PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2009, № 3, p. 61–63

Mathematics

SOME GAME-THEORETICAL MODELS OF INFORMATION SECURITY PROBLEMS

K. V. SAGHATELYAN[1*], V. I. TAIRYAN[2]

[1] *Chair of Optimal Control and Approximate Methods, YSU*
[2] *Department of Applied Mathematics, RAU*

In the present paper the game models of information security are considered. A few formulations of information security problems are introduced and quite simple game models are built. Specific solutions of several matrix games and a duel type games are derived.

***Keywords*:** information security, two-person games, infinite games.

Recently there appeared a large number of articles dedicated to information security. Besides the technical tools (such as cryptographic methods or computer network protection software) of information protection, conceptual mathematical models of information security are also needed. The research object here may be as a home PC protection, as well as information network (not necessarily computer network) security of some political or economical unions (see, for example, [1–4]).

In all those cases we need to develop some protection tools against supposed attacks. Such an attack may realize a child trying to watch an adult TV channel, or hackers attacking information database of a large company, or economic and military diversion of a country or group of countries. In all of mentioned cases there is a conflict situation and, very often, lack of information at both attacking and protecting party. All this leads to consideration of these problems within the frames of game-theoretical decision models.

I. The simplest model is the model of finite antagonistic (matrix) game. Let us consider the following situation. Given n objects requiring protection. Denote by $a_i, i=1,...,n$, the cost of i-th object and by b the cost of attack. Assume that the attacker (the first player) attacks one of the objects, while the defender (the second player) possesses resource to protect only one object. If the attack proceeds on the unprotected object, then the defender loses that object, and if the attack proceeds on the protected object, then the attacker loses this object, as well as the cost of the attack. This situation may be presented as a matrix game with matrix A:

$$A=\begin{pmatrix} -b & a_1-b & a_1-b & \dots & a_1-b \\ a_2-b & -b & a_2-b & \dots & a_2-b \\ \dots & \dots & \dots & \dots & \dots \\ a_n-b & a_n-b & a_n-b & \dots & -b \end{pmatrix}.$$

* E-mail: ksaghatelyan@ysu.am

It is easy to check that in this game there is no balance in pure strategies, hence, solution should be sought in mixed strategies. Let us denote the optimal strategy of the first player (attacker) and the second player (defender) by $p=(p_1,p_2,...,p_n)$ and $q=(q_1,q_2,...,q_n)$ respectively; the value of the game we denote by v. It is obvious, that the game with matrix A is strategically equivalent to the game with matrix A':

$$A'=\begin{pmatrix} 0 & a_1 & a_1 & ... & a_1 \\ a_2 & 0 & a_2 & ... & a_2 \\ ... & ... & ... & ... & ... \\ a_n & a_n & a_n & ... & 0 \end{pmatrix}.$$

It is easy to see, that in the case $a >0, i=1,2,...,n$, the strategies of both players should be completely mixed strategies and, therefore, the game can be brought to solution of systems of linear equations

$$\begin{cases} \sum\limits_{i\neq 1} p_i a_i = v, \\ \sum\limits_{i\neq 2} p_i a_i = v, \\ ... \; ... \; ... \\ \sum\limits_{i\neq n} p_i a_i = v, \\ \sum\limits_{i=1}^{n} p_i = 1. \end{cases} \qquad \begin{cases} a_1 \sum\limits_{i\neq 1} q_i = v, \\ a_2 \sum\limits_{i\neq 2} q_i = v, \\ ... \; ... \; ... \\ a_n \sum\limits_{i\neq n} q_i = v, \\ \sum\limits_{i=1}^{n} q_i = 1. \end{cases}$$

Making simple calculations, we can obtain the following solution of the game:

$$p_i = \frac{1}{a_i \sum\limits_{j=1}^{n} \frac{1}{a_j}}, \qquad q_i = 1 - \frac{n-1}{a_i \sum\limits_{j=1}^{n} \frac{1}{a_j}}, \qquad i=1,2,...,n,$$

and the value of the game equals to

$$v = \frac{n-1}{\sum\limits_{j=1}^{n} a_j} - b.$$

II. In the previous example we supposed that players allocate their all resource to protect or attack one object. Let's consider now the case, when each player has a single resource, which it distributes between the objects. Assume that each party allocates *i*-th part of his resource to attack the object, for the attacker and the defender these values are $0 \le x_i \le 1$ and $0 \le y_i \le 1$ respectively. In this case we get the following antagonistic game on simplexes:

$$\Gamma =< S_{n-1}, S_{n-1}, H >, \text{ where } S_{n-1} = \left\{ x \in R_+^n : \sum_i x_i = 1 \right\}, \quad H = H(x,y).$$

In particular case, when there are only two objects, this game turns to a game on the unit square $\Gamma =< [0,1],[0,1], H(x,y) >$, where x and y are parts of resources assigned for the first object. This game is a duel type game, in which the payoff function has discontinuity on the diagonal $x = y$, i.e. it has the following form:

$$H(x,y)=\begin{cases} L(x,y), x<y, \\ f(x), x=y, \\ M(x,y), x>y. \end{cases}$$

There is vast literature devoted to duels, including games with several objects. As an example let's consider a simple game with two objects $\Gamma = <[0,1],[0,1], H(x,y)>$ and the payoff function

$$H(x,y)=\begin{cases} a, x>y, \\ 0, x=y, \\ b, x<y. \end{cases}$$

Without loss of generality suppose that $a>b$. Let's check the availability of solution in pure strategies. It is easy to see that

$$\max_{x\in[0,1]}\min_{y\in[0,1]} H(x,y)=0, \quad \min_{y\in[0,1]}\max_{x\in[0,1]} H(x,y)=b,$$

therefore, there is no solution in pure strategies. As an auxiliary game let's consider a matrix game $\ddot{H}=\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$. In this game the players' optimal strategies have the form $p^0=(\frac{b}{a+b},\frac{a}{a+b})$, $\quad q^0=(\frac{a}{a+b},\frac{b}{a+b})$, therefore, we expect the optimal strategies in game Γ to have the form

$$F^0(x)=\begin{cases} 0, x<0, \\ b/(a+b), 0\le x<1, \\ 1, x\ge 1, \end{cases} \qquad G^0(y)=\begin{cases} 0, y<0, \\ a/(a+b), 0\le y<1, \\ 1, y\ge 1. \end{cases}$$

Since $H(0,0)=H(1,1)=0$, we obtain

$$H(F^0,y)=\frac{a}{a+b}H(0,y)+\frac{b}{a+b}H(1,y)=\frac{ab}{a+b},$$

$$H(x,G^0)=\frac{b}{a+b}H(x,0)+\frac{a}{a+b}H(x,1)=\frac{ab}{a+b},$$

$$H(F^0,G^0)=\frac{a}{a+b}\cdot\frac{a}{a+b}H(0,1)+\frac{b}{a+b}\cdot\frac{b}{a+b}H(1,0)=\frac{a^2b+ab^2}{(a+b)^2}=\frac{ab}{a+b}.$$

Thus, (F^0,G^0) is an equilibrium situation in game Γ, and the value of the game is $ab/(a+b)$. So, the solution of game Γ practically does not differ from the solution of the matrix game $\ddot{H}$, and optimal strategies of both – attacker and defender, is to concentrate all resources, with corresponding probabilities on one of the objects, and not dissipate them among objects.

Received 17.03.2009

REFERENCES

1. **Bier V. M.** Fourth Int. Conf. on Math. Methods in Reliability. Santa Fe, New Mexico, June 2004.
2. **Tairyan V., Tairyan E.** Proc. of Int. Conference of Sequrity. M.: MGU, 2006 (in Russian).
3. **Saghatelyan K., Tairyan V., Tairyan S.** Trudy Nauchn. Konf. RAU. Yerevan, 2008 (in Russian).
4. **Chkhartishvili A.** Game-theoretical Models of Information Control. M., 2004 (in Russian).

Ինֆորմացիոն անվտանգության խնդիրների որոշ խաղային մոդելներ

Աշխատանքում դիտարկվում են ինֆորմացիոն անվտանգության խնդիրների խաղային մոդելներ: Բերված են ինֆորմացիոն անվտանգության մի շարք խնդիրների ձևակերպումներ և կառուցված են բավականին պարզ խաղային մոդելներ: Մի քանի մատրիցային խաղերի և մենամարտային տիպի խաղի համար ստացված են կոնկրետ լուծումներ:

Некоторые теоретико-игровые постановки задач информационной безопасности

В работе рассматриваются игровые модели задач информационной безопасности. Приведены постановки нескольких задач информационной безопасности и построены достаточно простые игровые модели. Получены конкретные решения нескольких матричных игр и игры типа дуэли.