Reliability Engineering and System Safety 123 (2014) 81–90

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Optimal defense with variable number of overarching and individual protections

Gregory Levitin [a,b,*], Kjell Hausken [c], Yuanshun Dai [a]

[a] Collaborative Autonomic Computing Laboratory, School of Computer Science, University of Electronic Science and Technology of China, China
[b] The Israel Electric Corporation Ltd., P.O. Box 10, Haifa 31000, Israel
[c] Faculty of Social Sciences, University of Stavanger, N-4036 Stavanger, Norway

ARTICLE INFO

Article history:
Received 13 June 2013
Received in revised form
3 November 2013
Accepted 4 November 2013
Available online 11 November 2013

Keywords:
Overarching protection
Individual protection
Expected damage
Defense
Attack

ABSTRACT

The article considers a system consisting of identical elements. Each element can be protected individually. The groups of elements can have overarching protection. To destroy an element having both types of protections the attacker must always penetrate/destroy the overarching protection and then destroy the individual protection of the element. Both the attacker and the defender have limited resources. The resources needed to defend and attack the overarching protection are fixed, as is also the number of elements that can be protected by single overarching protection. The defender chooses the number of overarching protections and the number of individual protections within each protected group to minimize the expected damage caused by the attack. The attacker chooses the number of attacked overarching protections and after attacking the overarching protections it chooses the number of attacked elements to maximize the expected damage. The three period minmax game is formulated and an enumerative procedure for its solving is suggested. The influence of the game parameters on the optimal defense and attack strategies is discussed.

1. Introduction

The optimal defensive resource allocation has been intensively studied in the last decade. Examples of works considering resource for various kinds of systems, where the defender maximizes reliability and system safety, and the attacker maximizes an opposite objective, are by Azaiez and Bier [1], Bell et al. [2], [3]), Brown et al. [4], Golany et al. [6], Guikema [7], Guikema and Aven [8], Haimes et al. [10,9], Patterson and Apostolakis [20], Salazar et al. [22]. See Hausken and Levitin [12] for a review.

For many systems a balance has to be struck between protecting individual system elements and protecting the system as a whole. For example, a power generating plant may design protection around its outer boundaries, or may design individual protections to varying degrees of the plant's various components. Similarly, a country may protect its border against other countries (e.g. Chinese wall, US border towards Mexico), a city may design borders towards its surroundings, or assets (e.g. Fort Knox, water production plants) may be protected individually.

Another example of combination of individual and common (overarching) protection is deploying anti-aircraft systems aimed at preventing the airborne attacks on objects located in some area and protecting these objects from strikes individually (by using bunkers, protective casings etc.) Hiding the targets is a special case of overarching protection as without detecting the targets the attacker cannot strike them. Overarching protection can alternatively be referred to as group, collective, or outer protection.

When an attacker attacks a system that has both individual and overarching protection, it destroys the system only if it succeeds in destroying/penetrating the overarching protection and then succeeds in destroying the individual protection. Thus, the defender enjoys the two-layer defense. However deploying the overarching protection may be very costly. Having limited defense resources the defender must distribute them optimally to achieve the lowest possible probability of system destruction.

Early works on the balance between individual and overarching protection have been done by Powell [21] and Haphuriwat and Bier [11]. Powell considered the allocation of defensive resources between target hardening and border security, assuming discrete attacker target choice. Haphuriwat and Bier [11] considered the defender's optimal investment in protecting the targets individually and collectively, assuming a conditional probability of a successful attack determined parametrically by a power-law function. It was assumed that the attacker chooses a single target and spends all its resources on attacking this target. Levitin [15,17] and Levitin et al. [16] analyzed the importance of multilevel protections and their optimal allocation in complex systems. Korczak et al. [13,14], 2007 analyzed multilevel protection against single and multiple destructive factors in multi-state systems. Accounting for strategic attackers, Golalikhani and Zhuang [5] allowed the

* Corresponding author. Tel.: +972 481 837 26; fax: +972 481 837 24.
E-mail address: levitin@iec.co.il (G. Levitin).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.11.001

defender to protect any subset or arbitrary layers of targets due to functional similarity or geographical proximity.

In Levitin and Hausken [18] the first model of overarching and individual protections of pure series and parallel systems with free choice of the attacked and defended elements was considered and the optimal resource distribution between these two types of protections was analyzed. In Levitin et al. [19] the model was extended to the general case of k-out-of-n systems with the damage proportional to the unsupplied demand. Both models considered only systems with single overarching protection. In reality it may be impossible to provide a single overarching protection because this protection can have limited capacity (standard casings, protected premises or bunkers, protected data storage facilities with limited capacity, anti-missile systems covering limited areas etc.). Thus, the defender can distribute the protected facilities into groups and protect these several groups with their overarching protections. In addition, most systems have structure more complex than series or parallel.

In this paper we consider a more general system in which the expected damage depends on the number of destroyed elements and allow the elements to be distributed among different groups with separated overarching protections. In addition we allow the defender to leave some elements without individual protection and analyze the influence of the attacker's ability to detect the unprotected elements on the optimal strategies of the actors.

We assume that deploying each overarching protection requires a fixed defense resource and that each protection has fixed capacity (number of elements it can protect) and vulnerability. Attacking each overarching protection also requires a fixed resource.

We also assume that all the individually protected elements are protected with the same effort as technical or organizational reasons prevent using different individual protections (for example, a contractor can supply only identical individual protections in a reasonable time).

Section 2 presents the model. Section 3 derives the expected damage inflicted by the attack and defines the three period minmax game. Section 4 presents the enumerative procedure for solving the game. Section 5 considers two extreme special cases. Section 6 provides examples of the optimal strategy analysis for different system parameters. Section 7 concludes.

2. The model

Acronyms

OP	overarching (group) protection
IP	individual protection

2.1. Notation

Variable	Description
R, r	total attacker's and defender's resources
X,x	attacker's and defender's resources required to attack and protect each OP
Y,y	relative attacker's and defender's resources required to attack and protect each OP: $Y=X/R$, $y=x/r$
A, a	costs of attacker's and defender's effort unit in individual contest
N	number of elements
n	capacity of each OP (number of elements in each group)
q	number of protected groups
Q	number of attacked OPs, $1\le Q\le q$
V	vulnerability of each OP
z	number of protected elements in each group with OP, $1\le z\le n$
Z	number of attacked elements
m	intensity of attacker–defender contest for each system element (individual contest)
g	defender's effort superiority parameter in the individual contests
c	each element's performance
F	system demand
v	element vulnerability
D	expected damage caused by the attack
w	cost of unsupplied demand unit
W	cost of destroyed element
$\eta=F/c$	ratio of system demand to performance of single element (minimal number of elements needed to satisfy the demand)
$\pi=wF/W$	ratio of cost of totally unsupplied demand F to the cost of destroyed element
b	number of unprotected elements detected by the attacker
Λ_b	probability that b unprotected elements are detected by the attacker
λ	probability that any unprotected element is detected by the attacker

2.2. The model description

The defender has N elements. Each element has performance c. The defender can protect elements individually or can protect groups of n elements with OPs. When the defender's total resource is unlimited, the number of protected groups q can vary from 0 to $\lceil N/n\rceil$. When the defender's total resource is limited the overall resource used for the OPs xq cannot exceed r. From this follows that $q\le\min(N/n,\ r/x)=\min(N/n,\ 1/y)$. In each group the defender protects z out of n elements individually. In the unprotected group it protects all the elements individually, see Fig. 1 (we assume that the defender cannot leave any element without any protection as in this case the attacker can attack all the elements with negligible efforts and destroy all the unprotected elements). Thus, the total number of individually protected elements is $qz+N-qn=N-q(n-z)$ and the total number of elements that have both OP and IP is qz.

Choosing proper q and z allows the defender to flexibly distribute the OP and IP. For example when $q=\lceil N/n\rceil$ all elements are protected by OP (belong to protected groups) and varying z the defender can determine the number of IPs. When $q=\lceil N/n\rceil$ and $z=0$ all the elements are protected by OPs, but no element has IP.

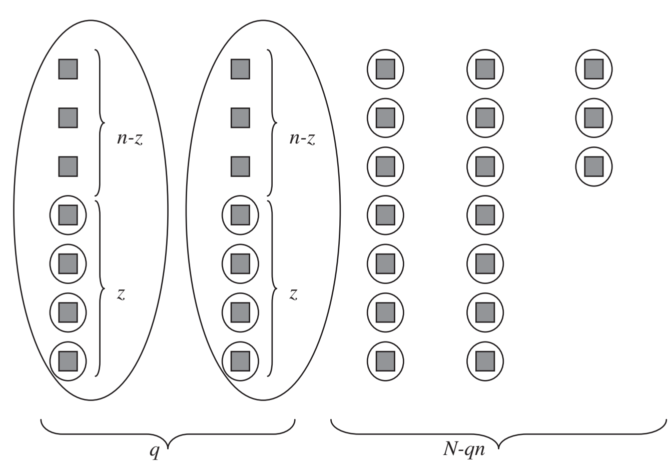

Fig. 1. Overarching and individual protections.