Iranian Journal of Operations Research
Vol. 6, No. 2, 2015, pp. 58-72

A Three-Level Mathematical Model for an *r*-interdiction Hierarchical Facility Location Problem

M. Akbari-Jafarabadi[1], R. Tavakkoli-Moghaddam[2,*], M. Mahmoodjanloo[1], Y. Rahimi [2]

In general, any system may here we focus of losing critical facilities by natural disasters or terrorist attacks. This paper focuses on identifying critical facilities and planning to reduce the effect of this event. A three-level model is suggested in the form of a defender-attacker-defender. It is assumed that the facilities are hierarchical and capable of nesting. Also, the attacker budget for the interdiction and defender budget for fortification are limited. At the first level, a defender locates facilities in order to enhance the system capability with the lowest possible cost and full covering customer demand before any interdiction. The worst-case scenario losses are modeled in the second-level. At the third level, a defender is responsible for satisfying the demand of all customers while minimizing the total transportation and outsourcing costs. We use two different approaches to solve the model. In the first approach, the third level of the proposed model is coded in GAMS environment. its second level is solved by an explicit enumeration method, and the first level is solved by tabu search. In the second approach, the first level is solved by the bat algorithm.

Keywords: r-*interdiction median three-level model, Hierarchical facility location, Integer programming, Meta-heuristics.*

Manuscript was received on 21/11/2015 revised on 03/06/2016 and accepted for publication on 24/06/2016

1. Introduction

A critical infrastructure can be defined as those elements that result in significant disruption of the system in its ability to perform its function. These elements can include transportation linkage (e.g., bridges, tunnels and rail), facilities (e.g., port terminals, production facilities, warehouses, operation centers, emergency response facilities and hospitals), critical stockpiles (e.g., vaccine, drugs and food), key personnel (e.g., water system operators) and land marks that may contribute to the loss of well-being (Church et al. [9]). When systems lose their critical linkages and key facilities due to natural disaster or intentional attack, the system performance may be at risk (Aksen et al., [2]). Unfortunately, nowadays terrorists with easy access to information and using modern instrumentations are able to identify best possible ways to maximize the damage to the public. For example, in the event on September 11, 2001, following the terrorist attack, all US borders were closed and all flights were canceled for several days. Two years later, a deadly SARS outbreak disrupted, among many other industries, the furniture manufacturing sector of China, which accounted for about 15% of all the furniture sold in the US. In the 2003 Istanbul bombings by al-Qaeda suicide bombers in Great Britain and the Consulate General Staff and Great Britain Bank, 57civilians were killed and 700 were wounded. Attacks on the telecommunication tower in

[*]Corresponding Author.
[1] Department of Industrial Engineering, University of Science and Technology of Mazandaran, Behshahr, Iran, Email: maryamakbari.math@gmail.com
[2] School of Industrial Engineering, College of Engineering, University of Tehran, Tehran, Iran, Email: tavakoli@ut.ac.ir

Afghanistan in 2008 and on an ambulance station in Northern Ireland are other examples (Aksen et al. [2]).

Therefore, the identification and protection of critical infrastructures and physical assets under a worst-case scenario attracted the attention of operations research (OR) professionals. The roots of protection planning can be traced back to military defense applications, in which enemy attacks are analyzed, called interdiction models. Interdiction models are used in detection communication paths or sensitive networks. Using these models, system vulnerabilities, identification, care and support programs are planned. An interdiction model usually looks at the target system and its vulnerabilities from the attacker's point of view. A typical objective of the attacker (i.e., interdictor) is to identify the most critical assets or infrastructures of a network or a service system. The loss of those due to an interdiction will cause the maximum degree of disruption (Aksen et al. [2]). In these systems, disruption is typically considered in two ways, interdiction on nodes and edges. The models presented in the area of node interdiction are classified in two categories, namely, r-interdiction median (RIM) and r-interdiction covering (RIC) problems.

In the model to be presented here, a three-level model as a defender-attacker-defender is based on a game theory approach. In level one, a defender is to locate facility as the original decision maker. For each of a location strategy adopted by a defender, the attacker is to maximize the service costs by disrupting a system in level two. The defender's reactions include the way to assign customers to the facility and fortify them in the third level of the model. In fact, in the first level, a defender locates facilities at safe of the sites to enhance the capability of the system and at the lowest cost possible as well as full covering customer demand before interdiction. The worst-case scenario losses are modeled in the second-level interdiction problem. And in the third level, a defender is responsible for satisfying the demand of all customers while minimizing the total transportation costs and outsourcing costs. Given that the proposed model is NP-hard, we use a hybrid approach based on tabu search (TS) and bat algorithm (BA) for the level one and exact methods for the levels two and three.

2. Literature Review

For the first time, Church et al. [9] used *p*-median and maximal covering models in interdiction problems at the same time. In their article, an attacker with identification of the most critical facilities aims to apply the worst attack possible to facilities. So that after the interdiction, the highest possible cost is imposed on the system and has the greatest impact on reducing the amount of covering the demand of the systems. Also, two median and facility location with fixed costs models to minimize the costs were provided by Daksin and Snyder [20]. Church and Scaparra [2] presented *r*-median interdiction model considering a fortification concept of some facilities against possible interdiction. Also in another work in 2008, they proposed another *r*-median interdiction model with fortification and used an implicit enumeration algorithm to solve it. The proposed model was based upon the classical *p*-median location model and assumed that the efficiency of the system was measured in terms of accessibility or service provision costs. In a bi-level formulation, the top level problem involved the decisions about which facilities to fortify in order to minimize the worst-case efficiency reduction due to the loss of unprotected facilities. The worst-case scenario losses were modeled in the lower-level interdiction problem (Scaparra et al. [18]).

Losada and Scaparra [13] considered an uncapacitated *p*-median system that was subject to external manmade or natural disruptions. They formulated the problem of protecting against the worst-case losses when taking into account facility recovery issues. Their model was a mixed-integer bi-level problem with integer variables controlled by both upper and lower levels. Aksen et al. [2] developed a budget constrained extension of the *r*-interdiction median problem with fortification

(RIMF). The objective in the RIMF model was to find the optimal allocation of resources to provide system protection, consisting of p facilities so that the r possible disruptions were minimized. According to this fortification model, other studies considered adding new hypotheses to the problem, such as the capacity of the facility of Scaparra and Church [18], security budget constraint of Aksen et al. [2], random number of possible losses of Liberatore, Scaparra and Daskin [11], and propagation of disturbances in a wide area.

Alguacil et al. [4] presented a tri-level programming model (i.e., defender-attacker-defender) for the pathology of electrical power networks against possible attacks. Liberatore et al. [11] presented the stochastic r-interdiction median problem with fortification (S-RIMF). This model optimally allocated defensive resources among facilities to minimize the worst-case impact of an intentional disruption. Aksen et al. [3] first introduced the concept of partial interdiction and outsourcing demands after interdiction. They formulated the model as a bi-level of attacker-defender from the perspective of the attacker.

Additionally, Zhang et al. [22] comprehensively explored the partial interdiction median problem for multi-sourcing supply systems (PIM-MS), which had three characteristics: (1) limited capacity for each facility, (2) partial interdiction, and (3) a multi-sourcing delivery strategy for supply systems. They formulated their model as a bi-level programming ore. Furthermore, Aliakbarian et al. [5] offered a bi-level model for the r-interdiction median problem with fortification for critical hierarchical facilities.

The literature review demonstrates that there is a gap in considering perspectives of the attacker and defender simultaneously. Also, most of the existing studies assume that all facilities are in one level. In order to fill these gaps, we contribute to the literature in the following ways:

- Developing a three-level integer programming model to minimize the total fixed charge of the facility to minimize the total cost of current facilities established after interdiction. In this model, we investigate the problem from the defender's perspective. Then, in the second and third levels, the problem is investigated the attacker's perspective under a strategic game.
- Considering hierarchical facilities.
- Considering the possibility of outsourcing the demands and the possibility of fortification for a defender.
- Developing two meta-heuristic algorithms to solve large instances. One approach is a single-solution based meta-heuristic algorithm (i.e., Tabu Search, TS), and another approach is population-based meta-heuristic algorithm Bat Algorithm, BA.

The rest of our work is organized as follows. In the next section, problem description and its assumptions are discussed. The three-level model for the problem is presented in Section 3. In Section 4, the approach for solving the model is proposed. Section 5 shows the computational results. In the last section, the conclusion is provided.

3. Modeling Framework

3.1. Three Level r-interdiction Median Problem for Hierarchical Facilities (THFRIM)

Consider a general supply/life system composed of several facilities and demand nodes that receive service or goods from their nearest facility sites. A limited resource budget is given to protect critical facilities in the system to prepare for the destructive attacks or natural disasters. Locating the facility is due to the fixed charge facilities and the costs of the current system (i.e., Level 1). The

problem is modeled as a Stackelberg game between intelligent attacker (i.e., Level 2) and a defender (i.e., Level 3). A typical objective of the attacker (i.e., follower) is to identify the most critical facilities to interdiction and make the most disruptive attack. The objective defender (i.e., leader) is responsible for satisfying the demand of all customers while minimizing total transportation costs and outsourcing costs. The related assumptions, parameters and decision variables are given below.

Assumptions:

(i) Flow pattern: customers and/or goods flow through levels of hierarchical systems. The flow pattern is in either a single-flow or multi-flow pattern. A single-flow pattern starts from level 0, passes through all levels, and ends at the highest level (or it starts from the highest level and ends at level 0). A multi-flow pattern can be from any lower (higher) level *m* to any higher (lower) level *n*, where *n*, $m \in \{0, 1, 2\dots k\}$. In here, a multi-flow pattern is considered [16].

(ii) Service varieties: a system is classified as nested or non-nested according to the service availability at the levels of hierarchy. In a nested hierarchy, a higher-level facility provides all the services provided by a lower level facility and at least one additional service. We assume that the facilities are nested hierarchically.

(iii) Spatial configuration: coherence refers to the spatial configuration of levels. In a coherent system, all demand sites assigned to a particular lower-level facility are assigned to one and the same higher-level facility [16].

(iv) To estimate worst-case losses, we assume that the attacker has complete information regarding the components of the system, including the position of each node and fortified facilities.

(v) Distribution of defensive resources is determined before interdiction and will not change during the attack.

Index sets:

I	Set of demands nodes (customers), $i \in I$
J	Set of potential sites for construction of the type 1 (level 1) service facilities; $j \in J$
K	Set of potential sites for construction of type 2 (level 2) service facilities; $k \in K$.

Parameters:

a_i	Demand of customer *i*
β_i	Percentage of customer *i* that needs to particular service of level 2
$d_{ij}^{(1)}$	Distance between customer *i* and facility type 1 at site *j*
$d_{ik}^{(2)}$	Distance between customer *i* and facilities type 2 at site *k*
$d_{jk}^{(3)}$	Distance between *j*th facility type 1 and *k*th facility of type 2
$c_j^{(1)}$	Capacity of the *j*th facility of type 1
$c_k^{(2)}$	Capacity of the *k*th facility of type 2
B_{att}	Maximum number of facilities that attacker can interdict (attacker's power)
$b^{(1)}$	Maximum number of facilities of type 1 that attacker can interdict
$b^{(2)}$	Maximum number of facilities of type 2 that attacker can interdict
B_{def}	Maximum number of facilities that defender can fortify (defender's power)
$p^{(1)}$	Maximum number of facilities of type 1 that defender can fortify

$p^{(2)}$ Maximum number of facilities of type 2 that defender can fortify
$CS_{(1)}$ Unit shipment cost of demand per unit distance for service of type 1
$CS_{(2)}$ Unit shipment cost of demand per unit distance for service of type 2
$CO^{(1)}$ Unit outsourcing cost of demand for service of type 1 (independent of distance)
$CO^{(2)}$ Unit outsourcing cost of demand for service of type 2 (independent of distance)
$f_j^{(1)}$ Fixed cost of construction of facility type 1 in site *j*
$f_k^{(2)}$ Fixed cost of construction of facility type 2 in site *k*.

Decision variables:

U_{ij} 1, if customer i is assigned to facility type 1 at site j
0, otherwise
W_{ik} 1, if customer i is assigned to facility type 2 at site k
0, otherwise
V_{jk} 1, if customer of particular service in type 1 of facility j is assigned to type 2 of facility k
0, otherwise
$S_j^{(1)}$ 1, if a facility type 1 located at site j is interdicted by attacker
0, otherwise
$S_k^{(2)}$ 1, if a facility type 2 located at site k is interdicted by attacker
0, otherwise
$Y_j^{(1)}$ 1, if a facility type 1 at site j is fortified by defender
0, otherwise
$Y_k^{(2)}$ 1, if a facility type 2 at site k is fortified by defender
0, otherwise
$X_j^{(1)}$ 1, if facility type 1 is located at site j
0, otherwise
$X_k^{(2)}$ 1, if facility type 2 is located at site k
0, otherwise.

3.2. Mathematical Programming Model

We present a new tri-level mathematical model as follows:

$$Z_1 = min_X(Z_2 + \sum_{j\in J} f_j^{(1)}.X_j^{(1)} + \sum_{k\in K} f_k^{(2)}.X_k^{(2)}) \quad (1)$$

s.t.

$$\sum_{j\in J} c_j^{(1)}.X_j^{(1)} + \sum_{k\in K} c_k^{(2)}.X_k^{(2)} \geq \sum_{i\in I} a_i \quad (2)$$

$$\sum_{k\in K} c_k^{(2)}.X_k^{(2)} \geq \sum_{i\in I} \beta_i.a_i \quad (3)$$

$$X_j^{(1)} \in \{0,1\}, \qquad \forall\, j \in J \quad (4)$$

$$X_k^{(2)} \in \{0,1\}, \qquad \forall\, k \in K. \quad (5)$$

(6)

$$Z_2 = max_S\, Z_{att}(S)$$

s.t.

$$\sum_{j\in J} b^{(1)}.S_j^{(1)} + \sum_{k\in K} b^{(2)}.S_k^{(2)} \le B_{att} \tag{7}$$

$$0 \le S_j^{(1)} \le X_j^{(1)}, \qquad \forall\, j \in J \tag{8}$$

$$0 \le S_k^{(2)} \le X_k^{(2)}, \qquad \forall\, k \in K \tag{9}$$

$$S_j^{(1)} \in \{0,1\}, \qquad \forall\, j \in J \tag{10}$$

$$S_k^{(2)} \in \{0,1\}, \qquad \forall\, k \in K. \tag{11}$$

$$\begin{aligned} Z_{att}(S) = min_{U,W,V,Y}(\, & CS_1 \times \sum_{j\epsilon J}\sum_{i\in I} a_i.d_{ij}^{(1)}.U_{ij} + CS_2 \times \sum_{k\in K}\sum_{j\epsilon J}\sum_{i\in I} \beta_i.a_i.d_{jk}^{(3)}.V_{jk} \\ & + CS_1 \times \sum_{k\in K}\sum_{i\in I}(1-\beta_i).a_i.d_{ik}^{(2)}.W_{ik} + CS_2 \times \sum_{k\in K}\sum_{i\in I}\beta_i.a_i.d_{ik}^{(2)}.W_{ik} \\ & + CO^{(1)} \times (\sum_{i\in I}(1-\beta_i).a_i.(1-(\sum_{j\in J}U_{ij} + \sum_{k\in K}W_{ik}))) + CO^{(2)} \\ & \times (\sum_{i\in I}\beta_i\,.a_i.(1-(\sum_{j\in J}U_{ij} + \sum_{k\in K}W_{ik}))) + CO^{(2)} \\ & \times (\sum_{j\in J}\sum_{i\in I}\beta_i.a_i.U_{ij}.(1-\sum_{k\in K}V_{jk}))) \end{aligned} \tag{12}$$

s.t.

$$\sum_{j\in J} U_{ij} + \sum_{k\in K} W_{ik} \le 1, \qquad \forall\, i \in I \tag{13}$$

$$\sum_{k\in K} V_{jk} \le 1, \qquad \forall\, j \in J \tag{14}$$

$$\sum_{j\in J} p^{(1)}.Y_j^{(1)} + \sum_{k\in K} p^{(2)}.Y_k^{(2)} \le B_{Def} \tag{15}$$

$$\sum_{i\in I} a_i.U_{ij} \le c_j^{(1)}.\left(1 - S_j^{(1)}.\left(1 - Y_j^{(1)}\right)\right).X_j^{(1)}, \qquad \forall\, j \in J \tag{16}$$

$$\sum_{i\in I} a_i.W_{ik} + \sum_{j\in J}\sum_{i\in I}\beta_i.a_i.U_{ij}.V_{jk} \le c_k^{(2)}.\left(1 - S_k^{(2)}.\left(1 - Y_k^{(2)}\right)\right).X_k^{(2)}\ , \forall\, k \in K \tag{17}$$

$$U_{ij} \in \{0,1\}, \qquad \forall\, i \in I\,, j \in J \tag{18}$$

$$W_{ik} \in \{0,1\}, \qquad \forall\, i \in I\,, k \in K \tag{19}$$

$$V_{jk} \in \{0,1\}, \qquad \forall\, j \in J, k \in K \tag{20}$$

$$Y_j^{(1)} \in \{0,1\}, \qquad \forall\ j \in J \tag{21}$$

$$Y_k^{(2)} \in \{0,1\}, \qquad \forall\ k \in K. \tag{22}$$

New slack variables W'_{ijk} for linearization of the third-level of the model is defined as follows:

$$U_{ij} + V_{jk} \geq 2W'_{ijk}, \qquad \forall i \in I, j \in J, k \in K \qquad (23)$$

$$W'_{ijk} \in \{0,1\}, \qquad \forall i \in I\ , j \in J, k \in K \qquad (24)$$

In the above formulation, relations (1) to (5) represent the level 1, relations (6) to (11) represent the level 2, and relations (12) to (22) represent the level 3 of the defender-attacker-defender model. The objective function (1) consists of two terms. The first term is to minimize the total fixed charge of the facility and the second term is to minimize the total cost of the current facilities established after interdiction**.** Constraint (2) ensures that the total capacity of the established facility is (i.e., types 1 and 2) more than the demands of the population. Constraint (3) ensures that the total capacity of the type 2 facility is established more than the percentage of the population area that needs a particular service of level 2.

The objective function of the second level is to maximize the objective function of the third level, i.e; Expression (6)). Constrain (7) shows the maximum attacker power using the variables $S_j^{(1)}$ and $S_k^{(2)}$. Constrains (8) and (9) are related to attacker's awareness of the facilities established in existing locations, that is, the attacker considering that the defender is established facilities in sites 1 and 2 or not, can decide on disturbance of facilities.

The objective function of the third level consists of two terms to minimize the cost of customer service inside the system and to minimize the cost of outsourcing services, as shown by (12). Relations (13) and (14) ensure that each customer is assigned to a facility; otherwise, it will be provided through outsourcing. In equality (15) shows the defensive power of a defender. Relations (16) and (17) show capacity constraints for each facility. Based on these restrictions, the amount of the demand capacity allocated to each facility will be the maximum size to the amount of the expected value of facility's capacity after considering the condition of attacker's interdiction and defender's fortification. Relation (17) also refers to the defensive power of the defender, so that the number of facilities that are fortified should not be more than intended. Relations (4), (5), (10), (11) and (18) to (22) specify the binary variables.

4. Solution Approaches

A three-level optimization problem, which is developed as a bi-level optimization problem, is also NP-hard [7, 10]. The use of bi-level programming needs a great deal of effort to solve these problems. Sakawa and Nishizaki [17] divided. Computational methods for solving the BOPs into three general categories:

- Vertices counted approach, which is based on the extreme point of the set of decision-making lower-level rational answers, an extreme point of the feasible region.
- Kuhn-Tucker approach, in which the upper-level problem with constraints to include low-level optimal conditions is solved.
- Penalty function approach in which a penalty expression is added to the objective function to satisfy the optimality of the lower level.

As the bi-level programming problem solving methods meta-heuristic methods can be noted. A meta-heuristic optimization algorithm is an innovative method that can be used for various problems to with small changes. Using meta-heuristic algorithms notably increases the ability to find high-quality solutions for hard optimization problems. Meta-heuristic algorithms have also been used to solve bi-level programming problems. A group of meta-heuristic algorithms is single-based solution (S-Metaheuristic) algorithms. These algorithms change the answer during the search process and

focus on local search. S-Metaheuristic algorithms include simulated annealing (SA), iterative local search (ILS), tabu search (TS) and noisy method (NM).

Nowadays, the utilization of hybrid meta-heuristic and exact methods is a convenient option for solving this class of problems (Talbi, [21]). Aksen and Aras [1] presented a hybrid algorithm based on TS to solve a problem of the bi-level defender-attacker problem. Also, there are other instances of the use of TS in *p*-median problems with the fixed charge in the literature (Aras and Aksen, [2]). Since of the model variables three levels are binary, the problem is a pure integer programming one. However, further attempts to solve larger instances are unsuccessful due to the huge required computational time. Due to this limitation, we propose a hybrid meta-heuristic algorithm and an exact solution. We use tabu search (TS) and bat algorithm (BA) for the first level, and an enumeration method for the second and third levels of the model, on Intel (R) Core (TM) i5-3230M @ 2.60 GHz and 4/00 GB Ram. Hence, we call them TS-EX-EX and BA-EX-EX, respectively.

4.1. TS-EX-EX Solution

Tabu search (TS) is a celebrated meta-heuristic algorithm that has widely been applied to many difficult combinatorial optimization problems in the literature [1]. Here, to solve the first level model for decision on the facility location of types 1 and 2, we use the TS algorithm. Also, as mentioned in the previous section, TS is a single-based solution algorithm; therefore, a good starting point can make a good impact in achieving better performance and faster algorithm. Here, for the first solution, greedy search is used. In this approach, the rate of creating a unit of facility capacity is achieved by dividing fixed costs of each location on its capacity, followed by opening the facility that has the lowest rate. As long as the limits of 1 and 2 are satisfied, this process will continue. The algorithm continues by neighborhood search and the current solution are randomly selected. If there is no facility in that location, it will be opened. If the facility of the location is open, it will be closed on a condition with the remaining capacity of a lesser demand. The number of times to repeat the search is set with the algorithm parameter, *CandidateListSize*.

The objective function of the problem in the first level has two terms. In the first term, the maximum cost of services in the worst-case scenario (i.e., attacker), and the second, the fixed costs of facilities are estimated. Solutions $X^{(1)}$and $X^{(2)}$ produced in the first level, for evaluation and cost estimates, will be sent to the second level, in which the amount of Z_2^* is calculated. Also, to solve the attacker-defender system, an explicit enumeration method is used for the attacker's level, and an exact solution of an integer programming problem is used for the defender's level.

4.2. BA-EX-EX Solution

BA is a bio-inspired algorithm developed by Yang in [22] and is found to be very efficient. Yang's idealized rules are as follows:
(i) The first characteristic is echolocation behavior. All bats use echolocation to a sense distance.
(ii) The second characteristic is the frequency. Bats fly randomly with velocity v_i at position x_i with a fixed frequency f_{min} with varying wavelength λ and loudness A_0 to search for prey.
(iii) To adjust the loudness, it is assumed that the loudness to be varied from a positive large A_0 to a minimum constant valueA_{min}.

Each bat is associated with a velocity v_i^t and a location x_i^t at iteration t, in a d-dimensional search in the solution space. Among all the bats, there exists a current best solution x^*. In Yang's method, the movement of the virtual bat is simulated by:

$$f_i = f_{min} + (f_{max} - f_{min}).\beta, \quad (25)$$
$$v_i^t = v_i^{t-1} + \left(x_i^{t-1} - x^*\right).f_i, \quad (26)$$
$$x_i^t = x_i^{t-1} + v_i^t. \quad (27)$$

In order to provide an effective mechanism to control the exploration and exploitation and switch to the exploitation stage, if required, we need to vary the loudness A_i and the rate r_i of pulse emission in the iterations. Since the loudness usually decreases once a bat has found its prey, while the rate of pulse emission increases, the loudness can be chosen to be any value of convenience, between A_{min} and A_{max}, assuming $A_{min} = 0$ means that a bat has just found the prey and temporarily stops emitting any sound.

$$A_i^{t+1} = \alpha A_i^t, \qquad r_i^{t+1} = r_i^0[1 - exp(-\gamma t)]. \quad (28)$$

With these assumptions, we have α and γ as constants. For any $0 < \alpha < 1$ and $\gamma > 0$, we have.

$$A_i^t \to 0, \quad r_i^t \to r_i^0, \quad as \ \ t \to \infty \quad (29)$$

Here, after solving the first level of the model with TS, we use the bat algorithm to solve the first level and BA-EX-EX to solve the full version.

5. Computational Experiment

Here, the computational results are presented. We test performance of both the TS and BAT algorithms on a number of instances, which are randomly generated. The first and second levels of the proposed hybrid algorithms are coded in MATLAB 2012 environment. For the solution of the third level of the model, for each response generated in the second level, GAMS is used. Codes are executed on a computer with processor Intel (R) Core (TM) i5-3230M @ 2.60 GHz and an internal memory of4/00 GB and Windows 7 operating system.

5.1. Generation of Random Test Instance

We generated nine THFLRIM instances in total, where n_k, R_j , n_j and R_i are number of type 2 facilities, rate of type 2 facility, number of type 1 facilities and rate of customer nodes, respectively. The instances in our test bed are named to be indicative of the n_k, n_j and number of example, values. For example, 263 means there are 2 number facility site of type 2 and 6 number facility site of type 1. Also, $rF1, rF2$ and rC are radius of a region for type 1 facility, a radius of a region for type 2 facility and a radius of customers node, respectively (see Fig. 1). The template of random instance generation is given in Table 1.

Table 1. Random problem generation template employed in the computational study

Parameters	Values
n_k	2,3
R_j	2, 3, 4
n_j	$n_k \times R_j$
R_i	5
n_i	$n_j \times R_i$
a_i	$Random\ \{20, 30, 40, \dots, 150\}$

β_i	$Random\ \{0.1, 0.15, \ldots, 0.3\}$
$d_{ij}^{(1)}, d_{ik}^{(2)}, d_{jk}^{(3)}$	$d_{ij}^{(1)} = \left[(x_i - x_j) + (y_i - y_j)\right]^{1/2}$
$c_j^{(1)}, c_k^{(2)}$	Capacity of each facility determined randomly, so that capacity of each facility is more than capacity of the customers.
B_{att}	2500
$b^{(1)}, b^{(2)}$	$b^{(1)} = 100\ , b^{(2)} = 1000$
B_{def}	2500
$p^{(1)}, p^{(2)}$	$p^{(1)} = 100\ , p^{(2)}$=1000
$CS_{(1)}, CS_{(2)}$	$CS_{(1)} = 0.04\ , CS_{(2)} = 0.5$
$CO^{(1)}, CO^{(2)}$	$CO^{(1)}$=$3 \times CS_{(1)} \times 200 = 3 \times 0.04 \times 200 = 24$
	$CO^{(2)} = 3 \times CS_{(1)} \times 200 = 3 \times 0.5 \times 200 = 300$
$f_j^{(1)}, f_k^{(2)}$	$f_j^{(1)}$=$Random\ \{500,550,600, \ldots, 1000\}$
	$f_k^{(2)} = Random\ \{5000,5500, \ldots, 10000\}$

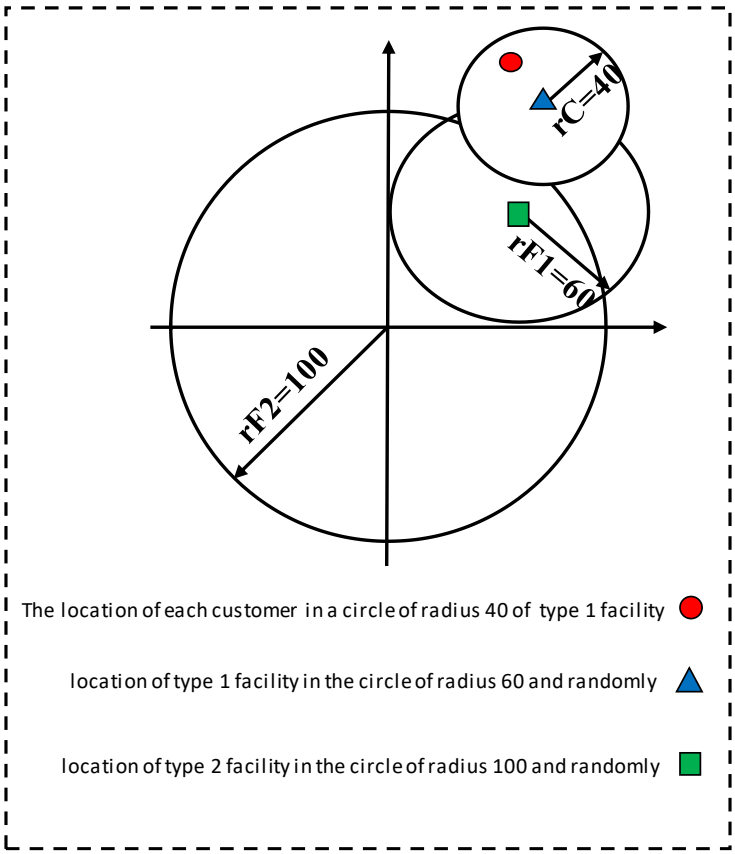

Figure 1. Locations of type 1 and type 2 facilities and customers

5.2. Parameter Calibration

It is clear that the performance of an algorithm largely depends on the parameters. In fact, different parameters may produce different answers. So, tuning the parameters of the algorithm correctly is very important for obtaining an optimal response. Here, for tuning the parameters of the TS algorithm,

we use a statistical methodology, called response surface methodology (RSM), which was introduced by GE and KB (1951). RSM is used to estimate the optimal parameters influencing the process. In this methodology, regression equation analysis is used to evaluate the different levels of the parameters (Mohammadi et al., [14], Mohammadi et al., [15]). The method is that, a series of different levels of various parameters have been studied and best-fit regression equation parameters on different levels and optimal values for the parameters are recommended. The parameters of the algorithm should first be determined, and then for parameter are considered two levels and desirable values of the parameters are achieved by fitting the best regression equation on different levels of the parameters. The tuned parameters of the proposed TS are shown in Table 2.

Table 2. TS parameters settings

Algorithm	Parameters	Setting
Tabu search	Max Iteration	19
	Tabu Tenure	2
	Max Improve Length	5
	Candidate List Size	3

5.3. Comparison of The Results

Nine random instances were generated and were first solved by the TS-EX-EX method, and then the BA-EX-EX method is used for solve instances. The objective function value of the first level, the optimal solutions variables and CPU time for each instance are depicted in Table 3. The results show that each of the two parts of the first-level objective, Z_2 and fixed charge cost have different behaviors. In fact, by increasing the fixed charge facility costs, the costs of the current services are reduced. Eventually, the best solution will be searched between the two exchanges. Also, the results of the TS algorithm were compared with the results obtained by the BA algorithm. Table 3 shows that the performance of TS is better in terms of the CPU time and the obtained best solution.

Table 3. Result of solving the model by the BA-EX-EX method

	BA-EX-EX							
Ins ID	Best Solution	X_1^*	X_2^*	S_1^*	S_2^*	Y_1^*	Y_2^*	CPU time (Sec.)
261	2738400	001000	10	001000	10	001000	10	241
262	4410100	000111	01	000111	01	000111	01	4728
263	3396900	110000	01	110000	01	110000	01	3284
281	5705200	11010010	01	11010010	01	11010010	01	18620
282	5184200	00111100	10	00111100	10	00111100	10	24373
283	----------	----------	-----	----------	-----	----------	-----	----------
361	----------	----------	-----	----------	-----	----------	-----	----------
362	----------	----------	-----	----------	-----	----------	-----	----------
363	----------	----------	-----	----------	-----	----------	-----	----------

Table 4. Result of solving the model by the SA-EX-EX method

		SA-EX-EX						
Ins ID	Best Solution	X_1^*	X_2^*	S_1^*	S_2^*	Y_1^*	Y_2^*	CPU time (Sec.)
261	2692100	001000	11	001000	11	001000	11	58
262	3312500	100000	11	100000	11	100000	11	540
263	2787800	010010	11	010010	11	010010	11	653
281	2919300	01000101	11	01000101	11	01000101	11	1481
282	2842400	00100100	11	00100100	11	00100100	11	1430
283	5737500	11111101	10	11111101	10	11111101	10	9296
361	4319000	101101	011	101101	011	101101	011	9159
362	4689700	101111	011	101111	011	101111	011	4974
363	2757900	101110	101	101110	101	101110	101	6090

5.4. Sensitivity Analysis

Here, a sensitivity analysis is performed in order to validate the model. To do this, by keeping all parameters and changing only one of them, we should check the models behavior. The desired parameters for checking their effects on the behavior of the model's on an objective function include attacker's power and budget of interdiction (i.e., defensive power). The analysis results are shown in tables 4 and 5, and Figs. 2 and 3.

According to Table 5 and Fig. 2, as expected, an increase in the attacker's budget increases the costs. Because the attacker's budget is more, further facilities are attacked and more facilities lose their service capacity. As a result, to satisfy customer's requirements, it the capacity is needed to be increased and further outsourcing is required.

Also, Table 6 shows that increasing the defensive power reduces the cost, as expected. Fig. 3 depicts the trend of this change.

Table 5. Analysis of the interdiction budget on the cost

Interdiction budget (attacker power)	**Cost in TS**
500	3277500
2500	3297500
6000	3352500
10000	3367500

Table 6. Analysis of the fortification budget on the cost

Fortification budget (defender power)	**Cost in TS**
500	3307500
2500	3307500
6000	3277500
10000	3308000

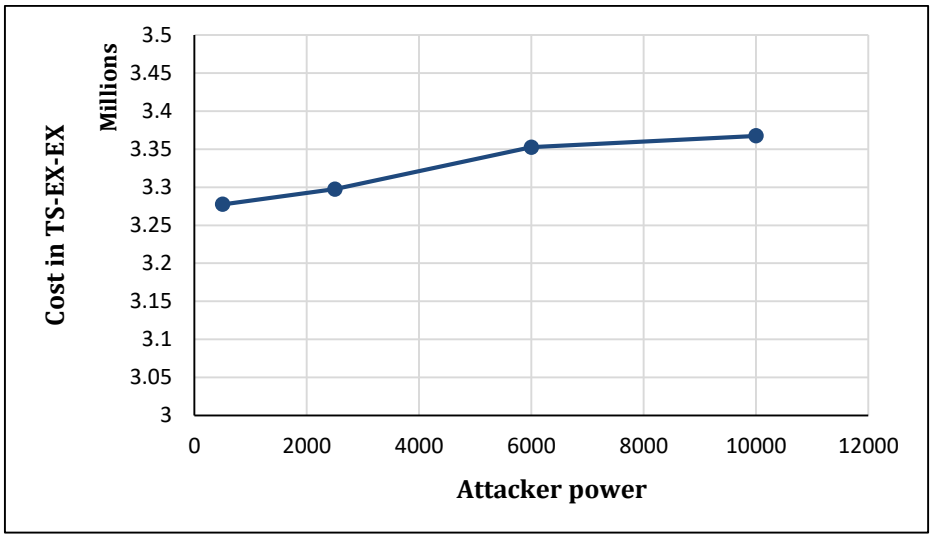

Figure 2. Analysis of the interdiction budget on the cos.

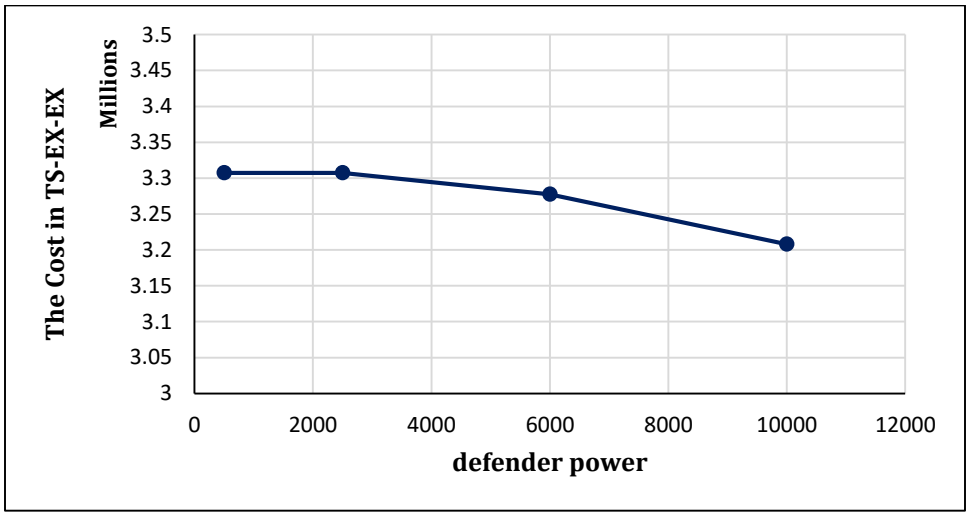

Figure 3. Analysis of the interdiction budget on the cost

6. Conclusion

We presented a mathematical model to design the service system in order to protect facilities with a focus on the most effective localization. An *r*-median interdiction three-level model on leader-follower games was presented. The three-level model was suggested in the form of the defender-attacker-defender. It was assumed that the facilities had a hierarchical structure with capability of nesting. The attacker budget for interdiction and the defender budget for fortification have been limited. We have used two different methods to solve this three-level programming model. First, a combination of tabu search-explicit enumeration-exact solution (i.e., TS-EX-EX) was designed to solve the model. In the second method, we used a combination of the bat algorithm-explicit enumeration-exact solution (i.e., BA-EX-EX). Also, to tune the parameters of the algorithm, a statistical methodology, called response surface methodology (RSM), was used. We suggested that the problem could be modeled dynamically and internal failures of the system were considered for outside attacks of the system.

References

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

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

[3] Aksen, D., Sengül Akca, S. and Aras, N. (2014), A bilevel partial interdiction problem with capacitated facilities and demand outsourcing, *Computers & Operations Research*, 41, 346–358.

[4] Alguacil, N., Delgadillo, A. and Arroyo, J. M. (2014), A trilevel programming approach for electric grid defense planning, *Computers & Operations Research*, 41, 282–290.

[5] Aliakbarian, N., Dehghanian, F. and Salari, M. (2015), A bi-level programming model for protection of hierarchical facilities under imminent attacks, *Computers & Operations Research*, 64, 210–224.

[6] Aras, N. and Aksen, D. (2008), Locating collection centers for distance- and incentive-dependent returns, 111(2), 316–333.

[7] Bard, J.F. (1991), Some properties of the bilevel programming problem, *J. Optimiz. Theory App,* 68, 371–378.

[8] Box GE and Wilson K.B. (1951), On the experimental attainment of optimum conditions, *Journal of the Royal Statistical Society: Series B (Methodological),* 13(1), 1–45.

[9] Church, R.L. and Scaparra, M.P. (2007), Protecting critical assets: the r-interdiction median problem with fortification, Geographical Analysis, 39, 129–146.

[10] Jeroslow, R.G. (1985), The polynomial hierarchy and a simple model for competitive analysis, *Math. Program*, 32, 146–164.

[11] Liberatore, F., Scaparra, M.P. and Daskin, M.S. (2011), Analysis of facility protection strategies against uncertain numbers of attack: the stochastic r-interdiction median problem with fortification, *Computers & Operations Research,* 38(1), 357–66.

[12] Losada, C., Scaparra, M.P., Church, R.L and Daskin, L.S. (2012), The stochastic interdiction median problem with disruption intensity levels, *Annals of Operations Researc,* 201(1), 345-365.

[13] Losada, C., Scaparra, M.P. and Church, R.L. (2010), On a bi-level formulation to protect uncapacitated p-median systems with facility recovery time and frequent disruptions, 36, 591–598.

[14] Mohammadi, M., Jolai, F. and Rostami, H. (2011), An M/M/c queue model for hub covering location problem. Mathematical and Computer Modelling, *Mathematical and Computer Modelling,* 54, 2623–2638.

[15] Mohammadi, M., Jolai, F. and Tavakkoli-Moghaddam, R. (2013), Solving a new stochastic multi-mode p-hub covering location problem considering risk by a novel multi-objective algorithm, *Applied Mathematical Modeling,* 37, 10053–10073.

[16] Sahin, G. and Sural, H. (2007), A review of hierarchical facility location models, *Computers & Operations Research,* 34, 2310–2331.

[17] Sakawa, M. and Nishizaki, I. (2009), Cooperative and Non-cooperative Multi-level Programming, Springer, Dordrecht, Heidelberg, London.

[18] Scaparra, M.P. and Church, R.P. (2008), A bilevel mixed-integer program for critical infrastructure protection planning, *Computers & Operations Research,* 35, 1905–1923.

[19] Scaparra, M.P. and Church, R.L. (2010), Protecting supply system to mitigate potential disaster: a model to fortify capacitated facilities. Working Paper No. 209, Kent Business School, University of Kent, UK.

[20] Snyder, L.V. and Daskin, M.S. (2005), Reliability models for facility location: the expected failure cost case, *Transportation Science*, 39(3), 400–416.
[21] Talbi, E. G. (2013), Metaheuristics for Bi-level Optimization, Springer, Heidelberg, New York.
[22] Yang. Xin.she. (2010), A new metaheuristic Bat-Inspired Algorithm, Springer, 284, 65–74.
[23] Zhang, X., Zheng, Z., Zhang, S.H. and Du, W. (2016), Partial interdiction median models for multi-sourcing supply systems, *International Journal of Advanced Manufacturing Technology*, 84(1), 165–181.
[24] Zhu, Y., Zheng, Z., Zhang, X. and Cai, K. (2013), The r-interdiction median problem with probabilistic protection and its solution algorithm, *Computers & Operations Research*, 40, 451–462.