Pesquisa Operacional (2014) 34(2): 215-235

Printed version ISSN 0101-7438 / Online version ISSN 1678-5142
www.scielo.br/pope
doi: 10.1590/0101-7438.2014.034.02.0215

DEFENSE-ATTACK INTERACTION OVER OPTIMALLY DESIGNED DEFENSE SYSTEMS VIA GAMES AND RELIABILITY

Isis Didier Lins[1*], Paulo Renato Alves Firmino[2], Diogo de Carvalho Bezerra[3], Márcio das Chagas Moura[1], Enrique López Droguett[1], Leandro Chaves Rêgo[4] and Carlos Renato dos Santos[5]

Received June 21, 2013 / Accepted December 1, 2013

ABSTRACT. This paper analyzes defense systems taking into account the strategic interactions between two rational agents; one of them is interested in designing a defense system against purposeful attacks of the other. The interaction is characterized by a sequential game with perfect and complete information. Reliability plays a fundamental role in both defining agents' actions and in measuring performance of the defense system for which a series-parallel configuration is set up by the defender. The attacker, in turn, focuses on only one defense subsystem in order to maximize her efficiency in attacking. An algorithm involving backward induction is developed to determine the equilibrium paths of the game. Application examples are also provided.

Keywords: Defense systems configuration, system reliability, sequential games of complete and perfect information.

1 INTRODUCTION

System security is a major concern in various sectors of modern economy. Some sectors, such as telecommunications, power generation and transmission, shipping, digital security and even national governments (e.g., national security issues as protection of tropical forests and deposits of fossil fuels) have a strong interest in defending their facilities against intentional attacks. These attacks generate losses and unplanned additional costs, such as fines due to unavailability, (re)investment in security, repairs, social and environmental impacts, reducing profit margins.

*Corresponding author
[1]Centro de Estudos e Ensaios em Risco e Modelagem Ambiental, Departamento de Engenharia de Produção, Universidade Federal de Pernambuco, PE, Brazil. E-mail: isis.lins@ceerma.org
[2]Departamento de Estatística e Informática, Universidade Federal Rural de Pernambuco, PE, Brazil.
[3]Núcleo de Gestão, Centro Acadêmico do Agreste, Universidade Federal de Pernambuco, PE, Brazil.
[4]Departamento de Estatística, Universidade Federal de Pernambuco, PE, Brazil.
[5]Departamento de Matemática, Universidade Federal do Piauí, PI, Brazil.

Thus, the design phase of defense systems may take into account the intelligence of an individual or group of individuals (attacker) that, in order to maximize her utility, tends to circumvent security in order to access a productive system (main system) belonging to the state, to an organization, to an individual or to a group of organizations/individuals (defender). As the attacker, the defender is also interested in maximizing her own utility, but by protecting the main system in order to produce normally, without external interferences. The strategic interaction between intelligent agents (in this case, a defender and an attacker), in which the welfare of each depends not only on their own actions but also on the actions of the others can be formalized by game theory (Mas-Colell et al. [30], Myerson [32], Osborne & Rubinstein [33]).

An effective defense system must be formed by components that work properly at the time in which they are demanded. Thus, in the design of defense systems, not only the rationality characteristics of intentional attacks should be incorporated, but also aspects of reliability of its components. In this context, the intrinsic failures of the defense system components can be modeled using reliability theory (Modarres et al. [31]).

Recent studies have analyzed the strategic interaction between defender and attacker considering various systems, looking forward to incorporating reliability to traditional analysis via games. For example, Bier et al. [2] consider series or simple parallel systems and determine the best way to allocate investments in each system component in order to protect the main system from intentional attacks of intelligent agents. Azaiez & Bier [1], in turn, take series-parallel systems into account, in which the defender minimizes the maximum expected cost associated to a possible attack. In both studies, the probability of successfully defending a particular component depends only on the amount invested in it.

Levitin & Ben-Haim [18] and Hausken & Levitin [11] use the universal generating function (UGF, Levitin [17]) to evaluate the performance of the main system after a possible attack. These authors also consider the separation of components in protection groups in order to hamper the complete damage of the operating system with just one attack. Hausken & Levitin [11] also indicate the type of defense to be used in each protection group. However, these suggestions have two main limitations: i) first, they consider only one alternative for defending the protection group; ii) the possibility of introducing redundancies in order to enhance the performance of the defense system and thus avoid unwanted interventions in the main system is not considered.

Levitin & Hausken [19] compare the efficiency of investment in protection and redundancy of components in the system while Levitin & Hausken [20, 21] evaluate the incorporation of false targets to protect the main components of the system. Other works involving games and reliability are Levitin & Hausken [22, 23, 24].

Haphuriwat & Bier [10], Golalikhani & Zhuang [8] and Hausken [12] evaluate the effectiveness between individual (target hardening) and collective (overarching) protection. From these, only [12] explicitly considers different configurations of the main system (series, parallel or series-parallel) and models a simultaneous move game between defender and attacker. The other two are rather concerned with homeland security.

Overall, the above-mentioned studies present the following shortcomings: i) although some of them focus on determining security investment policies, they do not provide useful information about the real physical configuration that the defense system should have in order to minimize the likelihood of a successful attack – in other words, there is no determination of which components should comprise the system as well as what level of redundancy they should have; ii) in many cases they only suggest the allocation of defense resources for each of the main system components without a further analysis of how such investment should be reversed in concrete defense alternatives; iii) in despite of using some concepts of reliability, the probabilities of proper functioning of defense components are not incorporated into the game modeling.

This paper aims at modeling the strategic interaction between defender and attacker in order to determine configurations for the defense system. More specifically, the focus is to indicate which available components in market must compose the protection barrier as well as the redundancy level of each of them. For this purpose, a hybridism between games and reliability is used and, besides the allocation of investment efforts, series-parallel configurations for the defense system are suggested. They can incorporate different defense alternatives according to an evaluation of their reliability and cost characteristics.

It is assumed that both agents are rational, risk-neutral and have common knowledge about the intentions and possible actions of others; the information is complete and perfect. In addition, the game to be modeled is sequential and finite, consisting of two moves: first, the defender acts through the implementation of a series-parallel defense system and then the attacker acts against a particular subsystem. Both defender and attacker problems are translated into mathematical programming models, in which each of them seeks to optimize their respective payoff functions, taking into account constraints related to budget and others intrinsic to the modeling of the defense system.

An algorithm based on backward induction is proposed and developed to provide the equilibrium paths of the game. The algorithm analyzes all possible configurations of the defense system and returns the one(s) representing subgame perfect Nash equilibria in pure strategy, that is, when there is no interest of any of the agents in taking any other action (either the choice of another defense system by the defender or the attack to another defense subsystem by the attacker). It is further assumed that each component of the defense system has only two possible states: operational or unavailable.

It is worth emphasizing that this work does not intend to present new developments with respect to either game theory or reliability engineering individually. The purpose is to show how their combination can be useful to decision-making. Owners of main systems may use it to optimally design a defense system and attackers may use it to determine where the most profitable regions to attack are located. These aspects are summarized in the proposed backward induction algorithm, which operates essentially as a tool for the decision-maker for choosing the configuration of the defense system and an optimal attack strategy.

The paper is organized as follows. Section 2 introduces important aspects of reliability, games and vulnerability. Section 3 describes the sequential game model as well as the problems of the agents. Section 4 presents the proposed algorithm that uses backward induction to obtain the game equilibrium paths. Section 5 provides two application examples. Section 6 gives some concluding remarks. Figure 1 shows the notation used throughout the paper.

2 Theoretical Background

2.1 Aspects of Reliability Theory

The reliability function can be expressed as the probability of a given system of performing its intended function satisfactorily under specific conditions during a predetermined period of time. Mathematically, it is defined as the probability that the system operates without failures in the range $[0, t]$:

$$R(t) = P(T \geq t | b_1, b_2, \ldots, b_k), t \geq 0, \tag{1}$$

where T is a random variable representing the time before system failure and $(b_1, b_2, \ldots, b_k)$ are operational and environmental conditions of the system. Additionally, the mean reliability on the interval $[0, t]$ is defined as being the average value of the reliability curve for such period of time:

$$R = \frac{1}{t} \int_0^t R(\tau) d\,\tau, t \geq 0. \tag{2}$$

In the context of reliability, block diagrams are commonly used to describe the logical way of how the functioning of components ensure system reliability. It is important to note that block diagrams represent how components are functionally disposed which does not necessarily correspond to their physical configuration (Kuo & Zuo [15]). Figure 2 shows some examples of block diagrams.

In this paper, series-parallel systems are considered. A series-parallel system consists of q ($q \geq 1$) subsystems in series, which in turn are made up of g_i ($g_i \geq 1, i = 1, 2, \ldots, q$) components (identical or not) in parallel. Assuming a series-parallel system with subsystems consisting of not necessarily identical components that operate independently, system reliability is given by:

$$R_S(t) = \prod_{i=1}^{q} \left[1 - \prod_{k=1}^{g_i} (1 - R_{ik}(t)) \right], \tag{3}$$

where $R_{ik}(t)$ is the reliability of the kth component of the ith subsystem.

Among the performance measures provided by the block diagram analysis, minimum cut-sets are a highlight topic. A minimum cut-set is a set of events whose simultaneous occurrence leads to system failure. In the case of series-parallel systems, the failure of all components of any subsystem consists of a minimum cut-set. That is, a series-parallel system becomes unavailable if at least one of its series subsystems fails. As the components of each subsystem are arranged in parallel, a subsystem becomes completely inoperable if and only if all of its components fail. For more details, see Kuo & Zuo [15].

a_i	Attacker action
A_j	Action set of player j ($j = D$ for defender and $j = A$ for attacker)
b	Structure index used in the backward induction algorithm
$b_1, b_2, \ldots, b_k$	Environmental and operational conditions
d_r	rth design of the defense system, defender action
e_j	Effort of player j
g_i	Number of components of the ith defense subsystem
h_{ri}	Terminal history
H	Set of terminal histories
i	Subsystem index
j	Player index
J	Set of players
k	Defense alternative index
ℓ	Number of feasible defense system designs
m	Contest intensity level
n_j	Number of actions of player j
c_k, o_k	Acquisition and operational costs of the kth defense alternative
O_k	Attack cost in acting against the kth defense alternative
p_k	Probability of a successful defense of the kth defense alternative
q	Number of defense subsystems
r	Index of defense system design
$R(t)$	Reliability function
$R_S(t)$	System reliability function
R	Mean reliability
s_A	Strategy of attacker
s_D	Strategy of defender
s	Strategy profile
S	Set of strategy profiles
u, U	Defender and attacker payoffs
v_k	Vulnerability of the kth defense alternative
w_i	Defender resource to invest in the ith defense subsystem
W	Attacker resource
z	Defender gain if the main system is operational
z'	Defender loss if the main system is unavailable
Z	Attacker gain in the case of a successful attack
Z'	Attacker loss in the case of unsuccessful attack
$\phi(d_r, a_i)$	Defender total expected gain with respect to the defense of subsystem i
$\Phi(d_r, a_i)$	Attacker total expected gain with respect to the attack of the subsystem i
$\delta(d_r, a_i)$	Defender total expected loss with respect to the defense of the subsystem i
$\Delta(d_r, a_i)$	Attacker total expected loss with respect to the attack of the subsystem i

Figure 1 – Notation.

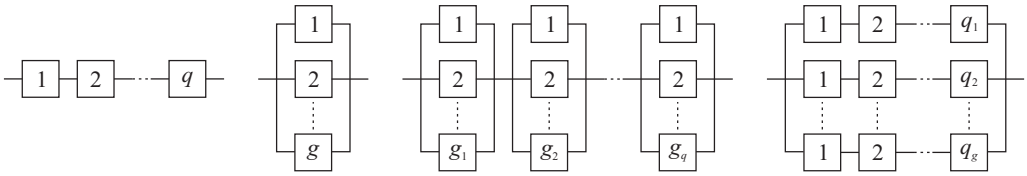

Figure 2 – Examples of block diagrams. From left to right: series, parallel, series-parallel, parallel-series.

In this paper, it is assumed that both attacker and defender are aware of reliability theory and of the minimum cut-sets concept. In this way, the attacker must dedicate all her efforts and resources against at most one subsystem, otherwise she would be inefficient.

In the defense series-parallel system, the ith subsystem is responsible to defend a particular subset of the main system. Thus, the ith defense subsystem itself involves g_i defense components that can be of various types, which eventually leads to a complex combinatorial problem. In fact, the choice of defense systems configurations involving different types of alternatives is a specific case of redundancy allocation problems, which are extensively studied in the context of reliability optimization. In general, a redundancy allocation problem consists on determining the number of components to be allocated in each series subsystem in order to maximize system reliability taking into account cost constraints. There are also recent works that deal with multi-objective redundancy allocation problems, which aim at optimizing reliability and other objectives such as system cost (Taboada et al. [37], Lins & Droguett [26, 27, 28]). For more on redundancy allocation problems, see Kuo et al. [14].

2.2 Basic Concepts of Game Theory

Game theory began with the publication of the book by Von Neumann & Morgenstern, *The Theory of Games and Economic Behavior* in 1944. This publication introduced the idea that the conflict could be formally and mathematically analyzed and provided the terminology for this purpose. Game theory involves the logical analysis of conflicts and cooperations that occur through interdependent strategic interactions. The welfare of a player is determined by her own behavior, as well as by the others'. The essential elements of a game are: players, actions, payoffs, information and order of the game (Finus [5]).

The players (or agents) are the actors who strategically make decisions during the game. In general, there is a finite set J of players. Each player $j \in J$ takes an action. For the present paper, only two players are considered: $J = \{D : \text{defender}, A : \text{attacker}\}$. The set of all possible actions for the defender is $A_D = \{d_1, d_2, \ldots, d_r, \ldots, d_\ell\}$. And, for each d_r, the attacker has the same set of possible actions given by $A_A = \{a_0, a_1, \ldots, a_i, \ldots, a_q\}$. An strategy for the defender, s_D, corresponds to a choice of one of her actions while an strategy for the attacker is a function $s_A : A_D \mapsto A_A$ determining what to do for every possible choice of the defender. A particular combination of players' strategies define a strategy profile $s = \{s_D, s_A\}$. The set of all strategy profiles is denoted by S. Note that each strategy profile determines a sequence

of choices of the players, called a terminal history of the game. Let $h_{ri} = (d_r, a_i)$ represent a terminal history where the defender chooses the action d_r and the attacker chooses a_i. The set of terminal histories is called H.

The hypothesis of rationality is actually an "operational" assumption to allow for the existence of a function that represents the preferences of each player over the payoffs of the potential terminal histories of the game (Campello de Souza [3]). If the individual has a transitive and complete order of her preferences, then it is possible to obtain a function that establishes a relationship of each terminal history $h_{ri} \in H$ with the real line for each player. Such a function is called payoff and its representation is $u : H \mapsto \mathbb{R}$ for the defender and $U : H \mapsto \mathbb{R}$ for attacker in a way that for every terminal history there is a unique payoff associated, $u(h_{ri}) \in \mathbb{R}$ and $U(h_{ri}) \in \mathbb{R}$ (Mas-Colell et al. [30]). In a sequential game, if a strategy profile s implies the occurrence of the terminal history h_{ri}, then it is defined that $u(s) = u(h_{ri})$ and $U(s) = U(h_{ri})$.

A game is said of complete information if all players have knowledge about the other players profiles, including their possible actions and payoffs. On the other hand, a game is of perfect information if each agent, when taking a decision, is fully informed about all events that have previously occurred (Rasmusen [35]). Additionally, in a sequential game, the order of the game refers to the sequence in which players take their decisions and adopt a certain action.

Formally, in a game with two players, the strategy profile (s_D^*, s_A^*) forms a Nash equilibrium if s_A^* is a best response of the attacker given that the defender has chosen s_D^* and s_D^* is a best defender response if the attacker has selected s_A^*. It means that s_D^* must satisfy the condition $u(s_D^*, s_A^*) \geq u(s_D, s_A^*)$ for all $s_D \in A_D$, and s_A^* must satisfy $U(s_D^*, s_A^*) \geq U(s_D^*, s_A)$ for every $s_A : A_D \mapsto A_A$.

A sequential game is characterized by a game tree that begins at a starting node and ends in a terminal node (terminal history). Intermediate and starting nodes are called decision nodes, which are partitioned into information sets. In a sequential game, an information set for a player is a set of decision nodes in which the current player and not another is taking the decision. Such a player knows that she is in a single node of the information set, but without knowledge about which node. In the case of games with perfect information, information sets have only one decision node, not leaving doubts for the player about the node she has reached. In this way, it is important to note that the strategies adopted by the players are pure strategies. A subgame is the part of a sequential game that starts on a decision node and contains all decision nodes that follow the initial one. For further details, see Fiani [4], Finus [5] and Fudenberg & Levine [6].

In general, sequential games can present many Nash equilibria. However, many of them can be based on non-credible threats, which is a choice of a strategy that does not implement a best response for the player in a decision node that is not reached if the Nash equilibrium strategies are used.

A procedure for obtaining some Nash equilibria of a sequential game is called backward or reverse induction, due to the fact that the resolution of the game begins from the last player's actions' analysis until the decision of the first player. In every step of the backward induc-

tion, the current player attempts to identify her best actions. In addition, the backward induction eliminates equilibria based on non-credible threats. When a strategy profile is selected as Nash equilibrium through the backward induction method in a sequential game of perfect information, it is said that it is a subgame perfect Nash equilibrium (Fiani [4], Rasmusen [35]). For more details about sequential games, backward induction and non-credible threats, see Fudenberg & Tirole [7], Myerson [32] and Osborne & Rubinstein [33].

The interdependence between the strategies adopted by the defender and the attacker impacts the payoffs of each of them. In this way, the modeling of the strategic interaction used in this paper (Section 3) is based on a two-move sequential game of perfect and complete information. In other terms, this paper considers a game where the defense system is firstly put into operation and then the attacker may act against it. In addition, the set of equilibrium paths of the game is found by an algorithm (Section 4) that incorporates backward induction.

2.3 Vulnerability

Hann [9] defines system security as the probability that an agent (attacker) does not perform the desired function under given conditions for a certain period of time. A dispute is modeled as a non-cooperative game between multiple agents that make irreversible investments, which can represent money or any other resource of value, depending on the context, to increase their chances of winning the contest and getting a prize (Rai & Sarin [34]). Election campaigns, competition for monopoly, wars, sports and safety systems are some examples of disputes.

In recent works involving reliability and game theory [18, 11, 21, 25], the probability of a successful defense using a particular security alternative in a non-cooperative game with two players has been given by:

$$p_k = \frac{e_{Dk}^m}{e_{Dk}^m + e_{Ak}^m} = \frac{1}{1 + \left(\frac{e_{Ak}}{e_{Dk}}\right)^m}, \tag{4}$$

where e_{Dk} and e_{Ak} are, respectively, the effort to defend and to attack alternative k and m is the dispute intensity (see Levitin & Hausken [25]). Note that p_k can be interpreted as the proportion of the defender effort with respect to the total effort of both agents. Also, the higher the value of m, the higher is the impact of the relative effort on the probability of a successful defense. The complement of the probability p_k is the vulnerability of the kth defense alternative:

$$v_k = 1 - p_k = \frac{e_{Ak}^m}{e_{Dk}^m + e_{Ak}^m} = \frac{1}{\left(\frac{e_{Dk}}{e_{Ak}}\right)^m + 1}. \tag{5}$$

The defender effort can be represented by the cost of acquiring and operating the defense alternative k and the attacker effort, in turn, can be characterized by the investment in attacking alternative k. In this way, the vulnerability expression in Equation (5) becomes:

$$v_k = \frac{O_k^m}{(c_k + o_k)^m + O_k^m} = \frac{1}{\left(\frac{c_k + o_k}{O_k}\right)^m + 1}, \tag{6}$$

where O_k is the unit cost of attacking the defense alternative k, while c_k and o_k are, respectively, the unit cost of acquisition and operation of defense alternative k. In all mentioned works, the probability of a successful defense depends only on the intentional nature of attacks/defenses. However, in order to perform a successful defense, the component should be little vulnerable as well as *reliable*, that is, it should properly function in the moment of attack. Thus, when incorporating the reliability of defense alternative k to Equation (4), the probability of a successful defense becomes:

$$p_k(t) = (1 - v_k)R_k(t). \tag{7}$$

Equation (7) is then used to calculate the probability of a successful attack to subsystem i of the defense configuration r, denoted from now on by $P(d_r, a_i)$ is given by:

$$P(d_r, a_i) = \prod_{k=1}^{g_i}(1 - p_k(t)), \quad r = 1, 2, \ldots, \ell \text{ and } i = 1, 2, \ldots, q \tag{8}$$

and $P(d_r, a_0) = 0$. Equation (8) is used in the calculation of the agents' payoffs, which are presented in the next section along with the mathematical formulation of the defender and the attacker problems.

3 GAME MODELING

The problem consists on deploying a defense system configured in series-parallel with redundant defense components in order to defend a main system from intentional attacks. It is assumed that the strategic interaction takes place with perfect and complete information in two sequential moves: in a first moment, the defender implements a defense system configuration, then the attacker chooses a defense subsystem to attack. It is assumed that both defender and attacker have limited resources.

In order to estimate the reliability under uncertainty about which time the attacker will act against a given defense subsystem, it is considered the average reliability over mission time previously defined, as given in Equation (2). Thus, the reliability is considered constant for the period evaluated, that is, $R_k(t) = R_k$. It is also assumed that the two agents know about systems' reliability and, therefore, the attacker attacks only one defense subsystem with the purpose of making the entire defense system unavailable in order to have free access to the main system.

Defender and attacker are supposed rational and risk-neutral. The risk neutrality assumption is an option to simplify the mathematical handling and is part of an initial analysis of strategic interactions in the context of systems design. The defender has the set of actions (or defense configurations) $A_D = \{d_1, d_2, \ldots, d_r, \ldots, d_\ell\}$, where ℓ is the number of feasible configurations of the defense system. The attacker, in turn, after any choice of the defender has the same set of actions (or possible subsystems to attack) $A_A = \{a_0, a_1, \ldots, a_i, \ldots, a_q\}$, where q is equal to the number of subsystems and a_0 represents "do nothing", that is, the attacker attacks none of the security subsystems. This particular situation can emerge if the attack costs are greater than the available resource or if the attacker payoff is less than the one she would obtain by attacking

any of the defense subsystems. In this case, the probability of a successful attack to any of the defense subsystems – Equation (8) – is set to 0 and the main system is supposed ideal, that is, if no attack is performed against the defense system, the main system is assumed operational and the defender fully obtains the associated production gains. The decisions of the two agents are interdependent, which means that the game is not defined by the choice of just one of them but by a particular combination of strategies chosen by both.

From the choice of strategies by each player, a strategy profile is created and a terminal history (d_r, a_i), $r = 1, 2, \ldots, \ell$ and $i = 0, 1, \ldots, q$ is determined. Thus, the set of all terminal histories is the Cartesian product of each set of actions: $H = A_D \times A_A$. The model of the sequential game of perfect and complete information is illustrated in Figure 3. Note that the information sets, represented by the initial and intermediate decision nodes, are unitary and that the sense of game's resolution is inverse to the order of the players' decisions.

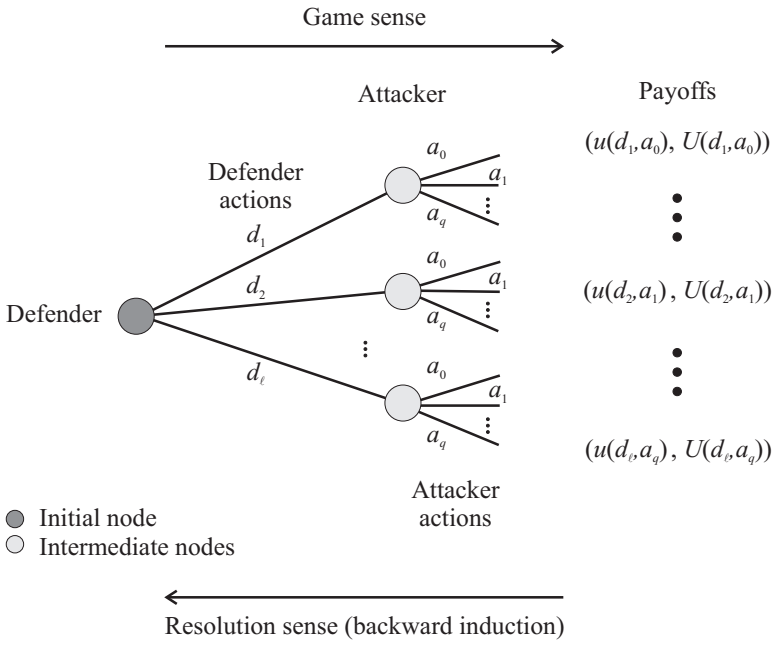

Figure 3 – Game model.

Both attacker and defender are rational agents and seek to maximize their respective payoff functions. The payoff function of each agent involves the difference between the expected total gain and loss related to their choices.

3.1 Attacker Problem

In the case of the attacker, the payoff function is given by:

$$U(d_r, a_i) = \Phi(d_r, a_i) - \Delta(d_r, a_i), \tag{9}$$

where $\Phi(d_r, a_i)$ is the expected total gain, $\Delta(d_r, a_i)$ is the expected total loss related to the attacker choice of a_i, where d_r is the defense system implemented by the defender.

The total expected gain is formed by the expected return of a successful attack $Z \cdot P(d_r, a_i)$ and by the resource available for attack (W):

$$\Phi(d_r, a_i) = Z \cdot P(d_r, a_i) + W, \quad r = 1, 2, \ldots, \ell \text{ and } i = 1, 2, \ldots, q, \tag{10}$$

where Z is the gain if the attack is successful.

The expected total loss is, in turn, the sum of the expected loss due to an unsuccessful attack with the costs of attacking the defense alternatives belonging to the ith subsystem:

$$\Delta(d_r, a_i) = Z' \cdot [1 - P(d_r, a_i)] + \sum_{k=1}^{g_i} O_{ik}, \quad r = 1, 2, \ldots, \ell \text{ and } i = 1, 2, \ldots, q \tag{11}$$

and $\Delta(d_r, a_0) = 0$, where Z' is the loss of the attacker if the attack is unsuccessful; O_{ik} is the cost of attacking the defense alternative k of the ith subsystem. Rearranging Equation (9), to any configuration $d_r \in A_D$ of the defense system, the attacker problem is defined as follows.

Attacker Model

$$\max_{a_i \in A_A} \quad U(d_r, a_i) \tag{12}$$

$$\text{s.t.} \quad \sum_{k=1}^{g_i} O_{ik} \leq W, \quad i = 1, 2, \ldots, q \tag{13}$$

That is, the attacker must choose a subsystem $a_i \in A_A$ in order to maximize Equation (12), taking into consideration constraint (13). If constraint (13) is not active, the related slack is considered as part of the attacker payoff (thus, W is incorporated to Equation (10) as part of the expected gain).

It should be emphasized that the configuration d_r adopted by the defender may be related to a cost that forbids a return greater than W. In these cases, there is no incentive for the attacker to act against any of the defense subsystems and a_0 is chosen. Consequently, the attacker payoff is W itself as an attack will no longer be performed. Since $P(d_r, a_i) \to 0$ as investments in the ith subsystem increases and the attacker is risk-neutral, return Z should be (much) greater than the loss Z' in order to compensate a possible small probability of a successful attack.

3.2 Defender Problem

For the defender, the payoff function is:

$$u(d_r, a_i) = \phi(d_r, a_i) - \delta(d_r, a_i), \tag{14}$$

where $\phi(d_r, a_i)$ is the total expected gain and $\delta(d_r, a_i)$ is the expected total loss of the defender associated to the defense system configuration d_r and to the attacker's option a_i. The expected

total gain $\phi(d_r, a_i)$ is formed by the expected return of the main system when operational and by the total resource available for acquisition of the defense system:

$$\phi(d_r, a_i) = z \cdot [1 - P(d_r, a_i)] + \sum_{i=1}^{q} w_i, \quad r = 1, 2, \ldots, \ell \quad \text{and} \quad i = 0, 1, \ldots, q, \tag{15}$$

where z is the return of the main system when it is operational and w_i is the available resource for investment in the defense of the ith subsystem. The expected total loss is given by the sum of the expected loss due to a well succeeded attack with the total cost of acquisition and operation of the defense system:

$$\delta(d_r, a_i) = z' \cdot P(d_r, a_i) + \sum_{i=1}^{q} \sum_{k=1}^{g_i} (c_{ik} + o_{ik}), \quad r = 1, 2, \ldots, \ell \quad \text{and} \quad i = 0, 1, \ldots, q, \tag{16}$$

where z' is the defender loss when the defense is not well succeeded; c_{ik} is the cost of acquisition of the defense alternative k for the ith subsystem and o_{ik} is the related operational cost.

The parameter z' can be interpreted as the combination of the opportunity cost of the main system, the cost of recovery of the main and defense systems, costs related to the company's image, among others. In general, $z' \geq z$, which means that, if the company is unavailable, it loses at least what it would win if it were operational (opportunity cost).

The defender problem is defined in Equations (17)-(20). It is observed that Equation (17) is obtained after a reorganization of Equations (14)-(16).

Defender Model

$$\max_{d_r \in A_D} \quad u(d_r, a_i^*) \tag{17}$$

$$\text{s.t.} \quad \sum_{k=1}^{g_i} c_{ik} \leq w_i, \quad i = 1, 2, \ldots, q \tag{18}$$

$$g_i \geq 1, \quad i = 1, 2, \ldots, q \tag{19}$$

$$a_i^* = \underset{a_i \in A_A}{\operatorname{argmax}}\, U(d_r, a_i) \tag{20}$$

Thus, the defender must choose a defense system configuration $d_r \in A_D$ in order to maximize the difference between the expected gain and expected loss (Eq. (17)) considering resource constraints (Eq. (18)), as well as the constraints of the minimum number of components in each subsystem (Eq. (19)). Equation (20) is obtained by solving the attacker's problem (Eqs. (12) and (13)). When constraint (18) is not active, the slack is incorporated into the defender's payoff and, for this reason, the sum of resources $w_i, i = 1, 2, \ldots, q$ is part of the total expected gain in Equation (15). It is also emphasized that resources w_i are associated only to the acquisition of the defense alternatives and not to their operation. In this way, Equation (18) involves only the acquisition cost of defense components.

4 RESOLUTION ALGORITHM

In order to solve the sequential game described in Section 3, the backward induction technique has been used. Thus, given a defense system configuration, the attacker decides which is the best strategy to be adopted according to the performance metrics of the underlying block diagram. Once the attacker problem is solved, the strategy that maximizes the defender payoff is evaluated. In this way, the subgame perfect Nash equilibria can be obtained and, consequently, potential non-credible threats are discarded. The game resolution algorithm is shown in Figure 4. The input parameters (line 1) in bold represent vectors. For example, $\mathbf{w} = \{w_1, w_2, \ldots, w_q\}$ is the vector of defender resources, whose elements are associated with each of the defense subsystems.

```
1   procedure BACKWARDINDUCTION(ℓ, q, m, z, z′, w, c, o, Z, Z′, W, O)
2     gEq ← ⟨⟩
3     for r = 1, ..., ℓ do
4       sgEq ← ⟨⟩; p ← ⟨⟩; eq ← ⟨⟩
5       for i = 0, ..., q do
6         p[i] = 1 − P(i); p ← p · ⟨p[i]⟩
7         eq.U = U(r, i) (Eq. (9))
8         eq.a = i
9         if attacker constraint is violated (Eq. (13)) then
10          eq.U = W
11          eq.a = 0
12        if |sqEq| > 0 then
13          if eq.U ≥ sqEq[1].U then
14            if eq.U > sqEq[1].U then
15              sgEq ← ⟨⟩
16            sgEq ← sgEq · ⟨eq⟩
17        else sgEq ← sgEq · ⟨eq⟩
18      end for
19      for b = 1, ..., |sgEq| do
20        sqEq[b].u = u(r, sgEq[b].a) (Eq. (14))
21        sqEq[b].d = r
22        if |gEq| > 0 then
23          if sgEq[b].u ≥ gEq[1].u then
24            if sgEq[b].u > gEq[1].u then
25              gEq ← ⟨⟩
26            gEq ← gEq · ⟨sgEq[b]⟩
27        else gEq ← gEq · ⟨sgEq[b]⟩
28      end for
29    end for
30    return gEq
31  end procedure
```

Figure 4 – Backward induction algorithm.

Each element of vectors $sgEq$ and gEq is a data structure eq consisting of d, u, a and U, which correspond respectively to the defender action, the defender payoff, the attacker action and the attacker payoff. The $sgEq$ vector stores the equilibrium paths of each subgame in which the attacker acts, while the gEq saves the entire game equilibrium paths.

After the construction of the rth feasible configuration of the defense system in accordance with constraints (18) and (19), the probability of a successful defense is calculated for each subsystem i (line 6). The attacker payoff is obtained via Equation (9) (line 7) and the current subsystem i is stored in eq (line 8). Then, the associated constraint is verified (line 9). If it is violated, the attacker payoff is set to the available resource W and the chosen action is "do nothing" ($i = 0$), otherwise they remain the same. Afterwards, $sgEq$ is updated according to the following rules (lines 12-17):

i. If eq presents a payoff value for U greater than the one contained in one (and only one) of the structures already stored in $sgEq$, clear $sgEq$ and add eq to it;

ii. If eq presents a payoff value for U equal to the ones contained in the structures stored in $sgEq$, add eq to $sgEq$;

iii. If $sgEq$ is empty, add eq;

iv. Otherwise, ignore eq.

When all subsystems of configuration r are evaluated in accordance with the attacker perspective, one can move to the defender problem. The defender payoff is calculated for each structure b contained in $sgEq$. The payoff value as well as the defender action (configuration r) are stored in the bth structure of $sgEq$ (lines 20-21). It is important to note that the verification of the defender constraints is not necessary at this point of the algorithm, since they have already been considered in the construction of the defense system configuration. Then, the gEq is updated according to rules similar to those presented on the update of $sgEq$ (lines 22-27). In (i)-(iv) simply replace eq for $sgEq[b]$, $sgEq$ for gEq and U for u. After evaluating all the feasible defense system configurations, the algorithm returns the vector gEq formed by structures that represent the subgame perfect equilibrium paths of the entire game.

It is important to note that different strategy profiles can result the same payoffs for the agents and consequently there can be multiple equilibrium paths. For example, suppose d_1 and d_2 are two possible configurations of the defense system and that $A_A = \{a_0, a_1, a_2\}$ is the attacker's set of actions. Yet, suppose that it is worth attacking, thus a_0 is not a suitable action for the attacker in either configuration. Assume that the payoffs associated with history (d_1, a_1) are u (for the defender) and U (for the attacker). It is possible that the histories (d_1, a_2), (d_2, a_1) and (d_2, a_2) give precisely the payoffs u and U to their respective agents. In the case of a sequential game and of perfect information, agents are indifferent to adopt any actions related to the multiple equilibrium paths. Thus, (d_1, a_1), (d_1, a_2), (d_2, a_1) and (d_2, a_2) are equilibrium paths which result in the same pair of payoffs (u, U); the defender is indifferent whether adopting d_1 or d_2 and the attacker is indifferent between choosing a_1 or a_2 in such cases.

The defense system configurations used in algorithm of Figure 4 are obtained by an exhaustive recursion that returns only feasible designs with respect to constraints (18)-(19). All algorithms have been implemented in C++.

5 APPLICATION EXAMPLES

In this section two examples of application are provided. The first one is greatly simplified and it is solved step-by-step in order to better clarify the resolution algorithm shown in Figure 4. The second example involves a more complex case, with more than five million alternatives of defense configurations. In both examples, the gain due to main system operation and the loss due to its unavailability are considered equal, implying that $z = z'$, and the dispute intensity is $m = 1$. All experiments were run on a PC with Windows operating system, processor of 2 GHz and 2 GB of RAM.

5.1 Example 1

In this example, the defense system consists of two subsystems in series. It is assumed that there is only one defense alternative available, whose characteristics are: $R_1 = 0.9$, $c_{i1} = 1$ monetary unit (m.u.), $o_{i1} = 0.1$ m.u., $O_{i1} = 0.385$ m.u., for $i = 1, 2$.

The defender must choose the defense system configuration by defining the number of redundancies that should be allocated in each of the two subsystems, considering the available amount of resources $w/2$ to invest per subsystem. The attacker, in turn, should select at most one defense subsystem to attack, given the available resource W. For this example: $w = 4$ m.u., $z = z' = 200$ m.u., $W = 0.8$ m.u., $Z = 50$ m.u. and $Z' = 2$ m.u.

In accordance with constraints (18) and (19), there are four feasible configurations for the defense system (see Fig. 5). The vulnerability and the probability of a successful defense for each component are equal to 0.2593 and 0.6667, respectively. Table 1 presents the probability of a successful attack per subsystem for each feasible design (results from Eq. (8)).

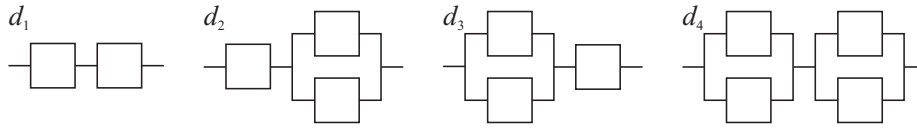

Figure 5 – Feasible configurations for the defense system, Example 1.

Table 1 – Probability of a successful attack per subsystem for d_1 to d_4, Example 1.

Subsystem	d_1	d_2	d_3	d_4
1	0.3333	0.3333	0.1111	0.1111
2	0.3333	0.1111	0.3333	0.1111

The first step is to analyze what happens if the defender opts for d_1. For both subsystems of d_1, the attacker has the same payoff $U(d_1, a_1) = U(d_1, a_2) = 15.75$ m.u.; the defender has also the same payoff whichever subsystem is selected by the attacker $u(d_1, a_1) = u(d_1, a_2) = 68.48$ m.u. Note that the attacker can afford the related costs and that either a_1 or a_2 provide a payoff greater than W. Hence, "doing nothing" is not a plausible action at this step and $u(d_r, a_0)$ need not to be evaluated (Fig. 6-a). In a second moment, d_2 is evaluated and the attacker discards a_0 and a_2, since they result in lower payoffs when compared to a_1. Thus, $u(d_2, a_0)$ and $u(d_2, a_0)$ are not calculated and $u(d_2, a_1) = 67.38$ m.u. However, the profile $s = (d_2, a_1)$ is eliminated by the defender, since the payoffs resulting from d_1 are greater than the one related to d_2 (Fig. 6-b). Analogously, if the defender chooses d_3, then the attacker eliminates a_0 and a_1 and then the history (d_3, a_2) is eliminated by the defender (Fig. 6-c). In the last step, the attacker has payoff $U(d_4, a_1) = U(d_4, a_2) = 3.81$ m.u. (once again "doing nothing" is not interesting for the attacker) while the defender payoff is $u(d_4, a_1) = u(d_4, a_2) = 155.16$ m.u. Thus, the defender eliminates d_1 and the terminal histories (d_4, a_1) and (d_4, a_2) constitute two equilibrium paths for the game and the payoffs associated with them are identical and equal to the ordered pair (155.16, 3.81), see Figures 6-d and 7.

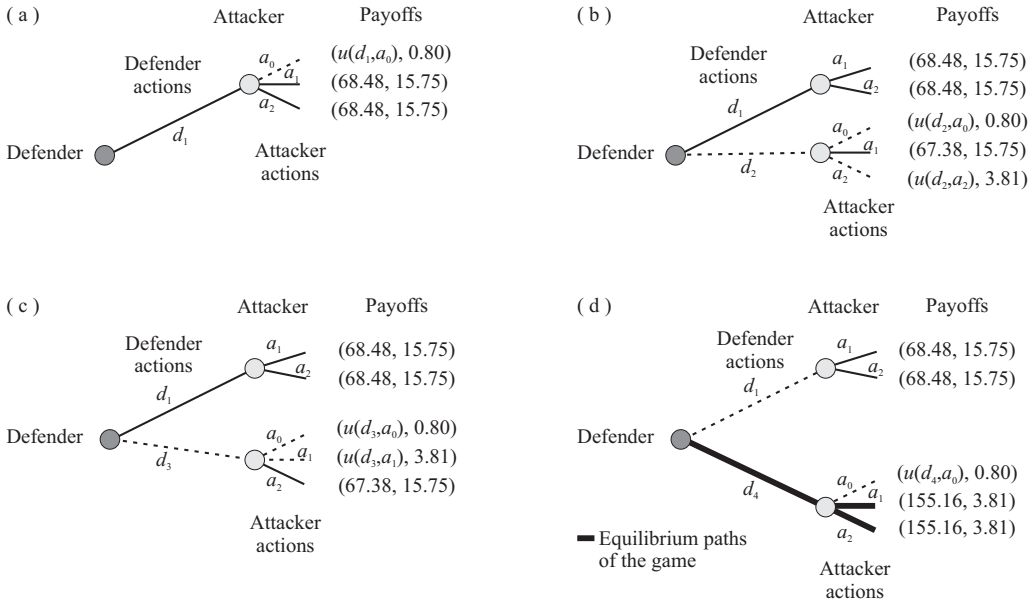

Figure 6 – Game resolution, Example 1.

Table 2 shows the agents' payoffs for each possible history (d_r, a_i), $r = 1, 2$ and $i = 0, 1, 2$. The defender payoffs in italic are additional information, given that their computation are unecessary, as previously commented. The equilibrium paths are also indicated in Table 2.

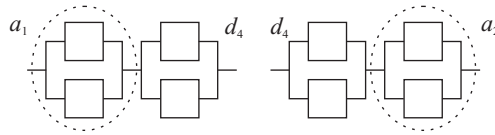

Figure 7 – Equilibrium paths, Example 1.

Table 2 – Payoffs of defender and attacker for each pair (d_r, a_i), Example 1.

Defender action	Attacker action	Defender payoff	Attacker payoff
d_1	a_0	*201.80*	0.80
	a_1	68.48	15.75
	a_2	68.48	15.75
d_2	a_0	*200.70*	0.80
	a_1	67.38	15.75
	a_2	*156.26*	3.81
d_3	a_0	*200.70*	0.80
	a_1	*156.26*	3.81
	a_2	67.38	15.75
d_4^*	a_0	*199.60*	0.80
	a_1^*	**155.16**	**3.81**
	a_2^*	**155.16**	**3.81**

5.2 Example 2

In this example, the defender has interest in creating a defense system with three subsystems in series and it is assumed that each of them can be formed by different combinations of four defense alternatives available in the market. The features of these alternatives are presented in Table 3, in which the costs c_{ik}, o_{ik} and O_{ik} are in m.u. In addition, $w_i = 22$ for $i = 1, 2, 3$, $z = z' = 250{,}000$, $W = 22.50$, $Z = 55{,}000$ and $Z' = 20$ (all values in m.u.).

Table 3 – Characteristics of defense alternatives, Example 2.

Alternative	R_k	c_{ik}	o_{ik}	O_{ik}
1	0.9000	3.0	0.20	1.540
2	0.8917	2.5	0.25	1.925
3	0.9167	4.0	0.37	3.850
4	0.9500	6.0	0.70	4.420

The defender has 5,832,000 feasible configurations for the defense system. The attacker, in turn, can choose one of the three defense subsystems to attack. Note that the amount of feasible configurations is 1,458,000 times greater than for Example 1.

Algorithm of Figure 4 has provided a defense system configuration with four alternatives of type 1 and four alternatives of type 2 in each of the 3 subsystems (Fig. 8). As the defense subsystems are equal, the attacker can choose any one of them to attack. Thus, the outcome of the game consists of three subgame perfect Nash equilibria and the associated payoffs are $u(d, a_1) = u(d, a_2) = u(d, a_3) = 249{,}388.60$ m.u. for the defender and $U(d, a_1) = U(d, a_2) = U(d, a_3) = 55.32$ m.u. for the attacker.

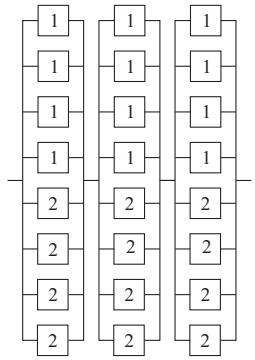

Figure 8 – Selected configuration for the defense system, Example 2.

Suppose that instead of the O_{ik} listed in Table 3, the attacker uses $\alpha \cdot O_{ik}$, where $\alpha = \{0.1, 0.2, \ldots, 0.9\}$. By reducing the attacker effort, the equilibria of the game change, as presented in Table 4. For example, for $\alpha = 0.1$, the defender purchases five alternatives of type 2 and none of the others for every subsystem (subsystems are divided by "|") and the attacker does not attack. The related payoffs are 250,024.75 m.u. and 22.50 m.u. (W) for the defender and the attacker, respectively. Notice that, as the attacker effort decreases, the probability of a successful defense per alternative increases and the attacker tends to not enter the game, since she would have a smaller payoff than the current available resource W. Also, the defender tends to invest in alternatives with lower probabilities of successful defense as the attacker decreases the associated efforts. However, it is important to emphasize that the defense system has to be implemented and, in these cases, it mainly serves to discourage a purposeful attack. Otherwise, if no defense system were adopted, the attacker would have free access to the main system, which is her ultimate objective that the defender attempts to avoid.

6 CONCLUSION

In this work, the problem of designing defense systems has been handled from the perspective of game theory supported by reliability to measure the performance of defense systems and to identify plausible actions for the defender and the attacker. The probability of a successful defense has incorporated not only investments in defense / attack, but also the reliability of the defense alternatives. In this aspect, the approach adopted in this work is more realistic, since the probability of the defense alternative of performing the desired task at the time of a possible attack is taken into account.

Table 4 – Equilibrium paths for different attacker effort levels, Example 2.

α	p_1	p_2	p_3	p_4	d^*	u	a^*	U
0.9	0.6280	0.5471	0.5113	0.5862	4 4 0 0|4 4 0 0|4 4 0 0	249,591.50	1, 2 or 3	34.38
0.8	0.6498	0.5716	0.5377	0.6123	4 4 0 0|4 4 0 0|4 4 0 0	249,994.60	0	22.50
0.7	0.6732	0.5985	0.5670	0.6407	6 1 0 0|6 1 0 0|6 1 0 0	250,000.15	0	22.50
0.6	0.6984	0.6280	0.5997	0.6720	4 3 0 0|4 3 0 0|4 3 0 0	250,002.85	0	22.50
0.5	0.7254	0.6605	0.6364	0.7064	6 0 0 0|6 0 0 0|6 0 0 0	250,008.40	0	22.50
0.4	0.7547	0.6966	0.6778	0.7446	3 3 0 0|3 3 0 0|3 3 0 0	250,012.45	0	22.50
0.3	0.7865	0.7369	0.7251	0.7872	0 6 0 0|0 6 0 0|0 6 0 0	250,016.50	0	22.50
0.2	0.8210	0.7822	0.7794	0.8349	2 3 0 0|2 3 0 0|2 3 0 0	250,022.05	0	22.50
0.1	0.8587	0.8334	0.8425	0.8887	0 5 0 0|0 5 0 0|0 5 0 0	250,024.75	0	22.50

The strategic interaction has been modeled by a sequential game of perfect and complete information and an algorithm based on backward induction has been proposed in order to find the related subgame perfect Nash equilibria. Both agents were supposed to be risk-neutral and future works can incorporate, for example, agents with risk aversion. If the access to the main system signify the occurrence of severe events (e.g., human and environmental accidents), the defender would be risk-averse and her payoff function would change accordingly.

Additionally, situations of incomplete and imperfect information can be considered [36, 29] (e.g. uncertainty about the opponent's financial resources, attacker's lack of knowledge about the reliability of the defense alternatives) as well as games involving more than two moves. For example, Levitin [16] considers a main system with a multilevel configuration [13] and proposes optimal protection groups for one or more of its components to account for their security. Since the component is reached only if all related protection layers are destroyed, the interaction between defender and attacker would take place with more than two moves. Also, if a component is eventually reached by the attacker, the main system not necessarily stops to operate given its multilevel design. In this way, not only a more complex game modeling would be required, but also more elaborated reliability aspects concerning the main system would be necessary.

In this paper, all possible defense system configurations were evaluated by means of an exhaustive recursive algorithm. However, as the quantities of subsystems and / or defense alternatives increase, such an assessment can become prohibitive due to the great number of combinations. In these cases, nature-based heuristics like genetic algorithms can be used in order to find the defender set of actions, as described in Lins et al. [29]. Nevertheless, the proposed backward induction algorithm can be used in the resolution of the strategic interaction of perfect and complete information between defender and attacker despite the method used to obtain the defender set of actions (either exact or heuristic).

ACKNOWLEDGMENTS

The first, fourth, fifth and sixth authors thank the Brazilian Research Funding Agency CNPq for the financial support.

REFERENCES

[1] AZAIEZ MN & BIER VM. 2007. Optimal resource allocation for security in reliability systems. *European Journal of Operational Research*, **181**: 773–786.

[2] BIER VM, NAGARAJ A & ABHICHANDANI V. 2005. Protection of simple series and parallel systems with components of different values. *Reliability Engineering & System Safety*, **87**: 315–323.

[3] CAMPELLO DE SOUZA FM. 2007. *Decisões racionais em situações de incerteza*. Recife, 2 ed.

[4] FIANI R. 2006. *Teoria dos jogos*. Rio de Janeiro: Elsevier, 2 ed.

[5] FINUS M. 2001. *Game theory and international environmental cooperation*. Cheltenham: Edward Elgar.

[6] FUDENBERG D & LEVINE DK. 1998. *The theory of learning in games*. Cambridge: The MIT Press.

[7] FUDENBERG D & TIROLE J. 1991. *Game theory and international environmental cooperation*. Cambridge: The MIT Press.

[8] GOLALIKHANI M & ZHUANG J. 2011. Modeling arbitrary layers of continuous-level defenses in facing with strategic attackers. *Risk Analysis*, **31**: 533–547.

[9] HANN D. 2008. Examination of the interplay of realibility and security using system modeling language. In: *Proceedings of the 55th Annual Reliability & Maintainability Symposium (RAMS)*. Fort Worth, Texas.

[10] HAPHURIWAT N & BIER VM. 2011. Trade-offs between target hardening and overarching protection. *European Journal of Operational Research*, **213**: 320–328.

[11] HAUSKEN K & LEVITIN G. 2009. Minmax defense strategy for complex multi-state systems. *Reliability Engineering & System Safety*, **94**: 577–587.

[12] HAUSKEN K. 2013. Combined series and parallel systems subject to individual versus overarching defense and attack. *Asia-Pacific Journal of Operational Research*, **30**: 1250056 (33 pages).

[13] HE P, WU K, XU J, WEN J & JIANG Z. 2013. Multilevel redundancy allocation using two dimensional arrays encoding and hybrid genetic algorithm. *Computers & Industrial Engineering*, **64**: 69–83.

[14] KUO W, PRASAD VR, TILLMAN FA & HWANG CL. 2001. *Optimal reliability design: fundamentals and applications*. United Kingdom: Cambridge University Press.

[15] KUO W & ZUO MJ. 2003. *Optimal reliability modeling: principles and applications*. Hoboken: John Wiley & Sons.

[16] LEVITIN G. 2003. Optimal multilevel protection in series-parallel systems. *Reliability Engineering & System Safety*, **81**: 93–102.

[17] LEVITIN G. 2005. *The universal generating function in reliability analysis and optimization*. London: Springer.

[18] LEVITIN G & BEN-HAIM H. 2008. Importance of protections against intentional attacks. *Reliability Engineering & System Safety*, **93**: 639–646.

[19] LEVITIN G & HAUSKEN K. 2008. Protection vs. redundancy in homogeneous parallel systems. *Reliability Engineering & System Safety*, **93**: 1444–1451.

[20] LEVITIN G & HAUSKEN K. 2009. False targets efficiency in defense strategy. European Journal of Operational Research. *European Journal of Operational Research*, **194**: 155–162.

[21] LEVITIN G & HAUSKEN K. 2009. False targets vs. redundancy in homogeneous parallel systems. *Reliability Engineering & System Safety*, **94**: 577–595.

[22] LEVITIN G & HAUSKEN K. 2009. Intelligence and impact contests in systems with redundancy, false targets, and partial protection. *Reliability Engineering & System Safety*, **94**: 1727–1741.

[23] LEVITIN G & HAUSKEN K. 2009. Meeting a demand *vs.* enhancing protections in homogeneous parallel systems. *Reliability Engineering & System Safety*, **94**: 1711–1717.

[24] LEVITIN G & HAUSKEN K. 2009. Parallel systems under two sequential attacks. *Reliability Engineering & System Safety*, **94**: 763–772.

[25] LEVITIN G & HAUSKEN K. 2010. Separation in homogeneous systems with independent identical elements. *European Journal of Operational Research*, **203**: 625–634.

[26] LINS ID & DROGUETT EL. 2008. Multiobjective optimization of redundancy allocaion problems in systemas with imperfect repairs via ant colony and discrete event simulation. In: *Proceedings of the European Safety & Reliability Conference (ESREL)*. Valencia, Spain.

[27] LINS ID & DROGUETT EL. 2009. Multiobjective optimization of availability and cost in repairable systemas via genetic algorithms and discrete event simulation. *Pesquisa Operacional*, **29**: 43–66.

[28] LINS ID & DROGUETT EL. 2011. Redundancy allocation problems considering systems with imperfect repairs using multi-objective genetic algorithms and discrete event simulation. *Simulation Modelling Practice and Theory*, **19**(1): 362–381.

[29] LINS ID, RÊGO LC, MOURA MC & DROGUETT EL. 2013. Selection of security system design via games of imperfect information and multi-objective genetic algorithm. *Reliability Engineering & System Safety*, **112**: 59–66.

[30] MAS-COLELL A, WHINSTON MD & GREEN JR. 1995. *Microeconomic theory*. New York: Oxford University Press.

[31] MODARRES M, KAMINSKY M & KRIVTSOV V. 1999. *Reliability engineering and risk analysis*. New York: Marcel Dekker.

[32] MYERSON RB. 1991. *Game theory: analysis of conflict*. Cambridge: Harvard University Press.

[33] OSBORNE MJ & RUBINSTEIN A. 1994. *A course in game theory*. The MIT Press.

[34] RAI BK & SARIN R. 2009. Generalized contest success functions. *Economic Theory*, **40**: 139–149.

[35] RASMUSEN E. 2006. Games and information: an introduction to game theory.

[36] SANTOS CR, LINS ID, FIRMINO PRA, MOURA MDC & DROGUETT EL. 2010. A method for optimal allocation of defensive alternatives: analysis of a strategic interaction with a multi-objective approach. In: *Proceedings of the 10th International Probabilistic Safety Assessment and Management Conference (PSAM 10)*. Seattle, WA, USA.

[37] TABOADA HA, ESPIRITU J & COIT DW. 2008. MOMS-GA: a multiobjective multi-state genetic algorithm for system reliability optimization design problems. *IEEE Transactions on Reliability*, **57**: 182–191.