The Task of Selecting the Protected Assets Within the Limited Resources Based on the Model of Discrete Game Theory

Alexander Yu. Bykov
Information Security Department
Bauman Moscow State Technical University
Moscow, Russia
abykov@bmstu.ru

Maksim V. Grishunin
Information Security Department
Bauman Moscow State Technical University
Moscow, Russia
zux2@ya.ru

***Abstract*—The game setting of the zero-sum problem for selecting the protected assets is considered. There are two players in the game: the defender and the forward. The attacker chooses assets for the attack; the defender chooses assets for defense. The task is formulated in such a way that each player must solve his own problem of linear Boolean programming. It is proposed to reduce this problem to a matrix game for which algorithms of finding a saddle point in pure strategies, if it exists, or in mixed strategies are known. In this case, the problem, as a rule, is a problem of large dimension, to reduce the dimension of the matrix, algorithms for the search of unmixed solutions that determine the rows and columns of the matrix are developed. An example of solving the problem of finding a saddle point in mixed strategies is presented, the probabilities for admissible solutions and the game price are assessed.**

Keywords— information security; zero-sum game; discrete optimization; saddle point, payment game matrix, pure strategy, mixed strategy

I. INTRODUCTION

Consider the game task of selecting protected security resources and selecting attacks on protected assets against attacking the resources of the defense and attack sides. We will use the concepts: the protected asset is what is protected, and the resource is what is used for protection (e.g. [1, 2]).

Protected assets can be:

- Integrity, accessibility and confidentiality of data stored on computer facilities or mobile devices;
- Integrity of applications, installed on the computer;
- Others.

The resources of the protection system can be the cost of protection, processor time; RAM; disk storage; other resources. Consider the task of allocating resources between assets, while using the model of two players with zero sum. Game theory has been widely used to solve various problems related to the protection of information.

An algorithm for finding optimal solutions in convex distributed online problems was developed in [3]. A modification of the algorithm of the Arrow-Hurwicz method is proposed to search for a saddle point in order to fulfill the global network criterion of Savage, using the method of Lagrange multipliers. An application to computer network security in which service providers cooperate to detect the signature of malicious users is developed to illustrate the practical value of the proposed algorithm.

In [4], a routing algorithm is described in mobile sensor networks based on models of game theory. This algorithm is based on a dynamic Bayesian signaling game and the achievement of a perfect Bayesian equilibrium (PBE). The algorithm allows to protect nodes from anonymous user actions.

In [5] it is shown how evolutionary game theory can help in the organization's economy to optimize the costs of information security systems. In the work, information security breaches are described by possible economic losses. Two types of security violations are considered: targeted attacks and the manifestation of spontaneous (accidental) threats. The game considers the ratio of investments in information security and possible losses.

In [6], dynamic games with players that have incomplete information about the resources of other players, as applied to cyber physical systems, are considered. Also, the authors consider the denial-of-service attack and develop an algorithm to compute the saddle-point.

In [7], the application of the theory of games in steganography is considered. The authors note that this topic is practically not covered, since until recently adaptive attacks in the field of steganography have not been conducted. Two players are considered: the introduction player and the detection player. An algorithm for finding the saddle point in mixed strategies is proposed.

In [8], an optimal strategy for protecting the network using the Moving Target Defense (MTD) concept based on the Markov game was considered. The essence of MTD - certain elements of the network change over time, making it difficult to "defeat" the target. The Markov decision-making process is used to describe the transitions between multi-states of the network. Dynamic game is used to describe multiphase protection and attack steps in MTD conditions.

In [9], the authentication was investigated at the physical level, while using the radio channel information to detect spoofing attacks in multiple- input multiple-output (MIMO) systems. The authors represent the interaction between the receiver and the spoofing node as a zero-sum game.

In [10], the application of learning based on game theory for the analysis of large amounts of data is considered. This approach can be useful for analyzing social network data. The authors consider a linear game model of many players (agents) whose data is stored in a large repository; confidential information is associated with each agent. The model is continuous, the search for solutions satisfying the Nash criterion is considered.

In [11], the allocation of resources in multiple-access listening channels is considered. The model considers several users who want to transfer confidential data to the legitimate recipient. On the receiving side there is an eavesdropper who passively listens to the channel and tries to decode messages. The authors obtain a coarse correlated equilibrium, a Pareto point and a Nash bargaining solution.

In [12] is considered an effective solution to the stochastic zero-sum games with lack of players information about each other. The paper discusses the problem of revealing the player's own secret information to obtain the enemy's secret information and suggests strategies for solving it.

In [13], the application of the theory of games for security in mobile ad hoc networks (MANETs) is considered. It is proposed to use the theory of medium-field games, which is oriented to a set of players (in the limit an infinite number of players), each of which tends to optimize some functional. The proposed scheme may allow a separate node in MANETs to make security decisions without centralized administration.

In [14], a review of the existing solutions of game theory to network security problems, the article is an overview. The classification of games according to various criteria is presented: by the number of game steps (static, dynamic, stochastic); on completeness of information about previous moves of players; on the completeness of information about the functions of winning other players. Various game models are considered: models of cooperative games; models of non-cooperative games. Various combinations of game class attributes are described.

In [15], to assign security classes to objects of the information system and to distribute data on these objects in order to reduce the dimension of the discrete optimization problem, an artificial admission of the optimization task to the game of two players with non-conflicting interests is used. One player is responsible for assigning security classes to objects, and the second is responsible for assigning data to objects. The solution is sought for by Nash equilibrium.

II. SETTING THE TASK OF ALLOCATING THE RESOURCES OF THE PROTECTION SYSTEM BETWEEN THE PROTECTED ASSETS

A. Basic reference data

Basic sets:

1) $Z = \{z_1, z_2, ..., z_m\}$ – the set of protected assets, $M = \{1,2, ..., m\}$ – the set of indices of these assets.
2) $R = \{r_1, r_2, ..., r_l\}$ – the set of limited resources of the defense, $L = \{1,2, ..., l\}$ – the set of indices of these resources.
3) $N = \{n_1, n_2, ..., n_s\}$ – the set of limited resources of the attacking side, $S = \{1,2, ..., s\}$ – the set of indices of these resources.

Parameters of elements of sets and its ratio:

1) $w_i \geq 0, \forall i \in M$ - possible damage in case of violation of the security of the i*th* protected asset (asset value).
2) $p_{np\,i} \in [0,1], \forall i \in M$ - probability (or possibility) of preventing an attack on the i*th* asset while protecting.
3) $a_{ki} \in [0,1), \forall k \in L, i \in M$ - the normalized value of the k*th* restricted resource used to provide protection for the i*th* asset. The entire resource is considered equal to 1
4) $b_k \in [0,1], \forall k \in L$ - the maximum normalized value of the k*th* restricted resource allocated for protection.
5) $c_{ki} \in [0,1), \forall k \in S, i \in M$ - the normalized value of the k*th* restricted resource of the attacking side used to attack the i*th* asset. The entire resource is considered equal to 1.
6) $d_k \in [0,1], \forall k \in S$ - the maximum normalized value of the k*th* restricted resource of the attacking side.

B. Required parameters

For the defense, we introduce the Boolean variable $x_i \in \{0,1\}, \forall i \in M$, $x_i = 1$ if the i*th* asset is protected, $x_i = 0$ - otherwise, the variable elements vector $\vec{X}$. For a part of the attack, we introduce a similar variable $y_i \in \{0,1\}, \forall i \in M$, $y_i = 1$, if the attack side performs an attack on the i*th* protected asset, $y_i = 0$ - otherwise, the variable elements are vector $\vec{Y}$.

C. Quality indicators

For a zero-sum game, the quality of two players is determined by the damage to the defense side. The damage can be defined as follows:

$$U(\vec{X},\vec{Y}) = U_{max}(\vec{Y}) - U_{\text{пр}}(\vec{X},\vec{Y}) = \sum_{i \in M} w_i y_i - \sum_{i \in M} p_{pr\,i} w_i x_i y_i, \quad (1)$$

where $U_{max}(\vec{Y}) = \sum_{i \in M} w_i y_i$ - the maximum damage that can be caused by the attacking side in the absence of protection;

$U_{\text{пр}}(\vec{X},\vec{Y}) = \sum_{i \in M} p_{pr\,i} w_i x_i y_i$ - prevented damage by the defense side.

D. Restrictions

Restrictions on the use of limited resources by the protection side:

$$\sum_{i \in M} a_{ik} x_i \leq b_k, \forall k \in L. \quad (2)$$

Restrictions on the use of limited resources by the attacking side:

$$\sum_{i \in M} c_{ik} y_i \leq d_k, \forall k \in S. \quad (3)$$

Thus, when deciding each of the players with a fixed decision of the other player, it is necessary to solve the problem of linear Boolean programming. We will assume that the solutions consisting of all 1 are inadmissible by restrictions.

III. SADDLE POINT SEARCH ALGORITHMS

The game model with a quality score (1) and restrictions (2), (3) can be reduced to a game defined by the payment matrix. The dimension of this matrix can be quite large: the number of rows is equal to the number of admissible $\vec{X}$ satisfying constraints (2) and the number of columns is equal to the number of admissible $\vec{Y}$ satisfying constraints (3). Elements of the matrix are the values of the exponent (1) for

given $\vec{X}$ and $\vec{Y}$. In the case of a payment matrix, a saddle point is often sought in pure strategies or if it does not exist in mixed strategies. To find solutions to solutions in mixed strategies for the payment matrix of the game, it is necessary to formulate a special problem of linear programming [14, 15], for its solution one can use, for example, the simplex method.

To reduce the dimension of the matrix, one can use the notion of strategy dominance. Strategy B is dominated by strategy A if, for any behavior of other players, the use of strategy B leads to a worse outcome than the use of A. If there is some admissible vector $\vec{X}$ (or $\vec{Y}$) containing 0 and 1, then the replacement in vector 1 by 0 , also gives the permissible $\vec{X}$ (or $\vec{Y}$), and the value of the exponent (1) will not be reduced (or increased for $\vec{Y}$) for a given $\vec{Y}$ (or $\vec{X}$). Therefore, the initial vector $\vec{X}$ (or $\vec{Y}$) is dominated by any vector obtained from it by replacing any 1 by 0. Therefore, it suffices to find the admissible vectors containing the maximum number of ones for the construction of the matrix (the replacement of any 0 by 1 gives an inadmissible vector with respect to constraints).

Let us consider two recursive algorithms for searching mutually unmodified admissible solutions for the vector $\vec{X}$ (for the vector $\vec{Y}$, algorithms are similar). The first algorithm starts with the initial vector $\vec{X} = \|0, 0, \dots, 0\|^{\mathrm{T}}$, the second algorithm starts with the initial vector $\vec{X} = \|1, 1, \dots, 1\|^{\mathrm{T}}$.

A. A recursive algorithm for searching non-dominated solutions, starting with a null vector

Step 1. Set the initial solution $\vec{X} = \|0, 0, \dots, 0\|^{\mathrm{T}}$, set Num = 0 (these parameters will be the input of the recursive algorithm or the parameters of the recursive function that implements it).

Step 2. Calling the recursive function, in this function, in a loop

for (int i = Num; i <m; i ++).

Create a copy of the vector $\vec{X}$, in the copy we assume that the element $x_i = 1$, if the new vector is allowed by constraints (2), then we call the recursive function for it, instead of the Num parameter, we pass i + 1.

Step 3. If in a cycle all new vectors are inadmissible by the constraints (2), i.e. the recursive function has not been called once, then the original vector $\vec{X}$ is the desired one, put it in the list, exit from the recursive function.

B. A recursive algorithm for searching non-dominated solutions, starting with a unit vector

Step 1. Set the initial solution $\vec{X} = \|1, 1, \dots, 1\|^{\mathrm{T}}$, set Num = 0 (these parameters will be the input of the recursive algorithm or the parameters of the recursive function that implements it).

Step 2. Calling the recursive function, in this function, in a loop

for (int i = Num; i <m; i ++).

Create a copy of the vector $\vec{X}$, in the copy we assume that the element $x_i = 0$, if the new vector is allowed by constraints (2), then it is the desired one, put it in the list, otherwise, for it we call the recursive function, instead of the parameter Num, we pass i + 1.

Step 3. Exit the recursive function.

The first algorithm works faster if the permissible solutions are greater 0, than 1. The second one works faster - otherwise. We can introduce the following rule: $\min_{k \in L} \frac{b_k}{\sum_{i \in M} a_{ik}} < 0.5$, then we use the first algorithm, otherwise, the second one.

Calculating the values of the function for the vectors $\vec{X}$ and $\vec{Y}$, which determine the rows and columns of the matrix, one can find a saddle point in pure strategies, if it exists. If there is no saddle point in pure strategies, then it can be found in mixed strategies, solving the problem of linear programming [14, 15].

IV. EXAMPLE OF SOLUTION OF THE PROBLEM

Consider the solution of the problem of small dimension by the example of protection of mobile devices assets: the number of protected assets is 8, the number of defender's limited resources with the cost of protection is 4, the number of limited resources of the attack side is 1 (the cost of attack). Parameters of the protected assets: possible damage, the cost of conducting attacks on assets, the probability (possibility) of preventing attacks on assets are presented in Table I. The values of possible damage and cost are given in conventional units. The parameters of the defender's limited resources, including the cost of protection, and the values of the right-hand parts of the restrictions on the use of these resources are presented in Table II.

For given initial data, the payment matrix constructed by the algorithms described above has a size of 49 x 6 (49 solutions for the defender, 6 solutions for the attacker). By checking the matrix and eliminating the dominant rows (columns) [14, 15], the dimension of the matrix is reduced to 13 x 6. There is no saddle point for the resulting matrix in pure strategies.

As a result of searching for a saddle point in mixed strategies by solving the linear programming problem, probabilities for the permissible solutions of the defender and the attacker are presented, presented in Table III. The price of the game in this case (winnings of the attacker and defender's loss) is 19,700 conventional units, which indicates the need to increase the resources allocated to the defense.

V. CONCLUSION

The game statement of the problem with a zero-sum of the defender and the attacker is provided with restrictions on the resources for selecting the defended assets by the defender and selecting the assets for attacking. It is proposed to reduce this problem to a matrix game for which the algorithms for finding the saddle point are known. To reduce the dimension of the matrix, algorithms for searching non-dominant solutions that determine the rows and columns of the matrix are developed.

The reliability of the proposed solutions is based on the use of known proven algorithms, is confirmed by checking

the found saddle point by calculating the price of the game on a given model.

TABLE I. PARAMETERS OF THE PROTECTED ASSETS: POSSIBLE DAMAGE, COST OF THE ATTACK, PROBABILITY (POSSIBILITY) OF PREVENTING AN ATTACK

№	Name of the protected asset	The extent of possible damage in case of a security violation ($w_i, \forall\, i \in M$)	Cost of attack ($c_{i1}, \forall\, i \in M$)	The probability of preventing an attack ($p_{\text{пр}\,i}, \forall\, i \in M$)
1.	Integrity and data availability on the device	4000	50	0,80
2.	Data privacy on the device	10000	600	0,99
3.	Integrity and availability of transmitted data	3000	60	0,70
4.	Confidentiality of transmitted data	8000	500	0,90
5.	Application integrity on the device	5000	100	0,80
6.	Prohibition of unauthorized installation of applications	8000	120	0,90
7.	Confidentiality of data on the device in case of loss or theft	10000	1000	0,50
8.	Protect your camcorder from unauthorized use by applications	8000	500	0,90
Total allocated to attack (d_1)			1500	

TABLE II. PARAMETERS OF THE PROTECTED ASSETS: POSSIBLE DAMAGE, COST OF THE ATTACK, PROBABILITY (POSSIBILITY) OF PREVENTING AN ATTACK

Asset number	Values of the limited resource of the mobile device used to protect the asset ($a_{ki}, \forall\, k \in L, i \in M$)			
	CPU load	RAM load	Storage load	Cost of protection
1.	0,03	0,05	0,01	100
2.	0,10	0,10	0,05	1000
3.	0,05	0,10	0,02	200
4.	0,15	0,10	0,05	900
5.	0,10	0,10	0,02	400
6.	0,10	0,10	0,01	500
7.	0,10	0,10	0,01	1200
8.	0,10	0,10	0,01	1000
Total allocated for protection, ($b_k, \forall\, k \in L$)	0.40	0,40	0,20	3000

TABLE III. THE RESULTS OF SOLVING THE TASK

№	Decision vectors	The choice of decisions
For the defender (vector $\vec{X}$)		
1.	1 1 1 0 1 0 0 0	0,0884
2.	1 1 1 0 0 0 1 0	$3{,}0300 \times 10^{-16}$
3.	1 1 1 0 0 0 0 1	0,4170
4.	1 1 0 0 1 1 0 0	0,4950
For the attackers (vector $\vec{Y}$)		
1.	1 1 1 1 1 1 0 0	0,2320
2.	1 1 1 0 1 1 0 1	0,4960
3.	1 0 1 1 1 1 0 1	0,0600
4.	1 0 1 0 1 1 1 0	0,2130

REFERENCES

[1] Bykov A. Panfilov F. Zenkovich S. Model and methods of multi-criteria selection of the security classes for objects in distributed information system and databases placement on objects. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2016, N 2(15), pp. 9-20. DOI: 10.21681/2311-3456-2016-2-9-20.

[2] Chesnokov V. Application of the community allocation algorithm in the information confrontation in the social networks. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2017, N 1(19), pp. 37-44. DOI: 10.21681/2311-3456-2017-1-37-44.

[3] Koppel A., Jakubiec F.Y., Ribeiro A. A Saddle Point Algorithm for Networked Online Convex Optimization. IEEE Transactions on Signal Processing. 2015. Vol. 63, iss. 19. P. 5149–5164. DOI: 10.1109/TSP.2015.2449255.

[4] Paramasivan B., Prakash M., Kaliappan M. Development of a secure routing protocol using game theory model in mobile ad hoc networks. Journal of Communications and Networks. 2015. Vol. 17, iss. 1. P. 75–83. DOI: 10.1109/JCN.2015.000012.

[5] Wang Q., Zhu J. Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory. 2016 2nd International Conference on Information Management (ICIM). 2016. P. 105–109. DOI: 10.1109/INFOMAN.2016.7477542.

[6] Gupta A., Langbort C., Başar T. Dynamic Games With Asymmetric Information and Resource Constrained Players With Applications to Security of Cyberphysical Systems. IEEE Transactions on Control of Network Systems. 2017. Vol. 4, iss. 1. P. 71–81. DOI: 10.1109/TCNS.2016.2584183.

[7] Schöttle P., Böhme R. Game Theory and Adaptive Steganography. IEEE Transactions on Information Forensics and Security. 2016. Vol. 11, iss. 4. P. 760–773. DOI: 10.1109/TIFS.2015.2509941.

[8] Lei C., Ma D., Zhang H. Optimal Strategy Selection for Moving Target Defense Based on Markov Game. IEEE Access. 2017. Vol. 5. P. 156–169. DOI: 10.1109/ACCESS.2016.2633983.

[9] Xiao Liang., Chen T., Han G., Zhuang W., Sun L. Channel-Based Authentication Game in MIMO Systems. 2016 IEEE Global Communications Conference (GLOBECOM). 2016. P. 1–6. DOI: 10.1109/GLOCOM.2016.7841657.

[10] Chessa M., Grossklags J., Loiseau P. A Game-Theoretic Study on Non-monetary Incentives in Data Analytics Projects with Privacy Implications. 2015 IEEE 28th Computer Security Foundations Symposium. 2015. P. 90–104. DOI: 10.1109/CSF.2015.14.

[11] Shah S. Chaitanya A., Sharma V. Resource allocation in fading multiple access wiretap channel via game theoretic learning. 2016 Information Theory and Applications Workshop (ITA). 2016. P. 1–7. DOI: 10.1109/ITA.2016.7888137.

[12] Li L., Shamma J. Efficient computation of discounted asymmetric information zero-sum stochastic games. 2015 54th IEEE Conference on Decision and Control (CDC). 2015. P. 4531–4536. DOI: 10.1109/CDC.2015.7402927.

[13] Yanwei Wang, Yu F.R., Tang H., Minyi Huang. A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks. IEEE Transactions on Wireless Communications. 2014. Vol. 13, no. 3. P. 1616–1627. DOI: 10.1109/TWC.2013.122313.131118.

[14] Xiannuan Liang, Yang Xiao. Game Theory for Network Security. IEEE Communications Surveys & Tutorials. 2013. Vol. 15, iss. 1. P. 472 – 486. DOI: 10.1109/SURV.2012.062612.00056.

[15] Bykov A. Yu., Panfilov FA, Khovrina A. The algorithm for choosing security classes for distributed information system objects and placing data on objects on the basis of reducing the optimization task to the problem of game theory with non-contradictory interests. Science and Education. Bauman Moscow State Technical University. Electron. journal. 2016. No. 1. DOI: 10.7463/0116.0830972.

[16] Wentzel E.S. Research of operations: tasks, principles, methodology: manual. Moscow: Knorus, 2014. 192 p.

[17] Strekalovsky AS, Orlov AV Bimatrix games and bilinear programming. - Moscow: Fizmatlit, 2007. 224 p.