Transportation Research Part E 114 (2018) 196–219

Contents lists available at ScienceDirect

Transportation Research Part E

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

A risk-averse location-protection problem under intentional facility disruptions: A modified hybrid decomposition algorithm

Sajjad Jalali[a], Mehdi Seifbarghy[a,*], Seyed Taghi Akhavan Niaki[b]

[a] Department of Industrial Engineering, Faculty of Industrial and Mechanical Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran
[b] Department of Industrial Engineering, Sharif University of Technology, P.O. Box 11155-9414 Azadi Ave, Tehran 1458889694, Iran

ARTICLE INFO

Keywords:
Facility location-protection problem
Conditional value-at-risk
Bi-level programming
Decomposition algorithm
Sample average approximation
Game theory

ABSTRACT

The rising disruptions of interdictors force supply chains' designers to embody the protection decisions when locating the facilities. In the presence of variability in the intensity of disruptions, a risk measure is incorporated into the decision-making. The designer-interdictor bi-level problem, therefore, optimizes the joint location and protection decisions with respect to the conditional value-at-risk. This configuration has been absent from the literature. An accelerated modified Benders decomposition algorithm is developed and enhanced by being hybridized with a sample average approximation-based genetic algorithm. We examine how this new configuration influences the optimal solutions and assess the effectiveness of the proposed method.

1. Introduction

Designing a supply chain (SC) structure involves making irreversible and non-repetitive decisions about the location of critical facilities and infrastructures that should perform reliably over a long-term horizon (Shen et al., 2011). However, the reliability may be threatened by a number of unprecedented but prohibitive events such as intentional disruptions. Recently, the threat of the malicious attacks has prompted some elaborate security precautions. For instance, Ukraine's administrative participants have tightened security measures after several targets (such as oil producer, power distributor, and banking systems) have been hit by the Petya Ransomware attack.[1] Therefore, the designer of an SC structure should take necessary precautions of protecting facilities against intentional disruptions in addition to the classical location decision. On the other hand, an interdictor follows the location and protection decisions meticulously and then devises an attack to demolish the designer's objective, at most. The designer's objective is to minimize the expected cost over all scenarios (mean measure) while hedging against the risk of the losses of the extreme scenarios (risk measure). Thus, there is a Stackelberg game between the designer (leader) and the interdictor (follower) with conflicting objectives. In this regard, the bi-level programming is the most well-known approach for mathematical formulation of the Stackelberg game (Gedik et al., 2014; Zhang et al., 2016).

In accordance with the aforementioned requirements, a risk-averse game-theoretic joint reliable facility location-protection problem under intentional disruptions is presented in this paper. More specifically, regarding the concise review presented in Table 1, the proposed model formulation in this paper is a non-trivial extension of the previous studies. It is a novel study as a result of considering the joint location and protection decisions, incorporating a mean-risk measure and using a hybridized solution method. In detail, Scaparra and Church (2008) were one of the pioneers of the reliable facility location problem under intentional disruptions. They proposed a location-fortification problem disjointedly assuming an existing set of opened facilities. Utilizing a bi-level

* Corresponding author.
E-mail addresses: sajjad.jalali@qiau.ac.ir (S. Jalali), m.seifbarghy@qiau.ac.ir (M. Seifbarghy), Niaki@Sharif.edu (S.T.A. Niaki).

[1] http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/1.

https://doi.org/10.1016/j.tre.2018.04.004
Received 8 October 2017; Received in revised form 5 April 2018; Accepted 6 April 2018
1366-5545/ © 2018 Published by Elsevier Ltd.

Table 1
Literature review.

Studies	Decisions (L, P, LPs)[a]	Optimization measures (EC, WC, MR)[b]	Methodologies (A, E, H)[c]
Scaparra and Church (2008)	P	WC	H
Schütz et al. (2009)	L	EC	A, E
Shen et al. (2011)	L	EC	A, H
O'Hanley and Church (2011)	P	WC	E
Liberatore et al. (2011)	P	EC, WC	H
Losada et al. (2012)	P	WC	E
Noyan (2012)	L	MR	E
Perea and Puerto (2013)	P	WC	E
Bricha and Nourelfath (2013)	L, P	EC	H
Bricha and Nourelfath (2014)	L, P	EC	H
An et al. (2014)	L	WC	E
Bricha and Nourelfath (2015)	L, P	EC	H
Konak et al. (2015)	L,P	WC	A,H
Jalali et al. (2016)	L	EC	H
Zhang et al. (2016)	L	EC	E, H
Naderi and Pishvaee (2017)	L	EC	A,E
Yu et al. (2017)	L	MR	E
Quddus et al. (2017)	L	EC	A,E,H
Karakose and McGarvey (2018)	P	WC	E
Current study	LPs	MR	A,E,H

[a] L: Considering location decision, P: Considering protection decision, LPs: Considering location and protection decisions simultaneously.
[b] EC, WC, and MR are abbreviations for expected, worst-case, and mean-risk costs to optimize a supply chain structure, respectively.
[c] A: Using approximation methods, E: Using exact methods, H: Using heuristic and *meta*-heuristics methods.

programming, the planner fortified a specific number of facilities in the upper-level while the interdictor hit the remaining unprotected facilities in the lower-level. Focusing on the extreme scenarios, the objective was to minimize the worst transportation cost. However, using an implicit enumeration approach, they failed to address the location and fortification decisions simultaneously while neglecting the mean-risk measure. To minimize the worst-case impact of intentional disruptions, Liberatore et al. (2011) considered the fortification of an existing set of facilities being exposed to an uncertain number of attacks. Perea and Puerto (2013) discussed the problem of designing a railway network where the edges were subjected to the failure due to the intentional attacks. A dynamic game-theoretic model was proposed to a robust design of the network aiming at maximizing the worst trip coverage scenario. Once the network was built, the optimal allocation of security resources was also adopted using a Stackelberg game. The resulted nonlinear programming was directly solved by the CONOPT solver provided in the GAMS commercial software. Karakose and McGarvey (2018) mitigated the impact of disruptions on the nodes or arcs of an existing transportation network using a set of protective resources. Concerning limited protective resources, they assumed that those resources made the corresponding arcs/nodes immune to the disruptions. Their proposed mixed-integer programming model identified the subset of protected arcs to hedge against the worst-case scenario using the special path aggregation method.

Bricha and Nourelfath (2013, 2014, 2015) conducted consecutive studies to extend the game-theoretic facility location-protection problem under intentional attacks. In terms of the small-sized instances, they found the equilibrium solution by solving the game with the basic backward induction algorithm. Our study, in fact, shares the most similarities with the recent studies and in particular, Bricha and Nourelfath (2013). In the same vein of their study, we target an un-capacitated facility location problem where the facilities are subjected to failures. The failure probability of the facilities is proportional to a contest between the protective and adversary efforts of the designer and the interdictor, respectively. The effort criterion mainly shows the intensity of protecting or interdicting a specific facility. Hence, analogous to the recent study, we characterize the protection and malicious strategies through the effort unit.

Albeit the similarities, our mathematical formulation is instantly distinguishable due to the joint consideration of the location and protection decisions and the incorporation of a risk measure. On one hand, Bricha and Nourelfath (2013) did not merge the un-capacitated facility location problem into the game-theoretic model and made the location decisions in the absence of the protection and malicious strategies. This disjointed approach may lead to a sub-optimal solution when the protection requirements need to be considered at the design stage of an SC structure. Thus, it is a significant contribution to undertake the location and protection decisions simultaneously. In this regard, a framework is provided to optimize jointly the location and protection decisions under the threat of a malicious strategy. On the other hand, by considering a finite number of scenarios, Bricha and Nourelfath (2013) found the optimal decisions in terms of the total expected cost of the SC structure, including the allocation, penalty and restoration expenditures. However, using the expectation criterion as a risk-neutral preference is not a robust choice for capturing the stochastic variables (e.g. total cost). It has been observed that a risk-averse approach can provide more robust solutions than a risk-neutral counterpart (Yu et al., 2017). To this aim, the conditional value at risk (CVaR) is a widely applied tool for satisfying the risk-averse preference. Defining the value-at-risk (VaR) as the minimum upper-bound for a stochastic variable at a specific confidence level, CVaR measures the expected cost beyond the VaR. Thus, we develop a risk-averse location-protection problem by customizing the CVaR formulation of Noyan (2012).