function corresponding to this level of problem is represented using a notation G(s, z). The attacker level problem corresponds to the worst case attack where the attacker selects an attack scenario s from a feasible attack scenario set S to raise costs as much as possible. The cost maximization function at the attacker level is a function of facilities being protected, hence it is represented as H(z). At the top level the problem involves the decision maker's budget allocation decisions to obtain optimal protection solution from a feasible protection solution set Z. From a game theoretic viewpoint, this level is also considered as a defender problem

with a cost minimization objective. The complete tri-level model involves a nested cost optimization problem of the form $\min_{z\in Z}\max_{s\in S}\min_{x,u\in X,U} Costs(z,s,x,u)$, seeking for an optimal protection set $z \in Z$. The schematic of the three levels of this nested optimization problem is presented in Appendix B. The following sections discuss the three levels of this nested optimization problem.

3.1.1. Defender level problem

The defender (top) level problem [DLP] is concerned with optimal utilization of available budget to secure facilities and determine the level of responsiveness and volume of backup production. The model can be written as follows:

[DLP]

$$\min_{z} H(z) \tag{1}$$

subject to:

$$\sum_{j\in J}\sum_{l\in L} c_{jl} z_{jl} \leqslant B \tag{2}$$

$$\sum_{l\in L} z_{jl} \leqslant 1 \quad \forall j \in J \tag{3}$$

$$z_{jl} \in \{0,1\} \quad \forall j \in J, l \in L \tag{4}$$

The defender objective function (1) represents the decision maker's objective of thwarting the worst case attack on facilities by prior protection of a set of facilities. The decisions involve selecting facilities to protect and determining their backup production capacity levels. Constraint (2) ensures that protection budget cannot be exceeded when making these decisions. Constraint (3) ensures that every facility is protected with at most one level of backup production. Constraint (4) sets a binary restriction on protection variable.

3.1.2. Attacker level problem

At this level, the problem involves attacker's objective of creating maximum network operation costs through the selection of optimal attack scenario s, given the protection decisions z of the defender. The model can be written as follows:

[ALP]

$$H(z) = \max_{s} G(s,z) \tag{5}$$

subject to:

$$\sum_{j\in J} s_j = r \tag{6}$$

$$s_j + \sum_{l\in L} z_{jl} \leqslant 1 \quad \forall j \in J \tag{7}$$

$$s_j \in \{0,1\} \quad \forall j \in J \tag{8}$$

Objective function (5) maximizes the network operation cost for the system user. Constraint (6) represents that attacker has capability of attacking only a finite number (r) of facilities. Constraint (7) prohibits attacks of protected facilities. Constraint (8) imposes binary restriction on the attack variable.

3.1.3. User level problem

The user level problem [ULP] allocates supply flow to customers in order to minimize the total costs of network operation, given the attack and protection solutions. The total costs include the transportation costs, the lost sales costs and the congestion costs. The model can be written as follows:

[ULP]

$$G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + \sum_{j\in J}\sum_{t=1}^{T} w\left(\sum_{i\in I} x_{ijt}\right)^{q}\right) \tag{9}$$

s.t.

$$\sum_{j\in J} x_{ijt} + u_{it} = h_{it} \quad \forall i,t \tag{10}$$

$$\sum_{i\in I} x_{ijt} \leqslant (1-s_j)\left(v_{jt} + \sum_{l\in L} m_{jl} a_{jl} z_{jl}\right) \quad \forall j,t \tag{11}$$

$$x_{ijt} \geqslant 0 \quad \forall i,j,t \tag{12}$$

$$u_{it} \geqslant 0 \quad \forall i,t \tag{13}$$

Objective function (9) minimizes the combined transportation costs, lost sales costs and the congestion costs of network operation subject to the protection and attacks. Congestion cost is expressed in the third term $\sum_{j\in J}\sum_{t=1}^{T} w\left(\sum_{i\in I} x_{ijt}\right)^q$, which is a convex non-linear function. Section 3.2 provides its rationale and derivation. Constraint (10) ensures that demands not fulfilled are accounted as lost sales so that lost sales penalty can be applied. Constraint (11) ensures that the flows (allocated units) are no higher than the facility capacity including the base capacity and the backup production if that facility is protected. It also ensures there is no allocation from an attacked facility. Constraints (12) and (13) ensure that allocation and unmet demand variables are non-negative.

It is important to note here that this modeling framework considers the presence of an intelligent adversary. This is different from disruptions such as the ones due to natural phenomena, where disrupted facilities can be random. Intelligent adversaries have the capability to decide which facilities to attack so as to create the maximum harm to the system. In this sense, the model assumes that the attacker knows the protection decisions of the defender and if any of the facility is protected, the attacker diverts its attack on to another facility so that it maximizes its benefit. As a result, the best protection strategy is reached through a sequential game between the two players, each time protecting the system against the next possible worst case loss. The protection strategy solutions reached in this manner may not be identical to the solutions derived from solving the worst case loss from a random disruption, and substituting the latter on this type of disruptive event may lead to suboptimal results. This is also demonstrated in Scaparra and Church (2008) highlighting the importance of modeling the problem in this kind of framework. The user level problem in this hierarchy is not necessarily modeling a different player, in fact the top level and the bottom level (user) problems can be the same players as their objectives align, i.e. both have cost minimization objective. This is true in many vertically integrated firms which are involved from high level strategic planning up to the last mile delivery. While the top level is concerned with allocation of protection budget prior to the disruption, it does so to fulfill the user level objective of optimal allocation of supply flows after disruption. In this analysis, we are considering a supply of homogeneous product within a vertically integrated supply network where the supply chain owner has total control and visibility on its operations. As such, the decision framework involves two players: the attacker disrupting the supply chain flows and the defender that optimally designs the protection and operates the supply chain flows.

3.2. Congestion cost function and linearization

Congestion cost resulting from demand overflow into facilities under a disruption contingency operation is represented using a power law cost function of the form:

$$f(\phi_{jt}) = w\phi_{jt}^{q} = w\left(\sum_{i\in I} x_{ijt}\right)^{q} \tag{14}$$

where $\phi_{jt} = \sum_{i\in I} x_{ijt}$ is the total amount of flow in a given time period to a facility and w and q are positive constants with $q \geqslant 1$. The advantage of using this congestion function is that it can be explicitly incorporated into the objective function of the optimization model as a cost term without requiring the queueing approach to model flows from the facility. Explicit incorporation of congestion cost enables the problem to be solved as a cost minimization problem which simultaneously minimizes congestion with other operational costs of the supply network. The congestion cost function implies that congestion costs tend to reach a positive infinity with increasing flows, even though it does not consider the capacity limit of facilities. Similar congestion modeling approach in other contexts can be observed in Weisbrod, Vary and Treyz (2001), Elhedhli and Hu (2005) and Konur and Geunes (2011, 2012).

The power law congestion cost function is non-linear and convex and hence it can be approximated by the maximum of the set of piece-wise linear and tangent hyperplanes (Elhedhli and Hu, 2005). In the following analysis, the set of all such tangent hyperplanes used to estimate the congestion costs due to flows from any facility (j) are represented with a notation K_j. (indexed k$\in K_j$) Each tangent hyperplane can be expressed with the following Taylor series expansion around a given flow, and ignoring the higher order terms:

$$f(\phi_{jt}^{k}) + f'(\phi_{jt}^{k})(\phi_{jt} - \phi_{jt}^{k}) = w(1-q)(\phi_{jt}^{k})^{q} + wq(\phi_{jt}^{k})^{q-1}\phi_{jt} \tag{15}$$

The linear approximation of congestion cost function $f(\phi_{jt})$ can therefore be expressed as a maximum among all the tangent hyper planes using the following expression:

$$f(\phi_{jt}) = \max_{k\in K_j}\left(w(1-q)\left(\sum_i x_{ijt}^{k}\right)^{q} + wq\left(\sum_i x_{ijt}^{k}\right)^{q-1}\left(\sum_i x_{ijt}\right)\right) \tag{16}$$

Utilizing the above approximation, the objective function of [ULP] can be stated as

$$G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + \sum_{j\in J}\sum_{t=1}^{T}\max_{k\in K_j}\left(w(1-q)\left(\sum_i x_{ijt}{}^k\right)^q + wq\left(\sum_i x_{ijt}{}^k\right)^{q-1}\left(\sum_i x_{ijt}\right)\right)\right) \tag{17}$$

which is equivalent to (details presented in Appendix B2),

$$G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + w\sum_{j\in J}\sum_{t=1}^{T}\eta_{jt}\right) \tag{18}$$

s.t.

$$\eta_{jt} - q\left(\sum_i x_{ijt}^k\right)^{q-1}\left(\sum_i x_{ijt}\right) \geqslant (1-q)\left(\sum_i x_{ijt}^k\right)^q \quad \forall j\in J, k\in K_j, t = 1\ldots T \tag{19}$$

The user level problem is further constrained to prohibit lost sales being incurred while the total system capacity is not fully utilized. This constraint implies an upper bound of zero for lost sale units if total system capacity is higher than total demand and a positive difference if total demand is higher than total system capacity. This assumption is rational under a service sensitive demand and a competitive market where failing to meet demand for extended periods may imply losing customers permanently to a competitor. Furthermore, the impact of congestion on supply flow characteristic may not be fully understood by omitting this aspect.

$$\sum_{i\in I} u_{it} \leqslant max\left(0, \sum_{i\in I} h_{it} - \sum_{j\in J}(1-s_j)\left(v_{jt} + \sum_l m_{tl}a_{jl}z_{jl}\right)\right) \quad \forall t \tag{20}$$

A big M variable and a binary variable y_t(1 if total system demand is higher than the total system capacity in any time period, else 0) are introduced to linearize above with the following three constraints:

$$My_t \geqslant \sum_{i\in I} h_{it} - \sum_{j\in J}(1-s_j)\left(v_{jt} + \sum_l m_{tl}a_{jl}z_{jl}\right) \quad \forall t \tag{21}$$

$$M(1-y_t) \geqslant \sum_{j\in J}(1-s_j)\left(v_{jt} + \sum_l m_{tl}a_{jl}z_{jl}\right) - \sum_{i\in I} h_{it} \quad \forall t \tag{22}$$

$$\sum_{i\in I} u_{it} - \left(\sum_{i\in I} h_{it} - \sum_{j\in J}(1-s_j)\left(v_{jt} + \sum_l m_{tl}a_{jl}z_{jl}\right)\right)(y_t) \leqslant 0 \quad \forall t \tag{23}$$

Incorporating these new constraints and the modified objective function for the user level problem [ULP'], the complete tri-level protection design model can be rewritten as:

$$[DLP]: \min_z H(z) \tag{1}$$

$$s.t.\ (2)-(4)$$

where

$$[ALP]: H(z) = \max_s G(s,z) \tag{5}$$

$$s.t.\ (6)-(8)$$

where,

$$[ULP']: G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + w\sum_{j\in J}\sum_{t=1}^{T}\eta_{jt}\right) \tag{24}$$

s.t. (10)-(13), (19), (21)-(23)

In this formulation, the term $w\sum_{j\in J}\sum_{t=1}^{T}\eta_{jt}$ in (24) represents the linearly approximated total congestion cost. Constraint (19) ensures that congestion at every facility at every time period is approximated with the maximum among all the tangent hyper planes. Constraints (21) – (23) are linear sets of constraints utilized to bound the lost sales so that the demands are always filled if capacity exists.

Implicit enumeration technique with a binary search tree is applied to find the optimal protection solution of the above tri-level

optimization model. The next section discusses the proposed methodology.

4. Solution methodology

A solution methodology that uses a recursive search algorithm is presented to solve the tri-level *MIP* model presented in Section 3.

4.1. Overview

The multi-level optimization problems form an important class of protection design problems, especially when modeling protection against intelligent attacks. The attacker makes interdiction decisions to maximize the minimum objective that a defender can obtain in solving its optimization problem, hence leading to a nested optimization model structure. This makes the problem difficult to solve and it lacks efficient and universal solution algorithms. Techniques that reformulate the problem into single level using dual transformations and complete enumeration of decision strategies are limited to solve only smaller instances with integer decision variables. Furthermore, reformulations and decompositions to reduce the size of the problem are not straightforward (Cappanera and Scaparra 2011). Readers are referred to Moore and Bard (1990) for detailed reference on discrete bi-level problems.

Our proposed tri-level model poses a similar challenge. In the nested optimization structure presented, integer protection decision variables in the defender problem appear as parameters in the constraints of the attacker problem, while both defender and attacker problem decision variables are parameters defining the constraint of the user level problem. In order to solve this complex model, we apply an implicit enumeration algorithm for its efficiency in that it does not require complex reformulation or the size restrictions of complete enumeration. This algorithm is based on the fact that at least one of the facilities that would be attacked in the worst-case attack must be included in the optimal fortification set (Church and Scaparra, 2007). This observation is recursively utilized in a binary search tree to arrive at an optimal protection strategy.

We apply an algorithm similar to Scaparra and Church (2008a) to identify facilities to secure and determine their levels of backup production volume and response speeds. Scaparra and Church (2008a) implicitly enumerate protection strategies in a binary search tree, but at every node of the search tree they solve the lower level (attacker) problem involving binary decisions of attacks. As a result the computational efficiency of the algorithm is dependent on the difficulty of solving this level of the bi-level problem. In the proposed algorithm, the lower level problem is solved for continuous decision variables involving only flow allocations. For this purpose the feasible attack scenarios are completely enumerated given the protection decisions at each node of the search tree. The attacker's solution is obtained indirectly by first solving the user level problem for all feasible attack scenarios and then selecting the scenario leading to the maximum network cost (worst case) as an optimal attack scenario. As no integer decisions are involved in solving attacker's optimization problem, the computational efficiency is not deteriorated, despite the requirement to completely enumerate attack scenarios.

4.2. Algorithm description

The algorithm proceeds with the generation of the root node of the search tree. At the root node feasible attack scenarios are first enumerated given that none of the facilities are protected, i.e., all z_{jl} variables set to zero. The user level problem [ULP'] is solved by calling *Cplex MIP* solver for each attack pattern. The pattern leading to maximum network cost is selected as the solution to the attacker problem. As per the observation in Church and Scaparra (2007), the attacked facilities become the candidate facilities for protection at the root node from where the implicit search for protection strategy begins utilizing the binary tree structure. For each node in the progression of the search tree where the attacker problem is to be solved, we follow the same procedure: a) generate feasible attack scenarios b) call *Cplex* to solve the user level problem for each scenario and c) select candidate facility sets for protection by comparing losses. The feasible attack scenarios are generated by enumerating all possible combinations of attacks at each node of the search tree ($^{n}C_{r}$), where n reduces by 1 at each subsequent node where the attacker problem is solved.

The flowchart of the algorithm is provided in Appendix B4. We illustrate the progression of the search tree in the following example.

4.3. Illustrative example

Consider a simple problem involving five facilities located in five states in the United Sates (U.S.) - *NY*, *CA, IL, TX* and *PA*. Among these facilities, two facilities are to be interdicted by the attacker ($r = 2$). Two levels of capacity volumes (high, low) and two levels of response speed levels (high, low) are considered, the combination of which leads to four different levels (l) of facility protection with backup production capability. Each level of protection incurs protection cost considered to be independent of facilities but dependent on the selected volume and response speeds of capacity backups. For a chosen ten units of available budget, each level of protection, c_{jl}, costs as follows: level 1 (high volume backup production, fast response speed) = 10 units; level 2 (high volume backup production, slow response speed) = 8 units; level 3 (low volume backup production, high response speed) = 6 units; level 4 (low volume backup production, low response speed) = 5 units.

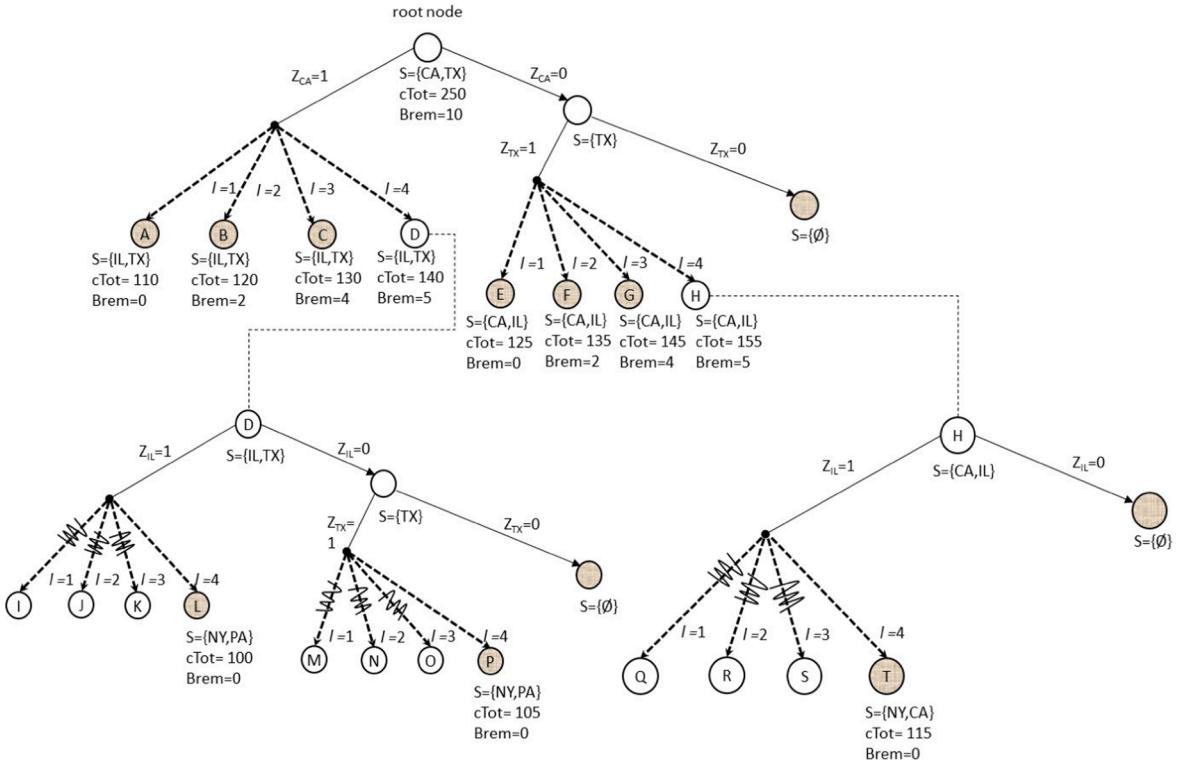


Fig. 1. Illustration of the binary search tree using implicit enumeration.

The enumeration tree corresponding to this illustrative problem is depicted in Fig. 1. Every node of this enumeration tree is characterized by a) total network cost b) attacked facilities, which are the candidate facilities for protection in the next stage and c) remaining budget of protection. At the root node of the tree in Fig. 1Figure 1, the attacker problem is solved without any facilities being protected by the defender. The worst-case attack plan (maximum network cost) is obtained for $S = \{CA, TX\}$ with a total network cost (*cTot*) of 250 monetary units. Among these two facilities, the facility at *CA* is arbitrarily selected for protection along the left branch of the tree. Note that this can be arbitrary because facility not selected in the left branch will remain a candidate facility for the right branch, since the right branch proceeds by excluding what is already selected in the left branch. Hence here, *CA* is excluded from protection in the right branch which leaves *TX* as its only candidate. The available budget is enough to protect *CA* on the left branch at any of the 1, 2, 3, or 4 levels of protection. So new nodes A, *B*, *C* and *D* are created in the left branch corresponding to protection of *CA* at levels $l = 1$, 2, 3 and 4 respectively. The attacker level problem is solved at each of these nodes *A*, *B*, *C*, and *D* given that the facility at *CA* is protected at level 1 for node A, at level 2 for node *B*, at level 3 for node *C* and at level 4 for node *D*. These attacked facilities, resulting network costs and the remaining budget (*Brem*) obtained after the protection are as shown for each node *A*, *B*, *C* and *D*.

The other child node obtained from the root node corresponds to the branch $Z_{CA,l} = 0$ (i.e., the facility at *CA* is not protected at any level *l* which leaves Texas as the only other candidate left for protection, this information is updated as $S = \{TX\}$ in this branch. Since no budget is used so far in this branch, the available budget is adequate to protect *TX* at levels 1, 2, 3, 4. Hence the branching is continued from this node. On the left branch corresponding to $Z_{TX,l} = 1$, four new nodes *E*, *F*, *G* and *H* are created corresponding to the four levels of protection that can be attained. The right branch from this node corresponds to $Z_{TX,l} = 0$ (i.e., the facility at Texas is not protected at any level and thus this branch leads to a node with $S = \{\emptyset\}$. The set *S* is shown null because no facility is available for further protection at this node, so it represents a fathomed node. The remaining budget at nodes *A, B, C, E, F* and *G* inFigure 1 Figure 1 are insufficient to protect further facilities. Therefore, these nodes become leaf nodes at this stage. For nodes *D* and *H*, the remaining budget allows further protection of a facility at $l = 4$.

Continuing the branching at node *D*, the facility at *IL* is arbitrarily selected for protection along the left branch. The available budget only allows a level $l = 4$ protection for this facility, which leads to the node *L* where the attacker problem can be solved by setting $Z_{CA,4} = Z_{IL,4} = 1$. This leads to $S = \{NY,PA\}$; however, the remaining budget is insufficient for further protection of a facility. Hence node L becomes a leaf node. The right branch from node *D* corresponds to $Z_{IL,l} = 0$, which leads to a node with $S = \{TX\}$.

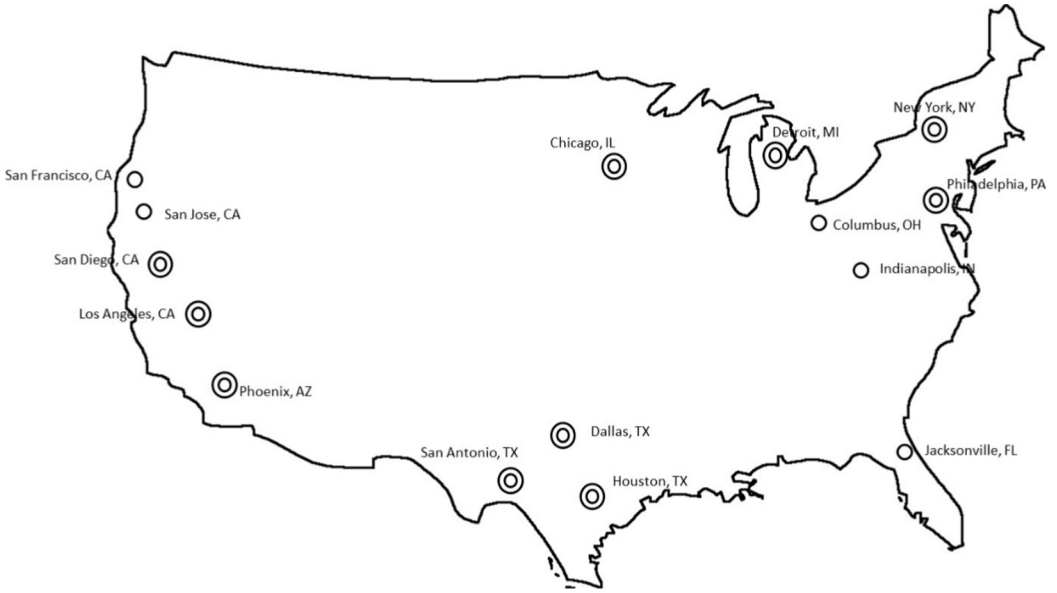


Fig. 2. Network configuration for 15 demands and 10 facility problem.

Table 2
Supply flow allocations under no congestion, linear and non-linear congestion.

Facilities	Without Congestion	With Linear Congestion	With Non-linear Congestion		
			Low	Moderate	High
1.New York, NY	20,652	20,652	20,652	20,652	12,780
2.Los Angeles, CA	0	0	0	0	0
3.Chicago, IL	13,652	13,652	13,652	13,652	12,660
4.Houston, TX	10,766	10,766	10,766	10,766	12,540
5.Philadelphia,PA	16,652	16,652	16,652	16,652	12,780
6.Phoenix, AZ	13,652	13,652	13,652	13,652	12,660
7.San Diego, CA	13,652	13,652	13,652	13,652	12,660
8.Dallas, TX	8195	8195	8195	7890	12,540
9.San Antonio TX	6984	6984	6984	7289	12,472
10.Detroit, MI	9547	9547	9547	9547	12,660

Continuing branching on this node leads to a leaf node P with $S = \{NY, PA\}$ on the left branch and a fathomed node with $S = \{\emptyset\}$ on the right branch.

The path with $Z_{CA,l} = 0$ leads to the node H with $S = \{CA, IL\}$. Since the protection of CA is not allowed in node H or any other child node along this path, it leaves IL as the only candidate for branching from node H. The available budget is sufficient to protect IL at level $l = 4$. When IL is protected, the left branch from this node leads to node T with $S = \{NY, CA\}$. As the available budget becomes insufficient for further protection at this stage, node T becomes a leaf node. Another fathomed node with $S = \{\emptyset\}$, results from the right branch from node H because both CA and IL cannot be protected in this branch. Continuing in this manner, we obtain nine leaf nodes—A, B, C, E, F, G, L, P and T, each with unique values of S *and* $cTot$ obtained as solutions to the attacker problem. Backtracking from the leaf node with least total network cost, i.e., node L (with a $cTot = 100$), we obtain optimal protection solution as securing both IL and CA with backup production at level 4, i.e., we select low volume capacity and low response speeds for backup production by securing these two facilities. Consequently, the attacker will attack facilities NY and PA to create the maximum possible cost to the system operator under this protection scenario.

5. Computational results

In this section, computational results and managerial insights are presented. The optimization problem was solved using ILOG

Table 3
Comparison of protection solutions under congestion and no-congestion models.

	Without Congestion	With Linear Congestion	With Non-linear Congestion		
			Low	Moderate	High
Attacks (Sj)	2	2	2	2	2
Protection Decisions (Zjl)	1(1), 5(4)	1(1), 5(4)	1(1), 5(4)	1(1), 5(4)	1(4), 3(4), 5(4), 10(4)
Total Network Costs (cTot)	17,552,758	17,575,284	17,578,374	24,207,733	3,626,415,156
Flow Ratios (fRatio)	2.96	2.96	2.96	2.83	1.02

Table 4
Difference in total costs under congestion and without congestion models.

Congestion profiles	$cTot_{ts}$	$cTot_{cs}$	φ (%)
$w = 0.1, q = 1.1$	17,578,374	17,578,374	0
$w = 1, q = 1.1$	17,808,919	17,808,919	0
$w = 10, q = 1.1$	20,114,369	20,114,369	0
$w = 0.1, q = 1.5$	18,218,284	18,218,284	0
$w = 1, q = 1.5$	24,208,019	24,207,733	0.002
$w = 10, q = 1.5$	84,105,367	83,917,369	0.224
$w = 0.1, q = 2.0$	57,452,123	57,051,093	0.703
$w = 1, q = 2.0$	416,546,404	389,161,124	7.037
$w = 10, q = 2.0$	4,007,489,218	3,626,415,156	10.508

Cplex 12.6 solver implemented using Java and Concert Technology on a Dell Latitude E5430 station with an Intel Core i5-3340 M processor at 2.7 GHz and 8 GB of RAM running Windows 7 operating system. The demand and distance data are derived from the US Census Bureau 2000 dataset (Daskin, 2004). The unit cost of lost sales is set at 2% higher than the maximum unit cost of transportation (i.e. maximum distance of all facility-demand pairs) which is maintained identical across all the experiments. A time horizon of four time periods is considered in which finite backup capacities can be added in each period. The facility base capacity level is determined by distributing the total network demand equally among the existing facilities with 80% utilization. All the input parameters for the experiments are provided in Appendix Table A1-A6.

An illustrative example is presented using 15 demand nodes *i* and 10 facilities *j*. The 10 facilities and the 15 demand nodes network used for this illustrative example are represented in Figure 2. The small circles are used to represent demand nodes and larger circles to represent facilities; concentric circles represent the existence of both demands and facility at the same location. This network is constructed by ranking demand node by population size and opening of ten ($j = 10$) facilities in the top ten demand nodes. The construction of the network in this manner prioritizes on local fulfillment of demands, while the model can be utilized for any other network configuration. The network is utilized to demonstrate the effects of considering congestion on the allocation decision of demand nodes and highlight the significance of considering congestion in protection designs for disruption risk mitigations. We further investigate the trade-off between congestion cost and other operational costs while analyzing network performance under varying levels of attacks and congestion severity. The computational efficiency of the algorithm is tested on larger network sizes and the results are presented.

5.1. Characteristic of flow allocations under congestion

The supply flow allocation characteristic under congestion effect is demonstrated in Table 2. This table represents allocations of flows to facilities under three scenarios: congestion effects are excluded (No-congestion approach), linear congestion function and non-linear congestion function. In the first scenario, the tri-level model is solved by removing the congestion term from the objective function. In the second scenario, we set the parameter $w = 0.1$ and q = 1 in the expression of the congestion function (17), so that the congestion cost is a linearly increasing function of flows. In the third scenario, we consider non linearity of congestion function under varying congestion profiles: i) low congestion ($w = 0.1, q = 1.1$) ii) moderate congestion ($w = 1, q = 1.5$) and iii) high congestion ($w = 10, q = 2.0$), under a finite budget level (B = 2680) and a finite attack level ($r = 1$).

It is observed from Table 2 that optimal supply allocations vary under different congestion considerations. The results show that the allocations that are optimal under low congestion can be suboptimal when congestion costs are significant. At moderate congestion, we observe that allocations change for two facilities, i.e., San Antonio, TX and Dallas, TX as compared to the no congestion or the linear congestion models. Increasing congestion further to high congestion, it is observed that the allocation decisions of the congestion model and the no-congestion models differ for every surviving facility.

Table 3 provides the optimal protection strategies (z_{jl}), resulting attacks (s_j), as well as total network costs ($cTot$) and maximum/

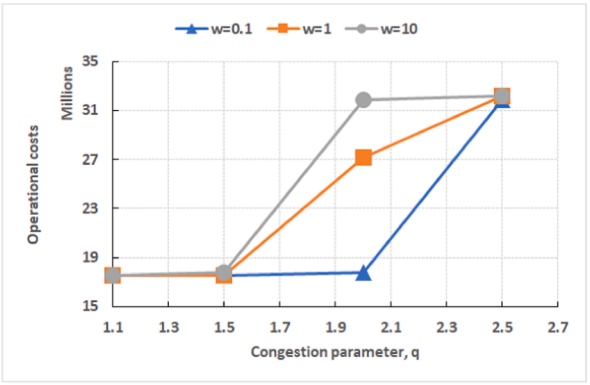
Table 5
Cost trade-offs in optimal protection design.

Model Type	r	w	q	Sj	Zjl	cTot	cFlow	cLS	cCong	fRatio
Without Congestion	1	0	–	2	1(1),5(4)	17,552,758	17,552,758	0	0	2.96
With Non-linear Congestion Costs	1	0.1	1.1	2	1(1),5(4)	17,578,374	17,552,758	0	25,616	2.96
	1	0.1	1.5	2	1(1),5(4)	18,218,284	17,552,758	0	665,526	2.96
	1	0.1	2	3	1(2),5(2)	57,051,093	17,797,897	0	39,253,196	2.53
	1	0.1	2.5	2	1(4),3(4),5(4),10(4)	2,052,546,943	31,881,848	0	2,020,665,095	1.02
	1	1	1.1	2	1(1),5(4)	17,808,919	17,552,758	0	256,161	2.96
	1	1	1.5	2	1(1),5(4)	24,207,733	17,553,673	0	6,654,061	2.83
	1	1	2	2	1(4),3(4),5(4),10(4)	389,161,124	27,192,724	0	361,968,400	1.26
	1	1	2.5	2	1(4),3(4),5(4),10(4)	20,236,919,203	32,218,681	0	20,204,700,523	1.01
	1	10	1.1	2	1(1),5(4)	20,114,369	17,552,758	0	2,561,611	2.96
	1	10	1.5	2	1(1),5(4)	83,917,369	17,782,906	0	66,134,463	2.53
	1	10	2	2	1(4),3(4),5(4),10(4)	3,626,415,156	31,882,196	0	3,594,532,960	1.02
	1	10	2.5	2	1(4),3(4),5(4),10(4)	202,079,223,907	32,218,681	0	202,047,005,227	1.01
Without Congestion	2	0	–	6,7	1(4),2(4),3(4),5(4)	26,194,341	26,194,341	0	0	1.45
With Non-linear Congestion Costs	2	0.1	1.1	6,7	1(4),2(4),3(4),5(4)	26,220,147	26,194,341	0	25,806	1.45
	2	0.1	1.5	6,7	1(4),2(4),3(4),5(4)	26,879,754	26,194,341	0	685,413	1.45
	2	0.1	2	6,7	1(4),2(4),5(4),10(4)	67,641,122	26,270,375	0	41,370,747	1.44
	2	0.1	2.5	3,8	1(4),2(4),5(4),10(4)	2,450,288,382	32,055,666	0	2,418,232,716	1.09
	2	1	1.1	6,7	1(4),2(4),3(4),5(4)	26,452,401	26,194,341	0	258,060	1.45
	2	1	1.5	6,7	1(4),2(4),3(4),5(4)	33,048,473	26,194,341	0	6,854,132	1.45
	2	1	2	3,8	1(4),2(4),5(4),10(4)	435,928,468	29,762,852	0	406,165,616	1.19
	2	1	2.5	3,8	1(4),2(4),5(4),10(4)	24,213,087,019	32,289,098	0	24,180,797,921	1.09
	2	10	1.1	6,7	1(4),2(4),3(4),5(4)	28,774,942	26,194,341	0	2,580,601	1.45
	2	10	1.5	6,7	1(4),2(4),5(4),10(4)	94,671,602	26,251,052	0	68,420,550	1.44
	2	10	2	3,8	1(4),2(4),5(4),10(4)	4,082,226,728	31,822,248	0	4,050,404,480	1.09
	2	10	2.5	3,8	1(4),2(4),5(4),10(4)	241,840,268,307	32,289,098	0	241,807,979,209	1.09
Without Congestion	3	0	–	6,7,10	1(4),2(4),3(4),5(4)	33,395,008	25,969,408	7,425,600	0	1.22
With Non-linear Congestion Costs	3	0.1	1.1	6,7,10	1(4),2(4),3(4),5(4)	33,419,578	25,969,408	7,425,600	24,570	1.22
	3	0.1	1.5	6,7,10	1(4),2(4),3(4),5(4)	34,064,760	25,969,408	7,425,600	669,752	1.22
	3	0.1	2	6,7,10	1(4),2(4),3(4),5(4)	75,225,321	25,969,408	7,425,600	41,830,313	1.22
	3	0.1	2.5	3,8,10	1(3),5(4),6(4)	2,515,715,051	30,609,728	10,425,600	2,474,679,723	1.26
	3	1	1.1	6,7,10	1(4),2(4),3(4),5(4)	33,640,711	25,969,408	7,425,600	245,703	1.22
	3	1	1.5	6,7,10	1(4),2(4),3(4),5(4)	40,092,529	25,969,408	7,425,600	6,697,521	1.22
	3	1	2	3,8,10	1(3),5(4),6(4)	440,407,860	30,609,728	10,425,600	399,372,532	1.26
	3	1	2.5	3,8,10	1(3),5(4),6(4)	24,787,832,559	30,609,728	10,425,600	24,746,797,231	1.26
	3	10	1.1	6,7,10	1(4),2(4),3(4),5(4)	35,852,035	25,969,408	7,425,600	2,457,027	1.22
	3	10	1.5	6,7,10		100,370,218	25,969,408	7,425,600	66,975,210	1.22

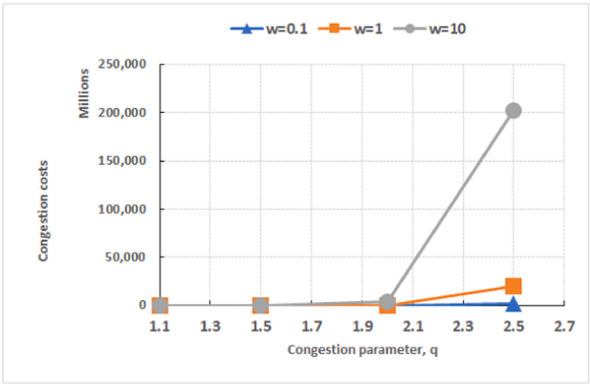
(*continued on next page*)

Table 5 (*continued*)

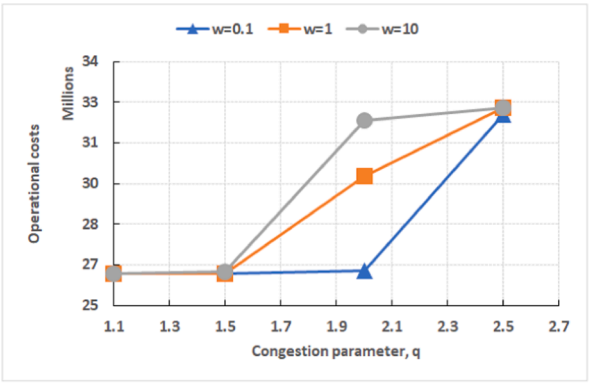
Model Type	r	w	q	Sj	Zjl	cTot	cFlow	cLS	cCong	fRatio
					1(4),2(4),3(4),5(4)					
	3	10	2	3,8,10	1(3),5(4),6(4)	4,034,760,648	30,609,728	10,425,600	3,993,725,320	1.26
	3	10	2.5	3,8,10	1(3),5(4),6(4)	247,509,007,637	30,609,728	10,425,600	247,467,972,309	1.26
					Min	17,552,758	17,552,758	0	0	1.01
					Average	19,542,093,340	26,063,887	2,788,320	19,513,241,133	1.55
					Max	247,509,007,637	32,289,098	10,425,600	247,467,972,309	2.96



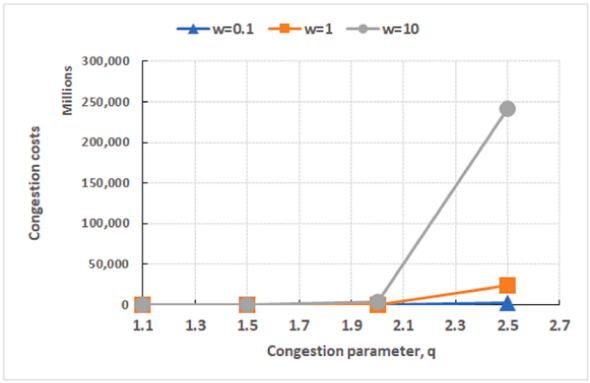
a) Operational costs vs q when r=1



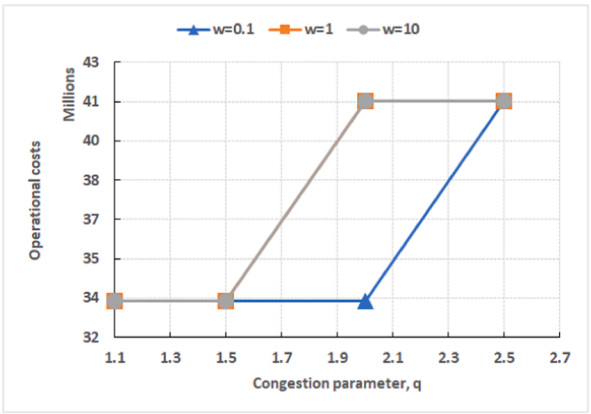
b) Congestion costs vs q when r=1



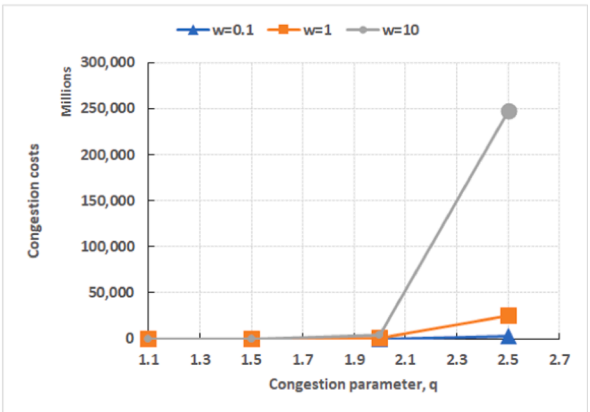
c) Operational costs vs q when r=2



d) Congestion costs vs q when r=2



e) Operational costs vs q when r=3



f) Congestion costs vs q when r=3

Fig. 3. Operational costs and congestion costs under varying attack levels and congestion profile settings.

Table 6
Computational time for various instances.

r	w	q	CPU time (s)		
			N(j) = 5	N(j) = 10	N(j) = 15
1	0.1	1.1	11	59	176
1	0.1	1.5	11	58	175
1	0.1	2	12	60	164
1	0.1	2.5	14	63	198
1	1	1.1	14	82	257
1	1	1.5	14	57	207
1	1	2	8	46	158
1	1	2.5	14	63	186
1	10	1.1	10	59	177
1	10	1.5	11	60	174
1	10	2	8	46	180
1	10	2.5	13	65	186
2	0.1	1.1	31	517	2544
2	0.1	1.5	28	542	2919
2	0.1	2	23	425	2170
2	0.1	2.5	32	586	2770
2	1	1.1	29	608	3685
2	1	1.5	27	516	2791
2	1	2	23	395	2332
2	1	2.5	32	637	2420
2	10	1.1	31	523	2550
2	10	1.5	33	529	2604
2	10	2	24	437	2285
2	10	2.5	37	551	2767
3	0.1	1.1	20	1953	19,536
3	0.1	1.5	21	1953	24,461
3	0.1	2	13	1394	14,969
3	0.1	2.5	22	2169	18,687
3	1	1.1	20	25	2752
3	1	1.5	21	2186	22,126
3	1	2	13	1461	14,679
3	1	2.5	24	2138	20,917
3	10	1.1	20	2164	19,342
3	10	1.5	21	2039	19,628
3	10	2	13	1460	15,185
3	10	2.5	22	2360	20,791
		Min	8	25	158
		Averages	20	785	6865
		Max	37	2360	24,461

minimum flow ratios (*fRatio*) obtained for this analysis under both no-congestion and congestion models. The flow ratio is a metric that is used to evaluate the balance of flows from facilities of the given network which affects the network costs of congestion. A decreasing flow ratio with increasing congestion severity as demonstrated in this Table suggests a more balanced flow requirement at higher congestion levels. As well, the optimal protection strategies under high congestion are observed to be different from the no-congestion model while it is identical under low and moderate levels of congestion. As balanced flow allocation achieves low costs of congestion, the protection design strategies that facilitate flow balance are generally preferable under high congestion severity. Therefore, designs which distribute available backup capacity in small units to higher number of facilities are desirable for flow balance and for minimizing the network congestion costs.

5.2. Network cost impacts and the value of incorporating congestion

In this section, we investigate what compromise on the network costs will be made if the decision maker relies on protection strategies and allocation decisions obtained by solving a no-congestion model. The total network costs resulting from the solution of a no-congestion model is compared to that of a congestion model to highlight the value of considering congestion in protection design models. Under the same levels of budget of protection (B = 2680) and attacks ($r = 1$) we compute the congestion value index (φ) which indicates the relative change in the total network costs when the flow allocations and protection strategy of a traditional model (congestion ignored) is utilized for designing protection of a congested network. It can be expressed as:

Table 7
Computational Time and congestion approximation errors.

Instances (*N(i)_N(j)_r*)	CPU time (s)				Congestion approximation error (%)			
	$K = 25$	$K = 50$	$K = 75$	$K = 100$	$K = 25$	$K = 50$	$K = 75$	$K = 100$
50_5_1	3	7	11	13	0.012	0.007	0.006	0.002
50_5-2	8	18	27	37	0.008	0.007	0.003	0.001
50_5_3	7	14	18	22	0.020	0.007	0.006	0.001
50_10_1	16	36	48	65	0.148	0.039	0.017	0.009
50_10_2	140	304	435	551	0.046	0.024	0.004	0.001
50_10_3	535	1176	1686	2360	0.048	0.021	0.003	0.001
50_15_1	41	96	150	186	0.241	0.059	0.027	0.016
50_15_2	559	1273	1995	2767	0.205	0.055	0.023	0.013
50_15_3	4262	9592	14,593	20,791	0.039	0.030	0.011	0.002

$$\varphi = (cTot_{ts} - cTot_{cs})/cTot_{cs} \tag{25}$$

The term $cTot_{cs}$ in the above expression represents the total costs (optimal objective function value) obtained from the model that considers congestion effects. The term $cTot_{ts}$ represents the total cost obtained when the protection strategy and allocations of a traditional model are substituted into this model. In Table 4 we summarize the results under varying congestion profiles.

In this illustrative example, the given network may incur up to 10% less in total costs by considering congestion effects. In optimal design of protections, the protection planner needs to look at the trade-off between congestion costs and the operational costs of transportation and lost sales. The next section deals with this trade-off analysis.

5.3. Congestion cost trade-off analysis

As the choice of parameters w and q affects congestion costs, we analyze the trade-offs with respect to these parametric variations. The protection strategies and the resulting costs under varying values of congestion parameters ($w = 0.1$, 1, 10 and $q = 1.1$, 1.5, 2.0, 2.5) is summarized in Table 5 and compared with that of the traditional model which ignores congestion. The congestion cost variations with the operational costs are graphically demonstrated in Figure 3. Under the dominance of congestion costs (high values of w and q or high congestion severity), the model tries to balance flow allocations among facilities in order to lower congestion costs. This may lead to reallocation of flows to the customers with demands being fulfilled from farther facilities, which may lead to an increase in transportation costs of the network. The dominance of transportation costs however, is observed to result in an unbalanced allocation of flows. This is because allocating more flows to nearby facilities will reduce network cost of transportation but make some facilities more congested than the others. The results in Table 5 demonstrate that under low congestion severity, the flow allocations and optimal protection solutions of a congestion model can be substituted with the traditional model solution as they are identical. As congestion costs become more dominant, however, the optimal protection strategies vary from the solutions provided by the traditional model and can be less relied upon.

An important consideration is how to recover the lost capacities or add extra capacities for protection when facilities are lost and network congestion costs are high. The results in Table 5 suggest that a high volume backup protection, i.e. centralized protection, is not a preferred protection strategy of such networks due to the risks of increased congestion costs resulting from unbalanced flow distribution. A simultaneous reduction of congestion costs and the lost sales can generally be achieved through a decentralized backup strategy in which capacities are added in smaller sizes but to a higher number of facilities. Such a strategy will yield low congestion costs owing to its balanced flow allocations.

As demonstrated in Table 5, a tendency towards decentralizing protection is therefore observed under higher attack levels and a limited protection budget. However, under high congestion severity (high w and q), marginal increase in congestion costs for unit flow recovered are much higher than decrease of lost sales costs through recovery. Under this condition, the congestion model may prescribe a protection strategy where recovered capacity volumes are lower compared to a decentralized protection. Such a strategy obviously raises the cost of lost sales but it is the dominance of congestion costs which makes this strategy favorable over a decentralized protection strategy. In the illustrative example, this scenario arises typically at congestion parameter settings of $w = 10$ and q greater than or equal to 2. As demonstrated in Table 5, under $w = 10$ and $q = 2.5$ and $r = 3$, the cost of lost sales (cLS) of the selected strategy (z_{jl}: 1(3), 5(4), 6(4)) is 40% higher than what can be achieved under a decentralized protection strategy (z_{jl}: 1(4), 2(4), 3(4), 5(4)) at this attack level. Nevertheless, this strategy is still selected for its lower congestion cost (about 5% lower than that of the decentralized strategy).

5.4. Computational efficiency

The computational efficiency of the algorithm is assessed under a larger network involving 50 demand nodes derived from the U.S. Census Bureau dataset (see Appendix Table A6). Table 6 summarizes the CPU times obtained under different parameter settings of attack levels (r), the total number of facilities considered $N(j)$ and the congestion profile parameters (w, q) and a finite budget level (B). The reported CPU times include both the time to generate feasible attack scenarios and user level problem solution times. These results demonstrate that under a finite budget of protection, the CPU times increase with both the increase in the number of attacks and the number of facilities. We further observe that the computational efficiency is affected by incorporating congestion term in the protection design model. The linear approximations of convex nonlinear congestion functions results in the addition of a set of constraints in the model. When the desired approximation error is low, interval granularity (K) is high i.e., the congestion cost function is approximated using higher number of tangent hyper planes. This has the effect of increasing problem size because of the new constraints that are added in the model. Table 7 highlights the CPU time and the relative error of congestion approximation under different interval granularity (K) for different problem combinations and a finite budget of protection ($B = 2010$ monetary units). It can be observed that as K is increased, the accuracy of the congestion cost is also increased, but it significantly deteriorates the CPU time.

As indicated in Table 6, the average computational time of the test instances on a 50 node network across all combinations was 6865 s. A maximum time of 24,461 s resulted under 3 facility attacks and 15 facilities. Although the CPU times are high, considering that the protection problem presented here is a strategic level decision, the computational efforts of the proposed solution algorithm is acceptable.

6. Conclusion

In this article, we examine the impact of congestion on protection design and recovery of a supply network subject to major disruption risk. The network involves discrete demands and supply facilities delivering homogeneous commodity. The production capacity of a facility is eliminated due to disruptions and remaining facilities are subject to congestion from demand overload. The problem involves optimal allocation of a fixed amount of protection budget to acquire backup capacity which can be added gradually over time and utilized for flow recovery. The network owner is assumed to be risk averse and utilizes its protection budget to add backup capacity that minimizes the worst-case sum of transportation costs, congestion costs and lost sales during contingency operations. The worst-case is modeled by considering an attacker who seeks to maximize the defender's minimum cost. Considering solution applicability in managing disruptions from an intelligent attacker, the model is developed on an interdiction-fortification framework involving tri-level optimization. This framework relies on the sequential game between the disruptive agent (attacker or interdictor) and the network owner (defender or fortifier). The protection strategies have been obtained from the solution of this model using implicit enumeration technique on a binary search tree. The tri-level model presented in this study is a difficult class of optimization problem even without the integration of congestion effects. The integration of non-linear congestion cost function makes the model more complex and its solution more challenging. The non-linear congestion cost function has been converted through piecewise linear approximation using tangent hyperplanes to the congestion function.

The experimental results from the study have demonstrated that congestion has a considerable impact on protection design decisions and cannot be ignored while making such decisions. Implementing the proposed model in practical applications requires proper estimation of the parameters involved in the congestion cost function as these parameters drive congestion costs. Accurate representation of congestion costs in the model enables appropriate selection of backup production capacity leading to cost effective contingency operations. Our analysis depicts that a centralized protection strategy which adds high volume back up capacity faster at higher response speeds is generally not desirable when congestion consequences are severe. Decentralizing protection provides a better risk mitigation strategy through a more balanced flow distribution and low congestion costs. This implies that the supply chain planners should spread out budget at multiple facilities so that recovery is more cost effective rather than concentrating it on a single or few facilities in which case the cost effectiveness is offset by high congestion costs. Such a strategy, while not widely used by global supply chains, showed its capability with the recent COVID-19 disruption. The recent success of 3M of providing N95 masks worldwide by significantly ramping up its capacity is based on both using decentralized manufacturing facilities and built-in surge capacity at these facilities (Bloomberg, 2020). Our proposed method allows assessing vulnerabilities of supply chains and provide fortification strategies in case of such surge in demand and need for matching capacity through protection mechanisms.

A limitation of the model presented in this paper is that it does not consider the equilibrium of the different stakeholders allowing distributed decision making. Our methodology is mostly applicable for analyzing supply chains which are vertically integrated so that all stakeholders collaborate to achieve a system-optimal supply chain recovery. Future study may address the issue of user equilibrium in a non-collaborative stakeholder environment. This study can also be extended by relaxing some of the assumptions, for instance partial capacity loss than complete loss through attacks may be a more realistic consideration. As well, complete protection of facilities may be relaxed in favor of partial protection since in practice, it is often difficult to achieve completely disruption-immune facilities.

Further, focusing more on the recovery aspect or the contingent mechanism of protection, the model lumps the cost of protection into the cost of backup capacity selection. Although this assumption is not restrictive, it may be possible to segregate budget into hardening of facilities and backup up production and let the model decide where to invest on hardening and where to invest on backup production. Robust optimization approach under demand uncertainty is another promising research extension of this study.

CRediT authorship contribution statement

Anubhuti Parajuli: Methodology, Software, Investigation, Formal analysis, Validation, Writing - original draft. **Onur Kuzgunkaya:** Supervision, Funding acquisition, Conceptualization, Resources, Writing - review & editing. **Navneet Vidyarthi:** Supervision, Funding acquisition, Conceptualization, Writing - review & editing.

Appendix A

Facility capacities, demands and distances data used for test instances.
See Table A1-A6.

Table A1
m_{tl} Proportion of capacity added each time period at high and low response speeds.

		Protection level l			
		1	2	3	4
Time period t	1	0.5	0.33	0.5	0.33
	2	1.0	0.67	1.0	0.67
	3	1.0	1.0	1.0	1.0
	4	1.0	1.0	1.0	1.0

Table A2
c_{jl} protection cost of facility j at level l.

Protection Level l	c_{jl}
1	$2,000
2	$1,340
3	$1,000
4	$670

Table A3
a_{jl} additional capacity for facility j at level l.

Protection Level l	a_{jl}
1	2,000
2	2,000
3	1,000
4	1,000

Table A4
Facility base capacity each time period for 10 cities 15 demand zone problem.

New YorkNY	Los Angeles CA	Chicago IL	Houston TX	Philadelphia PA	Phoenix AZ	San Diego CA	Dallas TX	San Antonio TX	Detroit MI
3400	3400	3400	3400	3400	3400	3400	3400	3400	3400

Table A5
Facility base capacity for 50 demand zone problem.

Numberoffacilities	*NewYorkNY*	*LosAngelesCA*	*ChicagoIL*	*HoustonTX*	*PhiladelphiaPA*	*PhoenixAZ*	*SanDiegoCA*	*DallasTX*	*SanAntonioTX*	*DetroitMI*	*SanJoseCA*	*IndianapolisIN*	*SanFranciscoCA*	*JacksonvilleFL*	*ColumbusOH*
5	10,950	10,950	10,950	10,950	10,950										
10	5475	5475	5475	5475	5475	5475	5475	5475	5475	5475					
15	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650	3650

Table A6
Distance and demand quantities data inputs.

City	Demand	NewYorkNY	LosAngelesCA	ChicagoIL	HoustonTX	PhiladelphiaPA	PhoenixAZ	SanDiegoCA	DallasTX	SanAntonioTX	DetroitMI	SanJoseCA	IndianapolisIN	SanFranciscoCA	JacksonvilleFL	ColumbusOH	AustinTX	MemphisTN	BaltimoreMD	MilwaukeeWI	BostonMA
New York NY	8104	1	2458	718	1421	78	2142	2429	1372	1584	489	2554	647	2573	836	480	1513	956	171	740	191
Los Angeles CA	3805	2458	1	1747	1381	2399	367	116	1250	1211	1985	294	1815	340	2154	1983	1235	1612	2324	1746	2601
Chicago IL	2935	718	1747	1	939	667	1446	1726	800	1049	238	1836	164	1855	864	277	975	482	607	86	854
Houston TX	2029	1421	1381	939	1	1345	1015	1300	225	189	1108	1605	868	1644	822	995	147	485	1253	1007	1607
Philadelphia PA	1523	78	2399	667	1345	1	2079	2367	1300	1509	446	2501	585	2521	764	417	1438	882	93	697	268
Phoenix AZ	1396	2142	367	1446	1015	2079	1	298	887	847	1683	609	1495	652	1792	1663	869	1262	1999	1457	2296
San Diego CA	1260	2429	116	1726	1300	2367	298	1	1182	1125	1963	409	1783	456	2087	1951	1154	1559	2290	1730	2578
Dallas TX	1234	1372	1250	800	225	1300	887	1182	1	253	998	1449	764	1485	906	913	181	420	1211	856	1550
San Antonio TX	1189	1584	1211	1049	189	1509	847	1125	253	1	1238	1448	1000	1488	1011	1141	75	632	1418	1107	1767
Detroit MI	960	489	1985	238	1108	446	1683	1963	998	1238	1	2069	240	2087	837	166	1164	626	401	252	617
San Jose CA	922	2554	294	1836	1605	2501	609	409	1449	1448	2069	1	1926	47	2340	2090	1462	1775	2433	1821	2681
Indianapolis IN	804	647	1815	164	868	585	1495	1783	764	1000	240	1926	1	1948	701	169	926	387	510	246	808
San Francisco CA	800	2573	340	1855	1644	2521	652	456	1485	1488	2087	47	1948	1	2373	2112	1501	1805	2455	1838	2699
Jacksonville FL	762	836	2154	864	822	764	1792	2087	906	1011	837	2340	701	2373	1	672	960	588	683	947	1019
Columbus OH	715	480	1983	277	995	417	1663	1951	913	1141	166	2090	169	2112	672	1	1067	512	343	334	644
Austin TX	682	1513	1235	975	147	1438	869	1154	181	75	1164	1462	926	1501	960	1067	1	559	1347	1034	1695
Memphis TN	666	956	1612	482	485	882	1262	1559	420	632	626	1775	387	1805	588	512	559	1	792	561	1137
Baltimore MD	664	171	2324	607	1253	93	1999	2290	1211	1418	401	2433	510	2455	683	343	1347	792	1	645	360
Milwaukee WI	605	740	1746	86	1007	697	1457	1730	856	1107	252	1821	246	1838	947	334	1034	561	645	1	862
Boston MA	598	191	2601	854	1607	268	2296	2578	1550	1767	617	2681	808	2699	1019	644	1695	1137	360	862	1
El Paso TX	585	1899	712	1243	672	1831	348	629	569	500	1472	954	1259	995	1468	1423	526	973	1746	1271	2066
Nashville TN	584	761	1786	395	667	687	1442	1739	615	824	473	1934	252	1962	501	335	752	196	597	481	944
Denver CO	583	1626	843	910	876	1571	587	835	661	799	1146	933	993	956	1461	1158	768	876	1501	904	1762
Seattle WA	578	2409	957	1734	1891	2375	1111	1060	1683	1786	1932	714	1870	681	2454	2010	1770	1869	2330	1686	2490
Washington DC	578	204	2304	597	1221	127	1977	2269	1182	1387	399	2417	492	2439	649	328	1317	763	35	639	394
Charlotte NC	560	533	2126	590	928	456	1779	2076	928	1105	512	2274	431	2301	341	352	1039	519	367	665	723
Fort Worth TX	555	1403	1218	822	237	1330	854	1150	34	238	1024	1419	790	1455	938	941	171	451	1241	876	1580
Portland OR	542	2444	822	1753	1834	2406	1002	928	1633	1717	1961	572	1882	538	2437	2029	1707	1850	2356	1712	2536
Las Vegas NV	518	2236	232	1523	1231	2178	257	260	1076	1075	1760	375	1596	414	1972	1763	1088	1414	2105	1519	2376
Tucson AZ	514	2120	455	1438	933	2054	116	367	824	759	1673	715	1474	759	1727	1641	787	1216	1973	1456	2280
Oklahoma City OK	514	1328	1189	689	413	1260	840	1137	191	420	909	1357	689	1389	985	852	357	424	1176	732	1495
New Orleans LA	489	1159	1686	824	328	1081	1320	1612	445	517	932	1893	705	1930	495	790	468	349	989	905	1349
Cleveland OH	481	408	2054	311	1115	358	1744	2028	1024	1257	96	2146	263	2166	771	124	1183	631	307	340	552
Long Beach CA	475	2454	27	1745	1364	2394	351	90	1236	1193	1982	320	1810	366	2141	1978	1218	1602	2319	1745	2599
Albuquerque NM	455	1813	674	1123	752	1749	330	624	588	615	1359	862	1166	898	1485	1334	614	939	1670	1138	1969
KS City MO	448	1096	1365	408	649	1035	1047	1333	455	705	640	1483	451	1508	950	619	636	374	960	438	1249
Fresno CA	440	2460	201	1743	1487	2405	491	313	1333	1329	1977	120	1827	162	2227	1993	1343	1664	2336	1731	2592
VA Beach VA	437	295	2375	715	1215	232	2037	2332	1206	1391	542	2504	588	2528	549	439	1325	790	180	768	471
Atlanta GA	436	749	1941	587	701	671	1587	1884	717	881	601	2107	428	2137	287	438	817	333	579	671	939
Sacramento CA	419	2505	353	1787	1604	2453	630	467	1439	1454	2018	91	1883	77	2321	2046	1463	1749	2388	1768	2628
Mesa AZ	419	2128	387	1434	995	2064	21	316	868	827	1671	630	1481	673	1773	1649	849	1245	1985	1446	2283
Oakland CA	411	2561	331	1844	1632	2509	641	447	1472	1476	2076	39	1936	13	2361	2100	1489	1792	2443	1827	2687
Tulsa OK	399	1228	1277	593	441	1160	933	1229	236	485	810	1435	589	1466	916	752	416	340	1077	639	1395
Omaha NE	394	1150	1317	433	796	1097	1029	1300	588	828	669	1405	528	1425	1101	689	764	536	1030	431	1286
Minneapolis MN	392	1022	1527	354	1057	984	1274	1526	862	1109	539	1570	510	1584	1192	626	1042	703	938	295	1124
Colorado Springs CO	379	1635	826	922	825	1577	549	809	614	742	1159	935	996	961	1436	1163	713	854	1505	922	1776
Miami FL	375	1091	2345	1189	968	1027	1979	2267	1108	1149	1160	2557	1027	2593	327	996	1114	870	958	1273	1259
Saint Louis MO	353	878	1593	260	680	813	1266	1557	546	792	456	1717	233	1742	754	399	717	245	734	328	1040
Wichita KS	349	1267	1203	588	559	1204	875	1165	341	573	820	1341	620	1369	1031	788	511	445	1125	617	1424
Santa Ana CA	348	2441	40	1732	1348	2381	335	78	1220	1177	1970	333	1797	379	2125	1965	1202	1587	2305	1733	2586

Appendix B

B1: Schematic of the three levels of the tri-level problem

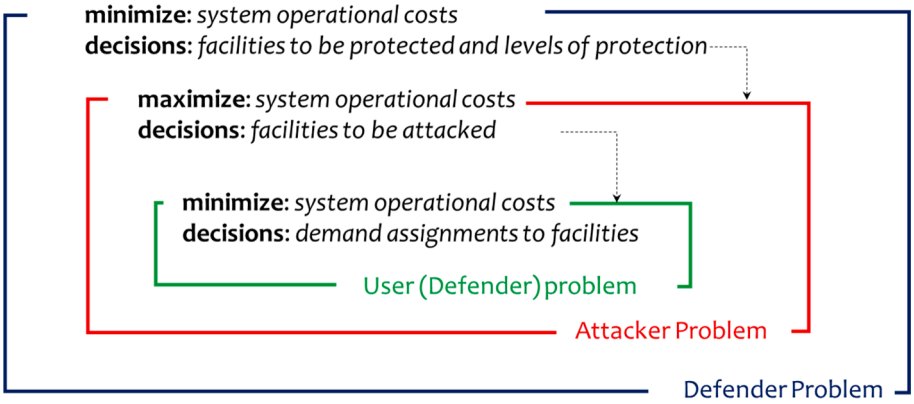


Fig. B1. Tri level model illustration.

B2: Linearizing the max function term in the congestion cost expression

$$G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + \sum_{j\in J}\sum_{t=1}^{T}\max_{k\in K_j}\left(w(1-q)\left(\sum_i x_{ijt}{}^k\right)^q + q\left(\sum_i x_{ijt}{}^k\right)^{q-1}\left(\sum_i x_{ijt}\right)\right)\right) \tag{B.1}$$

The above min max expression (B.1) can be converted into a conventional linear programming form by introducing a variable η_{jt}, so that the transformed objective (B.1) can be represented by the following:

$$G(s,z) = \min_{x,u}\left(\sum_{i\in I}\sum_{j\in J}\sum_{t=1}^{T} d_{ij}x_{ijt} + \sum_{i\in I}\sum_{t=1}^{T}\beta_i u_{it} + w\sum_{j\in J}\sum_{t=1}^{T}\eta_{jt}\right) \tag{B.2}$$

$$\eta_{jt} - q\left(\sum_i x_{ijt}^k\right)^{q-1}\left(\sum_i x_{ijt}\right) \geq (1-q)\left(\sum_i x_{ijt}^k\right)^q \quad \forall j \in J, k \in K_j, t = 1\ldots T \tag{B.3}$$

The new constraint (B.3) guarantees that η_{jt} for each j and t will be greater than or equal to each of $\sum_{j\in J}\sum_{t=1}^{T}\left((1-q)\left(\sum_i x_{ijt}{}^k\right)^q + q\left(\sum_i x_{ijt}{}^k\right)^{q-1}\left(\sum_i x_{ijt}\right)\right)$ for all k. By minimizing η_{jt}, it will lead to the maximum of these expressions.

B3: Linear approximation error of congestion function

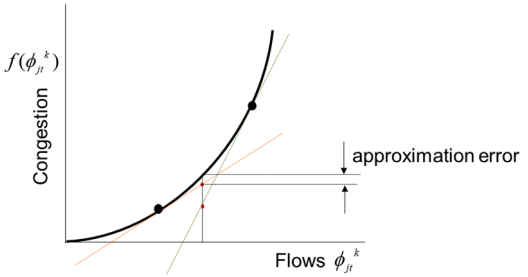


Fig. B3. Congestion function and linear approximation illustration.

The deviation resulting from the linear approximation of congestion cost to that of the actual value is explained by the following Figure. With more number of tangent hyperplanes used (high interval granularity) for estimation, the higher is the accuracy of the results.

B4: Flowchart of Search Tree Algorithm

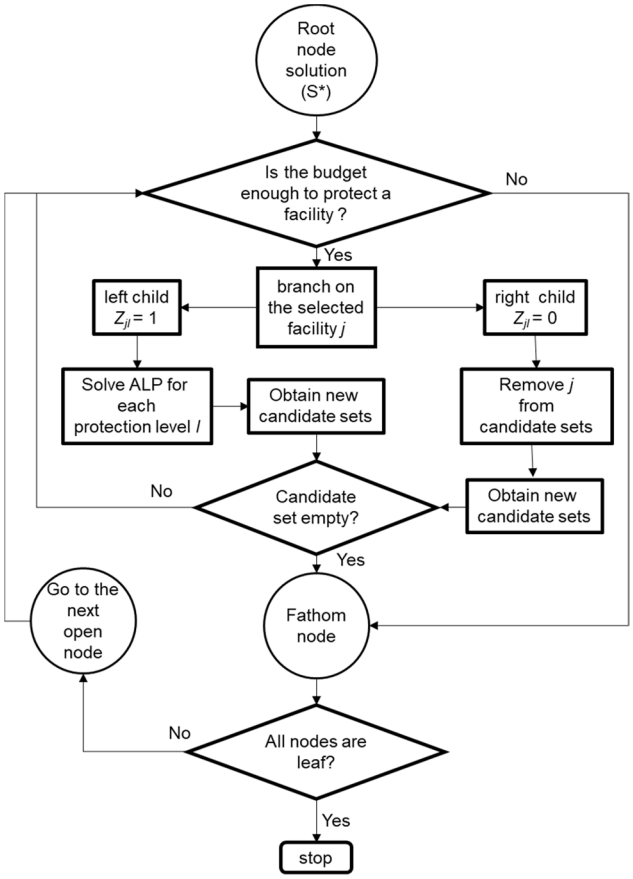


Fig. B4. Flowchart of search tree algorithm.

Reference

Aboolian, R., Berman, O., & Krass, D. (2012). Profit maximizing distributed service system design with congestion and elastic demand. Transportation Science, 46(2), 247-261.

Aksen, D., Piyade, N., Aras, N., 2010. The budget constrained r-interdiction median problem with capacity expansion. Central European Journal of Operations Research 18 (3), 269–291.

Aksen, D., Aras, N., 2012. A bilevel fixed charge location model for facilities under imminent attack. Computers & Operations Research 39 (7), 1364–1381.

Alumur, S.A., Nickel, S., Rohrbeck, B., Saldanha-da-Gama, F., 2018. Modeling congestion and service time in hub location problems. Applied Mathematical Modelling 55, 13–32.

Alkaabneh, F., Diabat, A., Elhedhli, S., 2019. A Lagrangian heuristic and GRASP for the hub-and-spoke network system with economies-of-scale and congestion. Transportation Research Part C: Emerging Technologies 102, 249–273.

An, S., Cui, N., Bai, Y., Xie, W., Chen, M., Ouyang, Y., 2015. Reliable emergency service facility location under facility disruption, en-route congestion and in-facility queuing. Transportation research part E: logistics and transportation review 82, 199–216.

Azad, N., Hassini, E., 2019. Recovery strategies from major supply disruptions in single and multiple sourcing networks. European Journal of Operational Research 275 (2), 481–501.

Azizi, N., Vidyarthi, N., Chauhan, S.S., 2018. Modelling and analysis of hub-and-spoke networks under stochastic demand and congestion. Annals of Operations Research 264 (1–2), 1–40.

Bao, S., Zhang, C., Ouyang, M., Miao, L., 2019. An integrated tri-level model for enhancing the resilience of facilities against intentional attacks. Annals of Operations Research 283 (1–2), 87–117.

Berman, O., Krass, D., Menezes, M.B., 2007. Facility reliability issues in network p-median problems: Strategic centralization and co-location effects. Operations Research 55 (2), 332–350.

Berman, O., Krass, D., 2019. Stochastic location models with congestion. In: Location science. Springer, Cham, pp. 477–535.

Bier, T., Lange, A., Glock, C.H., 2020. Methods for mitigating disruptions in complex supply chain structures: a systematic literature review. International Journal of Production Research 58 (6), 1835–1856.

Bitran, G.R., Tirupati, D., 1989. Tradeoff curves, targeting and balancing in manufacturing queueing networks. Operations Research 37 (4), 547–564.

Bloomberg, 2020, https://www.bloomberg.com/news/features/2020-03-25/3m-doubled-production-of-n95-face-masks-to-fight-coronavirus, accessed on May 31, 2020.

Camargo, R.S., Miranda Jr, G., Ferreira, R.P.M., Luna, H.P., 2009. Multiple allocation hub-and-spoke network design under hub congestion. Computers & Operations Research 36 (12), 3097–3106.

Cappanera, P., Scaparra, M.P., 2011. Optimal allocation of protective resources in shortest-path networks. Transportation Science 45 (1), 64–80.

Choi, T.Y., Rogers, D., and Vakil, B. (2020) Coronavirus Is a Wake-Up Call for Supply Chain Management. Harvard Business Review, March 2020. https://hbr.org/2020/03/coronavirus-is-a-wake-up-call-for-supply-chain-management, accessed on May 31, 2020.
Church, R.L., Scaparra, M.P., 2007. Protecting critical assets: The r-interdiction median problem with fortification. Geographical Analysis 39 (2), 129–146.
Church, R. L., Scaparra, M. P., & Middleton, R. S. (2004). Identifying critical infrastructure: The median and covering facility interdiction problems. Annals of the Association of American Geographers, 94(3), 491-502.
Cui, T., Ouyang, Y., Shen, Z.M., 2010. Reliable facility location design under the risk of disruptions. Operations Research 58 (4-part-1), 998–1011.
Daskin, M.S., 2004. SITATION—facility location software. Northwestern University, Evanston, IL, Department of Industrial Engineering and Management Sciences.
Dolgui, A., Ivanov, D., Sokolov, B., 2018. Ripple effect in the supply chain: an analysis and recent literature. International Journal of Production Research 56 (1–2), 414–430.
Ebrahim Nejad, A., Niroomand, I., Kuzgunkaya, O., 2014. Responsive contingency planning in supply risk management by considering congestion effects. Omega 48, 19–35.
Elhedhli, S., Hu, F.X., 2005. Hub-and-spoke network design with congestion. Computers & Operations Research 32 (6), 1615–1632.
!"count(.//sb:host[1]//child::*//sb:date)" > Forghani, A., Dehghanian, F., Salari, M., Ghiami, Y., . A bi-level model and solution methods for partial interdiction problem on capacitated hierarchical facilities. Computers & Operations Research 114.
Fortune, 2020. https://fortune.com/2020/02/21/fortune-1000-coronavirus-china-supply-chain-impact/, accessed on May 31, 2020.
Goldbeck, N., Angeloudis, P., Ochieng, W., 2020. Optimal supply chain resilience with consideration of failure propagation and repair logistics. Transportation Research Part E: Logistics and Transportation Review 133.
Hopp, W.J., Yin, Z., 2006. Protecting supply chain networks against catastrophic failures. Working Paper, Dept. of Industrial Engineering and Management Science. Northwestern University, Evanston, IL.
Ivanov, D., 2020. Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transportation Research Part E: Logistics and Transportation Review 136.
Ivanov, D., Dolgui, A., Sokolov, B., 2018. Scheduling of recovery actions in the supply chain with resilience analysis considerations. International Journal of Production Research 56 (19), 6473–6490.
Ivanov, D., Sokolov, B., Dolgui, A., 2014. The Ripple effect in supply chains: trade-off 'efficiency-flexibility-resilience' in disruption management. International Journal of Production Research 52 (7), 2154–2172.
Jalali, S., Seifbarghy, M., Niaki, S.T.A., 2018. A risk-averse location-protection problem under intentional facility disruptions: A modified hybrid decomposition algorithm. Transportation Research Part E: Logistics and Transportation Review 114, 196–219.
Kian, R., Kargar, K., 2016. Comparison of the formulations for a hub-and-spoke network design problem under congestion. Computers & Industrial Engineering 101, 504–512.
Kim, S., 2013. A column generation heuristic for congested facility location problem with clearing functions. Journal of the Operational Research Society 64 (12), 1780–1789.
Klibi, W., Martel, A., 2012. Modeling approaches for the design of resilient supply networks under disruptions. International Journal of Production Economics 135 (2), 882–898.
Konur, D., Geunes, J., 2011. Analysis of traffic congestion costs in a competitive supply chain. Transportation Research Part E: Logistics and Transportation Review 47 (1), 1–17.
Konur, D., Geunes, J., 2012. Competitive multi-facility location games with non-identical firms and convex traffic congestion costs. Transportation Research Part E: Logistics and Transportation Review 48 (1), 373–385.
Li, X., Ouyang, Y., 2010. A continuum approximation approach to reliable facility location design under correlated probabilistic disruptions. Transportation research part B: methodological 44 (4), 535–548.
Li, Q., Zeng, B., Savachkin, A., 2013. Reliable facility location design under disruptions. Computers & Operations Research 40 (4), 901–909.
Liberatore, F., Scaparra, M.P., 2011. Optimizing protection strategies for supply chains: comparing classic decision-making criteria in an uncertain environment. Annals of the Association of American Geographers 101 (6), 1241–1258.
Liberatore, F., Scaparra, M.P., Daskin, M.S., 2011. Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification. Computers & Operations Research 38 (1), 357–366.
Liberatore, F., Scaparra, M.P., Daskin, M.S., 2012. Hedging against disruptions with ripple effects in location analysis. Omega 40 (1), 21–30.
Lim, M., Daskin, M.S., Bassamboo, A., Chopra, S., 2010. A facility reliability problem: Formulation, properties, and algorithm. Naval Research Logistics 57 (1), 58–70.
Losada, C., Scaparra, M.P., Church, R.L., Daskin, M.S., 2012. The stochastic interdiction median problem with disruption intensity levels. Annals of Operations Research 201 (1), 345–365.
Losada, C., Scaparra, M.P., O'Hanley, J.R., 2012. Optimizing system resilience: A facility protection model with recovery time. European Journal of Operational Research 217 (3), 519–530.
Marianov, V., Serra, D., 2003. Location models for airline hubs behaving as M/D/c queues. Computers & Operations Research 30 (7), 983–1003.
Marufuzzaman, M., Ekşioğlu, S.D., 2017. Managing congestion in supply chains via dynamic freight routing: An application in the biomass supply chain. Transportation Research Part E: Logistics and Transportation Review 99, 54–76.
Moore, J.T., Bard, J.F., 1990. The mixed integer linear bilevel programming problem. Operations research 38 (5), 911–921.
Ni, N., Howell, B.J., Sharkey, T.C., 2018. Modeling the impact of unmet demand in supply chain resiliency planning. Omega 81, 1–16.
Niroomand, I., Kuzgunkaya, O., Bulgak, A.A., 2012. Impact of reconfiguration characteristics for capacity investment strategies in manufacturing systems. International Journal of Production Economics 139 (1), 288–301.
Parajuli, A., Kuzgunkaya, O., Vidyarthi, N., 2017. Responsive contingency planning of capacitated supply networks under disruption risks. Transportation Research Part E: Logistics and Transportation Review 102, 13–37.
Pavlov, A., Ivanov, D., Dolgui, A., Sokolov, B., 2017. Hybrid fuzzy-probabilistic approach to supply chain resilience assessment. IEEE Transactions on Engineering Management 65 (2), 303–315.
Poudel, S.R., Quddus, M.A., Marufuzzaman, M., Bian, L., 2019. Managing congestion in a multi-modal transportation network under biomass supply uncertainty. Annals of Operations Research 273 (1–2), 739–781.
Putnik, G., Sluga, A., ElMaraghy, H., Teti, R., Koren, Y., Tolio, T., Hon, B., 2013. Scalability in manufacturing systems design and operation: State-of-the-art and future developments roadmap. CIRP Annals 62 (2), 751–774.
Qi, L., Shen, Z.J.M., Snyder, L.V., 2010. The effect of supply disruptions on supply chain design decisions. Transportation Science 44 (2), 274–289.
Scaparra, M.P., Church, R.L., 2008. A bilevel mixed-integer program for critical infrastructure protection planning. Computers & Operations Research 35 (6), 1905–1923.
Scaparra, M.P., Church, R.L., 2008. An exact solution approach for the interdiction median problem with fortification. European Journal of Operational Research 189 (1), 76–92.
Scaparra, M.P., Church, R.L., 2012. Protecting supply systems to mitigate potential disaster: A model to fortify capacitated facilities. International Regional Science Review 35 (2), 188–210.
Schmitt, A.J., 2011. Strategies for customer service level protection under multi-echelon supply chain disruption risk. Transportation Research Part B: Methodological 45 (8), 1266–1283.
Smith, J.C., Song, Y., 2020. A survey of network interdiction models and algorithms. European Journal of Operational Research 283, 797–811.
The World Economic Forum COVID Action Platform, 2020, https://www.weforum.org/agenda/2020/05/this-is-what-global-supply-chains-will-look-like-after-covid-19/, accessed on May 31, 2020.
Tomlin, B., 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. Management Science 52 (5), 639–657.
Wang, W., Koren, Y., 2012. Scalability planning for reconfigurable manufacturing systems. Journal of Manufacturing Systems 31 (2), 83–91.

Weisbrod, G., Vary, D., Treyz, G., 2001. Economic implications of congestion, NCHRP Report #463. DC, National Cooperative Highway Research Program, Transportation Research Board, Washington.
Xu, S., Zhang, X., Feng, L., Yang, W., 2020. Disruption risks in supply chain management: a literature review based on bibliometric analysis. International Journal of Production Research 1–19.
Zhang, M., Batta, R., Nagi, R., 2011. Designing manufacturing facility layouts to mitigate congestion. IIE Transactions 43 (10), 689–702.