European Journal of Operational Research 243 (2015) 200–210

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Stochastics and Statistics

Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks

Huadong Mo [a,*], Min Xie [a], Gregory Levitin [b]

[a] Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong
[b] The Israel Electric Corporation Ltd., Israel

ARTICLE INFO

Article history:
Received 23 April 2014
Accepted 4 December 2014
Available online 11 December 2014

Keywords:
Vulnerability
Intentional attacks
Truncated normal distribution
Destruction probability
Resource allocation

ABSTRACT

This paper presents a study of the problem of resource allocation between increasing protection of components and constructing redundant components in parallel systems subject to intentional threats. The defender aims at minimizing the entire system destruction probability during certain time horizon by using the best resource allocation strategy which is determined by redundant components construction pace. Different from previous works which focus on the static resource allocation strategy, we propose a dynamic resource distribution strategy with geometric construction pace model and show its advantage over constant construction pace. The vulnerability model considering a most probable attack time and uncertainties of attack time estimates is provided and a destruction probability is evaluated to quantitatively define the ability of the system to survive an intentional attack. The random time of intentional attack is represented by truncated normal distribution. Through the modeling of the most probable attack time and quantifying the uncertainty of the knowledge of defender about this time, the influence of these factors on the optimal resource allocation strategy is investigated. Proper decision regarding the resource allocation is crucial in protecting safety-critical systems, i.e. nuclear power plant, communication base station, power network. Case studies are presented to illustrate the influence and strategy.

1. Introduction

Classical reliability theory has developed advanced strategies for analyzing internal threats (e.g., failures originating from components and performance degradation) and provided novel techniques for improving system reliability (e.g., maintenance, redundancy and protection), see Lu and Meeker (1993), Ye, Shen, and Xie (2012), Xing and Levitin (2013), Wang (2002) and Tillman, Hwang, and Kuo (1977). After the September 11, 2001, terrorist attack and Fukushima nuclear accident, the survivability of system exposed to external threats has attracted increasing concern. Furthermore, the 2006 undersea cable network interruption caused by earthquake in Taiwan, the 2003 America Northeast Blackout and 2010 telecommunication disruption of Visa, PayPal by malicious destruction provide strong evidence that external threats can have transnational influence on society and economy (Bier & Hausken, 2013; Shan & Zhuang, 2013).

The external threats include intentional impacts (Perea & Puerto, 2013) (e.g., terrorist, warfare, intrusion, and human disruption) and unintentional impacts (natural disasters, e.g., earthquakes, tsunami, floods and hurricane and technological impact, e.g., power outage, structural collapse, and network cut-off). Compared to unintentional impacts, analysis of intentional attacks is not a trivial task and the main concern is to propose a framework for investigating the vulnerability of the system under intentional attacks since the behavior model of the intentional attacks has more uncertainty and is still under open discussions (Bricha & Nourelfath, 2013; Ouyang, Zhao, Pan, & Hong, 2014). Finding the most cost-effective risk reduction strategies has always been the essential problem in reliability engineering and risk analysis (Levitin, Xing, & Dai, 2014a). To achieve the optimal risk averting strategy, the defender must strike a balance among different defense measures. Deploying separated redundant components and enhancing protection of existing components is two of such measures (see, for example, Bier, Haphuriwat, Menoyo, Zimmerman, & Culpen, 2008; Levitin, Xing, & Dai, 2014b; Apostolakis & Lemon, 2005; and Levitin & Hausken, 2009).

The techniques for developing defense strategies usually include two sequential steps: evaluation of system vulnerability and determination of risk reduction measures. The system vulnerability model is commonly regarded as a contest between a defender and an attacker over system or its parts, expressed by a contest success function (Bricha & Nourelfath, 2013; Hausken, 2010; Zhang & Ramirez-Marquez, 2013). Analyzing the risk reduction strategies,

* Corresponding author. Tel.: +852 54873365.
E-mail address: huadongmo2-c@my.cityu.edu.hk (H. Mo).

http://dx.doi.org/10.1016/j.ejor.2014.12.006
0377-2217/

most of the researches are focused on forming the mathematical frameworks for static cases.

Azaiez and Bier (2007), and Bier, Nagaraj, and Abhichandani (2005) applied game theory to address optimal defenses against intentional impacts. They yield the best trade-off between defensive investments and the success probability or expected damage caused by an attack for series or parallel systems. They assumed that defender had full information about the contest and that both defender and attacker are strategic. Hausken (2007, 2008, 2013) considered strategic attack and defense for series– parallel system, and concluded that defender/attacker benefits from the parallel/series system. It is more realistic and practical to presume that defender and attacker do not have full information about each other. Examples are imperfect information, false targets and imperfect false targets (Hausken & Levitin, 2009b; Lins, Rego, Moura, & Droguett, 2013; Ma et al., 2013; Peng, Levitin, Xie, & Ng, 2010; Zhang & Ramirez-Marquez, 2013).

A large portion of the current studies consider the contest between defender and attacker, as a static battle. These works are based on the conventional assumption that both contestants can accomplish their entire resource in one-shot effort. Zhuang, Bier, and Alagoz (2010), and Fu and Lu (2012) pointed out that in reality, many contests last for several stages and require contestants to endure a long time, dynamically distributing their resource during time horizon. Taking the time-dependent scenario into consideration, Zhuang et al. (2010), Levitin and Hausken (2010), and Golalikhani and Zhuang (2011) expanded vulnerability analysis and optimal resource allocation into time sequential model. Also, Zio, Sansavini, Maja, and Marchionni (2008), Ramirez-Marquez and Rocco (2012), and Rocco, Ramirez-Marquez, Salazar, and Yajure (2011) introduced dynamic resource allocation in various applications, such as transportation, network system and power system. They considered the optimization problems for an exogenously given resource.

Many aforementioned works assume that the defender and the attacker all have pre-determined total resource budget and derive the optimal resource allocation strategy based on such assumption (Bier et al., 2005; Bricha & Nourelfath, 2013; Wang, Ren, Korel, Kwiat, & Salerno, 2014). However, in reality, even though they have total resource budget, the resource available does not always equal to total resource budget at the beginning of the contest and increases over time. Examples can be found in supply chain transportation, power distribution grid and communication networks where the defender needs time to gather resource to build critical infrastructures or accomplish protection strategy and the attacker also has to gather resource to carry out an attack (Levitin & Hausken, 2011; Zhang & Ramirez-Marquez, 2013).

Thus, it is more reasonable to assume that the defender and the attacker obtain their resources in a stockpiling manner with certain rate over a certain time period. The model of optimal defense with stockpiling resources was first suggested in Levitin and Hausken (2011). It was assumed that the resource stockpiling pace starts at the same time and is constant for both the defender and the attacker. A parallel system where the attacker should succeed in attacking all components to destroy the entire system was considered. The attack time was assumed to be uniformly distributed along a given finite time horizon, which means that the defender has absolutely no information about the attack time.

The models above are all based on the assumption that the attacker does not have any preference in attack time. However, in many situations this is not the case. For example, service systems with multiple servers, power supply grids with multiple power generations, transportation networks, wind farms with multiple wind turbines are characterized by critical events, such as maximal website traffic, peak power demand and largest production capacity (Cedeno and Arora, 2013; Lau and Mcsharry, 2010). Since both agents have full information about each other and causing the greatest damage is the main drive for the attacker, it is reasonable for the attacker to attack the system during the critical event. The attack time is thus believed to be associated with the time distribution of the critical event. Therefore, the attacker can have preferred attack time and the defender can have some information about the most probable attack time, though this information may be uncertain.

The truncated normal distribution is widely used to model the time distribution of the critical event with uncertainties in many models (Cedeno & Arora, 2013; Lau & Mcsharry, 2010; Ramirez-Marquez & Rocco, 2012; Torres, Brumbelow, & Guikema, 2009; Wei, Jin, & Shen, 2012; Yuan, Zhao, & Zeng, 2014). The attack time is usually restricted by lower and upper bounds (for example, by a system mission time or by a time of conflict situation). The truncated normal distribution fits the situations when the uncertain attack time is bounded and ensures that the attack during the time horizon happens with probability 1.

Other distributions have been studied in the previous works. The uniform distribution (Levitin & Hausken, 2011) does not allow taking into account the defender's partial knowledge about the possible attack time. Considering the normal distribution (Cedeno & Arora, 2013) makes the analysis more complicated as it does not consider the time boundary (horizon) and assume unrealistic attack times (though with low probability).

Consider, for example, a service network system that can offer more reliable service by increasing the protection of the existing servers or deploying more servers. The time of the maximal website traffic is modeled by a truncated normal distribution. In order to inflict the maximal damage, the hackers choose an attack time close to the maximal network traffic. This attack time can be modeled by the truncated normal distribution.

Though, complex system can have multiple operational states (Faghih-Roohi, Xie, Ng, & Yam, 2014; Hausken & Levitin, 2009a; Zhang & Ramirez-Marquez, 2013), we assume that an attack is successful only if all system components are destroyed. We focus on studying the influence of uncertain attack time on the system destruction probability, which is determined by the system vulnerability and corresponding attack probability. The system destruction probability over certain time horizon is studied as the measure of current and potential danger under an intentional attack. The defender aims at minimizing the entire system destruction probability over the finite time horizon.

We consider parallel systems such as service network system with several servers, power supply system with transmission lines (Ramirez-Marquez, Rocco, & Levitin, 2011; Yuan et al., 2014). In such systems both agents distribute resource among components evenly if they have full information about each other. This has been shown by Hausken (2007), and Levitin and Hausken (2011). Indeed if, for example, one of components is less protected and the attacker knows this, the attacker can destroy it with less resource, and then concentrates more resources on other targets. Thus, we assume that the attack and protection resources are evenly distributed among system components.

We study the influence of the most probable attack time and the uncertainty of its estimate on determining the constant and geometric construction pace strategies. A comparison between the two strategies is provided, considering the defense costs associated with these strategies.

The remainder of this paper is organized as follows. Section 2 presents the component vulnerability and redundant components construction models. Section 3 studies the influence of the most probable time of the attack on the vulnerability and destruction probability of entire system. Section 4 describes the approach used for evaluating the vulnerability and the destruction probability of the entire system and presents the optimal resource allocation strategies under different truncated normal distributions of the attack time. Section 5 concludes.