Reliability Engineering and System Safety 169 (2018) 51–62

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Locating and protecting facilities from intentional attacks using secrecy

Chi Zhang[a,*], José Emmanuel Ramirez-Marquez[b,c], Qing Li[d]

[a] *Department of Industrial Engineering, Tsinghua University, Beijing, 100084, China*
[b] *School of Systems and Enterprises, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030, USA*
[c] *Tecnologico de Monterrey, School of Engineering and Science, Campus Guadalajara, Zapopan, Jalisco, Mexico*
[d] *A.T. Kearney, 227 W Monroe St, Chicago, IL, 60606, USA*

ARTICLE INFO

Keywords:
Facility location
Multi-objective optimization
Intentional attacks
Secrecy
Simultaneous game

ABSTRACT

To preserve continued effective performance of facilities, their protection against intentional attacks needs to be considered while determining optimal facility location solutions. We propose a simultaneous game between a defender and an attacker to study facility protection against intentional attacks while keeping the information about protection resource allocation secret. To deal with the complexity of solving the proposed simultaneous game, we employ an algorithm with necessary adaptations to identify its mixed-strategy Nash equilibrium solution, which is used to evaluate the disruption inflicted by intentional attacks on the efficiency of a facility location solution. The facility location problem with protection against intentional attacks is then modeled as a multi-objective optimization problem, in order to balance the cost of opening facilities and the efficiency of facilities with and without facility failures inflicted by intentional attacks. MO-PSDA, a multi-objective evolutionary algorithm, is employed to solve the proposed multi-objective optimization problem.

1. Introduction

Facilities within a public service system (e.g., hospitals, airports, fire stations, post offices, etc.) or a supply chain (e.g., production facilities, warehouses, distribution centers, etc.) are considered as critical infrastructures due to their criticality for the economic development and social well-being of modern societies [1–5]. Their proper functioning is crucial for providing necessary supplies (e.g., food, water, medicines, etc.) and services (e.g., healthcare, firefighting, transportation, etc.), which are often termed as “lifelines” [4]. However, today, more than ever, these facilities are threatened by intentional attacks as demonstrated by the September 11, 2001 attack, the 2001 mail-based anthrax attacks, and the 2004 Madrid train bombing, to name just a few. Intentional attackers may attack the facilities for a variety of reasons (among these, political advantage).

Thus, there is an increasing interest in developing intelligent cost-effective approaches for locating these facilities and protecting them from intentional attacks. Intentional attackers have been known to be inventive and resourceful in terms of choosing the time, the targets, and the means of attacks [6,7]. Most importantly, attackers can be adaptive to change their attack strategies in response to protection strategies. Thus, the intelligence of the attacker should be fully addressed when developing optimal strategies to protect the facilities. For this purpose and as done in the literature [6–8], we consider the defender and attacker of the facilities as two fully strategic optimizing agents with opposite objectives: while the defender seeks to ensure the functioning of the facilities, the attacker seeks to destroy their functioning ability.

This research is mainly focused on one of the most widely investigated facility location models, the *p*-median problem, which is to locate *p* facilities to serve a given set of demand centers with the objective of minimizing the total demand-weighted distance between each demand center and its closest facility (hereafter, referred to as travel distance, or simply TD) [9–11]. Usually, demand centers are determined by aggregating customers located in close proximity to each other using a grid network or other clustering techniques, to simplify the problem [12]. Each demand center is located at the center of a cell or cluster with its demand equal to the total demand of all the customers within the cell or cluster. As done in the literature, Euclidean distance is used to compute the distance between demand centers and facilities and the path qualities between each pair of facility and demand center are assumed to be the same [9–11].

Existing systems defense and attack models can be categorized according to system structure, defense measures, and attack tactics and circumstances, as described by Hausken and Levitin [13]. The system structure studied in this research is a network of facilities, the defense measure employed is protection, and attack tactics and circumstances are attack against multiple facilities. For a specific configuration of facility locations, a protection/attack strategy is understood as protect-

[*] Corresponding author.
E-mail address: czhang@tsinghua.edu.cn (C. Zhang).

http://dx.doi.org/10.1016/j.ress.2017.08.005
Received 18 January 2017; Received in revised form 3 August 2017; Accepted 3 August 2017
Available online 4 August 2017
0951-8320/© 2017 Elsevier Ltd. All rights reserved.

Notations

I	The set of demand centers
J	The set of potential locations of facilities
i	Index of demand center
j	Index of potential facility location
p	The number of facilities to be located
u	Cycle index of running the algorithm finding Nash equilibrium solution
$\mathbf{z}$	Vector used to represent a facility location solution
$M_{\mathbf{z}}$	Set used to represent facility locations under solution $\mathbf{z}$
j'	Index of element of set $M_{\mathbf{z}}$
$\mathbf{f}$	Vector used to represent a protection strategy
F	Set containing all possible protection strategies
$\mathbf{g}$	Vector used to represent an attack strategy
G	Set containing all possible attack strategies
$d_{ij'}$	Distance between demand center i and facility j'
$x_{ij'}$	Decision variable representing if demand center i is assigned to facility j' (=1), or not (=0).
$\mathbf{s}$	Vector denoting the status of facilities
$\mathrm{TD}(\mathbf{s}\|\mathbf{z}, \mathbf{f}, \mathbf{g})$	Travelling distance under facility location solution $\mathbf{z}$, protection strategy $\mathbf{f}$, and attack strategy $\mathbf{g}$
δ_j	Probability of potential location j appearing in optimal facility location solution, $j = 1, 2, \ldots, \|J\|$
$\wedge$	And operator
$\vee$	Or operator
H	Number of solutions generated at each cycle during running the algorithm
T	Total running cycles of the algorithm
t	Index of cycles during running the algorithm, $t = 1, 2, \ldots,$ T
B	Subset of solutions
E	Set of non-dominated solutions

Acronyms

MO	Multi-Objective
MC	Monte Carlo
TD	Travelling Distance
ED	Expected Damage

ing/attacking a specific subset of the opened facilities with scarce resources.

To understand the disruption an intentional attack can inflict on facilities, Church et al. [4] proposed two models, namely the r-interdiction median problem and the r-interdiction covering problem, to determine the worst case of facility failures, that is to find the subset of r facilities which, when destroyed, would respectively maximize the travel distance and minimize the total coverage of demand centers. Stochastic interdiction median problem was also studied by Losada et al. [14]

Then, problems for determining optimal facility location solutions while taking into account the worst-case facility failures have been generally modeled into Stackelberg games [4,15–18]. In such a game, the planner, viewed as game leader, decides on the locations of p facilities in the first stage and then, the attacker, viewed as game follower, seeks to inflict the highest disruption on the facilities in the second stage. Multiple objectives (e.g. travel distance before and after the worst-case failures) have also been considered by some of this thread of studies by transferring the problem into single-objective optimization problems via weighted-sum approach [15,16].

Although these studies are helpful in revealing the vulnerability of facility networks and optimizing their efficiency under the worst case of facility failures, the possibility of protecting facilities to mitigate disruption and the attacker's ability of being adaptive are not well addressed. To tackle this problem, studies on protecting existing facilities in order to minimize the impact of the most disruptive attack have been conducted [1,19–21]. The problem is also generally viewed as a Stackelberg game, the first stage of which involves the defender's decision about which facilities to protect in order to minimize the disruption to be inflicted by the attacker on the efficiency of facilities. The second stage of the game involves the attacker's decision about which facilities to attack to render the highest disruption to the efficiency, which is usually modeled as the r-interdiction median or covering problem described by Church et al. [4].

However, these studies are solely focused on the protection of existing facilities, without considering the possibility of designing the facility locations that can better withstand intentional attacks. However, the decisions on the locations of facilities are often strategic in nature and the impact of facility location decisions spans a long time horizon [9–11,22]. That is, building those facilities involve large amount of capital resources and it is very costly to change their locations after they have been sited. For example, the locations of facilities, such as hospitals, airports, fire stations and so forth, usually stay unchanged for tens of years. Thus, minimizing the potential damage to facilities under intentional attacks and protection needs to be considered during the process of designing facility locations. To the best of our knowledge, this problem has not been properly addressed yet.

Another drawback of the studies on protecting existing facilities is that, by employing a Stackelberg game, they implicitly assume that the attacker knows, without any uncertainty, which specific facilities have been protected when deciding on the facilities to attack. This situation can be considered as the result of one of the defender's information disclosure policies- full and accurate disclosure. Comparatively, another policy is that the defender keeps such information secret. As a result, the attacker has to move without knowing the protection resource allocation.

Intuitively and as will be proved in Appendix B, secrecy can make the defender better off, under certain situations, compared to full and accurate disclosure. For example, Unmanned Aerial Vehicles (UAVs) have become one of the key national security tools owing to their effectiveness in aerial surveillance, intelligence gathering, and striking enemy targets [23]. When only limited amount of UAVs are available, the defender would prefer to hide the information on which facilities are under the protection of UAVs. This way, it becomes possible that an attack is caught and defeated by UAVs and thus, a better effect of protection can be achieved.

Zhuang and Bier [24] also described several protection measures, under which secrecy is better than full and accurate disclosure, such as a theft game, and onboard air marshals. Nikoofal and Zhuang [25] studied the merits of secrecy over full and accurate disclosure of information. However, they only considered systems with isolated components, and they did not consider mixed-strategy Nash equilibrium solutions.

We are also aware of a thread of studies on the protection of systems with structures fundamentally different from the facility location problems concerned in this research, such as single target [26–28], isolated components [29,30], series systems [31,32], parallel systems [33–35], series-parallel systems [36], voting systems [37,38], etc. Besides the difference of system structures with our research, these studies are also focused on identifying pure-strategy equilibrium and single-objective optimization solution.

To fulfill the current research gaps, this research is devoted to develop a holistic approach to determine optimal facility location solutions, while taking into account the effect of facility protection against intentional attacks using secrecy. To do so, we firstly model the problem of protecting facilities under a specific design from intentional attacks using secrecy into a simultaneous game. The rationale behind this is that in a simultaneous game, each player has to move without knowing their opponents' strategies, like the rock-paper-scissor game or the game of matching pennies. Note that it is not necessary for the two players to move literally at the same time. As long as no players know their oppo-