Reliability Engineering and System Safety 119 (2013) 1–10

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

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

Critical supply network protection against intentional attacks: A game-theoretical model

Naji Bricha, Mustapha Nourelfath *

Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation (CIRRELT), Department of Mechanical Engineering, Université Laval, QC, Canada G1K 7P4

ARTICLE INFO

Article history:
Received 25 November 2012
Received in revised form
25 April 2013
Accepted 3 May 2013
Available online 10 May 2013

Keywords:
Protection
Facility
Attack
Damage
Game theory
Vulnerability
Contest

ABSTRACT

A crucial issue in today's critical supply chains is how to protect facilities against intentional attacks, since it has become unacceptable to ignore the high impact of low probability disruptions caused by these attacks. This article develops a game-theoretical model to deal with the protection of facilities, in the context of the uncapacitated fixed-charge location problem. Given a set of investment alternatives for protecting the facilities against identified threats, the objective is to select the optimal defence strategy. The attacker is considered as a player who tries to maximise the expected damage while weighing against the attacks expenditures. The conflict on facilities vulnerability is modelled using the concept of contest. The vulnerability of a facility is defined by its destruction probability. Contest success functions determine the vulnerability of each facility dependent on the relative investments of the defender and the attacker on each facility, and on the characteristics of the contest. A method is developed to evaluate the utilities of the players (*i.e.*, the defender and the attacker). This method evaluates many expected costs, including the cost needed to restore disabled facilities, the backorder cost, and the cost incurred because of the increase in transportation costs after attacks. In fact, when one or several facilities are unavailable, transportation costs will increase since reassigned customers may receive shipments from facilities which are farther away. The model considers a non-cooperative two-period game between the players, and an algorithm is presented to determine the equilibrium solution and the optimal defence strategy. An illustrative example is presented. The approach is compared to other suggested strategies, and some managerial insights are provided in the context of facility location.

1. Introduction

Many governments have identified critical infrastructures that are, by default, potential targets of terrorist attacks. These infrastructures include critical supply chains, such as those of medical material and subsistence (food or food-related supplies, including bottled water), bulk petroleum, and petro-chemicals. Therefore, a crucial issue in today's supply chains is to protect vulnerable facilities against malevolent acts. Examples of such acts are cybercrimes, destruction, theft, and manipulation of information. The cost of protecting against malevolent acts on critical infrastructures has increased during recent years. However, planning for possible intentional attacks is an enormous financial and logistical challenge. When facilities are critical, industries face a new financial allocation dilemma. On the one hand, the implementation of all the security and protection recommendations when designing new facilities or fortifying existing ones would impose a huge financial burden on industries. On the other hand, it has become unacceptable to ignore the high impact of low probability disruptions caused by intentional attacks. Since it is generally impractical to secure all assets, it is important to optimise the protection of key supply chain facilities.

This article considers the uncapacitated fixed-charge location problem (UFLP) to deal with defence resource allocation. The facility location decisions are very important in supply chain design. The UFLP is a classical location problem and forms the basis of several location models. In this problem, we are given a set of customer locations with known demands and a set of potential facility locations. If we choose to locate a facility at a site, we incur a known fixed location cost. There is a known unit cost of shipping between each facility site and each customer location. The problem is to find the locations of the facilities, and the shipment pattern between the facilities and the customers, to minimise the sum of the facility location and shipment costs, subject to a requirement that all customer demands be satisfied. The additional strategic decision dealt with here is how to allocate optimally the protective resources among the facilities, knowing that these facilities are exposed to external intentional attacks. In other words, given a set of investment alternatives for

* Corresponding author. Tel.: +1 418 6562131x12355; fax: +1 418 6567415.
E-mail addresses: Naji.Bricha.1@ulaval.ca (N. Bricha), Mustapha.Nourelfath@gmc.ulaval.ca (M. Nourelfath).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.05.001

Nomenclature

n	number of facilities in the system
j	jth potential facility location, $j=1, 2, \ldots, n$
i	ith demand location, $i=1, 2, \ldots, u$
h_i	demand at customer location i
f_j	fixed cost of locating a facility at site j
ρ_{ij}	unit cost of shipping between facility site j and customer location i
X_j	binary variable, which is equal to 1 if a facility is to be located at candidate site j, and 0 otherwise
Y_{ij}	fraction of demand at customer location i which is served by a facility at site j
β_j	type of protection for facility j
p	index of protection type, $p=1, 2, \ldots, \beta_j$
B_{jp}	investment effort to protect a facility located at site j using protection type p
b_{jp}	unit cost of effort to protect a facility located at site j using protection type p
$\overline{B_{jp}}$	investment expenditure to protect a facility located at site j using protection type p
π_j	value from $p=1, 2, \ldots, \beta_j$
π_j^{opt}	optimal defence strategy value from $p=1, 2, \ldots, \beta_j$
$\mathbf{P}$	vector of protection strategy, $\mathbf{P}=(\pi_j)$
$\mathbf{P}_{\text{opt}}$	vector of the optimal protection strategy, $\mathbf{P}_{\text{opt}}=(\pi_j^{opt})$
$\mathbf{B}$	vector of investments to protection strategy $\mathbf{P}$, $\mathbf{B}=(B_{j\pi_j})$
$\mathbf{B}_{\text{opt}}$	vector of investments to protection strategy $\mathbf{P}_{\text{opt}}$, $\mathbf{B}_{\text{opt}}=(B_{j\pi_j^{opt}})$
$B_{j\pi_j}$	element of investments vector $\mathbf{B}$
$B_{j\pi_j^{opt}}$	element of investments vector $\mathbf{B}_{\text{opt}}$
λ_{jp}	binary variable λ_{jp} which is equal to 1 if a protection of type p is used for facility j
λ	matrix, $\lambda=(\lambda_{jp})$
α_j	attack type against any facility j
m	index of attack type ($m=0, 1, \ldots, \alpha_j$)
Q_{jm}	attack effort to attack facility located at site j using attack action m
q_{jm}	unit cost to attack facility located at site j using attack action m
$\overline{Q_{jm}}$	investment expenditure to attack facility located at site j using attack action m
ω_j	value from $m=0, 1, \ldots, \alpha_j$
ω_j^{opt}	value from m of the optimal attack strategy
$\mathbf{M}$	vector of attack strategy, $\mathbf{M}=(\omega_j)$
$\mathbf{M}_{\text{opt}}$	vector of the optimal attack strategy, $\mathbf{M}_{\text{opt}}=(\omega_j^{opt})$
$\mathbf{Q}_{\text{opt}}$	vector of attack effort of the optimal attack strategy, $\mathbf{Q}_{\text{opt}}=(Q_{j\omega_j^{opt}})$
$Q_{j\omega_j^{opt}}$	element of attack effort vector $\mathbf{Q}_{\text{opt}}$
μ_{jm}	binary variable which is equal to 1 if a type m attack is used for facility j
$\boldsymbol{\mu}$	matrix, $\boldsymbol{\mu}=(\mu_{jm})$
$\boldsymbol{\mu}_{\text{opt}}$	matrix, $\boldsymbol{\mu}_{\text{opt}}=(\mu_{jm})$
$\nu_{pm}(j)$	destruction probability of a facility j
$\nu_{p\omega_j^{opt}}(j)$	destruction probability of a facility j for the optimal defence strategy
$\boldsymbol{\nu}(\mathbf{P},\mathbf{M})$	matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{M})=(\nu_{pm}(j))$
$\boldsymbol{\nu}(\mathbf{P},\mathbf{M}_{\text{opt}})$	matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{M}_{\text{opt}})=(\nu_{p\omega_j^{opt}}(j))$
c_j	parameter that expresses the intensity of the contest concerning facility j
$C_R(\mathbf{P},\mathbf{M})$	expected cost required to restore the attacked facilities which depends on $\mathbf{P}$ and $\mathbf{M}$
$C_R(\mathbf{P},\mathbf{M}_{\text{opt}})$	expected cost required to restore the attacked facilities which depends on $\mathbf{P}$ and $\mathbf{M}_{\text{opt}}$
R_j	cost required to restore the attacked facility j
k	combinations index, ($k=0,\ldots,2^n-1$)
S_k	combinations of disabled and functional facilities for the facilities
S	set of combinations of disabled and functional facilities, $S=\{S_k\}$
T_k	cost incurred because of the increase in transportation cost when the combination is S_k
B	backorder cost
$\Delta C_{pm}(k)$	attack outcomes of combination k,
$TCI(\mathbf{P},\mathbf{M})$	expected value of the transportation cost increase which depends on $\mathbf{P}$ and $\mathbf{M}$
$TCI(\mathbf{P},\mathbf{M}_{\text{opt}})$	expected value of the transportation cost increase which depends on $\mathbf{P}$ and $\mathbf{M}_{\text{opt}}$
$D(\mathbf{P},\mathbf{M})$	expected damage which depends on $\mathbf{P}$ and $\mathbf{M}$
$U_d(\mathbf{P},\mathbf{M})$	defender expected utility which depends on $\mathbf{P}$ and $\mathbf{M}$
$U_d(\mathbf{P},\mathbf{M}_{\text{opt}})$	defender expected utility which depends on $\mathbf{P}$ and $\mathbf{M}_{\text{opt}}$
$U_a(\mathbf{P},\mathbf{M})$	attacker expected utility which depends on $\mathbf{P}$ and $\mathbf{M}$
$U_{\min}$	defender minimal utility
$U_{\max}$	attacker maximal utility

protecting the facilities, we want to determine how much to invest optimally in defending each facility, while taking into account that both the defender and the attacker are fully optimising agents.

The traditional UFLP assumes that, once constructed, the facilities chosen will always operate as planned. However, if a facility is attacked, it may become unavailable and customers must be served from other facilities that are farther away than their regular facilities. This may lead to excessive additional transportation costs, while it is possible to increase significantly the resilience of the system when attacked by protecting a few key facilities. As major threats in today's world involve strategic attackers, accounting for the viewpoints of both the defender and the attacker has become a necessity.

Even if there is a mature literature on facility design with probabilistic failure of components [3], the possibility of intentional strikes or attacks is not normally taken into account by such a design. Previous papers on facility location and supply chain design models under uncertainty have missed taking into account the attacker as a fully strategic optimising agent. In a pioneering work, the authors of [17] formulated reliability models for facility location to hedge against facility "failures" due, for example, to inclement weather, labour actions, sabotage, terrorism, or changes in ownership. In this model, the critical difference between intentional and non-intentional acts is however neglected. A broad range of models for designing supply chains that are resilient to disruptions is presented in a tutorial by Ref. [18], which reviews more than one hundred papers on the subject. For other reviews on facility location and supply chain design models under uncertainty, see Ref. [12]. The multi-level optimisation model presented in [15] aims at identifying the optimal allocation of limited protective resources across facilities by considering the event of a worst-case loss of a number of facilities. These types of protection models against worst-case disruptions are formulated as tri-level mixed integer programs: the top level problem involves the system planner's decisions about which facilities to secure (defender problem); the intermediate level problem models the worst-case scenario loss of unprotected facilities (attacker model); the bottom level problem reflects the fact that the system users try to operate within the system in an optimal way after the disruption (user model).

Historically, the military has had a long-term interest in identifying critical targets [6,7,20]. Many of these models are