Scientia Iranica E (2017) 24(2), 778–793

Sharif University of Technology
Scientia Iranica
Transactions E: Industrial Engineering
www.scientiairanica.com

Credibility-based fuzzy mathematical programming for bi-objective capacitated partial facility interdiction with fortification and demand outsourcing model

A. Azadeh[a,*], R. Kokabi[a] and D. Hallaj[b]

a. *School of Industrial and Systems Engineering, College of Engineering, University of Tehran, Iran.*
b. *Department of Industrial Engineering, Iran University of Science and Technology, Tehran, Iran.*

Received 7 February 2015; received in revised form 25 January 2016; accepted 9 April 2016

KEYWORDS
Facility interdiction; Fortification; Fuzzy mathematical programming; Chance constrained programming; Multi-Objective Mixed-Integer Non-Linear Programming (MOMINLP); Genetic algorithm.

Abstract. The concepts of fortification and partial interdiction have not been considered concurrently in previous studies. In this paper, we added the fortification and partial interdiction concepts to interdiction problem for the first time; the reason is that in interdiction situations, defenders decide to protect some important facilities according to their budgets, and attackers like to destroy most unprotected facilities according to their resources, and therefore, to cripple the defenders' systems. Moreover, we use the advantages of credibility-based fuzzy mathematical programming and introduce an integrated model based on uncertainty contexts. In this bi-objective model, decision-maker gives satisfaction degrees for constraints, and then we use the interactive possibility model to solve the bi-objective model with varying confidence levels. These confidence levels specify the knowledge of attacker and defender about themselves. In addition, we propose Genetic Algorithm (GA) to solve the suggested model. In the experiments, we generate problem instances and solve them by Multi-Objective Mixed-Integer Non-Linear Programming (MOMINLP) and the proposed genetic algorithm for various settings.

© 2017 Sharif University of Technology. All rights reserved.

1. Motivation and significance

Many military or service facilities are subject to disruptions; thus, planning to relieve the impacts of facility interdictions is very important in the context of facility location. Today, facility interdiction problem together with considering the techniques to mitigate the attacker disruptions are crucial factors in locating the sensitive facilities. In this paper, we propose the facility interdiction model with partial interdiction and fortification of the facilities with outsourcing demands concurrently, which have not been taken into account before; it is because the information is secure, and the attackers and defenders play a game in interdiction problems. On the one hand, the defenders like to protect their important facilities; on the other hand, the attackers like to cripple the defenders' systems according to their limited attacking budgets instead of destroying the whole of facilities. Thus, taking these problems into account, it is very important to consider the partial interdiction with fortification. However, in the interdiction problem, due to the high level of security and absence of adequate historical data, most parameters are uncertain and predicting the correct value for them is impossible; thus, we have applied fuzzy mathematical programming approaches in this

*. *Corresponding author. Tel.: 98 21 82084162; Fax: 98 21 88013102*
E-mail addresses: aazadeh@ut.ac.ir (A. Azadeh); kokabi.reza@ut.ac.ir (R. Kokabi); D_Hallaj@ind.iust.ir (D. Hallaj)

paper, which have not been considered before.

2. Introduction

Many military or service facilities are subject to the decrease in capacity due to natural disasters or intentional disruptions. In the last few years, topics of resilience, fortification of facilities, and security have become important in the OR community. In the context of intentional attacks, recent observations about world events show that facilities are vulnerable to terrorist attacks; thus, planning to relieve the impacts of facility interdictions can be an important issue for both private companies and public organizations. Several models are proposed for this situations [1-3]. By investigating the past terrorist attacks, we can conclude that terrorists applied unknown tactics and techniques to disrupt specific targets; thus, determining these targets is more important for defenders than decoding attacker's techniques. Usually, attackers wait for traffic times, and then attack their targets to optimize their resources in the best possible way to inflict maximum damage on defenders [4,5].

In modern attacks, the attackers are mostly interested in causing anarchy rather than in inflicting the serious damage on the defender's system, because the anarchic system cripples the whole system and causes bad psychological effect on it. On the other hand, the attackers have a limited budget, and allocation of the budget to destroy few facilities, not thoroughly yet, cannot cripple the system. Hence, attackers tend to disturb many parts of facilities rather than disturb the entire facilities. Designing critical system components for defenders is a critical factor as response to such terrorist acts and trends. The defender can mitigate the disruption of attacker when the possibility of failure is calculated in the design phase of the defender system. Based on this motivation, most models have been developed to decrease the post-attack effects of attacker. Most studies in this context have proposed rational attacks through the interdiction models. These models are constructed from the attackers' prospective to determine the worst attack, and then defender is entered to decrease the post-attack functionality. These models usually use the Stackelberg game for developing the bi-level or tri-level systems. The Stackelberg game was first introduced in [6]. The structure of models using the Stackelberg game is twofold. First, in the upward level, the attacker tries to strike maximum damage to the defender's system, then in the downward level problem, defender minimizes the post-attack costs levied on the system [7,8].

In recent research works on the interdiction models, the concept of protection/fortification has been added to interdiction models and has designed the resilient systems on behalf of the defender against the intelligent attacker. In these models, the roles of defender and attacker in Stackelberg game are exchanged. First, in an upward level, the defender protects some of the facilities from attacks, and then attacker in the downward level attacks the system and his objective is to inflict the maximum damage on the defenders system. Hence, in fortification models, the defender plays the leadership role and attacker plays a follower role [9].

In the concept of facility interdiction, there are few research works that have added the partial interdiction to the facility interdiction problems. In this paper, we have used this concept in our interdiction model. In partial interdiction, the performance of facilities does not necessarily end up in the attacker's disruption, but the capacity is reduced according the intensity of attacks [10]. Thus, we applied the multi-level attacks, such that the attacker can choose between them to disrupt the facilities. Also, we assigned the budget to attacker, and he must search for the best scenario to inflict the maximum damage on the defender's system. In the proposed model, we assume that if the capacity of system is reduced due to the attacks of the attacker, the unmet demand is outsourced by the external suppliers.

Most models for interdiction facilities use the bi-level programming and apply the Stackelberg game to determine their scenarios for post-attack and pre-attack decisions. In this models, it is assumed that the attacker knows the structure of defender's system and attacks them intelligently. But today, in the real world, the level of security in defenders and attackers' systems is high and attackers do not know the critical parts of defender systems, even if they know what is the critical parts of defenders system, but they do not know with what degree these parts are protected by defenders. Thus, the attacker mostly desires to attack many of the defender's facilities to reduce their capacities rather than attack few parts of facilities entirely. It increases the attacker's reliability for inflicting the maximum damage on defender's system. It seems that considering this assumption that attacker is intelligent and applying the bi-level programming, correction is not guaranteed. We must apply the integrated model to this situation.

In this paper, we used bi-objective model to formulate interdiction problem and integrated concepts of partial interdiction and fortification in capacitated budget constraints with outsourcing unmet demands. Also, we used the multi-level attacks in our model. In the bi-objective model, there are two objectives that contain the objectives of the defender and attacker. In the attacker's objective function, the objective is to maximize the damage inflicted on the defender system. This model assumes that if attacker inflicts maximum damage, then what optimum scenario the defender will encounter. Thus, the defender's objec-

tive function is to minimize the fixed charged facility location and shipment costs with outsourcing costs. It is obvious that in the interdiction problem, most parameters, such as demands, costs, and budgets, are uncertain; predicting correct values for them is impossible. Uncertainty parameters can significantly influence the entire performance of defender reactions to attacks, hence, neglecting it during the construction of model imposes high risks on defenders. Then, we applied the context of uncertainty to the parameters of our model. This model encompasses the actual conditions in interdiction models. In the literature of facility interdiction, there are few works that incorporate the issue of uncertainty in their models, and all of them have applied stochastic programming approaches. However, the absence of adequate historical data for interdiction parameters is obvious and makes the use of this approach unreasonable in the real life cases. To overcome this inadequacy, we employed fuzzy mathematical programming approaches in the facility interdiction model design. Fuzzy mathematical programming is a good tool to manage the uncertainty that comes from absence of knowledge in estimating the actual values of parameters. This paper proposes a new bi-objective credibility-based fuzzy mathematical programming model for partial interdiction problem with fortification to deal with epistemic uncertainty in the model parameters resulting from lack of knowledge.

The rest of this paper is organized as follows. In the next section, the background of facility interdiction, fortification, partial interdiction, and multi-objective linear programming approaches is described. In Section 3, the proposed model and its assumptions are described, and then the fuzzy mathematical model for the stated problem is presented. Interactive solution methodology for solving our interdiction problem is also presented in Section 4. In this section, we apply the TH method and propose genetic algorithm. Experimental results are given in Section 5. At last, concluding remarks are presented in Section 6.

3. Literature review

In the literature, first, we have reliability models for facility location in which the disruption is based on the failure of facilities. For review, see the paper of Snyder and Daskin (2005) [3]. The main characteristics of these papers are attacks that have been created by man or natural calamitous events. In attacks that have been created by man, someone attacks to inflict maximum damage on system. Interdiction models are distinct from one to another in the structure of the objective function values and in the underlying structure of the system. Many studies in this context include the interdiction of arcs in network models and facility interdiction problems. Also, the operational research studies have recently developed the fortification context in the facility interdiction problems. Wollmer introduced the first effort to explain the interdiction of arcs as an optimization model. Coverage-type service networks from attacker's perspective and r-facility Interdiction In Median (RIM) was the first study published by church et al. (2004) [11]. RIM included the maximization of the demand-weighted total distance by attacking r facilities, and the customers of the interdicted facilities have to be assigned to unscathed facilities. In the rest of this section, we discuss the research works done in the scope of network interdiction, fortification, and partial interdiction.

3.1. Interdiction and facility fortification models

The meaning of interdiction pertains to a destructive attack, where an attacker targets some facilities to weaken their performance; similarly, McMasters and Mustin (1970) assumed that the objective function of interdiction model is minimization of network flow capacity when the minimum capacity on arc is positive, and the cost of interdiction is a linear function of arc capacity reduction [12]. In most articles, interdiction models are formulated as mini-max or maxi-min bi-level programs. According to the study of Church and Spacarra (2007), the capacity decline due to partial interdiction is related to the severity level of the attack [13], as similarly studied by Wood (1993) [14]. Partial interdiction on arcs and interdiction budget to maximize the shortest path between supply and demand spots were considered by Fulkerson and Harding (1977) [15]. In the study of Smith et al. (2007), partial interdiction was the reduction of the interdicted arcs' flow capacity [1]. Aksen et al. (2012) integrated the partial interdiction idea into a facility interdiction model as a leader-follower game; the attacker had limited budget to cause interdiction, and the follower (defender) had to satisfy all customers' demand after attacking [4]. We can put the concept of interdiction against the concept of protection (fortification). Church and Scaparra (2007) extended r-interdiction median problem (RIM) by adding fortification to it (RIMF). This model identified q facilities to impede an attack in a network of p existing facilities. Maximizing the total demand satisfaction cost was the objective of attacker; it should be noted that attacker knew which facilities were protected [13]. They also developed a bi-level programming formulation of the RIMF. The model of Scaparra and Church (2008) is a multi-level problem with one leader and one follower, where the follower is the attacker; so, his or her strategy is based on the defender's decision [15]. Up to this point, the authors assumed that facilities are uncapacitated, but in study of Scaparra and Church (2010), they proposed RIMF with capacitated facilities, where upon inter-

diction, facilities' capacity was reduced [16]. Losada et al. (2010) proposed a stochastic approach. In this study, the facility was not destroyed within an attack certainly, and the probability of destruction of a facility depended on the resources' level allocated by the attacker [17]. Aksen et al. (2010) added budget constraint of facility protection and also the capacity expansion cost due to the reallocation of customers (looking for the interdiction of the attacker) to the RIMF. Then, they used implicit enumeration algorithm applied to a binary tree to solve it [18]. Their model was mentioned as BCRIMF-CE. Aksen and Aras (2012) combined BCRIMF-CE model with a fixed charge facility location problem, where defender determines which facilities to protect. In the objective function of the defender, they added the cost of fortification. Stackelberg game between defender (leader) and attacker (follower) was their solution strategy. The defender's problem was solved regardless of protection decisions at first, then facilities to be protected by defender and those to be interdicted by attacker were determined based on an implicit enumeration algorithm [9].

3.2. Fuzzy multi-objective mixed integer linear programming

In this work, we used the MOMILP method to solve our bi-objective model. In the literature of MOMILP models, Zimmermann (1978) proposed the first approach, called Max-Min, to solve the Multi-Objective Linear Programming (MOLP) models [19]. But, in this approach, the solution obtained by the Max-Min operator is probably not efficient, because this method selects a solution whose minimum degree of objectives' satisfaction is greater than other solutions and does not consider the importance of each objective function. Lie and Hwang (1993) proposed a complementary Max-Min approach to emend deficiency of Zimmermann's method. This method is called LH method [20]. This method is balanced with Max-Min and importance of each objective function. Next, Selim and Ozkarahan (2007) added a modified version of Werner's model to the LH method [21]. They used a compensation factor in their method and improved LH method. Li et al. (2006) represented a two-stage fuzzy approach for solving the MOLP models. In their method, in the first stage, the minimum degree of objectives is obtained with the Zimmermann's method. Then, in the second stage, the efficient solution with the maximum weighted satisfaction is selected [22]. Afterwards, Torabi and Hassini (2008) developed a single-stage method and improved a past method, called TH. The TH method is the combination of LH and MW methods [6].

In Table 1, features and strangeness of our pro-

Table 1. Features of the proposed model versus the other methods in facility interdiction location problems.

Papers vs. features	Interdiction	Fortification	Partial interdiction	Integrated multi-objective model	Uncertain parameters	Credibility-based fuzzy programming	Budget planning and capacitated nodes	Demand outsourcing
The proposed model	✓	✓	✓	✓	✓	✓	✓	✓
Wood (1993)	✓	✓	✓					
Church et al. (2004)	✓							
Church and Scaparra (2007)	✓	✓						
Smith et al. (2007)	✓		✓					
Scaparra and Church (2008)	✓	✓						
Scaparra and Church (2010)	✓	✓					✓	
Losada et al. (2010)	✓	✓	✓					
Aksen et al. (2010)	✓						✓	
Aksen and Aras (2012)	✓	✓					✓	
Aksen et al. (2012)	✓		✓				✓	✓

posed model versus other methods are represented.

4. The integrated credibility-based partial facility interdiction with fortification

The proposed interdiction model assigns facilities to candidate places and protects some of these facilities from attacks to minimize the defender's costs according to maximum damage of attacker. As mentioned before, we used the multi-objective function in our model, because we want to pursue the best strategy against the worst attacks of attackers. We used two objective functions. The defender's objective function that minimizes the fixed charge location cost, protection cost of facilities, and cost of assignment customers to the facilities; cost of outsourcing demands after attack is the first objective function. It has been assumed that the defender must satisfy the demands before and after the attack, and when he fails to do so, the customer demands are outsourced. The second objective function is that of the attacker. The attacker attempts to strike the maximum damage at the system. Attacker's objective function consists of maximizing the costs of customer's assignments to the facilities and the percentage of damage incurred on the defender's system. The objective functions of the defender and attacker are in conflict, and we cannot add them together. Then, we used the bi-objective optimization model. In this interdiction model, the defender determines what candidate' places construct the facility and which of them should be protected from attack. Moreover, according to the intention of attacker (maximizing the damages), this model assigns the demands to each facility before and after the attack.

4.1. Assumptions of the proposed model

We proposed Mixed Integer Programming (MIP) model for interdiction problem and transformed it to the Mixed Integer Linear Programming (MILP) model by linearization of its nonlinear statements. In this model, there are candidate places in which facilities can be constructed in this place, and there are customers with specific demands that must be satisfied before and after the attack. We considered the restriction of budget for attacker's attacks and for the defender in constructing facilities and protecting them. For the simplicity, the model assumed that each customer demands must be satisfied with one facility. In the other words, each customer must be allocated to one facility, or the whole of his demands must be outsourced. The model used the concept of partial interdiction, and attacker can attack the entire facility or inflict fractional damage on it. Also, the defender can protect the facilities before the attack. The model considered that attacker knows what facilities are protected, so he does not attack the protected facilities. When one facility is attacked, its capacity is reduced; if it cannot satisfy the customer demands assigned to the facility before the attack, then they will be assigned to other available facilities or outsourced unmet demands of customers entirely, according to its capacity customer demands. If the facility is not attacked, its customers are maintained after the attack. It has been assumed that before the attack, the defender must construct sufficient facilities to satisfy all customer demands, and it is not permitted to outsource some of their demands.

4.2. The mathematical model

The following properties are used in this model, which we propose for the integrated partial facility interdiction with fortification:

Index sets:

I	Set of customer nodes, I=$\{1, 2, \cdots, n\}$
J	Set of candidate facility sites, $J = \{1, 2, \cdots, m\}$

Parameters:

f_j	Fixed cost of constructing facility at site j
b_j	The required budget for attacking the whole of candidate site j
c_j	Protection cost of facility at site j
de_i	Demand of customer at node i
oc_i	Cost of outsourcing the demand of customer i per unit
q_j	The capacity of candidate site j according to its features
d_{ij}	Cost of allocating customer i to site j per unit
k	Available budget for defender
r	The budget of attacker for striking the system
mb	Policy of defender in considering a minimum budget for protecting the facilities

Decision variables:

$$X_j = \begin{cases} 1 & \text{if a facility is located at site } j \\ 0 & \text{otherwise} \end{cases}$$

$$Y_j = \begin{cases} 1 & \text{if the facilty at site } j \text{ is protected} \\ 0 & \text{otherwise} \end{cases}$$

$$U_{ij} = \begin{cases} 1 & \text{if before attack customer } I \text{ is allocated to site } j \\ 0 & \text{otherwise} \end{cases}$$

$$V_{ij} = \begin{cases} 1 & \text{if after attack customer } I \text{ is allocated} \\ & \text{to facility at site } j \\ 0 & \text{otherwise} \end{cases}$$

$$S_j = \begin{cases} 1 & \text{if facility at site } j \text{ is attacked by the} \\ & \text{attacker} \\ 0 & \text{otherwise} \end{cases}$$

$s_j =$ The fraction of attack inflicted on the facility at site j

$$W_i = \begin{cases} 1 & \text{if the demands of customer at node } i \\ & \text{are outsourced after the attack} \\ 0 & \text{otherwise} \end{cases}$$

The mathematical model of our bi-objective partial interdiction facility location problem with fortification is presented as follows:

$$\min Z_{\text{def}} = \left[\sum_{j\in J} f_j X_j + \sum_{j\in J} c_j Y_j\right] + \left[\sum_{i\in I}\sum_{j\in J} de_i d_{ij} U_{ij}\right] + \left[\sum_{i\in I} de_i oc_i W_i\right], \quad (1)$$

$$\max Z_{\text{att}} = \left[\sum_{i\in I}\sum_{j\in J} d_{ij} de_i (1-U_{ij}) V_{ij}\right] + \left[\sum_{j\in J} s_j f_j\right]. \quad (2)$$

Subject to:

$$\sum_{j\in J} U_{ij} = 1, \qquad i \in I, \quad (3)$$

$$\sum_{i\in I} U_{ij} \le nX_j, \qquad j \in J, \quad (4)$$

$$Y_j \le X_j, \qquad j \in J, \quad (5)$$

$$\sum_{j\in J} (f_j X_j + c_j Y_j) \le k, \quad (6)$$

$$\sum_{i\in I} de_i U_{ij} \le q_j, \qquad j \in J, \quad (7)$$

$$\sum_{j\in J} V_{ij} \le 1, \qquad i \in I, \quad (8)$$

$$\sum_{i\in I} U_{ij} \le nX_j, \qquad j \in J, \quad (9)$$

$$U_{ij}(1-S_j) \le V_{ij}, \qquad i \in I, \quad j \in J, \quad (10)$$

$$\sum_{j\in J} b_j s_j \le r, \quad (11)$$

$$S_j \le X_j - Y_j, \qquad j \in J, \quad (12)$$

$$\sum_{i\in I} de_i V_{ij} \le (1-s_j) q_j, \qquad j \in J, \quad (13)$$

$$S_j - s_j \ge 0, \qquad j \in J, \quad (14)$$

$$S_j - s_j \le (1-\varepsilon), \qquad j \in J, \quad (15)$$

$$W_i = 1 - \sum_{j\in J} V_{ij}, \qquad i \in I, \quad (16)$$

$$\sum_{j\in J} c_j Y_j \ge mb, \quad (17)$$

$$0 \le s_j \le 1, \qquad j \in J, \quad (18)$$

$$W_i, V_{ij}, S_j, U_{ij}, X_j, Y_j \in \{0,1\}, \quad i \in I, \quad j \in J. \quad (19)$$

Our proposed model has $(2mn+4m+n)$ variables and $(mn+8m+3n+2)$ constraints. In the model, Expression (1) represents the defender objective function. Its first component is related to fixed cost of opening facilities and protecting them. The second component is the cost of satisfying the customer demands by facilities before attack. The third component of the defender objective function is the cost of outsourcing the customer demands, and this objective function tries to minimize this cost. The attacker's objective function is shown in Expression (2). The first component of this function is the cost of reassigning the customers to the facilities after the attack. Part $(1-U_{ij})V_{ij}$ ensures that if customer i is allocated to facility j before attack, then the cost of allocating it to facility j is not computed in this component, because the attacker's objective function is interested in maximizing the post-attack costs.

The second part of attacker's objective function is related to the damages incurred by defender. Constraints (3) represent that each customer must be allocated to one facility before attack. Expressions (4) represent that one facility can accept more than one customer, and facility must exist, then we can assign customers to it. Constraints (5) describe that the opened facilities can be protected. Constraint (6) is the budget constraint for defender in order to construct and protect the facilities. In Constraints (7), we have mentioned that customers can be assigned to the facilities before attack until their capacity is sufficient. Constraints (8) represent that the customer must be assigned to one facility after the attack, or its demands can be outsourced. Expressions (9) represent that more than one customer can be allocated to specific facility

after the attack. Constraints (10) show that if customer i is allocated to facility j and attacker does not attack this facility, then customer i must be allocated to this facility after the attack.

Expression (11) is related to the budget of attacker in order to attack the system, and the attacker can damage the whole facility or fraction of it. Constraints (12) represent that the attacker knows about protected facilities and does not attack the protected facilities. Constraints (13) consider the reduced budget of facilities after attack and assign the customers to them according to their capacity. Constraints (14) and (15) describe the relation between S_j and s_j. These constraints explain that if $S_j = 0$, then $s_j = 0$; if $S_j = 1$, then $0 < s_j \leq 1$. ε is a positive small number. Constraints (16) specify the customers' nodes in which their demands are outsourced after the attack. In Constraint (17), the policy of defender in considering the minimum budget for protecting the facilities is modeled. The lower and upper bounds of variables s are described in Constraints (18). Finally, binary constraints in decision variables are described in Constraints (19).

4.3. The proposed credibility-based fuzzy chance constrained model

All the above-mentioned model's parameters are assumed to be deterministic. But, in most real-life situations as mentioned in Section 1, the parameters of interdiction design model are trained by uncertainty. To tackle this issue, we add the contexts of fuzzy programming to interdiction model for the first time, and a new hybrid credibility-based chance-constrained programming approach is proposed in this research. The credibility-based chanced-constrained approach is an efficient method that relies on high mathematical fuzzy concepts and can support different kinds of fuzzy numbers, such as triangular and trapezoidal forms of fuzzy numbers [23,24]. This method enables the decision-maker to satisfy some chance constraints at some given confidence levels. In this method, the decision-maker sets possibility distributions for the parameters of model, and the important feature of this method is that credibility measure is a self-dual measure. This means that if the credibility measure takes value 1, then the decision-maker believes that fuzzy event will surely happen; if it takes value 0, then the fuzzy event surely will not happen. But, if the possibility value takes value 1, then maybe it fails to happen; if this value takes 0, then it is possible that fuzzy event will happen. According to these features, Liu and Liu (2002) proved Expressions (20) and (21). Let $\tilde{v}$ be a fuzzy variable with membership function $\mu(x)$ and r be a real number. The credibility measure is defined as follows [25]:

$$\mathrm{Cr}\{\tilde{v} \leq r\} = \frac{1}{2}\left(\mathrm{Pos}\{\tilde{v} \leq r\} + \mathrm{Nec}\{\tilde{v} \leq r\}\right), \tag{20}$$

$$\mathrm{Cr}\{\tilde{v} \leq r\} = \frac{1}{2}\left(\sup_{x \leq r}\mu(x) + 1 - \sup_{x > r}\mu(x)\right). \tag{21}$$

According to Liu and Liu (2002), the expected value of $\tilde{v}$ can be determined as follows based on credibility measures:

$$E[\tilde{v}] = \int_0^{\infty} \mathrm{Cr}\{\tilde{v} \geq r\}\, dr - \int_{-\infty}^{0} \mathrm{Cr}\{\tilde{v} \leq r\}\, dr. \tag{22}$$

We assume in this research that $\tilde{v}$ is a trapezoidal fuzzy number defined by four constant points as $\tilde{v} = (v_{(1)}, v_{(2)}, v_{(3)}, v_{(4)})$. According to Expressions (23) and (24), the corresponding credibility measures and expected value of $\tilde{v}$ are computed as follows:

$$\mathrm{Cr}\{\tilde{v} \leq r\} = \begin{cases} 0 & r \in \left(-\infty, v_{(1)}\right] \\ \frac{r - v_{(1)}}{2\left(v_{(2)} - v_{(1)}\right)} & r \in \left(v_{(1)}, v_{(2)}\right] \\ \frac{1}{2} & r \in \left(v_{(2)}, v_{(3)}\right] \\ \frac{r - 2v_{(3)} + v_{(4)}}{2\left(v_{(4)} - v_{(3)}\right)} & r \in \left(v_{(3)}, v_{(4)}\right] \\ 1 & r \in \left(v_{(4)}, \infty\right) \end{cases} \tag{23}$$

$$\mathrm{Cr}\{\tilde{v} \geq r\} = \begin{cases} 1 & r \in \left(-\infty, v_{(1)}\right] \\ \frac{2v_{(2)} - v_{(1)} - r}{2\left(v_{(2)} - v_{(1)}\right)} & r \in \left(v_{(1)}, v_{(2)}\right] \\ \frac{1}{2} & r \in \left(v_{(2)}, v_{(3)}\right] \\ \frac{v_{(4)} - r}{2\left(v_{(4)} - v_{(3)}\right)} & r \in \left(v_{(3)}, v_{(4)}\right] \\ 0 & r \in \left(v_{(4)}, \infty\right) \end{cases} \tag{24}$$

$$E[\tilde{v}] = \frac{v_{(1)} + v_{(2)} + v_{(3)} + v_{(4)}}{4}. \tag{25}$$

Zhu and Zhang (2009) proved that if $\tilde{v}$ is trapezoidal fuzzy number and $\alpha > 0.5$, then Expressions (26) and (27) are obtained [25]:

$$\mathrm{Cr}\{\tilde{v} \leq r\} \geq \alpha \Leftrightarrow r \geq (2 - 2\alpha)v_{(3)} + (2\alpha - 1)v_{(4)}, \tag{26}$$

$$\mathrm{Cr}\{\tilde{v} \geq r\} \geq \alpha \Leftrightarrow r \leq (2\alpha - 1)v_{(1)} + (2 - 2\alpha)v_{(2)}. \tag{27}$$

To tackle uncertainty in the proposed interdiction model, all the parameters are presumed to be independent trapezoidal fuzzy numbers. To convert chance constraints to equivalent crisp constraints, we can directly apply Expressions (26) and (27).

There are three types of credibility-based fuzzy mathematical programming approaches: the chance-constrained programming [26], the expected value [25], and the dependent chance-constrained programming [23]. The expected value is the easiest one. The advantage of this method is that it does not increase the computational complexity of original model; however, it has no control on the confidence level of chance constraints' satisfactions. The chance-constrained programming copes with the deficiency of the expected value approach, but adding a constraint to each objective function causes an increase in the computational complexity of original model, and also such an approach needs more information on the ideal solutions. The dependent-chance programming model is analogous to chance-constrained programming, but it attaches more importance to confidence levels [24].

In this research, to design credibility-based fuzzy programming for interdiction problem, we have incorporated the expected value and the chance-constrained approach. For modeling the objective function, the expected value is used, and the chance-constrained programming approach is used to convert chance constraints with vague parameters into crisp equivalent constraints. In this hybrid approach, the number of constraints does not increase and there is no need for more information about objective functions. Moreover, this approach benefits from privileges of chance-constrained approach. According to the above-mentioned descriptions and by considering the trapezoidal independent possibility distributions of uncertain parameters of model, the proposed credibility-based fuzzy mathematical programming for interdiction problem can be formulated as follows. In this model, the fuzziness of parameters is represented with "$\sim$" above their names.

$$\min E[Z_{\text{def}}] = \left[\sum_{j\in J} E\left[\tilde{f}_j\right] X_j + \sum_{j\in J} E\left[\tilde{c}_j\right] Y_j\right] + \left[\sum_{i\in I}\sum_{j\in J} E\left[\widetilde{de}_i\right] E[\tilde{d}_{ij}] U_{ij}\right] + \left[\sum_{i\in I} E\left[\widetilde{de}_i\right] E\left[\widetilde{oc}_i\right] W_i\right],$$

$$\max E\left[Z_{\text{att}}\right] = \left[\sum_{i\in I}\sum_{j\in J} E\left[\widetilde{de}_i\right] E\left[\tilde{d}_{ij}\right] (1-U_{ij}) V_{ij}\right] + \left[\sum_{j\in J} E\left[\tilde{f}_j\right] s_j\right].$$

Subject to:

$$\sum_{j\in J} U_{ij} = 1, \qquad i \in I,$$

$$\sum_{i\in I} U_{ij} \le nX_j, \qquad j \in J,$$

$$Y_j \le X_j, \qquad j \in J,$$

$$\text{Cr}\left\{\sum_{j\in J}\left(\tilde{f}_j X_j + \tilde{c}_j Y_j\right) \le \tilde{k}\right\} \ge \alpha_1,$$

$$\text{Cr}\left\{\sum_{i\in I} \widetilde{de}_i U_{ij} \le \tilde{q}_j\right\} \ge \beta_j, \qquad j \in J,$$

$$\sum_{j\in J} V_{ij} \le 1, \qquad i \in I,$$

$$\sum_{i\in I} V_{ij} \le nX_j, \qquad j \in J,$$

$$U_{ij}(1-S_j) \le V_{ij}, \qquad i \in I, \quad j \in J,$$

$$\text{Cr}\left\{\sum_{j\in J} \tilde{b}_j s_j \le \tilde{r}\right\} \ge \alpha_2,$$

$$S_j \le X_j - Y_j, \qquad j \in J,$$

$$\text{Cr}\left\{\sum_{i\in I} \widetilde{de}_i V_{ij} \le (1-s_j)\tilde{q}_j\right\} \ge \delta_j, \qquad j \in J,$$

$$S_j - s_j \ge 0, \qquad j \in J,$$

$$S_j - s_j \le (1-\varepsilon), \qquad j \in J,$$

$$W_i = 1 - \sum_{j\in J} V_{ij}, \qquad i \in I,$$

$$\text{Cr}\left\{\sum_{j\in J} \tilde{c}_j Y_j \ge \widetilde{mb}\right\} \ge \alpha_3,$$

$$0 \le s_j \le 1, \qquad j \in J,$$

$$W_i, V_{ij}, S_j, U_{ij}, X_j, Y_j \in \{0,1\}, \qquad i \in I, \quad j \in J.$$

According to Eqs. (26) and (27) and by considering the expected value of trapezoidal fuzzy numbers, the credibility-based chance-constrained programming

model mentioned above can be converted into the following crisp equivalent MINLP model:

$$\min E[Z_{\text{def}}] = \left[\sum_{j\in J}\frac{f_{j(1)}+f_{j(2)}+f_{j(3)}+f_{j(4)}}{4}X_j + \sum_{j\in J}\frac{c_{j(1)}+c_{j(2)}+c_{j(3)}+c_{j(4)}}{4}Y_j\right] + \left[\sum_{i\in I}\sum_{j\in J}\frac{de_{i(1)}+de_{i(2)}+de_{i(3)}+de_{i(4)}}{4} \times \frac{d_{ij(1)}+d_{ij(2)}+d_{ij(3)}+d_{ij(4)}}{4}U_{ij}\right] + \left[\sum_{i\in I}\frac{de_{i(1)}+de_{i(2)}+de_{i(3)}+de_{i(4)}}{4} \times \frac{oc_{i(1)}+oc_{i(2)}+oc_{i(3)}+oc_{i(4)}}{4}W_i\right],$$

$$\max E[Z_{\text{att}}] = \left[\sum_{i\in I}\sum_{j\in J}\frac{de_{i(1)}+de_{i(2)}+de_{i(3)}+de_{i(4)}}{4} \times \frac{d_{ij(1)}+d_{ij(2)}+d_{ij(3)}+d_{ij(4)}}{4}(1-U_{ij})V_{ij}\right] + \left[\sum_{j\in J}\frac{f_{j(1)}+f_{j(2)}+f_{j(3)}+f_{j(4)}}{4}s_j\right],$$

subject to:

$$\sum_{j\in J}U_{ij}=1, \qquad i\in I,$$

$$\sum_{i\in I}U_{ij}\le nX_j, \qquad j\in J,$$

$$Y_j\le X_j, \qquad j\in J,$$

$$(2\alpha_1-1)k_{(1)}+(2-2\alpha_1)k_{(2)} - \sum_{j\in J}[X_j[(2\alpha_1-1)f_{j(1)}+(2-2\alpha_1)f_{j(2)}] + Y_j[(2\alpha_1-1)c_{j(1)}+(2-2\alpha_1)c_{j(2)}]]\ge 0,$$

$$(2\beta_j-1)q_{j(1)}+(2-2\beta_j)q_{j(2)} - \sum_{i\in I}U_{ij}[(2\beta_j-1)de_{i(1)}+(2-2\beta_j)de_{i(2)}]\ge 0, \quad j\in J,$$

$$\sum_{j\in J}V_{ij}\le 1, \qquad i\in I,$$

$$\sum_{i\in I}V_{ij}\le nX_j, \qquad j\in J,$$

$$U_{ij}(1-S_j)\le V_{ij}, \qquad i\in I, \quad j\in J,$$

$$(2\alpha_2-1)r_{(1)}+(2-2\alpha_2)r_{(2)} - \sum_{j\in J}s_j[(2\alpha_2-1)b_{j(1)}+(2-2\alpha_2)b_{j(2)}]\ge 0,$$

$$S_j\le X_j-Y_j, \qquad j\in J,$$

$$(1-s_j)[(2\delta_j-1)q_{j(1)}+(2-2\delta_j)q_{j(2)}] - \sum_{i\in I}V_{ij}[(2\delta_j-1)de_{i(1)}+(2-2\delta_j)de_{i(2)}]\ge 0, \quad j\in J,$$

$$S_j-s_j\ge 0, \qquad j\in J,$$

$$S_j-s_j\le(1-\varepsilon), \qquad j\in J,$$

$$W_i=1-\sum_{j\in J}V_{ij}, \qquad i\in I,$$

$$\sum_{j\in J}Y_j[(2\alpha_3-1)c_{j(1)}+(2-2\alpha_3)c_{j(2)}] - [(2\alpha_3-1)mb_{(1)}+(2-2\alpha_3)mb_{(2)}]\ge 0,$$

$$0\le s_j\le 1, \qquad j\in J,$$

$$W_i,V_{ij},S_j,U_{ij},X_j,Y_j\in\{0,1\}, \qquad i\in I, \quad j\in J.$$

We have assumed in this model that confidence levels must be greater than 0.5 (i.e., $\alpha_1,\alpha_2,\alpha_3,\beta_j,\delta_j > 0.50$).

5. The solution methodology

Our proposed model for the interdiction problem is the Multi-Objective Mixed-Integer Non-Linear Programming (MOMINLP). MOMINLP is very useful for many areas of application as any model that incorporates

the discrete phenomena requires the consideration of integer variables for issues, such as modeling the fixed charges, production levels, disjunctive constraints, etc. [27]. The utilization of integer variables into multi-objective modeling problems makes these problems too difficult to solve. There have been many developments in solving these models. Some researchers have concentrated on the use of metaheuristics to solve multi-objective problems. Some papers have concentrated on the interactive methods for the general type of MOIP problems due to their capabilities to solve the integer variables.

As mentioned earlier, there are several methods for solving the Multi-Objective Non-Linear Programming (MONLP) models. Among these, the fuzzy multi-objective programming approaches are more interesting, because the benefit of these methods is that they are capable of measuring the satisfaction degree of each objective function clearly. This issue can help decision-makers to choose their preferred solution according to the satisfaction degree and relative importance of each objective function. Hence, in this work, we use the TH method that is one of the best approaches in the fuzzy multi-objective programming context to convert our bi-objective model to the equivalent crisp single-objective model. This method was introduced by Torabi and Hassini (2008) [6] to solve the original MOMILP model. The steps of this method for solving the proposed model are represented as follows:

- **Step 1:** Determine the Positive Ideal Solution (PIS) and Negative Ideal Solution (NIS) for each objective function by solving the single objective model with the whole of the constraints. To obtain these solutions to two objectives of our model, we construct the trade-off table represented in Table 2, in which f_{def} denotes the defender objective function, and f_{att} denotes the attacker objective function. x^*_{def} is the optimum solution vector obtained by solving single-objective of defender model, and x^*_{att} is the optimum solution vector obtained by solving single objective of attacker prospective;

- **Step 2:** After determining PIS and NIS, we specify a linear membership function for each membership function as follows (according to Figures 1 and 2):

Table 2. Trade-off table for constructing ideal solutions.

Objective function	z^{PIS}	z^{NIS}
Defender	$f_{\text{def}}(x^*_{\text{def}})$	$f_{\text{def}}(x^*_{\text{att}})$
Attacker	$f_{\text{att}}(x^*_{\text{att}})$	$f_{\text{att}}(x^*_{\text{def}})$

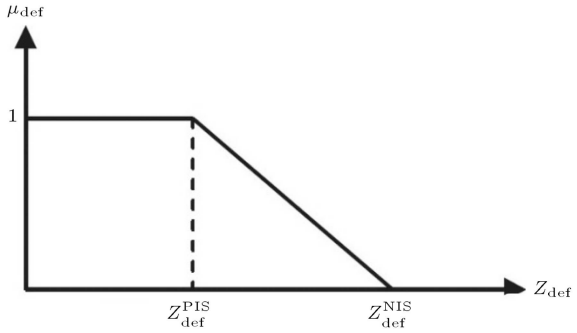

Figure 1. Linear membership function for Z_{def}.

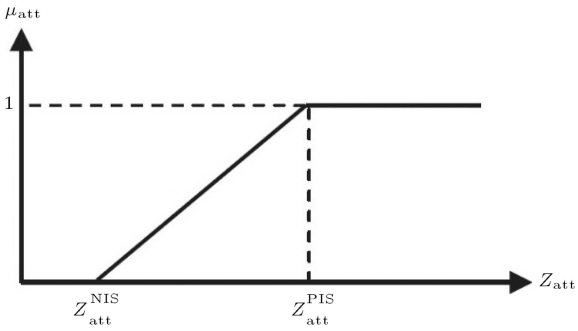

Figure 2. Linear membership function for Z_{att}.

$$\mu_{\text{def}}(x) = \begin{cases} 1 & \text{if } Z_{\text{def}} < Z^{\text{PIS}}_{\text{def}} \\ \frac{Z^{\text{NIS}}_{\text{def}} - Z_{\text{def}}}{Z^{\text{NIS}}_{\text{def}} - Z^{\text{PIS}}_{\text{def}}} & \text{if } Z^{\text{PIS}}_{\text{def}} \le Z_{\text{def}} \le Z^{\text{NIS}}_{\text{def}} \\ 0 & \text{if } Z_{\text{def}} > Z^{\text{NIS}}_{\text{def}} \end{cases} \tag{28}$$

$$\mu_{\text{att}}(x) = \begin{cases} 1 & \text{if } Z_{\text{att}} > Z^{\text{PIS}}_{\text{att}} \\ \frac{Z^{\text{NIS}}_{\text{att}} - Z_{\text{att}}}{Z^{\text{NIS}}_{\text{att}} - Z^{\text{PIS}}_{\text{att}}} & \text{if } Z^{\text{NIS}}_{\text{def}} \le Z_{\text{att}} \le Z^{\text{PIS}}_{\text{att}} \\ 0 & \text{if } Z_{\text{att}} < Z^{\text{NIS}}_{\text{def}} \end{cases} \tag{29}$$

$\mu_h(X)$ denotes the satisfaction degree of hth objective function for solution vector X;

- **Step 3:** Convert the MOMINLP model into the crisp equivalent single-objective model using the following formulation:

$$\max \gamma\lambda_0 + (1-\gamma)\sum_{h=1}^{2} w_h \mu_h(X),$$

s.t.

$$\lambda_0 \le \mu_h(X) \qquad h = 1, 2,$$

$$X \in F(X), \qquad \lambda_0, \gamma \in [0, 1], \tag{30}$$

where λ_0 denotes the minimum satisfaction degree of objectives. $F(X)$ is the set of model constraints,

described in Section 3. This method is the combination of satisfaction degree of objectives and weighted sum of these degrees to yield a balanced compromise solution. w_h indicates relative significance of hth objective function, and γ is the coefficient of compensation. γ controls the minimum degree of objectives' satisfaction along with the compromise degree among the objectives tacitly. Hence, the TH method can yield both unbalanced and balanced compromised solutions to a model based on decision-makers' preferences through adjusting the value of γ;

- **Step 4:** Given the parameters of γ and the coefficient vector of fuzzy goals (w), we solve the crisp single-objective model by the MINLP solver and obtain the optimum solution vector satisfying the decision-makers' preferences.

5.1. Genetic algorithm

As mentioned previously, our proposed model is a mixed integer non-linear programming. These characteristics cause the model to be hardly solved by exact methods [28]. Genetic algorithms are one of the best ways to solve a problem of which little is known. They are very general algorithms, and therefore, they will work well in any search space. All one needs to know is how capable the solution is in coping with different things, and how well a genetic algorithm will be able to create a high-quality solution. Genetic algorithms use the principles of selection and evolution to produce several solutions to a given problem. Genetic algorithms tend to thrive in an environment in which there is a very large set of candidate solutions and the search space is uneven and has many hills and valleys. The normal form of GA was presented by Goldberg (1988) [29].

GA is a general method that can be applied to any problem if the feasible solution to the problem can be showed as string that corresponds to genetic encoding of the solution (chromosome). Each chromosome has a fitness value that corresponds to the objective value of the associated solution. Initially, there is a legal population chromosome constructed at random. Next, a number of chromosomes are selected to produce a new chromosome (solution) that named offspring to the next generation. The mating of parents is done in a GA by applying the GA operator, such as crossover and mutation. The selection of parents and production of offspring are repeated until stopping rule is satisfied.

5.1.1. Representation

Determining facility location and the facility that must be protected or attacked is the most important issue. If these are determined, the remaining important decision is the issue of assignment of customer to facility before and after attack and fraction of attacks. For example, representation of a chromosome in this paper is illustrated in Figure 3.

X_j	1	0	1
U_{ij}	1	0	0
	0	0	1
Y_j	1	0	0
S_j	0	0	1
V_{ij}	1	0	0
	1	0	0
s_j	0	0	0.65

Figure 3. Representation of a chromosome.

The solution (chromosome) has 2 customers and 3 facilities; thus, each chromosome is represented by a $(2i + 4)j$ array (i customer and j facility), where the first row represents the facility that is open (=1) or closed (=0). The next ith row represents the customer's assignment to the facility before attack. Next row represents the protected facility. Next row represents the facility attacked by attackers. Next ith row represents the assignment of customer to facility after attack. Finally, the last row represents the fraction of attack occurring in an open facility.

5.1.2. Fitness evaluation

The fitness value of each chromosome reflects how good it is based upon its achievement of objective. For each chromosome, the solution to the corresponding interdiction problem specifies the cost of opening facility and protecting them and satisfying the customer demand before and after attack and damage incurred by defender. To specify the fitness for chromosome, we calculate Eq. (30).

5.1.3. Crossover and mutation

The crossover operator generates a new offspring by incorporating the information comprised in the chromosomes of the parents so that new offspring will have the good parts of the parent's chromosomes. We applied two-point crossover. In this method, we select two random integers, i.e. m and n, between 1 and number of candidate facility site (j). The function selects vectors entries, and includes the integer number less than or equal to m from the first parent, and the integer number from $m+1$ to n from the second parent. The algorithm then concatenates these genes to form a single gene.

The produced child may be infeasible, so sometimes we need to repair U_{ij} (column 2: $i + 1$) and V_{ij} (column $i + 3$: $2i + 3$) of produced child.

Mutation option determines how the genetic algorithm makes small random changes in the individuals in the population to create mutation children. Genetic

diversity is provided by mutation operator, and mutation empowers the GA to search a wider space. We used inversion mutation method.

5.1.4. Selection process

A tournament selection process is used for the proposed GA, in which the two selected chromosomes from the population are evaluated based on their fitness value and the one with the best fitness chromosome is copied into mating pool.

5.1.5. Termination

Unfortunately, in all optimization methods, proving the convergence of the optimal solution is difficult; therefore, when the fixed number of generation is obtained, the process will be stopped.

6. Experiments

The experimental results are shown in this section, and capability of model is checked with the examples. The examples are generated with the random distributions. Our model is constructed in Gams 23.5 software and all of the examples are solved by the MINLP solver of this software. This software is installed through the Core i5 system with the 2.40 GHz CPU and 8 GB of RAM. In the first stage of this section, we describe the procedure of constructing examples.

6.1. Random generation of test problems

The procedure of constructing parameters of examples is described as follows. The number of candidate facility sites generated from random distribution and number of customers is supposed to be $2m$ (m is equal to the number of candidate facilities). We supposed that fixed costs of opening facilities are highly related to the other costs. Also, we determined the protection costs so smaller than the fixed costs. We assumed that the costs of outsourcing the customers are lower than costs of assigning the customers to the candidate places. In Table 3, the template employed for the random distribution generation is represented. In this table, $U[lb, ub]$ symbolizes the random integer number between the lower bound lb and the upper bound ub, and $[U, B]$ shows the random number between U and B.

Table 3. Random problem generation template.

Parameters	Values
m	3-10
n	2 m
b_j	$U[100000, 150000]$
f_j	$U[100 \times 10^6, 500 \times 10^6]$
c_j	$U[15 \times 10^4, 20 \times 10^4]$
de_i	$U[10000, 100000]$
oc_i	$U[4000, 6000]$
q_j	$\frac{n}{2} \times [10000, 30000]$
d_{ij}	$U[500, 5000]$
k	$\bar{f} \times [0.6m, m]$
r	$m \times [40 \times 10^4, 130 \times 10^4]$
mb	$175000 \times m \times [0.2, 0.5]$

6.2. Solution of credibility-based interactive possibilistic model

Now, we generate various samples with different sizes according to the template represented in Table 3, which includes various classes of chance constraints and objectives' satisfaction degrees. Then, with the TH method and the various values of decision-makers' preferences, we solve the credibility-based interactive possibilistic method according to Section 4. The number of candidate facilities, customer nodes, and satisfaction degrees' classes in the generated problem instances is shown in Table 4.

According to Table 3, we construct 70 instances with different satisfaction degrees of decision-makers and solve these instances and obtain the optimum solutions through GAMS 23.5 software and the proposed GA each instance. The GA parameters are set as follows: crossover probability 0.8, mutation probability 0.3, maximum number of iteration 100, and number of population 100. To confirm the effectiveness of this algorithm, we run our proposed algorithm 10 times for each test problem, and then mean of fitness function is reported. The problem instances with analysis of various confidence levels are represented in Tables 5-8.

The above tables show that in different situations, the mutual knowledge the defenders and attackers have on each other can actually aid the decision-maker in

Table 4. The various classes for parameters of problem instances.

Instance type	Number of candidate facilities	Number of customer nodes	Classes of chance constraints	Classes of γ	Classes of w_h
No. 1	3	6	Low-high	Low-medium-high	Low-medium-high
No. 2	4	8	Low-high	Low-medium-high	Low-medium-high
No. 3	8	16	Low-high	Low-medium-high	Low-medium-high
No. 4	10	20	Low-high	Low-medium-high	Low-medium-high

Table 5. Problem instance with 3 candidate facilities and 6 customer nodes.

	Confidence levels	Importance of the first objective function ($w_1 = 1 - w_2$)	Coefficient of compensation γ	Objective function values ($\times 10^8$)				CPU time (sec)		Minimum satisfaction degree (λ)	
				Gams		GA		Gams	GA	Gams	GA
				Z_{att}	Z_{deff}	Z_{att}	Z_{deff}				
Instance type no. 1	Low	0.8	0	9.26	4.53	9.39	4.40	19	25	0	0
	Low	0.5	0	9.26	5.62	9.37	5.51	21	25	0	0
	Low	0.3	0	9.26	5.62	9.38	5.49	20	28	0	0
	High	0.8	0	7.90	3.73	7.98	3.7	20	28	0	0
	High	0.5	0	7.90	3.73	7.97	3.71	19	29	0	0
	High	0.3	0	9.30	11.8	9.42	11.4	20	28	0	0
	Low	—	1	9.26	4.78	9.30	4.72	22	30	0.46	0.44
	High	—	1	9.16	10.1	9.23	9.97	23	30	0.97	0.90
	Low	0.8	0.5	9.26	4.78	9.33	4.69	21	30	0.46	0.41
	Low	0.5	0.5	9.26	4.78	9.32	4.66	23	29	0.46	0.42
	Low	0.3	0.5	9.26	4.78	9.30	4.67	25	28	0.46	0.42
	High	0.8	0.5	9.16	11.0	9.17	9.05	21	31	1	0.95
	High	0.5	0.5	9.16	11.0	9.19	9.11	23	30	1	0.96
	High	0.3	0.5	9.30	11.0	9.19	9.10	22	31	0.96	0.92

Table 6. Problem instance with 4 candidate facilities and 8 customer nodes.

	Confidence levels	Importance of the first objective function ($w_1 = 1 - w_2$)	Coefficient of compensation γ	Objective function values ($\times 10^9$)				CPU time (sec)		Minimum satisfaction degree (λ)	
				Gams		GA		Gams	GA	Gams	GA
				Z_{att}	Z_{deff}	Z_{att}	Z_{deff}				
Instance type no. 2	Low	0.8	0	2.08	1.33	2.14	1.30	90	45	0	0
	Low	0.5	0	2.08	1.33	2.14	1.28	92	44	0	0
	Low	0.3	0	2.18	1.38	2.23	1.31	98	49	0	0
	High	0.8	0	1.80	0.73	1.86	0.65	95	46	0	0
	High	0.5	0	1.80	0.73	1.89	0.69	96	48	0	0
	High	0.3	0	1.80	0.73	1.86	0.66	97	48	0	0
	Low	—	1	9.26	0.47	9.35	0.40	100	48	0.46	0.43
	High	—	1	9.16	1.01	9.25	0.95	97	47	0.97	0.92
	Low	0.8	0.5	9.26	0.47	9.36	0.40	91	49	0.46	0.41
	Low	0.5	0.5	9.26	0.47	9.32	0.42	102	48	0.46	0.42
	Low	0.3	0.5	9.26	0.47	9.36	0.42	101	48	0.46	0.40
	High	0.8	0.5	9.16	1.10	9.20	1.02	99	47	1	0.96
	High	0.5	0.5	9.16	1.10	9.20	1.04	97	50	1	0.95
	High	0.3	0.5	9.16	1.10	9.25	1.06	102	51	0.96	0.92

determining the desirable degrees of satisfaction. Not surprisingly, the model will be solved through this situation; the optimum obtained solution determines the defender policy in constructing and protecting the facilities from attacks. For example, if the knowledge of defender and attacker in their structures is equal, then parameter γ chooses the values of 0.5 to 1. If defender intends to specify the best policy just according to the importance of his organization conditions and attacker's attacking of the facilities in a fixed manner, then parameter γ chooses the values of 1, etc. Moreover, in these instances, the different classes of

Table 7. Problem instance with 8 candidate facilities and 16 customer nodes.

	Confidence levels	Importance of the first objective function ($w_1 = 1 - w_2$)	Coefficient of compensation γ	Objective function values ($\times 10^9$)				CPU time (sec)		Minimum satisfaction degree (λ)	
				Gams		GA		Gams	GA	Gams	GA
				Z_{att}	Z_{deff}	Z_{att}	Z_{deff}				
Instance type no. 3	Low	0.8	0	2.88	1.59	2.92	1.54	491	66	0	0
	Low	0.5	0	3.54	3.40	3.57	3.28	510	59	0	0
	Low	0.3	0	3.82	4.12	3.83	4.06	478	68	0	0
	High	0.8	0	2.79	1.13	2.85	1.09	482	66	0	0
	High	0.5	0	3.49	4.03	3.52	4.01	512	70	0	0
	High	0.3	0	3.70	4.39	3.71	4.35	507	69	0	0
	Low	—	1	3.37	2.90	3.41	2.82	524	72	0.73	0.68
	High	—	1	3.19	3.41	3.24	3.19	514	70	0.84	0.80
	Low	0.8	0.5	3.35	2.92	3.41	2.89	498	65	0.74	0.72
	Low	0.5	0.5	3.37	3.20	3.40	3.16	513	67	0.73	0.71
	Low	0.3	0.5	3.37	3.11	3.44	3.08	502	65	0.73	0.69
	High	0.8	0.5	3.09	3.34	3.12	3.25	496	65	0.85	0.83
	High	0.5	0.5	3.12	3.39	3.15	3.36	514	68	0.87	0.84
	High	0.3	0.5	3.21	3.36	3.22	3.32	504	64	0.83	0.80

Table 8. Problem instance with 10 candidate facilities and 20 customer nodes.

	Confidence levels	Importance of the first objective function ($w_1 = 1 - w_2$)	Coefficient of compensation γ	Objective function values ($\times 10^9$)				CPU time (sec)		Minimum satisfaction degree (λ)	
				Gams		GA		Gams	GA	Gams	GA
				Z_{att}	Z_{deff}	Z_{att}	Z_{deff}				
Instance type no. 4	Low	0.8	0	3.04	1.92	3.10	1.84	1503	82	0	0
	Low	0.5	0	3.15	4.40	3.15	4.36	1483	89	0	0
	Low	0.3	0	3.68	4.97	3.73	3.68	1650	85	0	0
	High	0.8	0	2.84	1.62	2.87	2.83	1800	90	0	0
	High	0.5	0	3.50	4.57	3.59	3.55	1800	92	0	0
	High	0.3	0	3.78	5.19	3.82	3.79	1800	87	0	0
	Low	—	1	3.78	4.12	3.29	4.66	1800	93	0.81	0.90
	High	—	1	3.90	4.19	3.36	4.44	1800	86	0.76	0.87
	Low	0.8	0.5	3.78	4.29	3.42	4.54	1800	89	0.72	0.83
	Low	0.5	0.5	3.82	4.32	3.42	4.54	1800	96	0.74	0.83
	Low	0.3	0.5	3.90	4.35	3.44	4.81	1800	91	0.73	0.82
	High	0.8	0.5	3.72	4.25	3.33	4.63	1800	93	0.75	0.88
	High	0.5	0.5	3.68	4.28	3.33	4.63	1800	89	0.76	0.88
	High	0.3	0.5	4.01	4.40	3.50	4.74	1800	96	0.68	0.79

constraints' confidence levels show that the decision-makers could determine the importance of imprecise constraints and try to satisfy them according to their importance. On the other hand, according to Tables 5 and 6, it is clear that our proposed GA provides high-quality solution to small problems in a short time. As we know, in exact algorithms with an increase in the dimension of problem, solving time increases exponentially, and we can see the time increase in solving time in Tables 5-7 using Gams Solver. In addition, we can see that solving time in GA linearly increases as shown in Figures 4 and 5. In Table 8 and

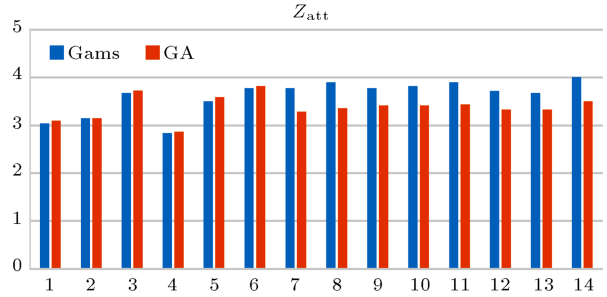

Figure 4. A comparison between instances shown in Table 8, considering the Z_{att}.

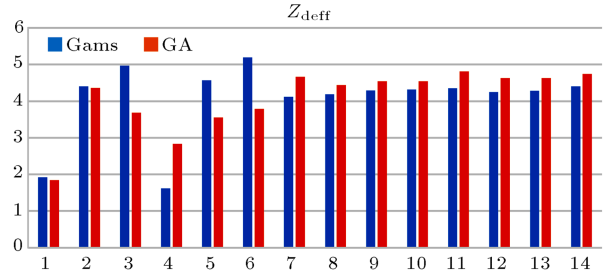

Figure 5. A comparison between instances shown in Table 8, considering the Z_{deff}.

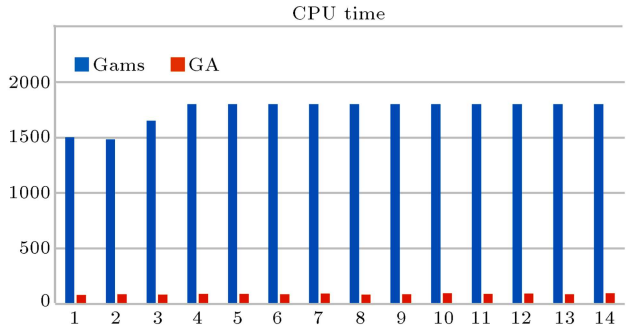

Figure 6. A comparison between instances shown in Table 8, considering CPT time.

Figure 6, in 1800 sec, the Genetic Algorithm gets a better solution than Gams solver in lesser time.

7. Conclusions

In this paper, we tackled credibility-based bi-objective fixed charge location problem with the contexts of fortification, partial attacks, budget constraints, capacity reductions, and outsourcing unmet demands. Then, we constructed the model with these conditions. This model is very applicable in real conditions, because we have added the contexts of fuzziness and uncertainty to the model for the first time. Also, we used the hybrid credibility-based chance constraint programming that overcomes the deficiency of other chance-constrained methods. We solved this model by interactive possibility TH method. This method helps us specify the decision-makers' satisfaction degrees. Also, this method tackles different levels of knowledge that attackers and defenders know about each other. In the following, we proposed Genetic algorithm to solve the proposed algorithm. In the experimental results section, we gave a template for constructing various instances. At last, we made different instances in sizes and parameters and analyzed these instances with different confidence levels and solved them by MINLP solver and Genetic algorithm to show the capability of the proposed model.

For future studies, this work has the potential to be extended to a great degree. For instance, considering the network of candidate facilities and existence roads in the model can be one of the available directions to follow in the related field. Most of attackers are interested in attacking the communication roads instead of facilities, because if one road is disconnected, then two candidate sites are damaged. Also, the cost of attacking the roads is lower than that of attacking the facility. Nevertheless, protecting the roads from attacks is so hard as well.

References

1. Smith, J.C., Lim, C. and Sudargho, F. "Survivable network design under optimal and heuristic interdiction scenarios", *Journal of Global Optimization*, **38**(2), pp. 181-99 (2007).
2. Smith, J.C. and Lim, C. "Algorithms for network interdiction and fortification games", In *Pareto optimality, Game Theory and Equilibria*, New York, Springer, pp. 609-44 (2008).
3. Snyder, L.V. and Daskin, M.S. "Reliability models for facility location: the expected failure cost case", *Transportation Science*, **39**(3), pp. 400-16 (2005).
4. Aksen, D., Şengül Akca, S. and Aras, N. "A bilevel partial interdiction problem with capacitated facilities and demand outsourcing", *Computers & Operations Research*, **41**, pp. 346-358. (2014), http://dx.doi.org/10.1016/j.cor.2012.08.013.
5. Chalk, P., Hoffman, B., Reville, R. and Kasupski, A., *Trends in Terrorism*, RAND Center for Terrorism Risk Management Policy, /http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG393.pdfS; 2005 [accessedAugust.12].
6. Torabi, S.A. and Hassini, E. "An interactive possibilistic programming approach for multiple objective supply chain master planning", *Fuzzy Sets and Systems*, **159**, pp. 193-214 (2008).
7. Aksen, D., Piyade, N. and Aras, N. "The budget constrained r-interdiction median problem with capacity expansion", *Central European Journal of Operations Research*, **18**(3), pp. 269-91 (2010).
8. Brown, G., Carlyle, M., Salmerón, J. and Wood, K. "Analyzing the vulnerability of critical infrastructure to attack and planning defenses", TutORialsin Operations Research, pp. 102-23 [INFORMS] (2005).

9. Aksen, D. and Aras, N. "A bi-level fixed charge location model for facilities under imminent attack", *Computers & Operations Research*, **39**, pp. 1364-1381 (2012).

10. Aksen, D., Sema, S.A. and Necati, A. "A bi-level partial interdiction problem with capacitated facilities and demand outsourcing", *Computers & Operations Research*, **41**, pp. 346-358 (2014).

11. Church, R.L., Scaparra, M.P. and Middleton, R.S. "Identifying critical infrastructure: the median and covering facility interdiction problems", *Annals of the Association of American Geographers*, **94**(3), pp. 491-502 (2004).

12. McMasters, A. and Mustin, T.M. "Optimal interdiction of a supply network", *Naval Research Logistics Quarterly*, **17**(3), pp. 261-268 (1970).

13. Church, R.L. and Scaparra, M.P. "Protecting critical assets: the r-interdiction median problem with fortification", *Geographical Analysis*, **39**(2), pp. 129-46 (2007).

14. Wood, R.K. "Deterministic network interdiction", *Mathematical and Computer Modelling*, **17**(2), pp. 1-18 (1993).

15. Fulkerson, D.R. and Harding, G.C. "Maximizing the minimum source-sink path subject to a budget constraint", *Mathematical Programming*, **13**(1), pp. 116-8 (1977).

16. Scaparra, M.P. and Church, R.L. "An exact solution approach for the interdiction median problem with fortification", *European Journal of Operational Research*, **189**(1), pp. 76-92 (2008).

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

18. Losada, C., Scaparra, M.P., Church, R.L. and Daskin, M.S. "Modeling approaches for the multi-source interdiction median problem", *Kent Business School Working Paper No. 187*, University of Kent, UK (2010).

19. Zimmermann, H.J. "Fuzzy programming and linear programming with several objective functions", *Fuzzy Sets and Systems*, **1**, pp. 45-55 (1978).

20. Lai, Y.J. and Hwang, C.L. "Possibilistic linear programming for managing interest rate risk", *Fuzzy Sets and Systems*, **54**, pp. 135-146 (1993).

21. Selim, H. and Ozkarahan, I. "A supply chain distribution network design model: an interactive fuzzy goalprogramming-based solution approach", *Internet. J. Advanced Manufacturing Technology*, **36**, pp. 401-418 (2008).

22. Li, X.Q., Zhang, B. and Li, H. "Computing efficient solutions to fuzzy multiple objective linear programming problems", *Fuzzy Sets and Systems*, **157**, pp. 1328-1332 (2006).

23. Liu, B. "Dependent-chance programming with fuzzy decisions", *IEEE Transactions on Fuzzy Systems*, **7**, pp. 354-360 (1999).

24. Pishvaee, M.S., Torabi, S.A. and Razmi, J. "Credibility-based fuzzy mathematical programming model for green logistics design under uncertainty", *Computers & Industrial Engineering*, **62**, pp. 624-632 (2008).

25. Liu, B. and Liu, Y.K. "Expected value of fuzzy variable and fuzzy expected value models", *IEEE Transactions on Fuzzy Systems*, **10**(4), pp. 445-450 (2002).

26. Liu, B. and Iwamura, K. "Chance constrained programming with fuzzy parameters", *Fuzzy Sets and Systems*, **94**, pp. 227-237 (1998).

27. Alves, M.J. and Clímaco, J. "A review of interactive methods for multiobjective integer and mixed-integer programming", *European Journal of Operational Research*, **180**, pp. 99-115 (2007).

28. Gen, M. and Cheng, R., *Genetic Algorithms and Engineering Optimization*, In John Wiley & Sons, Ed. 7, pp. 57-450 (2000).

29. Goldberg, D.E. and Holland, J.H. "Genetic algorithms and machine learning", *Machine Learning*, **3**(2), pp. 95-99 (1988).

Biographies

Ali Azadeh is a Professor of Industrial Engineering in College of Engineering in University of Tehran, Iran. He obtained his PhD degree in Industrial Engineering from USC University America in 1992, his MSc degree in Industrial Engineering from the California University, America in 1986, and his BSc degree in Mathematics from USF University, America. He serves on the Editorial Board of numerous reputable journals. He is the recipient of the Distinguished Researcher Award and the Distinguished Applied Research Award in the University of Tehran. He has published more than 200 papers in reputable academic journals and conferences.

Reza Kokabi is an MSc graduated student from University of Tehran, Iran, in 2015, and finished his BSc degree in University of Tabriz, Iran in 2012. Currently, he is worked in R&D Department of BSI. He is the member of the Talent Office of Iran, and his research interests are Business Process Management, Production Planning, Business Intelligence, Z-numbers, Fuzzy Optimization, and Location Optimization.

Diako Hallaj received his BSc degree in Industrial Engineering from Tabriz University, Iran, in 2013. He was admitted for MSc degree in 2014 and received his degree in 2016 from Iran University of Science and Technology. His favorite study is mathematical modeling, fuzzy programming, and meta-heuristic.