Models of Flood-attacks, mathematical catastrophe theory, theory of differential games and security strategies

Alexander K. Guts
Department of Cybernetics
Dostoevsky Omsk State University
Omsk, Russia
guts@omsu.ru

***Abstract*—Method of finding of the most optimal security strategies for computer protection from Flood-attacks is given based on differential game theory. Situation of "fallen" server we are describing using mathematical catastrophe theory**

***Index Terms*—Flood-attacks, information security, theory of differential games, optimal strategy, Nash equilibria, catastrophe theory**

I. Introduction

Flood attacks is to overflow computer system with such a large number of packets that cannot be processed. For example, if the system can only process 10 packets per second, and the attacker sends 20 packets per second to it, then other users, when trying to connect to the system, are refused in service, since all resources are occupied. With such attacks, the performance of the computer system or applications is significantly reduced. Obviously, with this method of attack there is a sharp increase in incoming traffic.

The purpose of this article is a mathematical description of the Flood-attack.

We see that incoming traffic plays an important role. Traffic is a parameter τ that characterizes a typical situation for a functioning computer system, traffic says that the system is able to cope with incoming packets with a certain margin of system reliability. An increase in traffic requires an increase in the free resources of the system for its processing.

Futher, we known that an important parameter of the stability and reliability of a computer system is its performance p, expressed both in the processing speed of incoming packets and the number of established connections. When the server receives the data packet, it is processed. It takes time and certain resources of a computer system. If a new package arrives and the server is busy receiving or processing the previous or other packet, then the newly arriving request-packet is queued, taking up part of the system's resources.

II. Models of Flood-attacks

A. Simple Model of Flood-attacks

Thus, the ability of system to function normally is determined by the number of responses to requests.

Denote by $x(t)$ the number of responses to requests (system resources involved in processing received packets) at time t.

Then

$$x(t+1) = x(t) + K[x(t)] + \tau, \tag{1}$$

where $K[x(t)]$ is the result of the processing requests at moment t. The equation reflects the requirement that more traffic requires an increase in the number of responses to requests [1].

For simplicity, we assume that $K[x(t)] = kx(t)$, where k is the quantity determining system performance

$$k = \{p - g[x(t)]\}, \tag{2}$$

and which is equal to the average processing speed of incoming packets p taking into account its fall or increase depending on the volume of employees resources: the more resources are loaded, the lower the speed processing incoming packets.

The x queued packet must go through the connection (or just go through the clogged channel, like a UDP packet) and after processing , and possibly generate a response for the computer that sent him. In other words, the package participates in its processing at least twice. Therefore, we will reflect this by accepting the assumption that $g[x] = x^2$.

Thus, $g[x(t)] = [x(t)]^2$ and then

$$x(t+1) = x(t) + [(p - p_0) - x^2(t)]x(t) + (\tau - \tau_0), \tag{3}$$

where some "typical" for this server performance values p_0 and traffic τ_0 are entered. During the transition to continuous time the equation (3) is reduced to the equation

$$\frac{dx}{dt} = [(p - p_0) - x^2(t)]x(t) + (\tau - \tau_0), \tag{4}$$

or

$$\frac{dx}{dt} = -\frac{\partial}{\partial x}V(x, p, \tau), \tag{5}$$

Where

$$V(x, p, \tau) = \frac{1}{4}x^4 - \frac{1}{2}(p - p_0)x^2 - (\tau - \tau_0)x. \tag{6}$$

From the form of the expression (6) we see that the server is potential dynamic system whose potential is described by "cusp" catastrophe [1].

B. Complex Model of Flood-attacks

In reality the incoming request during decapsulation is processed at all levels of the OSI model. In addition, attacks can performed simultaneously on the protocols of all seven levels. Consider this, we assume that $g[x(t)] = [x(t)]^7$. It means that we have the following model of Flood-arrack in the form of differential equation [2]:

$$\frac{dx}{dt} = [(p - p_0) - x^7(t)]x(t) + (\tau - \tau_0). \tag{7}$$

or

$$\frac{dx}{dt} = -\frac{\partial}{\partial x}V(x, p, \tau),$$

where

$$V(x, p, \tau) = \frac{1}{9}x^9 - \frac{1}{2}(p - p_0)x^2 - (\tau - \tau_0)x.$$

Dynamic system (7) is described by A_8 catastrophe [2].

But we can consider the following more complex model of the Flood-attacks:

$$\frac{dx}{dt} = [(p - p_0) - x^7(t)]G[x(t)] + (\tau - \tau_0), \tag{8}$$

i. e.

$$K[x(t)] = kG[x(t)],$$
$$k = (p - p_0) - x^7(t).$$

C. Stationary equilibrium

It is natural to assume that in everyday routine conditions the server has on average the same performance p and traffic τ. Moreover, the number of responses on average is more or less constant, i. e. $x(t) = x_0 = const$. In this case

$$\frac{dx}{dt} = 0$$

and therefore $x_0 = x_0(p, \tau)$ is a solution to the equation

$$\frac{\partial}{\partial x}V(x_0, p, \tau) = 0.$$

Such solutions are called the states of *stationary equilibrium*. The server thus abides as usually in a state of stationary equilibrium. If the computer system had performance $p < p_0$, i.e. not very high, traffic $\tau > \tau_0$ and was in equilibrium A, then with increasing traffic we get the catastrophic jump of such characteristic as quantity responses to inquiries. In other words, the we have the transition to new equilibrium B of the "fallen" server.

III. Nash equilibria

The stationary equilibrium state of the system, or stationary equilibrium, is state for which its characterizing parameter $x(t)$ does not change with time, i. e.

$$\frac{dx}{dt} = 0.$$

In our case the stationary equilibrium state says that the number of responses $x = const$. It is simplifieds description of server work.

However, the systems are often controlled by external factors $u_1, ..., u_N$, and in fact, their dynamics is described by the differential equation of the form

$$\frac{dx}{dt} = f(t, x, u_1, ..., u_N).$$

In this case, we can consider this equation in the framework of optimal control theory, and moreover, in the framework of the theory of differential games, and find the so-called Nash equilibrium.

In the theory of differential games each control factor u_i is considered to be in possession of the player i, who tries to use it to affect the system so to have a maximal winning or minimal losing. Player's wining/lossing is described by some given function $J_i(x, u_1, ..., u_N)$. Clearly, in reality, it is difficult to suggest that the factors can be changed completely independently from each other, and therefore, an equilibrium can be established in the system in a certain sense. In this case, Nash equilibrium means that if any player is trying to change their management strategy unilaterally while other players policy remains unchanged, he will have the greater loss.

"The Nash solution is characterized by an equilibria in which each player has an outcome that cannot be improved by a unilateral change of strategy. The Nash strategy safeguards against a single player deviating from the equilibrium strategy and is well suited for problems where cooperation between players cannot be guaranteed $< .. >$ A Nash differential game consists of multiple players making simultaneous decisions where each player has an outcome that cannot be unilaterally improved from a change in strategy. Players are committed to following a predetermined strategy based on knowledge of the initial state, the system model and the cost functional to be minimized" [3].

I think that the Nash game is very good description of situation in which a server administrator and hacker are reality existing.

IV. Non-zero-sum differential game and Nash equilibria

We consider the algorithm for finding Nash equilibria. It is natural to consider a *non-zero-sum game*, since the prizes of hacker and system administrator of the server are weakly related.

If a player forms "its" control action in the form of only a function of time $u(t)$ for the entire duration of the game, then $u(t)$ is the *program control* of the player. Earlier we called it using the term "control". However, a player can choose his own control depending on the position of x at the time point t the system is in. In this case, the player constructs a control action in the form of a function $u(t, x)$, which already depends on the position $\{t, x\}$, and for $u(t, x)$ the term *positional control* of the player is used. Often they simply write $u(x)$.

In the literature, we can meet other terminology [4].

We have an *open-loop strategies*, if apart from the initial data, Player i cannot make any observation of the state of the

system, or of the strategy adopted by the other player. In this case, his strategy must be open-loop, i.e. it can only depend on time $t \in [0,T]$. The set U_i of strategies available to the i-th player will thus consist of all measurable functions $t \to u_i(t)$ from $[0,T]$ into U_i.

Assume that, at each time $t \in [0,T]$, player i can observe the current state $x(t)$ of the system. However, he has no additional information about the strategy of the other player. In particular, he cannot predict the future actions of the other player. In this case, each player can implement a *Markovian strategy* (i.e., of feedback type): the control $u_i = u_i(t,x)$ can depend both on time t and on the current state x. The set U_i of strategies available to the i-th player will thus consist of all measurable functions $(t,x) \to u_i(t,x)$ from $[0,T] \times \mathbb{R}^n$ into U_i.

We will look for positional control (= Markovian strategy), or Nash positional equilibrium.

For the differential game of N players

$$\frac{dx}{dt} = f(x) + \sum_{j=1}^{N} g_j(x)u_j,$$
$$f(0) = 0,$$
$$x \in \mathbb{R}, \quad u_j \in \mathbb{R},$$

winning functions

$$J_i(x,u_1,...,u_N) = \int_0^{+\infty} [Q_i(x) + \sum_{j=1}^{N} R_{ij}(u_j)^2]dt,$$
$$(i = 1,...,N),$$
$$Q_i > 0, \quad R_{ii} > 0, \quad R_{ij} \geq 0,$$

existence of Nash equilibria

$$J_i(u_1^*, u_2^*, u_i^*, ..., u_N^*) \leq$$
$$\leq J_i(u_1^*, u_2^*, ..., u_{i-1}^*, u_i, u_{i+1}^*..., u_N^*), \qquad (9)$$
$$\forall u_i, \quad i = 1,...,N,$$

is reduced [5] to extremely difficult problem of finding a positive definite solution $V_i(x) > 0$ of the nonlinear Hamilton-Jacobi equation

$$(V_i)'_x(x)f(x) + Q_i(x) -$$
$$-\frac{1}{2}(V_i)'_x \sum_{j=1}^{N} [g_j(x)]^2 (R_{jj})^{-1} (V_j)'_x +$$
$$+\frac{1}{4}\sum_{j=1}^{N} R_{ij}[g_j(x)]^2[(R_{jj})^{-1}]^2[(V_j)'_x]^2 = 0, \qquad (10)$$

which is used to construct the Nash equilibrium [5] (see Theorem 10.4-2):

$$u_i^*(x) = u_i(V_i(x)) = -\frac{1}{2}R_{ii}g_i(x)(V_i)'_x, \qquad (11)$$
$$i = 1,...,N.$$

A. Nash equilibria of Simple Model

In this case [6], $N = 2$, player 1 is the server administrator, player 2 is hacker and

$$u_1 = p - p_0, \quad u_2 = \tau - \tau_0,$$
$$f(x) = -x^3, \quad g_1(x) = x, \quad g_2(x) = 1,$$

for $R_{11} = R_{22} = 1, R_{12} = R_{21} = 0$ the Hamilton-Jacobi equations are:

$$Q_1 + (V_1)'_x f(x) - \frac{1}{4}[g_1(x)]^2[(V_1)'_x]^2 -$$
$$-\frac{1}{2}[g_2(x)]^2(V_1)'_x(V_2)'_x = 0,$$
$$Q_2 + (V_2)'_x f(x) - \frac{1}{4}[g_2(x)]^2[(V_2)'_x]^2 -$$
$$-\frac{1}{2}[g_1(x)]^2(V_1)'_x(V_2)'_x = 0.$$

Assuming that

$$V_1(x) = V_2(x) = \frac{1}{2}x^2,$$

we obtain the Hamilton-Jacobi equations in the form

$$Q_1 - x^4 - \frac{1}{4}x^4 - \frac{1}{2}x^2 = 0,$$
$$Q_2 - x^4 - \frac{1}{4}x^2 - \frac{1}{2}x^4 = 0.$$

Hence,

$$Q_1 = \frac{5}{4}x^4 + \frac{1}{2}x^2 > 0,$$
$$Q_2 = \frac{3}{2}x^4 + \frac{1}{4}x^2 > 0.$$

These functions are positively defined.

Therefore, by Theorem 10.4-2 of [5], we have the Nash equilibrium

$$p^* = p_0 - \frac{1}{2}x^2, \qquad \tau^* = \tau_0 - \frac{1}{2}x, \qquad (12)$$

found by the formulas (11).

Winning functions are

$$J_1(x,p,\tau) = \int_0^{+\infty} [Q_1(x) + (p - p_0)^2]dt,$$
$$J_2(x,p,\tau) = \int_0^{+\infty} [Q_2(x) + (\tau - \tau_0)^2]dt.$$

Thus, the Nash equilibrium, and the optimal decisions made by the system administrator are achieved if this decision at the traffic of τ^* should correspond to the implementation of performance described by the parameter p^*.

Conducting differential games and calculating equilibria is useful from the point of view of determining the degree of reliability of the system under study. Equilibria are established if the system is able to resist. If there are many equilibria,

then the system administrator has at its disposal a range of resistance thresholds – security prevention measures consisting of pairs (τ^*, p^*), giving estimated characteristics of a possible set of security prevention – performance p^*, as well as traffics τ^*, allowing us to judge the degree of success of taken security measures.

The various strategies we are talking about can be obtained by taking, for example,

$$V_1(x) = V_2(x) = \frac{1}{2m}x^{2m}, \quad m \geq 1.$$

In this case,

$$Q_1 = x^{2m+2} + \frac{1}{4}x^{4m} + \frac{1}{2}x^{4m-2} > 0,$$

$$Q_2 = x^{2m+2} + \frac{1}{4}x^{4m-2} + \frac{1}{2}x^{4m} > 0.$$

and a series of optimal Nash equilibria has the form:

$$p^* = p_0 - \frac{1}{2}x^{2m}, \quad \tau^* = \tau_0 + \frac{1}{2}x^{2m-1}, \quad m = 1, 2, ...$$

B. Nash equilibrium of Model (8)

We consider function $G[x(t)] = x^{2s}$, $s = 1, 2, ...$

In this case, $N = 2$, player 1 is the server administrator, player 2 is hacker and

$$u_1 = p - p_0, \quad u_2 = \tau - \tau_0,$$

$$f(x) = -x^{7+2s}, \quad g_1(x) = x^{2s}, \quad g_2(x) = 1,$$

for $R_{11} = R_{22} = 1, R_{12} = R_{21} = 0$ the Hamilton-Jacobi equations are:

$$Q_1 + (V_1)'_x f(x) - \frac{1}{4}[g_1(x)]^2[(V_1)'_x]^2 -$$

$$-\frac{1}{2}[g_2(x)]^2(V_1)'_x(V_2)'_x = 0,$$

$$Q_2 + (V_2)'_x f(x) - \frac{1}{4}[g_2(x)]^2[(V_2)'_x]^2 -$$

$$-\frac{1}{2}[g_1(x)]^2(V_1)'_x(V_2)'_x = 0.$$

Assuming that

$$V_1(x) = V_2(x) = \frac{1}{2}x^2,$$

we obtain the Hamilton-Jacobi equations in the form

$$Q_1 = x^{8+2s} + \frac{1}{4}x^{4s+2} + \frac{1}{2}x^2,$$

$$Q_2 = x^{8+2s} + \frac{1}{4}x^2 + \frac{1}{2}x^{4s+2}.$$

These functions are positively defined.

Therefore, by Theorem 10.4-2 of [5], we have the Nash equilibrium

$$p^* = p_0 - \frac{1}{2}x^{2s+1}, \qquad \tau^* = \tau_0 - \frac{1}{2}x, \tag{13}$$

found by the formulas (11).

Winning functions are as in previous section.

C. Absence of the Nash equilibrium in Model (7)

The functions $V_i(x)$ must have a form x^{2d} and $Q_i > 0$. Hence function

$$(V_i)'_x f(x) \sim x^{2d-1}(x^8) = x^{2(d+4)-1}$$

and can not be a positive defined.

The conditions of the Theorem 10.4-2 of [5] are not satisfied.

V. Zero-sum differential game and Nash equilibria

We considered the Nash equilibria of non-zero-sum games for our models. But It would be helpful to consider the case of zero-sum differential game for our models, because such game presents the uncompromising confrontation of administrator and hacker.

We take a simple model in the following form

$$\begin{aligned} \frac{dx}{dt} &= [(p - p_0) - x^2(t)]x(t) + (\tau - \tau_0) = \\ &= f(x) + g_1(x)u_1 + g_2(x)u_2, \\ y &= h(x), \end{aligned} \tag{14}$$

where

$$u_1 = \tau - \tau_0, \quad u_2 = p - p_0,$$

$$g_1(x) = 1, \quad g_2(x) = x,$$

$$h(x) \geq 0,$$

and y is packet counter.

We look for the Nash equilibria (p^*, τ^*) such that

$$J(p^*, \tau) \leq J(p^*, \tau^*) \leq J(p, \tau^*)$$

with winning function

$$J(p, \tau) = \int_0^{+\infty} [h^2(x) + R(\tau - \tau_0)^2 - \gamma^2(p - p_0)^2]dt,$$

$$R > 0, \quad \gamma = const > 0.$$

Pair (p^*, τ^*) will be a Nash equilibrium (Theorem 10.2-2 of [5]), if

1) there exists a smooth positive semi-definite solution $V(x) \in C^1$ to the Hamilton-Jacobi equation

$$h^2 + V' f(x) - \frac{1}{4R}(V')^2 g_1^2 + \frac{1}{4\gamma^2}(V')^2 g_2^2 = 0,$$

$$V(0) = 0,$$

such that closed-loop system

$$\frac{dx}{dt} = f(x) + g_1(x)u_1^* + g_2(x)u_2^*,$$

$$u_1^* = -\frac{1}{2R}g_1(x)V'(x), \quad u_2^* = \frac{1}{2\gamma^2}g_2(x)V'(x)$$

is locally asymptotically stable;

2) system

$$\begin{aligned}\frac{dx}{dt} &= [(p-p_0)-x^2(t)]x(t) = \\ &= f(x)+g_1(x)u_1, \\ y &= h(x),\end{aligned} \tag{15}$$

is zero-state observable, i.e. if $u_1 \equiv 0$, $h \equiv 0$, then $x = 0$.

It is easy to see that these conditions are satisfied for

$$h(x) = \frac{1}{2}|x|, \quad V(x) = \frac{1}{2}x^2, \quad R = 1, \quad \gamma^2 = \frac{1}{4},$$

when

$$|x(0)| < \frac{1}{\sqrt{6}}.$$

VI. Von Stackelberg equilibria

When we meet the very strong hacker then his influence can be prevailing. In this case we must use the Von Stackelberg equilibria.

"A hierarchical nonzero-sum technique was derived by Von Stackelberg, where an equilibrium solution can be determined when one player's strategy has influence over another player's strategy. The Stackelberg technique has been accepted as the solution to a broad class of hierarchical decision making problems where one decision maker (called the leader) announces a strategy prior to the announcement of the second decision maker's (called the follower) strategy" [3].

The optimal reaction set for player 1 (the follower $u_1 \in U_1$) to a control $u_2 \in U_2$ is

$$\mathcal{R}_1(u_2) = \{\gamma \in U_1 \mid J_1(\gamma, u_2) \leq J_1(u_1, u_2)\ \forall u_1 \in U_1\}.$$

If player 2 is leading (hacker) then $u_2^* \in U_2$ is called a Stackelberg equilibrium for player 2, if for all $u_2 \in U_2$

$$\sup_{\gamma \in \mathcal{R}_1(u_2^*)} J_2(\gamma, u_2^*) \leq \sup_{\gamma \in \mathcal{R}_1(u_2^*)} J_2(\gamma, u_2),$$

then $u_1^* \in \mathcal{R}_1(u_2^*)$ is an optimal Stackelberg strategy for the follower.

I think that the Stackelberg equilibria are very importent for investigation of dangerous situations arising from attacks that are carried out by experienced hackers. Stackelberg security games are a modeling framework for scenarios in which a defender chooses a randomized security policy, and an adversary observes the distribution of the randomized policy and selects an attack accordingly [7].

VII. Conclusion

We have shown that it is possible to use the theory of differential games to the study of Flood-attacks. We have shown that in system "hacker-server administrator" there exist the Nash equilibria that are established in the system when some defined mediated connection between the external factors is reached.

References

[1] A. Guts and D. Lavrov, "Descrption of DDoS-attacks using cusp catastrophe," Mathematical Structures and Modelling, no. 1 (27), pp. 42–45, 2013.

[2] A. Guts and D. Lavrov, "Flood-attacks on conputer severs as catastrophe of type A_8," International Confeence Mathematical and computer modelling, pp. 33–34, 2017.

[3] M. Jonson, Differential game-based control methods for uncertain continuous-tme nonlinear systems. PhD. dissertation, University of Florida, 2011.

[4] A. Bressan, Noncooperative Differential Games. A Tutorial. Penn State University, 2010.

[5] F. Lewis, D. Vrabie and V. Syrmos, Optimal Control. New Jersey: John Wiley & Sons, Inc., 2012.

[6] T. Vahniy and A. Guts, "DDoS-atacks as differential game," Mathematical Structures and Modelling, no. 3 (39), pp. 182–186, 2016.

[7] P. Lee, A. Clark, B. Alomair, L. Bushnell, R. Poovendran, "Passivity-Based Distributed Strategies for Stochastic Stackelberg Security," Lecture Notes in Computer Science, Springer, Cham, vol. 9406, pp. 113–129, 2015.