Journal of Physics: Conference Series

PAPER • OPEN ACCESS

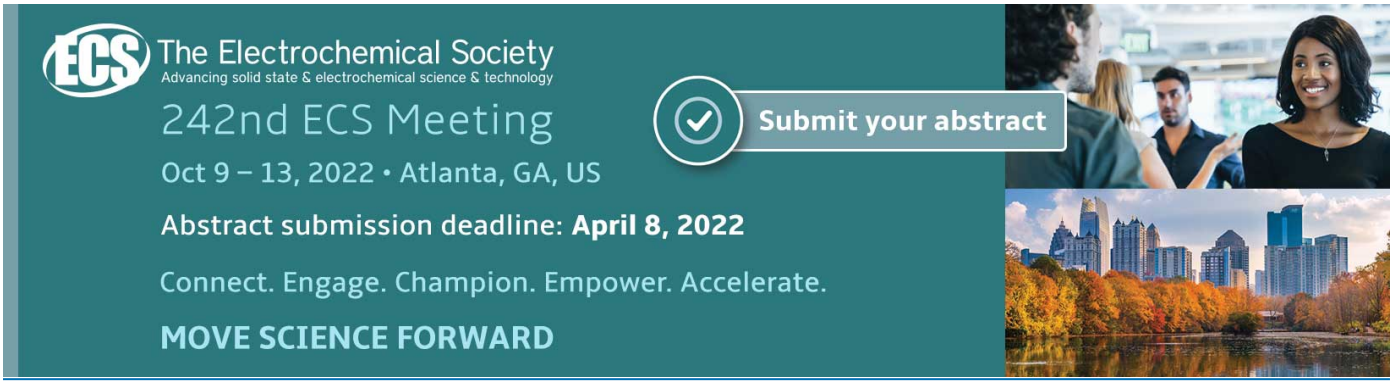
Mathematical differential game model of a computer system and its defence against DDoS-attacks

To cite this article: A K Guts 2022 *J. Phys.: Conf. Ser.* **2182** 012021

View the article online for updates and enhancements.

You may also like

- A passive DDoS attack detection approach based on abnormal analysis in SDN environment
Shimin Sun, Xinchao Zhang, Wentian Huang et al.
- A Comprehensive Analysis of DDoS attacks based on DNS
Lei Fang, Hongbin Wu, Kexiang Qian et al.
- DDoS Detection and Protection Based on Cloud Computing Platform
Tianwen Jili and Nanfeng Xiao



This content was downloaded from IP address 188.232.208.206 on 23/03/2022 at 16:48

Mathematical differential game model of a computer system and its defence against DDoS-attacks

A K Guts
Department of Cybernetics, Dostoevsky Omsk State University, pr. Mira, 55a, 644077 Omsk, Russia

E-mail: guts@omsu.ru

Abstract. The purpose of this article is a mathematical description of the DDoS-attack with the help of the differential game theory. The attacked computer system which has a performance limit is mathematically described. The hacker attack is successful if this limit is reached. The system administrator's strategy is successful if he can prevent the server from "falling". We find this strategy. Then we study an optimal Stackelberg strategies of hierarchial "administrator–hacker" game.

1. Introduction

The article deals with the task of defence against DDoS attacks. A DDoS (Distributed Denial of Service) attack is a denial of service hacker attack on a server. When it is executed, a situation is created in which users will not be able to access the site or web service due to its overload. The server lacks the required performance to service requests. As a result of the attack, the owners of resurses that are hosted on the server incurs serious losses.

2. Model of computer system

We constructed in [1] the model of computer system in the form of differential equation

$$\frac{dx}{dt} = [(p - p_0) - x^7(t)]G[x(t)] + (\tau - \tau_0), \tag{1}$$

$$t \in [0, T],$$

where x is the number of responses to requests (system resources involved in processing received packets) at time t, τ is traffic and p is a performance of computer system, and $G[x(t)]$ is the result of the processing requests at moment t. Here p_0 and τ_0 are "typical" characteristics for this server values.

In model (1) we took into account that the incoming request during decapsulation is processed at all levels of the OSI model, and that the attacks can performed simultaneously on the protocols of all seven levels.

In the case when only four levels of the OSI-model (network, transport, session, application) are taken into account, we have the equation

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


Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

The equations (1), (2) reflect the requirement that more traffic requires an increase in the number of responses to requests. 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.

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.

We have a daily, *stationary regime* of operation of a computer system, if

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

The stationary regimes $x = x(p, \tau)$ are found from the equilibrium equation

$$[(p - p_0) - x^m(t)]G[x] + (\tau - \tau_0) = 0.$$

In the case when $G[x] = x$ the stationary regimes can jump into each other if the controls p and τ are changed. Jumps are called *catastrophes*. For models (1) and (2), these are catastrophes like A_5 (butterfly) and A_8, which simulate a "falling" of system or its recovery.

Futher we use the theory of differential games. We have two player: τ is hacker control, and p is system administrator control.

Denote by $\mathbb{R}$ the set of real numbers.

3. System performance margin

It is obvious that the hacker is trying to increase traffic τ so that the system is not able to respond to requests. In other words, there is a certain segment $M = [x_1, x_2] \subset \mathbb{R}$ in which the function $x(t)$ is not long to take the value, i.e. $x(t) \notin M$. Compact set M will be called *target* or *terminal*.

Can a system administrator organize such a situation? What optimal strategy should he choose as a player? We will give answers to these questions.

Our equation (1) can be written as

$$\dot{x} = a(x, \tau) + b(x, p),$$

where

$$a(x, \tau) = -x^7 G[x] + (\tau - \tau_0), \quad b(x, p) = (p - p_0)G[x].$$

Let

$$\tau(t) \in Tr = [\alpha, \beta], \quad p(t) \in Pr = [\gamma, \delta].$$

Assume that

$$a(x, Tr) = \{a(x, \tau) : \tau \in Tr\} \ \ and \ \ b(x, Pr) = \{b(x, p) : p \in Pr\}$$

are the convex set for all $x \in \mathbb{R}$. (These conditions are valued for $G[x] = x$.)

Let the segment $[t_0, t_1] \subset [0, T]$ be given. The set $\tau[t_0, t_1]$ of admissible realizations of controls of the first player (hacker) is the set of all measurable functions $\tau : [t_0, t_1] \to Tr$. The set $p[t_0, t_1]$

of admissible realizations of the control of the second player (administrator) is called the set of all measurable functions $p : [t_0, t_1] \to Pr$.

The *positional strategy* of the first player is an arbitrary the function $\tau^{str} : \mathbb{R} \to Tr$.

Let us describe how a series of attacks by a hacker can be described.

A *series of hacker attacks* are sequential changes in traffic that can be at certain points in time. Therefore, we give the following definition.

Let $\Sigma = \{\sigma_i\}_{i=0}^{I}$ be a partition of the segment $[t_0, t_1] \subset [0, T] : t_0 = \sigma_0 < \sigma_1 < ... < \sigma_I = t_1$. The pair (τ^{str}, Σ) that is composed of the positional strategy of the first player τ^{str} and the partition Σ of the segment $[t_0, t_1]$ is called the *control rule* of the first player on the segment $[t_0, t_1]$.

Actually, a control rule of the first player is the series of attacks by a hacker.

The *attacked system* that corresponds to the initial state $x(t_0) = x_0$, a control rule (τ^{str}, Σ) and an admissible control realization $p \in p[t_0, t_1]$ we mean an absolutely continuous function $x : [t_0, t_1] \to \mathbb{R}$, that is determined from the step-by-step equations

$$\dot{x}(t) = a(x(t), \tau^{str}(\sigma_i) + b(x(t), p(t)),$$

which must hold for almost all $t \in [\sigma_i, \sigma_{i+1}]$ and for all $i = 0, ..., I - 1$. Moreover, the initial position for the segment $[\sigma_0, \sigma_1]$ is x_0, and the initial position $x(\sigma_i)$ for the segment $[\sigma_i, \sigma_{i+1}]$ coincides with the end position $x(\sigma_i)$ of the segment $[\sigma_{i-1}, \sigma_i]$.

We can say that the attacked system $x(t)$ exists and is unique for given the initial position $x(t_0) = x_0$, the partition Σ, the positional strategy of the first player (hacker) τ^{str}, and the admissible realization of the control $p \in p[t_0, t_1]$,

Let's denote it as follows:

$$x_\tau^{att}(t, t_0, x_0, \Sigma, \tau^{str}, p) = x(t) \quad \forall t \in [t_0, t_1].$$

Likewise, we define the positional strategy of the second player (administrator) and the *defended system* $x_p^{def}(t, t_0, x_0, \tau, p^{str}) = x(t)$, corresponding to the initial position $x(t_0) = x_0$, partition Σ and admissible realization of the first player's control $\tau \in [t_0, t_1]$.

We say that the control rule (τ^{str}, Σ) guarantees ε-*capture* on the segment $[t_0, t_1]$ for the initial state x_0, if for any realization of the control $p[t_0, t_1]$ there exists a time moment $t \in [t_0, t_1]$ such that

$$\rho(x_\tau^{att}(t, t_0, x_0, \Sigma, \tau^{str}, p), M) < \varepsilon,$$

where

$$\rho(x, M) = \inf_{m \in M} |x - m|.$$

The control rule (p^{str}, Σ) guarantees the *deviation* on the segment $[t_0, t_1]$ for the initial state x_0, if for any realization of the control $\tau \in \tau[t_0, t_1]$ we have

$$x_p^{def}(t, t_0, x_0, \Sigma, \tau, p^{str}) \notin M \quad \forall t \in [t_0, t_1].$$

Let a number $\varepsilon > 0$ and the control rules $(\tau^{str}, \Sigma_\tau), (p^{str}, \Sigma_p)$ of the first and second players on the segment $[0, T]$ are given.

A couple of rules $((\tau^{str}, \Sigma_\tau), (p^{str}, \Sigma_p))$ is called ε-*optimal*, if for any initial position $x_0 \in \mathbb{R}$ such that $\rho(x, M) > \varepsilon$, the following alternative holds:

1) there exists a time instant $T_0 \in [0, T]$ such that the control law $(\tau^{str}, \Sigma_\tau)$ guarantees ε-capture on the segment $[0, T_0]$, and the control rule (p^{str}, Σ_p) guarantees the deviation on the segment $[0, T_0]$

or

2) the control law (p^{str}, Σ_p) guarantees the deviation on the segment $[0, T]$.

In other words, a couple of control rules are ε-optimal, if the hacker at some point manages to almost bring down the system, but the administrator eliminates the threat, or, alternatively, the administrator successfully repels attacks.

In the article [2,3] the algorithms for constructing of an ε-optimal pair of control rules are given for a certain choice of ε. Therefore, the task of repelling DDoS-attacks within the framework of the computer system models (1), (2) is solvable.

4. Open-Loop Stackelberg equilibria

Now we turn to a class of hierarchial differential games in which onee player has priority of moves over other players, and shall study the Stackelberg strategies for our model of computer system.

In these games we have the leader and follower. The leader announces his strategy, and we first look for the follower's best response to any announced strategy of the leader. His strategy is derived from solving the optimization problem of the follower given the leader's strategy.

Consider the following differential game "administrator–hacker"

$$\frac{dx}{dt} = f(x, \tau, p) \equiv -x^m + px + \tau, \quad x(0) = x_0, \tag{3}$$

$$m = 5, 8,$$

with winning functions

$$J_a[x_0, \tau, p] = \int_0^T v_a(x, \tau, p)dt, \quad v_p(x, \tau, p) = p - \frac{p^2}{2} - \frac{x^2}{2},$$

$$J_h[x_0, \tau, p] = \int_0^T v_h(x, \tau, p)dt, \quad v_h(x, \tau, p) = \tau - \frac{\tau^2}{2} - \frac{x^2}{2}.$$

4.1. Leader is administrator

Let administrator announces the strategy $p = p^*(t)$ at time moment $t = 0$. The hacker, taking this strategy as given, chooses his control path $\tau^*(t)$ so as to maximize his winning function.

In other words, we look for an optimal open-loop Stakelberg's strategy for hacker $\tau^*(t)$ such that

$$\tau^*(t) = arg \max_{\tau(t)} J_h[x_0, \tau(t), p^*(t)].$$

Denoting by λ the vector of costate variables for this maximization problem, the hacker's Hamiltonian is

$$H_h(x, \tau, \lambda) = v_h(x, \tau, p^*(t)) + \lambda(t) f(x, \tau, p^*(t)) =$$

$$= \tau - \frac{\tau^2}{2} - \frac{x^2}{2} + \lambda[-x^m + p^*(t)x + \tau].$$

Given the time path $p^*(t)$, the optimality conditions for the hacker's strategy are [4]:

$$\frac{\partial v_h}{\partial \tau} + \lambda(t)\frac{\partial f}{\partial \tau} = 0, \tag{4}$$

$$\frac{d\lambda}{dt} = -\frac{\partial v_h}{\partial x} - \lambda(t)\frac{\partial f}{\partial x} \tag{5}$$

or

$$1 - \tau + \lambda = 0,$$

$$\frac{d\lambda}{dt} = x - \lambda[-mx^{m-1} + p^*(t)].$$

The above conditions are sufficient for the optimality of $\tau(t)$ because H_h is jointly concave in the variables x and τ.

Hence we have optimal Stackelberg strategy of hacker

$$\tau^*(t) = 1 + \lambda(t),$$

where $\lambda(t)$ can be found from system of differential equations:

$$\begin{cases} \frac{d\lambda}{dt} = x - \lambda[-mx^{m-1} + p^*(t)], \\ \frac{dx}{dt} = -x^m + xp^*(t) + 1 + \lambda, \\ x(0) = x_0, \quad \lambda(T) = 0. \end{cases}$$

Note that the above conditions (4), (5) are sufficient for the optimality of $\tau^*(t)$, if H_h is jointly concave in the variables x and τ [4].

4.2. Leader is hacker

Let hacker announces the strategy $\tau = \tau^*(t)$ at time moment $t = 0$. The administrator, taking this strategy as given, chooses his control path $p^*(t)$ so as to maximize his winning function, i.e. we look for an optimal open-loop Stakelberg's strategy for administrator $p^*(t)$ such that

$$p^*(t) = arg \max_{p(t)} J_a[x_0, \tau^*(t), p(t)].$$

We have the administrator's Hamiltonian

$$H_a(x, \tau^*, \lambda) = v_a(x, \tau^*(t), p) + \lambda(t) f(x, \tau^*(t), p) =$$

$$= p - \frac{p^2}{2} - \frac{x^2}{2} + \lambda[-x^m + px + \tau^*(t)].$$

Given the time path $\tau^*(t)$, the optimality conditions for the hacker's strategy are [4]:

$$\frac{\partial v_a}{\partial p} + \lambda(t)\frac{\partial f}{\partial p} = 0, \tag{6}$$

$$\frac{d\lambda}{dt} = -\frac{\partial v_a}{\partial x} - \lambda(t)\frac{\partial f}{\partial x} \tag{7}$$

or

$$1 - p + \lambda x = 0,$$

$$\frac{d\lambda}{dt} = x - \lambda[-mx^{m-1} + p].$$

Hence we have optimal Stackelberg follower-strategy of administrator

$$p^*(t) = 1 + \lambda(t)x(t),$$

where $\lambda(t)$ can be found from system of differential equations:

$$\begin{cases} \frac{d\lambda}{dt} = x - \lambda[-mx^{m-1} + 1 + \lambda x], \\ \frac{dx}{dt} = -x^m + x(1 + \lambda x) + \tau^*(t), \\ x(0) = x_0, \quad \lambda(T) = 0. \end{cases}$$

The above conditions (6), (7) are sufficient for the optimality of $p^*(t)$, if H_a is jointly concave in the variables x and p [4].

5. Acknowledgments

Author wishes to acknowledge for encouragement from Dr. L.A. Volodchenkova.

[1] Guts A K 2020 *14th International IEEE Scientific and Technical Conference Dynamics of Systems, Mechanisms and Machines, Dynamics 2020 – Proceedings* 9306135
[2] Dvurechensky P E and Ivanov G E 2012. *Proceedings of MFTI* **4** 51
[3] Dvurechensky P E and Ivanov G E 2014. *J. of computational mathematics and mathematical physics* **54** 224.
[4] Dockner E J, Jergensen S, Ngo Van Long and Sorger G 2000 *Differential Games in Economics and Management Science* (Cambridge: Cambridge University Press) p 114