European Journal of Operational Research 000 (2016) 1–10

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Innovative Applications of O.R.

Defense and attack for interdependent systems

Kjell Hausken*

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

ARTICLE INFO

Article history:
Received 25 February 2015
Accepted 15 June 2016
Available online xxx

Keywords:
Reliability
Interdependence
Game theory
Multi-state system

ABSTRACT

Two interdependent targets are analyzed to determine how failure of one or both impacts efforts to protect and attack the targets. If one target fails, the other fails with a certain probability, and vice versa. Examples are a control center and a communications network, two engines on a transport carrier, or an army and a navy. When both interdependence probabilities equal one, the system is in series. This is preferable for the attacker since attacking one target is sufficient. The substitution effect operates and the attacker is sensitive to differences in unit attack costs. When both interdependence probabilities equal zero, the defender benefits from the independence, and substitutes efforts optimally. Increasing the interdependence probability from one target to another causes both players to exert more efforts into the first target. High contest intensities for equally matched players, incurring equal unit effort costs, in an independent system is costly for both players. Otherwise, high contest intensities cause the disadvantaged player to withdraw. A disadvantaged defender can withdraw in an independent system, and a disadvantaged attacker can withdraw in a series system. The article illustrates how the players' efforts and expected utilities depend on the interdependence probabilities and a variety of system characteristics.

1. Introduction

We analyze two targets. The probability that each target operates is its reliability which depends on how it is defended and attacked. Each target can operate or fail causing four states. We model the interdependence between targets such that if one target fails, the other target fails with a certain probability. If both interdependence probabilities are zero, the targets are independent and destroying one does not impact the other. If both interdependence probabilities are one, destroying one target causes the other target to fail causing a series system where the defender needs to protect both targets.[1] Destroying one target may impact the other in varying degrees, and the two interdependence probabilities generally differ. The paper conducts an analysis for intermediate interdependence probabilities to determine the players' efforts and expected utilities.

Two interdependent targets are abundantly present in practice. Examples are a navy and an air force, a command/control center and a communications network, two engines on a transport carrier, two processors on a computer, two entrances to a joint gathering point, animals with two lungs[2] and two kidneys. Common in these examples is that the system operates if both targets operate, fails if both targets fail, and that system operation is unclear if one target fails, which this paper intends to clarify. Since targets interact in multifarious manners, it generally matters which of the two targets fail, depending on the system's objectives and environment. For example, assume a joint air/sea operation where operatives parachute into a sea operation. If the air force fails, analysis may determine that the sea operation to be conducted by the navy is impacted 60 percent (interdependence probability 0.6) since the operatives must be delivered through other means which are only 40 percent as capable of this delivery as the air force. Conversely, if the navy fails, the air force may be impacted only 30 percent (interdependence probability 0.3), since alternative delivery is 70 percent as capable as the navy.

Interdependent systems with multiple states are complex[3] in the sense that they cannot be represented with arbitrarily complex combinations of series and parallel configuration. Some such systems are analyzed as degraded systems. See Ebeling (1997) for a classical approach, Taylor (1980a, 1980b) for Markov

* Tel.: +47 51 831632; fax: +47 51 831550.
E-mail address: kjell.hausken@uis.no

[1] For analysis of interdependence when one defender is assigned to each target, see Enders and Sandler (2003), Hausken (2006), and Kunreuther and Heal (2003).

[2] Sean Swarner climbed the world's Seven Summits (including Mount Everest) and completed an Ironman with one lung.

[3] To handle complexity generally, Simon (1969) suggests "near decomposability". To reduce the number of parameters in complex systems, Azaiez and Bier (1995) apply aggregation. Taylor (1980a) proposes decomposition or enumeration. Hausken (2010) analyzes complex systems using game theory.

http://dx.doi.org/10.1016/j.ejor.2016.06.033
0377-2217/

analysis, and Hausken (2011) for a game theoretic analysis. Multi-state systems have also been analyzed. See Lisnianski and Levitin (2003) and Levitin (2009) for a reliability approach, Zio and Podofillini (2003) and Ramirez-Marquez and Coit (2005) for Monte-Carlo simulations, and Levitin (2007) for optimal element separation and protection in a complex multi-state series-parallel system. For a literature review see Hausken and Levitin (2012).[4]

A literature of interdependence in more complex infrastructures also emerges. Wu, Tang, and Wu (2016) and Chen, Du, Cao, and Zhou (2015) analyze cascading failures in interdependent infrastructures under attacks. Li, Sun, Ma, Wang, and Xia (2015) consider how clustering impacts the attack vulnerability of interdependent scale-free networks. Wang, Wu, and Li (2015) evaluate the attack robustness of a cascading load model in interdependent networks. Wang, Hong, and Chen (2012) analyze the vulnerability of interdependent power and water infrastructures. Johansson and Hassel (2010) analyze the vulnerability of interdependent railway infrastructures. Zhang et al. (2013) assess the robustness of interdependent transportation networks under targeted attack. Wang, Hong, Ouyang, Zhang, and Chen (2013) analyze the vulnerability of interdependent infrastructure systems focusing on the edges of networks rather than the nodes, exemplified by power and gas pipeline systems. Chopra and Khanna (2015) considers the interconnectedness and interdependencies of critical infrastructures in the US economy. Wu et al. (2016) analyze a power network and an oil network subject to terrorist attacks. Ouyang (2014) reviews interdependent infrastructures.

Hausken (2006, 2010) models the interdependence within the contest success function itself, by assuming that the defense of and attack against one target also operates against another target, to an extent specified by a so-called interdependence parameter. This means that if one target receives defense, the other target(s) also benefit(s) from that defense, and if one target is attacked, the other target(s) also suffer(s) an attack. In contrast, this paper keeps the contest success function unchanged, so that only the defense of and attack against each target determines whether that target operates or fails. Instead, the interdependence is conceptualized such that if one target fails, the other target fails with a certain probability known as the interdependence probability, or a fraction of the other target fails.

Section 2 presents the model. Section 3 analyzes the model. Section 4 illustrates the solution. Section 5 suggests how to estimate parameter values. Section 6 presents an example. Section 7 concludes.

2. The model

We analyze a system of two interdependent targets, which we call target 1 and target 2, see Fig. 1.

The defender values the operation of target i at $s_i > 0$, $i = 1{,}2$. The players have different valuations due to different preferences, beliefs, and risk attitudes. The attacker values the failure of target i at $S_i > 0$, $i = 1{,}2$. Destroying one target impacts the other. The interdependence between the targets is such that if target 1 gets destroyed causing state 2, the defender's expected value of target 2 (since target 1 has no value) is $(1-\alpha_{12})s_2$, $0 \le \alpha_{12} \le 1$, where α_{12} is the interdependence probability from target 1 to target 2. The interdependence α_{12} can be interpreted as the probability that target 2 fails when target 1 is destroyed, or that a fraction α_{12} of target 2 fails, which gives a probability $1-\alpha_{12}$ that target 2 operates when target 1 is destroyed, or that a fraction $1-\alpha_{12}$ of target 2 operates. For the attacker in state 2, its expected value is $S_1 + \alpha_{12}S_2$. For state 3, the expected values are $(1-\alpha_{21})s_2$ for the defender and $S_2+\alpha_{21}S_1$ for the attacker, $0 \le \alpha_{21} \le 1$, where α_{21} is the interdependence probability from target 2 to target 1. All parameters are assumed to be common knowledge for both players.

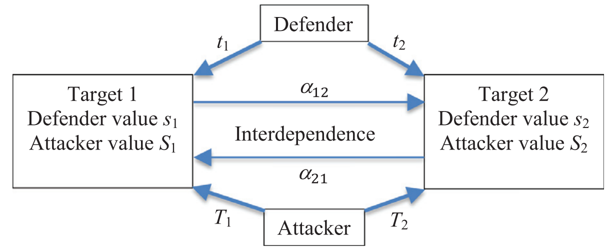

Fig. 1. Game between defender and attacker over two interdependent targets.

The defender exerts effort t_i at unit cost c_i to defend target i. The attacker exerts effort T_i at unit cost C_i to attack target i. Defending means to protect against attack, maintain, repair and ensure that it operates and breakdown is prevented. Attack means the opposite, i.e. destroying, ensuring breakdown or malfunctioning, and thus failure, which may sometimes include stealing the target, and may get aided by technological or natural factors. Ignoring the issue of time to obtain exclusive focus on strategic interaction, the reliability p_i expresses the probability that target i operates, and may be viewed as a contest between the defender and attacker. The most commonly used contest success function is the ratio form (Tullock, 1980), i.e.

$$p_i = \frac{t_i^{m_i}}{t_i^{m_i} + T_i^{m_i}} \tag{1}$$

where $\partial p_i/\partial t_i > 0$, $\partial p_i/\partial T_i < 0$, and $m_i \ge 0$ scales the intensity of the contest.[5] The reliability p_i expresses the probability that target i operates. That is, conflict exists regarding whether reliability should be high or low, similar to conflict between players over who gets a contested object often referred to as a rent. If the defender exerts infinite defensive effort, and the attacker exerts finite offensive effort, target i is completely reliable. Finite defensive effort and zero offensive effort also provides reliability 1. Conversely, if the attacker exerts infinite offensive effort, and the defender exerts finite defensive effort, target i has reliability 0. Finite offensive effort and zero defensive effort also provides reliability 0. Increasing contest intensity m_i makes p_i more sensitive to the efforts t_i and T_i.[6]

We assume that the system of two targets can be in the four states shown in Table 1.

[4] For defense and attack in reliability systems that are generally not interdependent, see Azaiez and Bier (2007) for optimal resource allocation, and Bier, Nagaraj, and Abhichandani (2005), Hausken (2008), and Hausken (2010) for protection of series and parallel systems with targets of different values. See Parnell, Borio, Brown, Banks, and Wilson (2008) and Parnell, Smith, and Moxley (2010) for recommendations of how to address bioterrorism, including modeling terrorists as intelligent adversaries. For various forms of secrecy see Bier, Oliveros, and Samuelson (2007), Zhuang, Dighe, and Bier (2009), Hausken (2014), and Zhuang, Bier, and Alagoz (2010). Hausken and He (2016) analyze protection where an original threat score depends on the terrorist's threat against each target, and a final threat score depends on additional protection.

[5] The contest intensity m_i is a parameter at the contest level, modeling the joint situation and circumstances in which the contenders are embedded, and is thus the same for both contenders for each target. In his axiomatization Skaperdas (1996) applies such a common parameter for multiple contenders for both the ratio form and difference or logit form. See Hirshleifer (1989) and Hausken (2008) for further analyses of these two forms. Results are usually qualitatively similar when using different forms. See Hausken and Levitin (2008), Hirshleifer (1995), and Nitzan (1994), for discussions of the contest intensity.

[6] When $m_i = 0$, t_i and T_i have equal impact on p_i regardless of their size which gives $p_i = 1/2$. $0 < m_i < 1$ gives a disproportional advantage of exerting less effort than one's opponent. When $m_i = 1$, the efforts have proportional impact on p_i. $m_i > 1$ gives a disproportional advantage of exerting more effort than one's opponent, i.e. economy of scale. $m_i = \infty$ gives a step function where "winner-takes-all".