A Search for Saddle Point in Protectable Assets Selection Problem Based on Continuous Game Theory Model

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

Ivan. A. Krygin
Information Security Department
Bauman Moscow State Technical University
Moscow, Russia
krygin.ia@gmail.com

***Abstract*. This article considers a continuous zero-sum game of two players with resources limitations between defender, selecting the assets to be protected, and attacker, selecting the assets to be attacked. Players' solutions are defense and attack probabilities vectors for each asset. The problem is formulated that each player must solve linear programming problem with fixed opponent's solution. The saddle point is suggested to search on simplices faces, defined by limitations. To find it two systems of linear equations is necessary to be solved: one to find defender's solution and another to find attacker's solution. Each player chooses solution on his face so that another player's parameter value is the same for any solution on his own face. To find a saddle with a guarantee it necessary to go over all combinations of simplices faces. An example of the solution of the problem is presented. The total game cost, probabilities of attacks on assets and probabilities of defense are calculated.**

Keywords. information security, zero-sum game, linear programming, saddle point, simplex, face of simplex, system of linear equations

I. INTRODUCTION

Game theory models are often used in problems related with information security. Consider some examples.

In [1] a game theory appliance in steganography is considered. Authors notice, there are a few articles related to this topic, because of adaptive attacks in steganography haven't been carried out until recently. Two players are considered: deplorer player and detection players are described. A saddle point searching algorithm in mixed strategies is suggested.

In [2] it is considered an optimal strategy of network protection with usage of Moving Target Defense principle, based on Markov game. An essence of MTD – moving network elements vary in time, making attack more difficult. Markov decision process is used to describe transitions between network multistates. Dynamic game is used to describe multiphase steps of defense and attack in terms of MTD.

In [3] it's investigated the PHY-layer authentication that exploits radio channel information to detect spoofing attacks in multiple- input multiple-output (MIMO) systems. Authors formulate the interactions between a receiver and a spoofing node in the spoofing detection as a zero-sum game.

In [4] it's investigated appliance of learning, based on game theory, to analyze big data. Such technique may be useful to analyze social networks. There are considered a linear game model of multiple players (agents), data storing in huge storages, each agent is related to sensitive information. Model is continuous, solution search satisfying Nash criterion is considered.

In [5] resource distribution in multiple access wiretap channels is considered. In model it's considered several users who want to confidentially transmit data to legitimate user. On receiver side there is an adversary, who passively listen to channel and try to decode messages. Stochastic game is considered, solutions are sought to be Nash and Pareto optimal.

In [6] an efficient stochastic zero-sum game with incomplete information is considered. In article it's investigated problem of own secret information disclosure to obtain adversary secret information and its solution strategies are suggested.

In [7] it's considered game technique to detect hardware trojans. Authors notice, the microcircuit industry is witnessing a massive outsourcing of the fabrication of ICs, and it brings up multiple opportunities for the insertion of malicious logic in the ICs. Authors suggest using game theory to detect such insertions.

In [8] it's considered a modelling of jamming attack in networks with wireless energy transfer. Authors have developed a game model, that allows to avoid energy interception. There are two players in the game: legitimate user and adversary. Each player has his own utility function, solution is sought as limited Nash equilibrity.

Information security software is often used to protect information in information processing and control systems (IPCS). This software is generally deployed on computational tools, which is used to solve target and supporting tasks in IPCS. In this case security software uses computational resources, and these resources are often limited, and their deficit is possible. This task becomes especially actual in

mobile security protection, which have limited computational resources.

The following definitions will be used:

- protected asset – something is needed to be protected
- resource – computational resource, used by security software

Protected resources are:

- integrity, availability, confidentiality of data, storing on devices
- integrity, availability, confidentiality of data, transferring over communication lines
- etc.

System resources are:

- security software cost
- CPU time
- RAM size
- Storage size
- Network
- etc.

Consider the problem of computer resources distribution between assets and use two-players zero-sum game (defender and attacker parties). Solution belonging to saddle-point, if it exists, is often a decision criterion in game-theory. Consider a possible approach to find a solution. Elements of selection set are continuous. It's necessary to find asset protection possibilities and attacks on assets possibilities. Some samples of game-theory usage for solving information security problems are presented in [1-4]

Proposed protected assets selection problem formulation is similar to formulation, discussed in [5], but in [5] was used the one cost limitation. In case of saddle point is impossible to find by optimized algorithm guaranteed result principle was applied.

II. FORMULATION OF SECURITY SYSTEM RESOURCES DISTRIBUTON BETWEEN PROTECTED ASSETS PROBLEM

A. Initial data

1) $Z = \{z_1, z_2, \dots, z_m\}$ - protected assets set, $M = \{1, 2, \dots, m\}$ - their indices set

2) $R = \{r_1, r_2, \dots, r_l\}$ – defender's limited resources set, $L = \{1, 2, \dots, l\}$ – their indicies set

3) $N = \{n_1, n_2, \dots, n_s\}$ – attacker's limited resources set, $S = \{1, 2, \dots, s\}$ – their indices set

B. Set elements parameters and relations between them

1) $w_i \geq 0, \forall\, i \in M$ – cost, if *i*-th protected asset security breach occurred (asset cost)

2) $p_{pr\,i} \in [0, 1], \forall\, i \in M$ – *i*-th asset attack prevention probability when defending

3) $a_{ki} \in [\,0,\ 1\,), \forall\, k \in L, i \in M$ – normalized *k*-th defender's limited resource value, used to protect *i*-th asset. The whole asset equals to 1

4) $b_k \in [\,0,\ 1\,),\ \forall\, k \in L$ – maximum normalized *k*-th limited resource value, allocated for protection

5) $c_{ki} \in [\,0,\ 1\,), \forall\, k \in S, i \in M$ – normailzed *k*-th attacker's limited resource value, used to attack *i*-th asset. The whole asset equals to 1

6) $d_k \in [\,0,\ 1\,), \forall\, k \in S$ – maximum normalized k-th attacker's limited resource value

C. Parameters

Define variable $p_i \in [0, 1], \forall\, i \in M$, signifying probability asset protection probability or its security degree. Variables forms vector $\vec{P}$. For attacker define variable $q_i \in [0, 1], \forall\, i \in M$, signifying asset attack probability or attack reliability degree. Variables form vector $\vec{Q}$.

D. Players indicators

For zero-sum game players quality indicators are defined by defender damage. Average cost damage is:

$$U(\vec{P}, \vec{Q}) = U_{max}(\vec{Q}) - U_{\text{пр}}(\vec{P}, \vec{Q}) = \sum_{i \in M} w_i\, q_i - \sum_{i \in M} p_{pr\,i} w_i\, p_i q_i \quad (1)$$

where $U_{max}(\vec{Q}) = \sum_{i \in M} w_i\, q_i$ maximum damage, may be caused by attacker without protection; $U_{\text{пр}}(\vec{P}, \vec{Q}) = \sum_{i \in M} p_{pr\,i} w_i\, p_i q_i$ – damage, prevented by defender

E. Limitations

Defender's limited resources usage limitation:

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

Attacker's limited resources usage limitation:

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

Thus, each player's decision (searching for unknown vectors $\vec{P}$ or $\vec{Q}$) with fixed opponent's solution implies linear programming problem solution

III. BASES OF ALGORITHM OF SEARCHING FOR SADDLE POINT ON THE DEFINED BY LIMITATIONS SIMPLEX FACES

Optimization problem for first player with fixed second player's decision is a linear programming problem. The first player wishes to minimize parameter (1) with limitations (2), and the second one wishes to maximize parameter (1) with limitations (3).

In [15] levels technique is suggested to find saddle point of convex-concave function. This method is approximate and is

required to solve convex programming problems. Also, it is pointed the saddle point always exists under given conditions.

The saddle point defined by solutions pair $\vec{P}^*$ and $\vec{Q}^*$ may be as on vertices of two simplices, defined by limitations (2) and (3), and on simplices faces. Optimized technique may be used to find saddle point if it is on vertices.

Simplices (polyhedron of allowable values) are in *m*-dimension metric space. In this case each limitation of inequalities (2) and (3) defines *(m-1)*-dimensioned hyperplane if becomes equality. As $p_i \in [0,1], \forall\, i \in M$ and $q_i \in [0,1], \forall\, i \in M$, allowable solutions are also inside of hypercube with sides are equal to 1. Hypercubes are constrained by *(m-1)*-dimensioned hyperplanes, defined by $p_i = 0, \forall\, i \in M,\ p_i = 1, \forall\, i \in M$ evaluations for defender and $q_i = 0, \forall\, i \in M,\ q_i = 1, \forall\, i \in M$ evaluations for attacker. In this way simplices are constrained by hyperplanes defined by limitations (2) and (3) (if inequalities become equalities) and hypercubes borders hyperplanes. An intersection of two *(m-1)*-dimensioned hyperplanes (if they intersect) is a *(m-2)*-dimensioned hyperplane; an intersection of three hyperplanes is (m-3)-dimensioned hyperplane etc. Separated point of m-dimensioned space in this interpretation is 0-dimensioned hyperplane. Simplices faces may belong to different dimensioned hyperplanes (in three dimensioned case the following terms are used: faces, edges, vertices). It is necessary to go over all faces for full search. Consider the technique of searching for possible solutions on faces, belong to same-dimensioned hyperfaces.

For each face it reachability is checked, that is allowable solution must exist for each player on his own face. It's not necessary to examine unreachable faces.

Saddle point on simplices faces, defined by limitations, must satisfy the following conditions if it exists. Point $\vec{P}^*$ on face must ensure that target function reaches maximum and takes the same values on each point on second player's face in vector space $\vec{Q}$. Similarly point $\vec{Q}^*$ on face must ensure that target function reaches minimum and takes the same values on each point on first player's face in vector space $\vec{P}$.

It is necessary to find *m* different points per each *(m-1)*-dimensioned face (not necessarily satisfying all the limitations (2) or (3)). Let $\vec{P}^{(1)}, \vec{P}^{(2)}, \dots, \vec{P}^{(m)}$ are points on face in vector space $\vec{P}$, and $\vec{Q}^{(1)}, \vec{Q}^{(2)}, \dots, \vec{Q}^{(m)}$ are points on face in vector space $\vec{Q}$. Define multipliers $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(m)}$ and $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$. So required points is found is the following form: $\vec{P}^* = \sum_{i \in M} \alpha^{(i)}\, \vec{P}^{(i)}$, $\vec{Q}^* = \sum_{i \in M} \beta^{(i)}\, \vec{Q}^{(i)}$.

System of equations 1 relatively unknown $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(m)}$:

$$\begin{cases} U(\vec{P}^*, \vec{Q}^{(1)}) = U(\vec{P}^*, \vec{Q}^{(2)}), \\ U(\vec{P}^*, \vec{Q}^{(1)}) = U(\vec{P}^*, \vec{Q}^{(3)}), \\ \dots\dots \\ U(\vec{P}^*, \vec{Q}^{(1)}) = U(\vec{P}^*, \vec{Q}^{(m)}), \\ \sum\limits_{i \in M} \alpha^{(i)} = 1. \end{cases}$$

System of equations 2 relatively unknown $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$:

$$\begin{cases} U(\vec{P}^{(1)}, \vec{Q}^*) = U(\vec{P}^{(2)}, \vec{Q}^*), \\ U(\vec{P}^{(1)}, \vec{Q}^*) = U(\vec{P}^{(3)}, \vec{Q}^*), \\ \dots\dots \\ U(\vec{P}^{(1)}, \vec{Q}^*) = U(\vec{P}^{(m)}, \vec{Q}^*), \\ \sum\limits_{i \in M} \beta^{(i)} = 1. \end{cases}$$

If found solutions $\vec{P}^*$ and $\vec{Q}^*$ satisfy limitations (2) and (3) and saddle point condition, then this is a required solution.

IV. EXAMPLE

Consider the solution of low dimension problem of protecting some assets: number of protectable assets – 8, number of defender's limited resources with defense cost -4, number of attacker's limited resources and attack costs – 4. Other data are generated by pseudorandom number generator.

Protected assets parameters, such as possible loss, probability (possibility) of assets attacks prevention are given in table 1. Possible damage values are given in conventional units. Defender's limited resources parameters, such as defense costs as resource and right sides of (2) values are given in table 2. Attacker's limited resources parameters, such as attack costs as resource and right sides of (2) values are given in table 2. Costs are given in conventional units.

TABLE I. PROTECTABLE ASSETS PARAMETERS

#	Size of possible damage $w_i, \forall\, i \in M$	Attack prevention probability $p_{pr\,i}, \forall\, i \in M$
1	4535,63	0,967
2	2075,96	0,607
3	3357,13	0,805
4	2972,23	0,769
5	3409,13	0,676
6	2260,05	0,973
7	2188,76	0,660
8	4280,74	0,708

TABLE II. DEFENDER'S RESOURCES

#	Defender's resources values $a_{ki}, \forall\, k \in L, i \in M$			
	Defense cost	Resource 1	Resource 2	Resource 3
1	392,038	0,340	0,345	0,153
2	144,472	0,176	0,319	0,392
3	292,657	0,273	0,160	0,426
4	147,133	0,130	0,151	0,381
5	128,114	0,218	0,229	0,410
6	252,678	0,451	0,263	0,250
7	194,546	0,437	0,300	0,318
8	329,060	0,101	0,345	0,246
Total $b_k, \forall k \in L$	940,349	1,200	1,179	1,634

TABLE III. ATTACKER'S RESOURCES

#	Attacker's resources values $c_{ki}, \forall\, k \in S, i \in M$			
	Attack cost	Resource 1	Resource 2	Resource 3
1	22,361	0,350	0,233	0,242
2	14,527	0,148	0,248	0,247
3	13,823	0,164	0,158	0,176
4	20,547	0,199	0,112	0,306
5	18,650	0,322	0,349	0,322
6	34,593	0,431	0,479	0,403
7	44,407	0,185	0,364	0,347
8	25,191	0,331	0,486	0,421
Total $d_k, \forall k \in S$	116,459	1,070	1,542	1,694

Because of going over faces the saddle point was found on faces belonging to 6-dimension hyperplanes (solution is sought in initial 8-dimension spaces). For defender hyperplane is defined by two 7-dimension hyperplanes intersection – one hyperplane containing face, defined by defense cost limitation, and another hyperplane defined by condition $p_6 = 0$. For attacker hyperplane is defined by two 7-dimension hyperplanes intersection – one hyperplane containing face, defined by resource 2 limitation, and another hyperplane defined by condition $q_6 = 0$. Solution is presented in table 4.

TABLE IV. SOLUTION

Vector $\vec{P}^*$								Game cost
0,422	0,751	0,778	0,634	0,409	0,000	0,532	0,576	8200, 144
Vector $\vec{Q}^*$								
0,607	0,779	0,736	0,437	0,378	0,000	0,915	0,737	

CONCLUSION

There is presented a continuous two players zero-sum game with resources limitation for choosing assets to protect by defender and choosing assets to attack by attacker. Each player solves linear programming problem with fixed opponent decision. If saddle point is on simplices faces, defined by limitations, then it is suggested to solve two systems of linear equations to find it.

Suggested solutions reliability is based on usage of known verifies algorithms, found saddle point is confirmed by check for compliance with conditions it must satisfy.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Kamhoua C., Zhao H., Rodriguez M., Kwiat K. A Game-Theoretic Approach for Testing for Hardware Trojans. IEEE Transactions on Multi-Scale Computing Systems. 2016. Vol. 2, iss. 3. P. 199–210. DOI: 10.1109/TMSCS.2016.2564963.

[8] Niyato D., Wang P., Kim D., Han Z., Xiao L. Game theoretic modeling of jamming attack in wireless powered communication networks. 2015 IEEE International Conference on Communications (ICC). 2015. P. 6018–6023. DOI: 10.1109/ICC.2015.7249281.

[9] Freudiger J., Manshaei M.H., Hubaux J. P., Parkes D.C. Non-Cooperative Location Privacy. IEEE Transactions on Dependable and Secure Computing. 2013. Vol. 10, iss. 2. P. 84 – 98. DOI: 10.1109/TDSC.2012.85.

[10] Lelarge M. Coordination in Network Security Games: A Monotone Comparative Statics Approach. IEEE Journal on Selected Areas in Communications. 2012. Vol. 30, iss. 11. P. 2210 – 2219. DOI: 10.1109/JSAC.2012.121213.

[11] Liang Xiao, Yan Chen, Lin W.S., Liu K.J.R. Indirect Reciprocity Security Game for Large-Scale Wireless Networks. IEEE Transactions on Information Forensics and Security. 2012. Vol. 7, iss. 4. P. 1368 – 1380. DOI: 10.1109/TIFS.2012.2202228.

[12] Ma C.Y.T., Yau D.K.Y., Rao N.S.V. Scalable Solutions of Markov Games for Smart-Grid Infrastructure Protection. IEEE Transactions on Smart Grid. 2013. Vol. 4, iss. 1. P. 47 – 55. DOI: 10.1109/TSG.2012.2223243.

[13] 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.

[14] A. Yu. Bykov, E. S. Shmatova The Algorithms of Resource Distribution for Information Security Between Objects of an Information System Based on the Game Model and Principle of Equal Security of Objects. Science and Education of the Bauman MSTU, 2015, No. 9, pp. 160–187. DOI: 10.7463/0915.0812283.

[15] Shmatova E. The Choice of Strategy for the Spurious Information System on the Basis of the Game Theory Model. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2015. No 5 (13). P. 36-40. DOI: 10.21681/2311-3456-2015-5-36-40.

[16] E. G. Golshtein, A. S. Nemirovsky, Yu. E. Nesterov Optimization techniques. Levels technique, it generalizations and applications. Economics and mathematical methods. 1995. V. 31. no. 3. pp. 164-180.