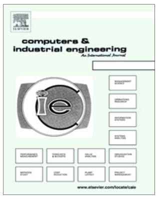
Computers & Industrial Engineering 102 (2016) 219–232

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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



A tri-level covering fortification model for facility protection against disturbance in r-interdiction median problem

Mehdi Mahmoodjanloo[a], Seyed Parsa Parvasi[b], Reza Ramezanian[b,*]

[a] *Department of Industrial Engineering, Mazandaran University of Science and Technology, Behshahr, Iran*
[b] *Department of Industrial Engineering, K.N. Toosi University of Technology, Tehran, Iran*

ARTICLE INFO

Article history:
Received 23 November 2015
Received in revised form 14 October 2016
Accepted 2 November 2016
Available online 5 November 2016

Keywords:
Tri-level programming
r-Interdiction median problem
Complete interdict
Probabilistic protection
Defense facility location
Full coverage
Genetic algorithm
Biogeography-based algorithm

ABSTRACT

The available literature for facility interdiction problems is separately modeled by the two r-interdiction covering and median approaches. In this paper, a tri-level defense facility location model for full coverage in r-interdiction median problem is addressed which considers both modeling approaches, simultaneously. The purpose of this model is to design a proper service system in a way that after a worst case scenario of disturbance, it can utilize its full capacity of providing services. In this regard, we have considered the defense facilities to provide extra protection for service facilities and the purpose is to optimally locate these facilities. The tri-level model is proposed based on leader-follower games as defender-attacker-defender framework. In order to solve the model, three approaches have been used. In the first approach (EX-EX-EX), explicit enumeration method is used for the first and second levels and an exact approach is used for the third level. In the second and third approaches, hybrid methods consisting of genetic algorithm, explicit exact enumeration and exact approach (GA-EX-EX) and biogeography-based algorithm, explicit enumeration method and exact approach (BBO-EX-EX) have been used to tackle the problem in a reasonable time. Finally, the proposed approaches are used to solve 27 random instance problems. Comparing the proposed meta-heuristics and the exact approach and studying the numerical examples solved using these approaches are quite satisfactory.

1. Introduction and literature review

The vital infrastructures have an important role in supply and service systems. As a result, protecting these infrastructures against deliberate disturbance and natural disasters is very important. The vital infrastructures include specific physical assets of a system that losing them will lead to a considerable disturbance in providing service (Aksen, Aras, & Piyade, 2013). Some examples of these assets are: community transport namely bridges, tunnels and railways; emergency departments; power plants and dams; telecommunication towers and/or national symbol which losing them might weaken public spirit (Aksen et al., 2013).

For example, since power plants are one of the vital infrastructures; in case of a military attack, the enemy will seek to damage them in order to damage people and factories. One of its examples is the 1987 attack on Shahid Salimi Neka power plant which considerably damaged the plant. In case of an attack on a power plant, the government will have to spend a lot of time and money in order to allocate the destroyed plant's customers to a new plant. As a result, with respect to the available budget and also the importance of these infrastructures for the government; we have to plan to protect and forficate them. Interdict problems with fortification can be used for modeling these issues in real world.

1.8. The importance of using facility interdiction models

Nowadays the attitude of terrorist organizations has changed. They are longer interested in direct attacks against a country. Instead, they try to cause the maximum damage and disturbance by attacking the vital infrastructures. For example, the 2003 bombing in Istanbul carried out by Al-Qaeda at the British consulate and a Britain bank caused a total of 757 casualties (57 dead and 700 injured). The 2008 attack n telecommunication towers in Afghanistan, the attack on an ambulance in North Ireland in 1999 (Aksen, Akca, & Aras, 2014) are some other examples of these types of attacks. Therefore, the statesmen in different countries and managers in various organizations have conducted numerous researches in order to improve the fortification of their vital infrastructures against deliberate and natural disasters. By providing security and fortification for vital infrastructures, interdiction

[*] Corresponding author.
E-mail addresses: Mehdi.Janloo@mazust.ac.ir (M. Mahmoodjanloo), Parsa.Parvasi@gmail.com (S.P. Parvasi), Ramezanian@kntu.ac.ir (R. Ramezanian).

http://dx.doi.org/10.1016/j.cie.2016.11.004
0360-8352/© 2016 Elsevier Ltd. All rights reserved.

models endeavor to maintain continuity of service for customers in case of intentional and unintentional disturbances.

The interdiction model was first used in network optimization (Wollmer, 1964). In general, interdiction models have numerous applications including the network optimization theory in interdiction supply networks, the vulnerability of power systems, supply chain and logistics system, reliability and military applications which are presented in Table 1.

Interdiction models are used in order to identify the communication paths and/or critical assets in a supply network. Using these models first the system's vulnerability is identified and then a plan for protecting and supporting them is designed. In this paper in a public supply network the location of service facilities are considered as nodes and the communication paths are considered as arcs. If one or more facilities are endangered or destroyed, an excess cost is imposed to the system for production and transportation. In general disturbance in these systems occurs by creating interdiction for nodes and arcs. The available literature for node interdiction can be divided into the two following groups: r-interdiction median models (RIM) and r-interdiction covering models (RIC) (Aksen & Aras, 2012).

1.9. R-interdiction coverage models (RIC) and R-interdiction median models (RIM)

As mentioned, interdiction on nodes is divided into two approach (RIC and RIM). In both of them, the attacker is seeking to interdict the facilities to make the most failures in service system. Also, the defender is seeking to protect these facilities to minimizing network services customers' damage.

A demand is covered when it falls inside the maximum distance, time or line of sight range of a facility. The goal in such facility location problems is to achieve the maximum demand coverage. For example, in the fire station location problem, the stations must be located in a way that demand points fall inside service maximum distance or travel time. As a result, a quick response to a demand from a neighborhood is guaranteed (Church, Scaparra, & Middleton, 2004).

Table 1
The application of interdiction models.

Application	Available literature
The network optimization theory in interdiction supply networks	Wood (1993), Israeli and Wood (2002), Snyder, Scaparra, Daskin, and Church (2006), Matisziw and Murray (2009), Altner, Ergun, and Uhan (2010), Parvaresh, Husseini, Golpayegany, and Karimi (2014)
The vulnerability of power systems	Salmeron, Wood, and Baldick (2004), Motto, Arroyo, and Galiana (2005), Arroyo and Galiana (2005), Alguacil et al. (2014)
Supply chain and logistics system	Lee (2001), Bundschuh, Klabjan, and Thurston (2003), Church et al. (2004), Scaparra and Church (2008a, b), Liberatore and Scaparra (2011), Snyder et al. (2012), Garcia-Herreros, Grossmann, and Wassick (2013), Bricha and Nourelfath (2013), Zhang, Zheng, Zhu, and Cai (2014), Liberatore, Ortuño, Tirado, Vitoriano, and Scaparra (2014)
Reliability	Snyder and Daskin (2005), Lim, Daskin, Bassamboo, and Chopra (2010), Peng, Snyder, Lim, and Liu (2011), O'Hanley and Church (2011), Wang and Ouyang (2013), Li, Zeng, and Savachkin (2013)
Military applications	Pan, Charlton, and Morton (2003), Patterson and Apostolakis (2007)

Church et al. (2004) utilized RIC models in facility interdiction problems for the first time. In their research, they defined the RIC problem as follows: out of P locations for providing service, a subset of R facilities is chosen that losing them will result in the maximum reduction of coverage.

Scaparra and Church (2008a) introduced the maximum coverage problem (MCP). The main assumption in this new interdiction model is to cover the maximum number of destructive interdiction patterns using a specific number of fortifiers. Also Liberatore, Scaparra, and Daskin (2011) proposed the maximum coverage model (MCP) from the perspective of fortifier in the beginning of their paper and then proposed the stochastic maximum coverage model (S-MCP).

Fig. 1 presents an example of RIC problems. In this figure small circles are customers and small squares are facilities. As shown in the figure, the RIC problem consists of a number of supply (facilities) and demand (customers) points and the customers are allocated to facilities. According to figure (1-a), attacker due to constraint's budget in attack to facilities, looking to determine which facilities to interdict to make the most failures in service system. It should be noted that Fig. 1-b is not necessarily an optimal solution.

Also, Church et al. (2004) utilized the RIM model in facility interdiction model for the first time. In their research the model is studied through the interdictor's perspective. In their research the interdictor tries to conduct the worst case of attack against facilities by identifying the most vital facilities which will result in the maximum efficiency reduction of the system.

Church and Scaparra (2007) by introducing the concept of facility fortification and integrating it into the RIM model, proposed the IMF problem. Two approaches for tackling the problem have been proposed by Scaparra and Church (2008a, b). Based on this fortification model, some other researches has have been conducted in this field by adding new assumptions to the problem. Some examples of these assumptions are facility capacity (Scaparra & Church, 2012), Security budged constraint (Aksen, Piyade, & Aras, 2010), random number of possible casualties (Liberatore, Scaparra, & Daskin, 2012; Liberatore et al., 2011) and disturbance spread over a large area (Liberatore et al., 2012).

Losada, Scaparra, and O'Hanley (2012) proposed an uncertainty model for the RIM problem called the stochastic interdiction problem with interdiction intensity levels. In this problem different combinations of interdiction intensity levels are studied. As a result, there will be uncertainty about the system's condition after an attack. The uncertainty in this case means that every facility after the attack will remain with the probability of effective. The main goal here is to identify scenarios and combinations of attacks that will cause the maximum disturbance and the distance from demand nodes to the locations of facilities will maximize. Zhu, Zheng, Zhang, and Cai (2013) studied the r-interdiction median problem with stochastic fortification. The goal of this problem is to identify vulnerable facilities and achieve a strategy to protect them.

In the recent papers, locating the facilities in danger and its effect and future expenses of them have been studied (Aksen & Aras, 2012; Aksen et al., 2013; Medal, Rainwater, Pohl, & Rossetti, 2014). Aksen et al. (2013) tackled the problem of location, fortification and interdiction simultaneously. The most striking innovation of this problem is locating the facilities with regard to the before and after interdiction scenarios simultaneously. Medal et al. (2014) studied a generalized variation of the p-center problem with the objective of minimizing the maximum distance from a demand point to the rth closes located facility.

Alguacil, Delgadillo, and Arroyo (2014), a Tri-level programming model defender-attacker-defender for the pathology of electrical power networks against possible attacks presented. The concept