On the problem of finding the optimal set of computer device protection tools

A A Aletdinova¹,², S A Zinoviev¹

¹ Automated Control Systems department, Novosibirsk State Technical University, 136, Nemirovicha-Danchenko, Novosibirsk, 630073, Russia
² Automated Control Systems department, National University of Oil and Gas «Gubkin University», 65k1 Leninskij, Moscow, 119991, Russia

Abstract. Protecting a computer device is an important task that requires software implementation, because not every user can choose the right set of security features for their device, and there are not many applications that can help a user choose the right set of security features. In this paper, the authors consider the following tools for finding the optimal strategy for protecting a computer device: the method of Savage, Hurwitz, Bayes, Monte Carlo, Thompson Sampling algorithm. Their features and advantages are highlighted. They are based on a software application that will allow users to calculate the optimal combination of tools designed to protect their computers, depending on the wishes of users and the characteristics of their devices. Such an application can be used by system administrators to select the optimal protection of the entire computer fleet. The authors conducted a series of experiments and comparative analysis of the simulation results. The average search time for an optimal strategy for protecting a computer device is estimated.

1. Introduction

The development of information technologies has led to the emergence of threats of information loss. To solve this problem specialists have begun to create various means of protection. However one means of protection may not be enough, a combination of them is required. In our opinion, it is quite difficult to choose the optimal set of security tools, because some of them may conflict with each other, require different amounts of computer resources, or provide an insufficient level of protection.

The vulnerability of software requires the creation of management systems that are resistant to external influences, which will not only resist threats, but also recover online. Scientists have described the robustness metrics to create fault-tolerant systems [2, 3], and indicators of the stability of control systems [4-7]. However there are other approaches to the assessment and selection of means of protection. Thus, scientists use the methods of hierarchies and target programming [5]. Their disadvantage is in a large number of variables, but they allow making decisions when searching for the optimal set of security features for a computer device. Another approach is based on game theory. In the game methods, the problems of protecting a computer device are considered, i.e. situations where attackers seek to cause maximum damage to the system, and a user / administrator tries to reduce the damage. Game theory has found applications in communications, networks and signal processing. This toolkit has become useful for solving many problems [6-9]. Solving the game theory problem can make it easier for users and administrators to find the best combination of security features.

The relevance of the research lies in the need to select and implement mathematical tools of game theory for application to the problem of finding the optimal set of computer device protection tools.
2. Problem Statement

2.1. Game Description. The participants in the game are a hacker and a user (or security administrator). You need to define a set of means of defense and attack. Let the user have \( S \) means of protection \( d_1, d_2, \ldots, d_S \), each of which has a corresponding price \( g_1, g_2, \ldots, g_S \) and protection efficiency \( e_i = (e_{i1}, e_{i2}, \ldots, e_{iK}) \) (\( i = 1, \ldots, S \)), where \( e_{ij} \) is the effectiveness of the \( i \)-th means of protection to neutralize the \( j \)-th threat. Based on the set of defense and attack tools, attack and defense strategies are developed. Let a hacker have \( K \) strategies for attacking a computer system \( a_1, a_2, \ldots, a_K \), each such strategy \( a_j(j = 1, \ldots, K) \) is the \( j \)-th threat that can disrupt the computer system. Each method of attack \( a_j(j = 1, \ldots, K) \) corresponds to the damage \( l_j \) that the administrator suffers if this attack is successful.

The administrative strategies are \( y_i = (z_{i1}, z_{i2}, \ldots, z_{i\beta}) \), where \( z_{ij} = 1 \), if the \( d_j \) protection method is involved, and \( z_{ij} = 0 \) otherwise. The task of the security administrator is to find the optimal set of protections. The hacker's goal is to cause maximum damage to the computer system.

Next, based on the formed attack and defense strategies, we will make a payment matrix \( C \), the elements of which are the administrator's losses in the case when he used the strategy \( y_i(i = 1, \ldots, M) \), and the hacker carried out the attack \( a_j(j = 1, \ldots, K) \).

The goal of the game is to find the optimal strategy for protecting a computer device.

2.2. About choosing the optimal set of computer device protection tools. The process of protecting the data of a computer device from intruders is an important task, during which user data will remain safe and the stable operation of the computer device will be maintained.

There are different approaches to the choice of the optimal set of computer system protection tools. In the simplest case, we can choose a strategy that minimizes the hacker's benefit. In some cases, other criteria can be used to select the optimal set of protection tools, for example, the criteria: Savage, Bayes, Hurwitz.

2.2.1. Savage's criterion of extreme pessimism. According to the Savage criterion, the optimal strategy is chosen, which in the worst conditions guarantees the maximum win. For the defender, the maximum benefit will be to minimize the damage caused to the computer system. Therefore, according to Savage's criterion \( W_f(A) = \max a_{ij} \), the defender chooses a strategy in which the smallest win is the largest among the smallest wins among all strategies. So, the optimal strategy is \( W_f = \min_j \max_i a_{ij} \).

2.2.2. Bayes maximum expectation criterion. The Bayes criterion assumes that the defender knows the probabilities \( p_i \) with which the attacker will apply his strategies. So \( W_f(A) = \sum_{i=1}^{n} p_i a_{ij} \), where \( a_{ij} \) is an element of the game matrix, denoting the damage inflicted by the attack with the number \( i \) on the defense with the number \( j \). Optimal strategy: \( W_f = \min_j \sum_{i=1}^{n} p_i a_{ij} \).

2.2.3. Hurwitz criterion of pessimism-optimism. This criterion occupies an intermediate position between the criteria of extreme pessimism and extreme optimism. According to the criterion: \( W_f(A) = c \max_i a_{ij} + (1-c) \min_i a_{ij} \), where \( c \in [0, 1] \) – pessimism coefficient. Extreme pessimism is a situation in which \( c = 1 \), and extreme optimism is a situation with \( c = 0 \), when the bet is made on the maximum possible win.

2.2.4. Upper confidence bound algorithm (UCB). To speed up the search for the optimal defense strategy with a huge number of defenses and attacks, we can use the Monte Carlo statistical testing method. With a large number of tests, this method allows finding a solution to the matrix game with a sufficiently high accuracy and gives a significant gain in time, since its complexity is linear.

The implementation of the Monte Carlo algorithm consists in finding several solutions with sequential statistical processing of the obtained data. This is done to find an objective and sustainable solution. This algorithm runs as follows: for each defender strategy \( y_i(i = 1, \ldots, M) \), \( N_{y_i} \) simulations with randomly selected attacks are performed, after which, for the resulting loss calculation results \( (x_{y_i1}, x_{y_i2}, \ldots, x_{y_iM}, \ldots, x_{y_iN_{y_i}}) \), their average values are calculated for each defender strategy: \( \bar{x}_{y_i} = \frac{1}{N_{y_i}} \sum_{j=1}^{N_{y_i}} x_{y_ij} \).

With the increase in the cost of \( N_{y_i} : M \bar{x}_{y_i} \rightarrow W_f(C) \) at \( N_{y_i} \rightarrow \infty \).
The criterion for the choice of the optimal strategy of the defender can be the choice of the strategy \( y_0 \), for which \( \bar{x}_{y_0} = \min_i \bar{x}_{y_i} \). This means that the strategy is chosen for which the average value of the results of the loss simulation is minimal.

To minimize losses, an upgraded Monte Carlo algorithm, called YCB1 (Upper-Confidence-Bound), is used. This algorithm is executed in \( n \) steps, where \( n \) takes values on the set \( \{1, 2, ..., N\} \), where \( N \) is the number of simulations. In the first step, \( M \), simulations are performed, one simulation for each defender strategy \( y_i \). In the following steps, \( x_{y_i} \) is modeled for \( y_i \), a strategy for which the minimum value is:

\[
\bar{x}_{y_i} = b \cdot \frac{2 \ln n}{n_{y_i}},
\]

where \( \bar{x}_{y_i} \) – average losses of the computer system when using the defender's strategy \( y_i \);

\( n_{y_i} \) – the number of simulations already performed for \( y_i \) strategies;

\( b \) is a constant used to set the desired balance between the width and depth of the search. The larger it is, the more often options will be considered for which the average losses of the computer system at the moment are not minimal. By selection, it was found that the optimal value of this constant is 5000, which allows the algorithm to work without errors. At other values of the coefficient, the algorithm performed worse.

### 2.2.5. Thompson Sampling Algorithm

The operation of this algorithm is based on the use of the beta distribution of a random variable, the probability density of which is concentrated on the interval \([0; 1]\), equal to \( f(x, \alpha, \gamma) = \frac{x^\alpha (1-x)^\gamma - 1}{B(\alpha, \gamma)} \), where \( B(\alpha, \gamma) = \int_0^1 x^\alpha (1-x)^\gamma dx \) is beta function [10].

Starting from the values \( \alpha_i = 1 \) and \( \gamma_i = 1 \), at which the beta distribution coincides with a uniform distribution, for each defense strategy \( i \), the value of the hypothetical probability of its choice \( p_i \) is determined as the result of a random variable test. At each iteration, a random attack is selected, the worst security administrator protection strategy with the largest damage \( Q_{RSF} \) and the best strategy with the smallest damage \( Q_{R&} \) from the payment matrix are searched. After that, the hypothetical probabilities \( p_i \) of the protection strategies \( i \) is determined as the result of testing a random variable having a beta distribution with new parameters.

### 3. Results

Based on the described game-theoretic approach, an application is created that calculates the optimal defense strategy from the available software products available to the security administrator according to one of the criteria implemented in it: Bayes, Savage, Hurwitz or Monte Carlo methods and the Thompson Sampling algorithm based on the entered values of RAM and system bit depth and the probabilities of hacker attacks. Figure 1 shows the interface for the creation of a matrix game that involves 18 defenses and 14 types of threats.

Moreover, two fields are used for entering data: the system bit rate (values 32 or 64) and the size of RAM. These are the parameters that are taken into account when searching for the optimal protection strategy, they are entered automatically and manually. Software products are selected, from which, after clicking on the “Create” button, players’ strategies are obtained. The "Probability" column in the attack table can be filled in automatically or manually. An example of a game matrix is shown in Figure 2.
If the Bayes criterion was used with approximately the same attack probabilities, and the optimism coefficient used in the Hurwitz criterion was equal to one, we can conclude that the results of the search for the optimal strategy using the Bayes, Hurwitz, Savage and Monte Carlo criteria coincided. The result of the search for the optimal protection strategy using the Thompson Sampling method coincided with the result obtained using the Monte Carlo method. The authors conducted 10,000 matrix games, the calculation results of which were obtained using the Monte Carlo and Thompson Sampling methods. The number of iterations for both methods is 10,000. The results of the Monte Carlo method did not match the results of the Savage criteria in 107 cases, while the results of the Thompson Sampling method were more accurate, they did not match the results of the Savage criterion in 6 cases. The average search time for the optimal protection strategy obtained using the Monte Carlo method is 39 milliseconds, while the same indicator when using the Thompson Sampling method is 50 milliseconds.
The method is 28 milliseconds. The influence of the probabilities of hacker attacks on the search for the optimal strategy using the Bayes criterion was studied. If the probabilities of the most unprofitable attacks for the system administrator are minimal, then the result of the search for the optimal set of defenses was a strategy that does not have the highest degree of security, this is due to the fact that the most unprofitable attacks were no longer such due to the low frequency of their occurrence. If the probabilities were approximately equal, or the probabilities of the most unprofitable attacks were much greater than the probabilities of hacker threats that did not cause much damage to the system administrator, the result using the Bayes test did not differ from the results obtained using the Savage and Hurwitz test with an optimism coefficient of one.

4. Conclusions
Thus, the criteria for finding the optimal strategy for protecting a computer device were considered: the method of Savage, Hurwitz, Bayes, Monte Carlo, Thompson Sampling algorithm and their advantages in a particular situation. The authors created a program that would facilitate the work of the security administrator and users. It allows conducting a comparative analysis of the results of modeling security features.

References
[1] Zhu Q and Basar T 2015 IEEE Control Systems Magazine 35(1) pp 46-65
[2] Ding K, Dey S, Quevedo D E and Shi L 2017 Control Systems Letters IEEE, vol 1(1) pp 146-151
[3] Renganathan V and Summers T 2017 Proc. Int. Symp. on Multi-Robot and Multi-Agent Systems pp 135-141
[4] Chen J and Zhu Q 2017 Information Forensics and Security IEEE Transactions on vol 12 (11) pp 2736-2750
[5] Nguyen H V, Shin S and Choi Y 2011 International Journal of Technology Management 54(2/3) pp 229-251
[6] Hamidouche K, Saad W and Debbah M 2016 Wireless Communications IEEE vol 23(6) pp 62-69
[7] Alabeld Abass A A, Kumbhkar R, Mandayam N B and Gajic Z 2019 Cognitive Communications and Networking IEEE Transactions on vol 5(1) pp 44-58
[8] Fielder A, Panaousis E, Malacaria P, Hankin C and Smeraldi F 2014 IFIP International Information Security Conference (Springer, Berlin, Heidelberg) pp 15-29
[9] Kaklad V, Shah H, Patel R and Doshi N A 2019 Procedia Computer Science 155 pp 680-685
[10] Agrawal S and Goyal N 2011 Analysis of Thompson sampling for the multi-armed bandit problem (arXiv preprint arXiv) 1111.1797