Reliability Engineering and System Safety 94 (2009) 588–595

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

False targets vs. redundancy in homogeneous parallel systems

Gregory Levitin [a,*], Kjell Hausken [b]

[a] The Israel Electric Corporation Ltd., Israel
[b] Faculty of Social Sciences, University of Stavanger, Norway

ARTICLE INFO

Article history:
Received 11 December 2007
Received in revised form
13 May 2008
Accepted 14 June 2008
Available online 18 June 2008

Keywords:
Risk
Demand
Defense
Attack
False targets
Redundancy
Damage
Survivability
Optimization

ABSTRACT

System defense against natural threats and disasters that have a stochastic nature includes providing redundancy and protecting system elements. The defense against strategic intentional attacks can also include deploying false targets aimed at misleading the attacker. Distribution of the available resources among different defensive means is an important problem that arises in organizing the defense of complex civil infrastructures, industrial systems or military objects. The article considers defense resource allocation in a system exposed to external intentional attack. The expected damage caused by the attack is evaluated as system unsupplied demand. The defender distributes its limited resource between deploying redundant genuine elements and false elements, both of which are targets of attack. The attacker attacks a subset of the elements and distributes its limited resource evenly among the attacked elements. Two cases are considered: in the first one the number of attacked elements and the vulnerability of each genuine element are fixed and the defense resource distribution is determined as a solution of an optimization problem; in the second one the number of attacked elements is the attacker's free choice variable and the element's vulnerability depends on a contest determined by the defender's and attacker's resources allocated to each element. The defender's optimal resource distribution strategy is determined as a solution of a two-period minmax game. It is shown that the optimal number of genuine elements decreases monotonically with the growth of the element cost and vulnerability, whereas the optimal number of false elements demonstrates non-monotonic behavior. The contest intensity is an important factor influencing the optimal defense resource distribution. It cannot be ignored when the defense strategy is determined, and it thus also impacts the attack strategy.

1. Introduction

1.1. Motivation

Classical reliability theory considers providing redundancy (increasing the number of system elements) and improving reliability of elements as measures of system reliability enhancement. When survivability of systems exposed to external impacts is concerned, the separation of elements and their protection against the impacts become essential ingredients of the defense strategy. When the external impacts are intentional, additional defense measures aimed at reducing the probability that an element is attacked can be effective. One such measure is deploying false elements (FEs), which are false targets. FEs attract the attacker and it allocates a part of its resource on their destruction. The defender makes a decision about the distribution of the system defense resources among different defensive measures.

In this paper, we consider two main actions available to the defender for reducing the expected damage associated with an attack: deployment of separated redundant genuine system elements and deployment of FEs. The redundancy, facilitated by increasing the number of genuine elements, is aimed at providing the system ability to perform its task when a subset of the system elements is destroyed by an attack. The FEs are aimed at reducing the probability of attacking genuine system elements, under the assumption that the attacker has limited resources and cannot distinguish genuine and FEs. Whether the defender should allocate the major part of its resource toward redundancy or false targets depend on a variety of factors determined in this article.

In [1] the optimal resource distribution between providing redundancy and protecting the system elements was considered. In order to analyze the pure effect of the FEs, this paper assumes that protection of any separated element is fixed and cannot be changed by the defender. This corresponds to many real life situations when standardized protection solutions such as protecting casings, bunkers, anti-missile systems, etc. are used and fixed budgets are allocated to protecting each separated system element.

The paper assumes that a successful attack on each element totally destroys this element. Only damage caused by the attack is

* Corresponding author.
E-mail address: levitin@iec.co.il (G. Levitin).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.06.006

considered without taking into account elements' failures. This simplification allows clearly understanding the interrelation between the redundancy and the FEs.

Examples of systems considered are power generators, water supply systems, telecommunications systems, or more generally any system required to meet a demand. The defender prefers the system to deliver its given performance without damage. The damage can be proportional to the probability of not meeting the demand, or proportional to the amount of unsupplied demand. The attacker prefers to inflict maximum damage by destroying as many system elements as possible. The phenomenon is modeled as a contest between a defender and an attacker over damage. Both agents allocate costly resources to win the contest.

Contests have variable intensity. Low intensity means that neither the defender nor the attacker can easily get the upper hand. This may be due to the lack of decisiveness, fierceness, ability, resources, competence, and due to factors outside the defender's and attacker's control (weather, chance, etc.). High intensity gives significant advantage of slight force superiority over one's opponent, which is a characteristic of "winner-take-all" contests.

Much of risk analysis has traditionally assumed strategic defenders facing a fixed and immutable threat. This suggests a need to proceed further and assume that both the defender and the attacker are fully strategic optimizing agents with different objectives.

1.2. Review of the previous works

The theory of defense against intentional attacks has attracted modest efforts over the last years. It has been common to consider a non-strategic attacker, either by assuming a fixed attack or a fixed attack probability. However, a few contributions have been made, and if we venture outside reliability engineering to economics and political science, accounts of intentional attacks are more common. Starting with the engineering approach, Azaiez and Bier [2] consider the optimal resource allocation for security in reliability systems. They determine closed-form results for moderately general systems, assuming that the cost of an attack against any given component increases linearly in the amount of defensive investment in that component. Bier et al. and Bier and Abhichandani [3,4] assume that the defender minimizes the success probability and expected damage of an attack. Bier et al. [3] analyze the protection of series and parallel systems with components of different values. They specify optimal defenses against intentional threats to system reliability, focusing on the tradeoff between investment cost and security. The optimal defense allocation depends on the structure of the system, the cost effectiveness of infrastructure protection investments, and the adversary's goals and constraints.

Bier et al. [5] assume that a defender allocates defense to a collection of locations, while an attacker chooses a location to attack. They show that the defender allocates resources in a centralized, rather than decentralized, manner, that the optimal allocation of resources can be non-monotonic in the value of the attacker's outside option. Furthermore, the defender prefers its defense to be public rather than secret. Also, the defender sometimes leaves a location undefended and sometimes prefers a higher vulnerability at a particular location even if a lower risk could be achieved at zero cost. Dighe et al. [6] consider secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. Zhuang and Bier [7] consider defender resource allocation for countering terrorism and natural disasters; see also [8–15].

Accounting more fully for strategic interaction, Enders and Sandler [16] provide an overview of the nature of terrorism, and Sandler and Enders [17] evaluate policy effectiveness and quantifies the economic impact of terrorism. More specifically, Arce and Sandler [18] present a model of terrorist attacks as signals where the government is uncertain about whether it faces a politically motivated or militant opponent. They determine two types of ex post regret: P-regret, where the government concedes to political types that would not subsequently attack; and M-regret, where the government does not concede to militant types that subsequently attack at greater levels. They then define a measure of the value of intelligence based on avoiding such regret. Counter-terrorism policy involves whether a government should focus on increased intelligence versus increased security defined as hardening targets. They evaluate the use of asset freezing in terms of the resources required by terrorists to reach objectives. Their article supports the empirical finding of intertemporal substitution of resources by terrorists.

Sandler and Siqueira [19] analyze two anti-terrorism policies when a nation is at risk at home and abroad. The deterrence decision involves external benefits and costs, while pre-emption typically gives external benefits when the threat is reduced for all potential targets. They show that with damages limited to home interests, a country overdeters. In contrast, for globalized terror, a country underdeters. Furthermore, pre-emption is usually under-supplied. They show that leader–follower behavior decreases deterrence inefficiency, but worsens pre-emption inefficiency, compared with simultaneous-choice allocations. Finally, targeted nations can never achieve the proper counter-terrorism policy through leadership.

Siqueira and Sandler [20] analyze a three-stage proactive game with terrorists, elected policymakers and voters. In each of the two countries, a representative voter chooses an elected policy-maker who determines proactive countermeasures to reduce a transnational terrorist threat. The voters' strategic choice is influenced by free riding on the other countries' countermeasures, and limiting a reprisal terrorist attack. Free riding causes low proactive countermeasures which benefit the terrorists. This gives a delegation problem where leadership by voters has a detrimental consequence on the well-being of targeted countries. The authors finally consider how domestic politics impacts how a terrorist threat is addressed.

Siqueira and Sandler [21] show that in many resources-allocation problems, strategic adversaries move sequentially and are likely to have private information about the effectiveness of their spending. It argues, as the current paper also does, that a defender often has to determine its defensive before an attacker decides where to attack. Defenders are also likely to have private information about the vulnerability of the assets they protect. The author argues that sequential decisions and private information about effectiveness causes a dilemma for the defender. Allocating more to a highly vulnerable site reduces the expected losses if that site is attacked, but also draws the attacker's attention, which increases the probability of an attack. Modeling as a signaling game, the analysis shows that secrecy concerns are generally stronger than vulnerability concerns when more vulnerable sites are weakly harder to protect on the margin. This causes the defender to allocate its resources independently of vulnerability. In contrast, if more vulnerable sites are easier to protect on the margin, vulnerability concerns may be stronger than secrecy concerns.

Powell [22] considers a defender's resource distribution against a strategic adversary in four settings. In the first, resources allocated to protecting one site have as a benchmark no effect on other sites. Second, the defender can allocate resources to border defense, intelligence or counterterrorist operations which may