Computers & Operations Research 39 (2012) 1364–1381

Contents lists available at SciVerse ScienceDirect

Computers & Operations Research

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

A bilevel fixed charge location model for facilities under imminent attack

Deniz Aksen [a,*], Necati Aras [b]

[a] College of Administrative Sciences and Economics, Koç University, Rumeli Feneri Yolu, Sarıyer, İstanbul, Turkey
[b] Department of Industrial Engineering, Boğaziçi University, Bebek, İstanbul, Turkey

ARTICLE INFO

Available online 16 August 2011

Keywords:
Fixed charge facility location
Protection
Interdiction
Bilevel programming
Tabu search
Hash function

ABSTRACT

We investigate a bilevel fixed charge facility location problem for a system planner (the defender) who has to provide public service to customers. The defender cannot dictate customer-facility assignments since the customers pick their facility of choice according to its proximity. Thus, each facility must have sufficient capacity installed to accommodate all customers for whom it is the closest one. Facilities can be opened either in the protected or unprotected mode. Protection immunizes against an attacker who is capable of destroying at most r unprotected facilities in the worst-case scenario. Partial protection or interdiction is not possible. The defender selects facility sites from m candidate locations which have different costs. The attacker is assumed to know the unprotected facilities with certainty. He makes his interdiction plan so as to maximize the total post-attack cost incurred by the defender. If a facility has been interdicted, its customers are reallocated to the closest available facilities making capacity expansion necessary. The problem is formulated as a static Stackelberg game between the defender (*leader*) and the attacker (*follower*). Two solution methods are proposed. The first is a tabu search heuristic where a hash function calculates and records the hash values of all visited solutions for the purpose of avoiding cycling. The second is a sequential method in which the location and protection decisions are separated. Both methods are tested on 60 randomly generated instances in which m ranges from 10 to 30, and r varies between 1 and 3. The solutions are further validated by means of an exhaustive search algorithm. Test results show that the defender's facility opening plan is sensitive to the protection and distance costs.

1. Introduction and literature review

The OR community's interest in the protection of critical facilities has grown substantially in the last decade. There exist a number of reliability models for facility location in the literature where the cause of disruption is based on failures of one or more facilities of a distribution or service network (see [1], for a review). The number of the so-called interdiction models that focus on man-made attacks to facilities is, however, relatively limited. In this type of models, the motivation is to examine system vulnerabilities from the perspective of the attacker and to anticipate the damage of terrorist attacks that are carried out to cause maximal disruption in service provision or accessibility. This analysis helps the system planners to understand the identification of facilities that are most likely to be targeted by the attackers and to establish protection plans to minimize the disruptions.

Church et al. [2] considered facility interdiction in a service network and formulated two models from an attacker's viewpoint given that there are p existing facilities serving the customers. In the r-interdiction median problem (RIM), the objective is to maximize the demand-weighted total distance by attacking r out of p facilities where the customers of the disrupted facilities have to be reassigned to undamaged facilities to get service. In the r-interdiction covering problem (RIC), the goal of the attacker is to determine a subset of r facilities among the set of p existing ones, which if destroyed will yield the greatest reduction in covered customer demand. It is not difficult to see that RIM (RIC) is the antithesis of the well-known p-median problem (maximal covering problem).

Instead of considering the redesign of an entire service network subject to terrorist attacks (e.g., by relocating facilities) a less costly and reasonable option can be the attempt of protecting some of its facilities. Previous research that addresses the protection issue within the context of facility location is relatively scarce. In this respect, we can mention the following nine studies:

(i) Church and Scaparra [3] incorporate the protection (fortification) of facilities into the RIM model and obtain the interdiction median problem with fortification (IMF). The aim in IMF is to identifying q facilities to be protected in a network of p existing facilities such that the total demand satisfaction cost expressed as the demand-weighted shortest distance between non-interdicted facilities and customers after the attack is as small as possible. Here, the objective of the attacker is to render r facilities out of service to maximize the total demand satisfaction cost provided that $q+r \leq p$ holds. Assuming that

* Corresponding author. Tel.: +90 212 338 1684; fax: +90 212 338 1653.
E-mail addresses: daksen@ku.edu.tr (D. Aksen), arasn@boun.edu.tr (N. Aras).

0305-0548/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cor.2011.08.006

the attacker has complete information about the protection status of the facilities, the authors solve IMF using the general-purpose commercial solver Cplex 7.0. The main drawback of the mathematical programming formulation of IMF is that it is based on an explicit enumeration of all possible ways of losing r out of p facilities. Therefore, the size of the problem grows exponentially as p and r increase, which results in long computation times.

(ii) With the intention of solving large size instances of IMF, Scaparra and Church [4] develop another formulation referred to as the maximal covering problem with precedence constraints (MCPC). They propose a solution procedure capitalizing on the reducibility of the new formulation to a smaller problem which can be solved to optimality by Cplex.

(iii) The same authors [5] propose a bilevel programming formulation of the r-interdiction median problem with fortification referred to as RIMF. A bilevel programming problem (BPP) is a multi-level optimization problem with two parties, one of whom takes the leader's position (first level), and the other one is the follower (second level) making his or her plan based on the leader's decision. When expressed in mathematical programming terms, a subset of the variables in the upper level problem is constrained to be a solution of the optimization problem in the lower level. In RIMF the lower level problem corresponds to the RIM described in [2] where the attacker (*follower*) has to solve a pure interdiction problem according to the outcome of the upper level fortification problem solved by the defender (*leader*). The solution methodology for RIMF is based on an implicit enumeration algorithm performed on a search tree. Larger instances of RIMF can be solved to optimality using this solution approach.

(iv) Scaparra and Church [6] extend the RIMF problem to the case where the facilities are capacitated and upon interdiction their capacities are reduced. The proposed optimization model has three levels: in the first level the decision is made by the system planner about which facilities to protect so as to minimize the lost sales cost and the maximum damage that occurs after the loss of r facilities; in the second level the attacker determines which r facilities to interdict; and in the third level the system planner allocates the demand points to the remaining facilities as cost-effectively as possible.

(v) The study of Losada et al. [7] deals with a novel variant of the interdiction median problem where facilities that are attacked are not destroyed with certainty, but continue to be operational with a given probability. The probability of a facility surviving an attack depends on the level of offensive resources invested into that attack. These levels are predetermined, and both the survival probabilities and the attack costs at different levels are known in advance. The model is formulated from the perspective of an interdictor whose aim is to allocate his offensive resources in such a way that the expected disruption (measured as the expected demand-weighted traveling distance) is maximized.

(vi) Motto et al. [8] present a bilevel model for the electric grid security under disruptive threat. An aggressor with limited resources, who acts as the leader in the upper level, tries to cause the maximum disruption to the electric grid. The system operator that represents the follower in the lower level responds to the aggressor by taking corrective actions with the aim of minimizing the disruption level.

(vii) In the context of biological conservation, O'Hanley et al. [9] solve the problem of protecting critical ecological sites in a region to minimize species losses under a protection budget constraint. They develop two optimization models. In the minimum expected coverage loss (ECL) model, which is formulated as an integer program, expected species losses are minimized over all possible loss patterns outside the reserve sites. In the minimax coverage loss (MCL) model, maximum species losses following the worst-case loss of a restricted subset of nonreserve sites are minimized. MCL is a mixed-integer bilevel program (MIBP) in which a conservation planner reserves (protects) sites in order to minimize species losses while a hypothetical adversary destroys a subset of unprotected areas in an attempt to maximize the same objective.

(viii) The stochastic version of RIMF—designated as S-RIMF—is addressed in an upcoming paper by Liberatore et al. [10]. They propose a maximum coverage type formulation for the model S-RIMF, which deals with a random number of losses and captures thereby the uncertainty in the extent of terrorist attacks. The objective of S-RIMF is to minimize the expected cost expressed as the probability-weighted sum of the costs associated with the worst-case interdiction patterns for every feasible value of r by using monotonically increasing and decreasing probability distributions.

(ix) Aksen et al. [11] add to the RIMF setting a budget constraint on the total cost of facility protections instead of fixing the number of protections a priori. Their new model, referred to as BCRIMF-CE, also incorporates the capacity expansion cost that incurs at some facilities due to the reassignment of customers following the interdiction of the attacker. The sum of capacity expansion costs incurred by those facilities which remain operational and receive new customers after the attack is added to the objective functions of the defender and the attacker. The authors solve the resulting bilevel programming model to optimality with an implicit enumeration algorithm applied on a binary tree similar to the methodology in Scaparra and Church [5].

In this paper we build on the BCRIMF-CE model, and combine it with a fixed charge facility location problem on behalf of the defender. In the resulting model, the defender determines the number and protection status of the facilities to be opened such that the total cost of demand satisfaction before and after the worst-case interdiction of at most r facilities by the attacker is minimized. The cost of protecting the facilities is not subjected to a budget constraint, but included directly in the objective function of the defender. This new scenario is designated the bilevel fixed charge location problem (BFCLP), where the number of facilities opened is a decision variable as is the case in the well-known uncapacitated facility location problem (UFLP). To the best of our knowledge, this is the first study addressing the unified problem of fixed charge facility location, protection, and interdiction as a static Stackelberg game between a system defender (*leader*) and an attacker (*follower*).

Since BFCLP is a bilevel program with binary variables appearing in both the upper and lower level problem (the leader's and the defender's problems), it is $\mathcal{NP}$-hard. We devise two methods for the solution of BFCLP. The first one is a tabu search heuristic, which iteratively explores a large solution space of diverse facility location-protection plans. For each plan, Cplex 11.2 is used to optimally solve the attacker's problem of selecting which facilities to interdict. The second approach is a sequential solution method in which the facility location and protection decisions in the upper level problem are separated. First, the defender's fixed charge facility location problem is optimally solved in the absence of protection decisions. Then, given the subset of unprotected opened facilities, an implicit enumeration algorithm applied on a binary tree is used to determine the particular facilities to be protected by the defender and those to be interdicted by the