Reliability Engineering and System Safety 165 (2017) 239–256

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Special versus general protection and attack of parallel and series components

Kjell Hausken

Faculty of Sciences, University of Stavanger, 4036 Stavanger, Norway

ARTICLE INFO

Keywords:
Special effort
General effort
Protection
Defense
Attack
Reliability
Vulnerability
Series system
Parallel system
Safety
Security
Terrorism

ABSTRACT

Special and general protection and attack of two components in parallel or series are analyzed in a simultaneous move game. The analysis differs from earlier research which assumes multiple protection levels. Each player chooses either two special efforts, one general effort, or one special effort and one general effort. This combines to 16 solutions expressed analytically and illustrated with examples. The defender prefers the parallel system. The attacker prefers the series system. We quantify how higher contest intensities typically cause higher efforts, how players prefer low unit effort costs, and how players fight for valuable assets. One insight is to clarify how a player is situated in one of these 16 solutions when striking a balance between special and general efforts, or eliminating one or two efforts, while facing an adversary also striking such a balance. In a rapidly changing world, realizing how strategies can be adjusted towards specialization versus generalization becomes increasingly important.

1. Introduction

Components[1] in a system can be protected[2] and attacked[3] individually, or the system as a whole can be protected and attacked. The literature confines attention to two protection layers[4] or arbitrarily many protection layers[5] where protection and attack operate separately on the individual components and each aggregate system.[6] This gives separate contests, vulnerabilities or attack probabilities for the components and each aggregate system. In contrast, this paper focuses on the common instances of one protection layer where such separation is unrealistic.[7] Special and general protection operate additively as joint protection of a component, and special and general attack operate

E-mail address: kjell.hausken@uis.no.

[1] Examples of components are any asset of value including e.g. the 22 target types, each with multiple subtypes, listed in the Global Terrorism Database, www.start.umd.edu/gtd, i.e. business, government (general), police, military, abortion related, airports & aircraft, government (diplomatic), educational institution, food or water supply, journalists & media, maritime (includes ports and maritime facilities), NGO, other, private citizens & property, religious figures/institutions, telecommunication, terrorists/non-state militias, tourists, transportation (other than aviation), unknown, utilities, violent political parties.

[2] Protection means strengthening or hardening the components or otherwise applying means to prevent that they become compromised, stolen or destructed, and ensure that they are operational. Examples are solid casings for electricity generators, particularly designed building materials that sustain various attack scenarios, security personnel, guards, inspectors, patrols, and surveillance officers.

[3] Attack means efforts to break through the protection to compromise, steal or destroy the components, and/or ensure that they are not operational. Nine examples of attack types from the Global Terrorism Database, www.start.umd.edu/gtd, are armed assault, assassination, bombing, facility/infrastructure attack, hijacking, hostage taking, unarmed assault, and unknown. Examples of 13 weapon types, also from the Global Terrorism Database and with subtypes, are biological, chemical, radiological, nuclear, firearms, explosives/bombs/dynamite, fake weapons, incendiary, melee, vehicle, sabotage equipment, other, unknown.

[4] Haphuriwat and Bier [7], Hausken [11,12], Levitin and Hausken [23], Levitin et al. [24], Peng et al. [31], Levitin and Hausken [21,22].

[5] Levitin [19], Korczak and Levitin [18], Levitin et al. [25].

[6] Examples of protecting an aggregate system, i.e. overarching protection, are border security, countering threats from adversaries through intelligence, public health measures such as medical education and immunization, and methods so that a population can withstand e.g. chemical, biological, and explosive terrorism.

[7] For research on one protection layer, see Azaiez and Bier [2], Bier et al. [4], and Brown et al. [6] and Hausken [10,8,9] for series/parallel systems and infrastructures. See Levitin [20] and Hausken and Levitin [15] for element separation and protection in multi-state systems. See Levitin, Xing, and Dai [26] for how users may partition and distribute sensitive data across multiple virtual machines in a cloud environment to prevent co-resident attacks. Bier et al. [3] analyzed protection based on differing measures of target attractiveness. Patterson and Apostolakis [30] assessed importance measures for ranking the system elements in complex systems. Michaud and Apostolakis [29] ranked the elements of water-supply networks. Zhuang and Bier [36] assessed protection against terrorism and natural disasters. Powell [33] considered resource allocation between target hardening and border security. For border security and control weapons of mass destruction, see Avenhaus and Canty [1], Boros et al. [5], Haphuriwat and Bier [7], and McLay et al. [28]. Lin Chen and Leneutre [27] evaluated intrusion detection in heterogeneous networks. See Hausken and Levitin [16] for a review.

http://dx.doi.org/10.1016/j.ress.2017.03.027
Received 12 August 2016; Received in revised form 9 March 2017; Accepted 22 March 2017
Available online 27 March 2017
0951-8320/

Nomenclature

t_i	defender's special protection effort for component i, i=1,2	c	defender's general unit cost of protecting both components
T_i	attacker's special attack effort for component i, i=1,2	C	attacker's general unit cost of attacking both components
t	defender's general protection effort for both components	m_i	contest intensity for component i
T	attacker's general attack effort for both components	m	contest intensity when m_1=m_2=m
r	defender's system valuation, $r\geq 0$	V_i	vulnerability of component i due to special and general protection and attack
R	attacker's system valuation, $R\geq 0$	u	defender's expected utility
c_i	defender's special unit cost of protecting component i	U	attacker's expected utility
C_i	attacker's special unit cost of attacking component i		

additively as joint attack on a component. This gives one contest or vulnerability or attack probability for each component, determined by the special and general efforts, defined as protections or attacks, allocated additively to each component.

This paper considers two components in parallel or series. Each component can be operated upon by one special effort designed particularly for that component, which gives two kinds of special efforts for each of two players, and can additively be operated upon by one general effort directed towards both components. Let us illustrate with examples.

First, assume that one component is human and another component is electrical equipment e.g. at a hospital, firm, agency or institution. One special attack operating only against humans is poisonous gas, and gas masks are a special protection. One special attack operating only against the electrical equipment is to eliminate the power supply, and one special protection is back-up power supply. One general attack operating against both components is explosive dynamite or a missile killing humans and destroying the electrical equipment. One general protection is extensive security including explosive detection dogs or antiballistic missiles.

Second, consider a firm using one computer to handle sensitive personnel information and a second computer to conduct other tasks. The firm can purchase one special firewall, antivirus and cryptography package to protect the first computer, an alternative specialized package to protect the second computer, and/or a joint package to protect both computers. Analogously, a hacker can specialize in attacking computers with sensitive personnel information, computers conducting other tasks, or computers in general.

Third, consider one component located at sea and a second component located on land. Protection and attack are possible by one special naval unit, one special army unit, or one combined unit capable of both sea and land protection and attack.

Fourth, consider a zoo with dangerous animals (component 1) and sophisticated animals (component 2). The zoo can hire one special guard to protect the dangerous animals and a second special guard to protect the sophisticated animals, or one general guard to protect both kinds of animals. The general guard's skill set comprises the two special guards' disjoint skill sets. Analogously, an attacker can specialize against component 1, specialize against component 2, or develop skills to attack both components. Other examples of disjoint skill sets which can be combined are combat experience and negotiation experience, competence in two languages, competence in two different kinds of cryptography, or any division of labor suitable for two components, allocated as efforts towards two components.

These four examples, and many others, cannot be analyzed by the currently available literature since multiple protection layers are not present. Protection and attack are not individual versus overarching where both or multiple layers have to be broken for the attack to succeed. Only one protection layer is present. This one layer is protected and attacked by special and general efforts which are additive. This paper analyzes the 16 possible combinations for how to allocate two special efforts and one general effort by a defender and an attacker. This enables strategic insight into resource allocation into special versus general protection and attack for two components.

The 11 identified references for individual and overarching protection and attack contributed as follows. Levitin [19] confined attention to protection and analyzed arbitrarily many layers for series and parallel systems. He developed a genetic algorithm for minimizing the protection cost subject to a survivability constraint, accounting for attack as external causes and failures as internal causes. Korczak and Levitin [18] analyzed multilevel protection against multiple destructive factors in multi-state series-parallel systems required to meet a demand, accounting for both attack and internal failures. Both Boolean and universal generating function techniques are used. Haphuriwat and Bier [7] considered the defender's optimal investment in protecting targets individually and collectively. They assumed a conditional probability of successful attack determined parametrically by a power-law function. They further assumed that the attacker chooses one target and spends all its resources on attacking this target. Hausken [11,12] analyzed a system of independent components, and combined series/parallel components, all of which can be protected and attacked individually. Hausken [11] showed for both the parallel and series systems that the defender always prefers overarching and individual protection and attack, while the attacker always prefers individual protection and attack. Hausken [12] compared a simultaneous game and a two period game and showed with reasonable assumptions that the defender prefers two protection layers, while the attacker prefers one protection layer. Levitin and Hausken [23] considered a minmax game where a defender and attacker with fixed resources defend and attack series and parallel systems individually and collectively. Levitin et al. [24] scrutinized a system of identical elements which can be protected and attacked individually and collectively. A bi-contest minmax game was designed where a successful attack, breaking through both layers, causes damage proportional to the unsupplied demand plus the destroyed equipment. Levitin et al. [25] generalized to a three period minmax game enabling the defender to choose the optimal number of overarching protections and the number of individual protections within each protected group. The attacker chooses the number of attacked overarching protections and after attacking the overarching protections it chooses the number of attacked elements. Peng et al. [31] applied a universal generating function and genetic algorithm to analyze a parallel system of components which can be unavailable due to internal failures or external impacts. The defender optimizes the system availability, accounting for maintenance cost and unsupplied demand, by adjusting the components' replacement frequency, and individual and overarching protection.

In related research, Levitin and Hausken [21,22] observed that overarching and individual protection and attack have similarities to an intelligence contest followed by an impact contest in a two period game. Both contests have to be won for successful destruction. For systems with redundancy, false targets, and partial protection, if the attacker wins the intelligence contest, it can proceed to attack the individually protected targets. Peng et al. [32] extended this research by assuming that the attacker's intelligence actions may not enable identifying which among one genuine and multiple false targets to