Game Theoretic Modeling of Network Security Attacks

Oleksii Ignatenko, Oleksander Sinetskiy
IPS NASU 40 Academika Glushkova str, Kyiv 187, Ukraine

o.ignatenko@gmail.com

ABSTRACT

This paper deals with modeling of network's dynamic using game theory approach. The process of interaction among players (network users), trying to maximize their payoffs (e.g. throughput) could be analyzed using game-based concepts (Nash equilibrium, Pareto efficiency, evolution stability etc). In this work we presented the model of TCP network's dynamic and proved existence and uniqueness of solution, formulated payoff matrix for a network game and found conditions of equilibrium existence depending of loss sensitivity parameter. We consider influence if denial of service attacks on the equilibrium characteristics and illustrate results by simulations.

1.0 INTRODUCTION

It is almost impossible now to imagine our life without computer networks. Only for several decades, the Internet has rapidly transformed the ways in which individuals, societies and even governments communicate, exchange information and conduct their economic and social activities. And this process is far from the ending. As was envisioned recently by Google's executive chairman Eric Schmidt: "the internet will disappear as everything in our life gets connected. There will be so many devices, sensors, things that you are wearing, things that you are interacting with that you won't even sense it. It will be part of your presence all the time."

It seems that future Internet has to be self-organizing, self-protecting, and self-optimizing. This next-generation communication environment will include interaction of intelligent devices that are capable of autonomously take decisions within highly dynamic and rapidly changing digital world. However, the continuous (and successful till now) development of networks, which is accompanied by exponential growing of their complexity, heterogeneity and distributiveness and which appears natural at the present time, creates new challenging problems. As mentioned in [1], to address these problems with appropriate approach we need to develop a new set of models based on control theory, game theory, and network optimization.

First, let us introduce a problem on a high level. Consider a interaction between selfish users in a network (network here is some common pool with limited resources). Each user can adopt a method of action (strategy) which have influence on whole network and other users. The examples of actions are: choose protocol, change rate or route of data flows. For every possible combination of adopted strategies (outcome) there is a reward or utility for each user, which indicates his/her preferences over outcomes. Selfishness (or rationality in game theory terminology) means that a user wants to maximize utility. For instance, when user wants to download big file he prefers to receive as much network resources as possible. However, if user wants to read news then small but stable connection is sufficient. This situation leads to obvious conflict when summary users' demand is bigger then network supply. If this happens network drops or delays users' data, so generally it is not good for users. From the other side, network underloading (when demand is smaller then network capacity) is also undesirable because leads to inefficiency of resource using.

Delivering information about network state to end user is a challenging problem and crucial part of any feedback based protocol. As a rule user has knowledge about successful delivery of his data (in other words he knows that network is probably underloaded) and about overload event (if he doesn't receive successful

ACK – acknowledgement packet) with some delay. This type of information is called binary feedback. The natural rate control based on this information called AIMD (additive increase, multiplicative decrease) scheme. There are another possibilities, but it was proved that AIMD algorithm will oscillate near the point of effective (all bottle-necks will be loaded) and fair (in some sense) allocation of network resources. AIMD was the core of first version of first successful protocol – TCP, which still carries 70 percent of the Internet traffic. Nowadays, TCP isn't one protocol but big family (number keeps increasing) of algorithms with different implementations of the origin idea.

Protocol development went through the competitive evolution between different protocols, abandonment of some of them and appearance of new ones. The possibility to deploy new versions of protocols gives user control to improve performance of his connection by choosing suitable algorithm. When many users are trying to achieve better performance it is difficult to predict consequences of such a competition. There is a problem how to ensure stable, fair and effective network behavior in the situation of dynamic and antagonistic interaction of selfish users. First natural approach to address this problem with optimization framework was developed in work by Kelly et al. [3]. Later it was shown that congestion control, routing and scheduling in wired and wireless networks can be thought of as fair resource allocation. The protocols in this framework are nothing else as algorithms that allow a decentralized solution of the problem. This idea to consider network as an algorithm for solving maximization problem of total network utility (sum of users' utilities) proved to be very fruitful [2]. The limitation in this approach is that protocol (in centralized or decentralized manner) dictates what strategy user should use.

It is natural to assume that users try to improve performance of their connection by choosing suitable protocol. The problem here lies in interaction between different implementations of TCP which could be "unfriendly". This means that one implementation is more "aggressive" and another is more "peaceful" in competition for resources. The question of protocols interaction is quite complex. Building analytic model for predicting network behavior for different protocols is a challenging problem. There are many approaches of investigation of complex networks from different directions (static, dynamic, deterministic etc). There is, however, novel systematic approach towards network modeling – the game theory. Game theory addresses problems in which multiple players with conflicting goals compete with each other. The evolutionary games concept is a part of game theory that focuses on studying interactions between populations rather than individual players. One of the earliest publications about the use of evolutionary games in networking is [4] that study through simulations some aspects of competition between TCP users. For this model it was shown that dynamic of this process described by difference equation has stable solution and users payoffs are forming a structure of evolutionary game known as Hawk-Dove game. Also there were identified conditions under which equilibrium is evolutionary stable.

There is another possible reason of inefficient, unstable or unpredictable network behavior – security violation. Unfortunately, networks have many security issues: illegal data access, viruses, network attacks, etc. One of the most dangerous attacker's activities are Denial of Service (DoS) attacks. DoS attack aims to stop the service provided by a target. When the traffic of a DoS attack comes from multiple sources, it called a Distributed Denial of Service (DDoS) attack. By using multiple attack sources, the power of a DDoS attack is amplified and the problem of defense is made more complicated. Currently we have numerous DoS attack types. Each attack uses some special exploit of Internet protocols or software weaknesses. Recently novel type of attack was developed. This low-rate attacks, using carefully calculate timing, imply significant inefficiencies that tremendously reduce system capacity or service quality. In the literature, this kind of network intrusion is called shrew attack or Reduction of Quality (RoQ) attack. This constant development of new attacks demands new solutions especially in attack detection area.

Intrusion Detection Systems (IDSs) is a software which is used to monitor events occurring in a network. An IDS is also used to analyze these events in order to determine whether an attack has occurred. Once an attack is detected, a report is sent to the network administrator. Current IDSs are not very sophisticated and rely on ad hoc schemes and experimental algorithms. Due to these, IDSs need theoretical tools to handle sophisticated, organized attacks. Game theoretic approaches have been proposed by many researchers to improve network security, for example to analyze high level "security investment game", but these models usually don't include network dynamics.

Game theory provides mathematical base for analyzing and modeling security problems with many agents which could interact in complex, dynamic environment. The advantage of game theory approach is s possibility of analyzing many different scenarios before adopting a certain strategy. Using mathematical modeling we can simulate network topology, controlling algorithms and users' actions. This model could greatly improve network administration by predicting future security problems and likely behavior of users *before* we actually start to build our network.

On the other hand network security measurements involve risk assessment. For example, one of the metrics is the probability of it being attacked. If we adopt game theory view on network dynamic then we can formulate conditions when interaction between rational users leads to an equilibrium state of the network. Network attack is a result of malicious actions of attacker. Attack changes equilibrium characteristics and could be therefore detected.

In this work we describing integrated approach based on game theory models. First, we introduce formal model of TCP network dynamic. We mainly focus on AIMD behavior because it is the most important mechanism of TCP congestion control. Using dynamic systems theoretic results we show existence and stability of network resources allocation point. Then we consider game between users in the network and formulate conditions for Nash equilibrium existence and uniqueness. We introduce network attacker into system and estimate attack influence on equilibrium characteristics. Finally, we show simulation results and make conclusions of future trends.

1.0 GAME THEORY. DEFINITIONS

We will limit our scope with non-cooperative games in strategic or normal form. A non-cooperativeness here does not imply that the players do not cooperate, but it means that any cooperation must be self-enforcing without any coordination among the players. Strict definition is as follows.

A non-cooperative game in strategic (or normal) form is a triplet $G = \{N, \{S_i\}_{i \in N}, \{u_i\}_{i \in N}\}$, where:

- N is a finite set of players, i.e., $N = \{1,...,N\}$;
- S_i is the set of admissible strategies for player *i*.
- $u_i : S \to R$ is the utility (payoff) function for player *i*, with $S = S_1 \times ... \times S_N$ (Cartesian product of the strategy sets).

A game is said to be static if the players take their actions only once, independently of each other. In some sense, a static game is a game without any notion of time, where no player has any knowledge of the decisions taken by the other players. Even though, in practice, the players may have made their strategic choices at different points in time, a game would still be considered static if no player has any information on the decisions of others. In contrast, a dynamic game is one where the players have some information about each others' choices and can act more than once, and where time has a central role in the decision-making. When dealing with dynamic games, the choices of each player are generally dependent on some available information. There is a difference between the notion of an action and a strategy. A strategy can be seen as a mapping from the information available to a player to the action set of this player.

Based on the assumption that all players are rational, the players try to maximize their payoffs when responding to other players' strategies. Generally speaking, final result is determined by non-cooperative maximization of integrated utility. In this regard, the most accepted solution concept for a non-cooperative game is that of a Nash equilibrium, introduced by John F. Nash. Loosely speaking, a Nash equilibrium is a state of a non-cooperative game where no player can improve its utility by changing its strategy, if the other players maintain their current strategies. Formally, when dealing with pure strategies, i.e., deterministic choices by the players, the Nash equilibrium is defined as follows:

A pure-strategy Nash equilibrium (NE) of a non-cooperative game $G = \{N, \{S_i\}_{i\in N}, \{u_i\}_{i\in N}\}$ is a strategy profile $s^* \in S$ such that for all $i \in \mathrm{N}$ we have the following:

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \text{ for all } s_i \in S_i .$$

Here $s_{-i} = [s_j]_{j\in \mathrm{N}, i\neq j}$ denotes the vector of strategies of all players except *i*. In other words, a strategy profile is a pure-strategy Nash equilibrium if no player has an incentive to unilaterally deviate to another strategy, given that other players' strategies remain fixed.

Another important concept is Pareto-dominance, which allow two strategies to be compared. The strategy profile $s^* \in S$ Pareto-dominates $s \in S$ if for all $i \in \mathrm{N}$ $u_i(s^*) \geq u_i(s)$. The strategy profile $s^* \in S$ is a Pareto-optimal profile if it is dominated by no other profile. In Pareto-optimal profile no player could make his payoff better without worsen payoff of some other player. Now consider the notion of best response. The best response (BR) of player i to the strategy profile s_{-i} is a correspondence $BR_i(s_{-i}) = \arg\max_{s_i\in S_i} u_i(s_i, s_{-i})$. The BR is a correspondence that is a set-valued function. In practice this means that for some situations player has (possible) many strategies with the same payoff. Using best response notion we can characterize Nash equilibrium as follows. A pure-strategy Nash equilibrium of a non-cooperative game $G = \{N, \{S_i\}_{i\in N}, \{u_i\}_{i\in N}\}$ is a strategy profile $s^* \in S$ such that $s^* \in BR(s^*)$. The strong side of Nash concept is that every game has at least one NE (under mild assumptions). From the other hand it is common situation to meet many NEs or to have Pareto-dominated NE.

Let us define the last metric. From network performance point of view it is important to measure the aggregated payoff. The social optimum of a game is a maximum of the sum of the utilities of all players. Any social optimum is Pareto optimal.

2.0 GAME THEORY FOR SECURITY PROBLEMS

Let us fix following notations to explain attack-defense interaction in networks. **Network** is a collection of nodes and links. Node can be a server, user or router. Legitimate users are rational and intersted in minimizing their own costs. Any user that launches an attack on a network is called **attacker**. IDS is a hardware or software system used to monitor the events occurring in a network or computer system. The main purpose of IDS is of course detection of attack. There are two possible issues: false alarms and missing detection.

Several different approaches have been proposed for detecting intrusions. A currently widely used method is to check monitored events (packets in the network, log files, etc.) against a known list of security attack signatures. This approach has the advantage of enjoying a relatively small false alarm rate and ease of implementation. The disadvantages are the need to maintain and update the attack signature database, and the restriction to detection of only the known attacks documented in the database. These information structures are also useful in detecting more organized multistep attacks. An alternative approach is the anomaly detection, where changes in the patterns of nominal usage or behavior of the system are detected.

Although this approach increases the probability of detecting undocumented new attacks it is difficult to implement, and has often a higher false alarm rate. We introduce an idea to develop game theory based detection of anomalies. A significant shortcoming of the current IDSs is the lack of a unifying mathematical framework to put the pieces into a perspective. Game theory can provide a basis for development of formal decision and control mechanisms for intrusion detection. Specifically, game theoretic models can be used to address issues like the following:

•Develop game model of network using huge amounts of data from detection mechanisms.

•Finding weaknesses and possible targets of an attacker in a large complex system.

•Reconfiguring the security system given the severity of attacks and making decisions on trade-offs like increasing security versus increasing system overhead or decreasing efficiency.

•Deciding on where to allocate or reallocate limited resources in real time to detect significant threats to vital subsystems in a large networked system.

• Analyzing of and modeling the interaction between different types of protocols, allocation algorithms and detection schemes.

Game theory provides a framework to model interaction between selfish, competitive users, malicious attackers and system administrator. Three key elements of such a system are: network dynamic model, game model and scenarios of malicious actions (attacks). Network dynamic modeling is a challenging problem, which was developed last decades. The work of F.Kelly et al. [3] was the first example of considering of Internet network resource allocation as an optimization problem. Later many authors [see for example 7 – 10] have developed generalizations of this framework. There are many approaches to investigation of complex networks from different angles (static, dynamic, deterministic etc) using control theory, Petri nets, Markov chains etc.

The evolutionary games concept is a part of game theory that focuses on studying interactions between populations rather than individual players. One of the earliest publications about the use of evolutionary games in networking is [11] that study through simulations some aspects of competition between TCP users. The evolutionary games based on the concept of the ESS (Evolutionary Stable Strategy), defined in 1972 by the biologist Maynard Smith [12]. Fundamental survey of applications of game theory to networks is [9]. In this paper we develop the line of research presented in [13] by Altman et al. We consider a model of users which are using different TCP connections. For this model it was shown that dynamic of this process described by difference equation has a stable solution and users payoffs are forming a structure of evolutionary game known as Hawk-Dove game. Also there were identified conditions under which equilibrium is evolutionary stable.

Considering distributed network of selfish players (e.g. the Internet) we meet problem of efficiency measuring. It is obvious that centralized planning could optimize overall performance of the system. Unfortunately, there are many reasons why it is not possible to construct centralized control over the Internet. However, game theory paradigm generated unexpected idea for dealing with such complex decentralized systems. If game has unique NE and users are rational players then network will operate near this point even without coordination. Game structure, defined by utilities and strategies determine network evolution toward equilibrium point. So it is important to characterize the equilibrium efficiency and to find conditions of existence and uniqueness. A well-known way of characterizing the efficiency of the NE is to calculate whether or not it is Pareto-optimal. However, it is not uncommon for non-cooperative game to have not Pareto-optimal NE. In the work [14] of Papadimitriou was introduced a concept of Price of Anarchy measure. Price of Anarchy (PoA) is equal to the ratio of the highest value of the social optimum to the lest optimal NE of the game. Another important metric is the Price of Stability which is defined similarly by replacing the denominator of the PoA with the best NE of the game.

We propose a concept for improving security through developing a game theoretic model for better understanding of processes in networks. On the first stage we build comprehensive network model with definite static game structure, which could be dependent on different parameters. Nash equilibriums determine possible dynamic of associated repeated game, so we could calculate metrics and characteristics. Based on this calculation IDS make decisions about anomalies and intrusions.

3.0 NETWORK DYNAMIC MODEL

We start with notation of network modeling. All propositions in this and following chapters could be found in [16] with detailed explanation.

Consider a network with M nodes. Every node has at least one service link with limited overall capacity p_i, $i = 1,...,M$ (e.g. processing rate, CPU time or network bandwidth). Let $I = \{1,...,M\}$, $K = \{1,...,L\}$ be sets of indexes of nodes and service links respectfully. There are N users, connected to this network. Let $x_j(t)$ be the transmission rate of j user, where $j \in J = \{1,...,N\}$. There is natural assumption about vector of rates $\overline{x} = (x_1,...,x_N)$: $x \in R_+^N$. Users choose their rates $x_j(t)$ at moment t. This means that packets streaming through link $k \in K$ with summary rate $y_k = \sum_{j \in s(k)} x_j(t)$, where $s(k)$ is a set of indexes of users, which use this link. In our simplified model there are no queues and information delays. If sum of transfer rates y_k less then node capacity p_k, then all packets are served. If summary rate of flows using the node's links is equal or bigger than the node capacity then overload event occurs (overload here is a synonym of packet loss). We will assume that routing is deterministic and uncontrolled and information about overload delivers to users momentarily. Let us fix the following notation throughout this paper. Denote $u_k(t)$, $k \in K$ as the service rate of k's link. The constituency matrix is the $M \times L$ matrix C whose c_{ij} element is equal to 1 if i's link belongs to j's node and otherwise is 0. Now we define a control set $U \subset R_+^K$, which contains all possible service rates for the system. Let U be a convex compact set from R_+^K and for any $u \in U$ the inclusion $\alpha u \in U$ holds for any $\alpha \in [0,1]$.Let P be $diag\{p_1,..., p_M\}$ - diagonal matrix. The routing matrix R is the $M \times M$ matrix defined for $i, j \in P$. Element r_{ij} is equal to 1 if the output of i's link is the input of j's link and otherwise is 0. The input matrix A is the $L \times N$ matrix defined for $i \in K, j \in J$. Element a_{ij} is equal to 1 if j's user uses i's link and otherwise is 0.

Overload conditions

When the system produces overload and how one can analytically predict it? This is important problem of network modeling.

Proposition 3.1. (Stability condition) If for $x(t)$, $t \in [t_0, t_1]$ there exist $u \in U$, $\alpha \in [0,1)$, such that $P^{-1} \sum_{k=0}^{M-1} \left(R^T\right)^k A\overline{x}(t) = \alpha u$, then the system doesn't produce any overload events.

If rates x satisfy stability condition then network will be lossless. But from practical point of view, there are many problems with applicability of this condition. First, in real network each user doesn't have information about system's current state and about rates of other users so he cannot calculate proper rate. Second, user cannot choose any rate he wants (at least in TCP scheme). Instead he chooses protocol, controlling his rate.

Geometric approach

Let $\overline{x}_0$ be an initial vector of rates and $\overline{\alpha}$, $\overline{\beta}$ vectors of parameters. According to original AIMD scheme user rates are increasing between overloads with rate $\overline{\alpha}$. When overload occurs rate drops to $\overline{\beta}x$. Now we will put into formal definitions.

Denote W as a set $\left\{ w \in R_+^N \mid P^{-1}\sum_{k=0}^{M-1}\left(R^T\right)^k A\, w \in U \right\}$. Let us define function $\alpha(x,X)=\max\{\alpha \ge 0 : \alpha x \in X\}$ and set $V=\{v \in U : \alpha(v,U)v = v\}$. Set V is a subset of boundary of U, which belongs to $\operatorname{int} R_+^K$ (V is "active" in the sense that in these and only in these points overload are happened).

Define t_i, $i \ge 1$ as a first moment of time $t_i > t_{i-1}$, such that $x(t_i) \in V$. We will assume that the RTT (round trip times) are the same for all connections and losses are synchronized: when the combined rates attain capacity, all connections suffer from a loss.

Consider following equation

$$\dot{x}(t) = \overline{\alpha} - \sum_{i=1}^{N_t}(I-B)x(t_i)\delta(t-t_i), \tag{1}$$

where δ is delta-function, $B = diag\{\beta_1,\ldots,\beta_N\}$, $N_t = \max\{n : t_n \le t\}$. Equation (1) is well-defined Caratheodory equation with discontinuous right-hand side, differential equations with impulses have been examined in many papers, which cannot all be referenced here. It is known that there is an almost continuous solution (continuous in all points except a set of measure zero)

$$x(t) = \alpha t - \sum_{i=1}^{N_t}(I-B)x(t_i)\eta(t-t_i), \tag{2}$$

where η is the Heaviside step function. Explicit formula (2) is not very practical but gives us important information about solution existence and its continuity in almost all points.

Condition 3.1. For any $x \in W$, such that $P^{-1}\sum_{k=0}^{M-1}\left(R^T\right)^k Ax \in V$ it is true that $Bx \in W$.

Let us explain Condition 2.1 informally. W is the vector set of possible users rates. W is convex compact set and $x(t) \in W$ for $t \ge t_0$. As mentioned $x(t)$ is an almost continuous function, and drops only happened when $x(t) \in V$. After drop event users rates equal to $Bx(t)$. The condition 2.1 means that after applying decreasing operator B user rate still will be in the admissible set W.

Main result

Now we can formulate the main result of this section – existence and uniqueness of the limit solution.

Proposition 3.2. Let us consider admissible pair $\overline{\alpha}$, $\overline{\beta}$. If Condition 3.1 holds then for any $\overline{x}_0 \in W$ solution of (1) exists and is converging to unique periodical solution $\hat{x}(t)$.

Using this property, we can calculate $\overline{x}^*$ directly $\overline{x}^* = (I-B)^{-1}\overline{\alpha}T = T\overline{\gamma}$.

Now we consider a competition between users which use AIMD version of TCP with different parameters. Their connections are sharing a common network. We will assume that users send their packets exactly the same way, so we can reduce network topology to single link type with capacity c, calculated from the solution (2).

4. NETWORK GAME MODEL

In order to formulate game for our dynamic system in strategic form we must specify the players, their strategies, and their potential payoffs. We assume that there are N AIMD strategies s_i with control parameters (α_i, β_i), $i = 1,\ldots,N$. Denote S as a set of all possible strategies. We consider payoff of the form $J_i(s) = Thp_i(s) - \lambda R(s)$, where $\bar{s} = (s_1,\ldots,s_N)$ - vector of strategies; $Thp_i(s) = 0.5(1+\beta_i)x_i^*$ - average throughput of i 's player; $\lambda \geq 0$ - tradeoff parameter (sensitivity to losses); $R(s) = \dfrac{1}{T(s)}$ - loss rate.

Example. Let us calculate payoffs for two strategies:

$$J_1(s_i,s_i) = J_2(s_i,s_i) = \frac{(1+\beta_i)}{4}c - \lambda\frac{2\gamma_i}{c},\ J_1(s_1,s_2) = \frac{(1+\beta_1)\gamma_1 c}{2(\gamma_1+\gamma_2)} - \frac{\lambda}{c}(\gamma_1+\gamma_2),$$

$$J_1(s_2,s_1) = \frac{(1+\beta_2)\gamma_2 c}{2(\gamma_1+\gamma_2)} - \frac{\lambda}{c}(\gamma_1+\gamma_2),\ J_2(s_1,s_2) = J_1(s_2,s_1),\ J_2(s_2,s_1) = J_1(s_1,s_2)$$

Equilibrium in N protocols game.

Consider game with N AIMD strategies. We assume that all s_i are ordered lexicographically, $s_1 \geq s_2 \geq \ldots \geq s_N$, where $s_i \geq s_j$ means that $\alpha_i \geq \alpha_j$ and $\beta_i \geq \beta_j$. In other words protocols are sorted by aggressiveness ordering.

Proposition 4.1. If λ is sufficiently small than the most aggressive protocol is dominant strategy.

Proof. Suppose $\alpha_1 \geq \alpha_i$, $\beta_1 \geq \beta_i$ for all $i = 2,\ldots,N$. Consider payoffs for the first player $J_1(s_1,s_{-1})$ and $J_1(s_j,s_{-1})$. Let us find period for both strategy profiles:

$T(s_1,s_{-1}) = \dfrac{c}{\gamma_1 + A}$, where $A = \sum\limits_k \gamma_k$ is sum, defined by strategy set s_{-1}, $T(s_j,s_{-1}) = \dfrac{c}{\gamma_j + A}$. Note, that $T(s_1,s_{-1}) < T(s_j,s_{-1})$.

Calculate throughputs:

$$Thp_1(s_1,s_{-1}) = \frac{(1+\beta_1)x_1^*}{2} = \frac{\gamma_1(1+\beta_1)c}{2(\gamma_1+A)} = \frac{(1+\beta_1)c}{2(1+A/\gamma_1)},\ Thp_1(s_j,s_{-1}) = \frac{(1+\beta_j)x_j^*}{2} = \frac{(1+\beta_j)c}{2(1+A/\gamma_j)}.$$

Calculate payoffs:

$$J_1(s_1,s_{-1}) = Thp_1(s_1,s_{-1}) - \frac{\lambda}{c}(\gamma_1 + A),\ J_1(s_j,s_{-1}) = Thp_1(s_j,s_{-1}) - \frac{\lambda}{c}(\gamma_j + A).$$

Condition of dominating of first strategy is

$$Thp_1(s_1,s_{-1}) - \frac{\lambda}{c}(\gamma_1 + A) > Thp_1(s_j,s_{-1}) - \frac{\lambda}{c}(\gamma_j + A),\ \frac{(1+\beta_1)c}{2(1+A/\gamma_1)} - \frac{(1+\beta_j)c}{2(1+A/\gamma_1)} > \frac{\lambda}{c}\gamma_1,$$

$$\lambda < \frac{c^2}{\gamma_1}\left[\frac{(1+\beta_1)c}{2(1+A/\gamma_1)} - \frac{(1+\beta_j)c}{2(1+A/\gamma_j)}\right].$$

And since expression in right side is positive we obtain the result.

For more subtle results about equilibrium's characteristics see [16].

Nash Mixed and Pure in Two Protocols Game

Here we investigate the game for two protocols and find conditions for Nash equilibrium. From definition it is clear that $J_i(s_k,s_k)=J_j(s_k,s_k)$ - we will write just $J(s_k,s_k)$, $J_i(s_k,s_p)=J_j(s_p,s_k), j\in\{1{,}2\}\setminus i$.

Using standard techniques for calculating Nash we obtain:

$$J_1(s_1)=pJ(s_1,s_1)+(1-p)J(s_1,s_2)\,,\; J_1(s_2)=pJ(s_2,s_1)+(1-p)J(s_2,s_2)$$

assuming the probability of player 2 using the first strategy is p. In Nash equilibrium the payoff can't be further increased, so these two values should be indistinguishable, which leads to the following equation

$$pJ(s_1,s_1)+(1-p)J(s_1,s_2)=pJ(s_2,s_1)+(1-p)J(s_2,s_2)$$

Or, after solving it for p:

$$p=\frac{J(s_1,s_2)-J(s_2,s_2)}{(J(s_1,s_2)-J(s_2,s_2))+(J(s_2,s_1)-J(s_1,s_1))}$$

Taking into account that p is a probability, we impose a natural restrictions on it: $0\le p\le 1$, where cases with $p=1$ or $p=0$ result in game having a pure-strategy equilibrium (with dominant strategy s_1 and s_2, respectively), and $0<p<1$ corresponds to the case of mixed-strategy Nash equilibrium.

Should we investigate the conditions for the former, we get

$$J(s_1,s_2)-J(s_2,s_2)=\frac{-\lambda(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}{c(1-\beta_2)(1-\beta_1)}+\frac{c\alpha_1(1+\beta_1)(1-\beta_2)}{2(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}+\frac{2\lambda\alpha_2}{c(1-\beta_2)}+\frac{1}{4}C(1+\beta_2)\,.$$

$$J(s_2,s_1)-J(s_1,s_1)=\frac{-\lambda(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}{c(1-\beta_2)(1-\beta_1)}+\frac{c\alpha_2(1+\beta_2)(1-\beta_1)}{2(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}+\frac{2\lambda\alpha_1}{c(1-\beta_1)}+\frac{1}{4}C(1+\beta_1)$$

Consequently,

$$p=1-\frac{2\alpha_2(1-\beta_1)}{\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2)}\text{ - }\frac{4\lambda(\alpha_1+\alpha_2)+c^2(\beta_1^2-1)}{c^2(1-\beta_1)(\beta_1-\beta_2)}+\frac{4\lambda\alpha_2}{c^2(1-\beta_1)(1-\beta_2)}\,.$$

Considering the case where game has pure-strategy equilibrium, we get two possible conditions: $p=1$ or $p=0$.

Solving the equations, we find the values of λ that correspond to the case of dominant strategy:

$$\lambda=\frac{c\beta_1\beta_2(\alpha_2\beta_1(1-\beta_1+2\beta_2)-\alpha_1(1-\beta_2)(1+\beta_1))}{4(\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2))(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}$$

$$\lambda=\frac{c\beta_1\beta_2(\alpha_2\beta_1(1+\beta_2)+\alpha_1(1-\beta_2)(1+2\beta_1-\beta_2))}{4(\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2))(\alpha_2(1-\beta_1)+\alpha_1(1-\beta_2))}\qquad\textbf{(3)}$$

Now, for the game to have mixed-strategy equilibrium the following system of inequalities must hold:

$p < 1$ and $p > 0$

After solving this system for λ we get

$$\frac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+\beta_1)+\alpha_2\overline{\beta}_1(\beta_1-2\beta_2-1))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)} < \lambda < \frac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+2\beta_1-\beta_2)-\alpha_2\overline{\beta}_1(1+\beta_2))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)} \qquad \textbf{(4)}$$

Proposition 4.2. If λ satisfies (4) then there is Nash equilibrium in mixed strategies. If λ satisfies (3) then there is Nash equilibrium in pure strategies

Extension for Protocols Parameters

The game settings in previous sections were limited by aggressive ordering of protocols. In this section we weaken this condition to cover protocol parameters relation that falls beyond the "aggressive-peaceful" scheme, namely situation when $\alpha_1 \le \alpha_2$ and $\beta_1 \ge \beta_2$.

Applying the same considerations as above, we get the same results for pure-strategy Nash equilibria, but for mixed-strategy equilibrium an additional constraint emerges.

Since we're looking for cases with $0 < p < 1$, we get the following conditions for $p > 0$:

$$\begin{cases} J(s_1,s_2) - J(s_2,s_2) > 0 \\ (J(s_1,s_2) - J(s_2,s_2)) + (J(s_2,s_1) - J(s_1,s_1)) > 0 \end{cases}$$

Similarly, $p < 1$ holds when $(J(s_1,s_2) - J(s_2,s_2)) + (J(s_2,s_1) - J(s_1,s_1)) > J(s_1,s_2) - J(s_2,s_2)$

(It can be shown that other case with $J(s_1,s_2) - J(s_2,s_2) < 0$ results $\lambda < 0$, which has no physical sense, recalling that λ is an error weight).

So, in the end we have the following system of inequalities:

$$\begin{cases} J(s_1,s_2) - J(s_2,s_2) > 0 \\ J(s_2,s_1) - J(s_1,s_1) > 0 \end{cases}$$

Or, after replacement of J and transformations

$$\begin{cases} \lambda < \dfrac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+2\beta_1-\beta_2)-\alpha_2\overline{\beta}_1(1+\beta_2))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)} \\ \lambda > \dfrac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+\beta_1)+\alpha_2\overline{\beta}_1(\beta_1-2\beta_2-1))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)} \end{cases}$$

Replacing

$$\mu_1 = \frac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+2\beta_1-\beta_2)-\alpha_2\overline{\beta}_1(1+\beta_2))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)}, \quad \mu_2 = \frac{C^2\overline{\beta}_1\overline{\beta}_2(\alpha_1\overline{\beta}_2(1+\beta_1)+\alpha_2\overline{\beta}_1(\beta_1-2\beta_2-1))}{4(\alpha_1^2\overline{\beta}_2^2-\alpha_2^2\overline{\beta}_1^2)}$$

We get two possible solutions to the system above:

$$\begin{cases}\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2)>0 \\ \mu_2<\lambda<\mu_1\end{cases} \text{ or } \begin{cases}\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2)<0 \\ \mu_1<\lambda<\mu_2\end{cases}$$

Since $\alpha_1 \le \alpha_2$ and $\beta_1 \ge \beta_2$ then $\mu_2 > \mu_1$, the actual solution is

$$\begin{cases}\alpha_2(1-\beta_1)-\alpha_1(1-\beta_2)<0 \\ \mu_1<\lambda<\mu_2\end{cases}$$

Proposition 4.3. If $\alpha_1 \le \alpha_2$ and $\beta_1 \ge \beta_2$ and $\alpha_1 < \alpha_2 < \dfrac{\alpha_1(1-\beta_2)}{1-\beta_1}$, $\mu_1 < \lambda < \mu_2$,

then there is evolutionary stable equilibrium in mixed strategies.

Formulated conditions are consistent with the previous result with regards to protocol parameters specifics.

5. NETWORK ATTACKS SIMULATIONS

We study in this section numerically dynamic system (1) and equilibriums of defined game with replicator dynamics. The practical value of these results could be divided on two parts. Firstly, this is analytical tool for predicting shares of network resources for given set of AIMD protocols. Secondly, we can model users' behaviour (taking into account usual game theory assumptions about rationality, common knowledge etc.) using replicator dynamic equation. This equation is rather quality solution tool that show a dynamic and shares of network resources for each users group.

Solution for dynamic system

Numerical simulations were made using Wolfram Mathematica environment. On the picture below we show convergence of AIMD scheme for 2 and 3 dimensions.

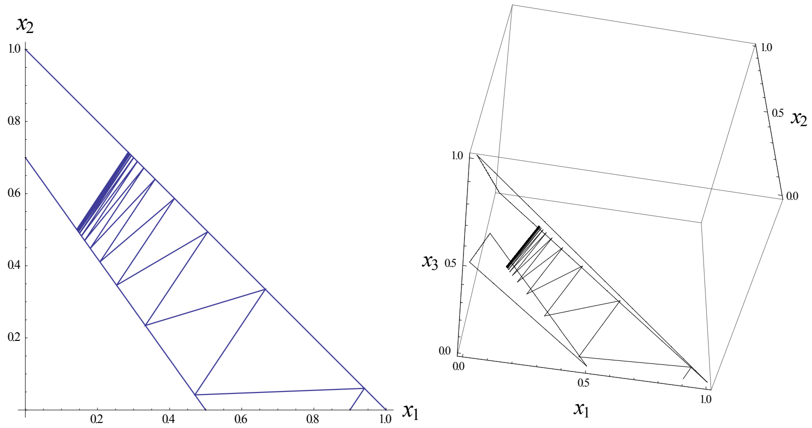

Fig. 1. **Simulations results for 2-d and 3-d systems**

Replicator Dynamics

We introduce here the replicator dynamics which describes the evolution in the population of the various strategies. In the replicator dynamics, the share of a strategy in the population grows at a rate equal to the difference between the payoff of that strategy and the average payoff of the population. More precisely, consider N strategies. Let x be the N-dimensional vector whose i element x_i is the population share of strategy i (i.e. the fraction of the population that uses strategy *i*). Thus, we have $\sum_i x_i(t)=1$, $x_i(t)\geq 0$. Then the replicator dynamics is defined as

$$\dot{x}_i(t)=x_i(t)K\left(\sum_{j\neq i}J(i,j)x_j-\sum_j x_j(t)\sum_{k\neq j}J(j,k)x_k\right)$$

We investigate a case with $N=3$ distinct strategies and pairwise payoff comparison:

$$J(s_1,X(t-\tau))=x_1(t-\tau)J(s_1,s_1)+x_2(t-\tau)J(s_1,s_2)+x_3(t-\tau)J(s_1,s_3)$$

$$\dot{x}_i(t)=x_i(t)K(J(i,X(t-\tau)-(x_1(t-\tau)J(s_1,X(t-\tau))+x_2(t-\tau)J(s_1,X(t-\tau))+$$
$$+x_2(t-\tau)J(s_1,X(t-\tau)))$$

We provide simulation results for the 3 sets of parameters (Fig. 4–6):

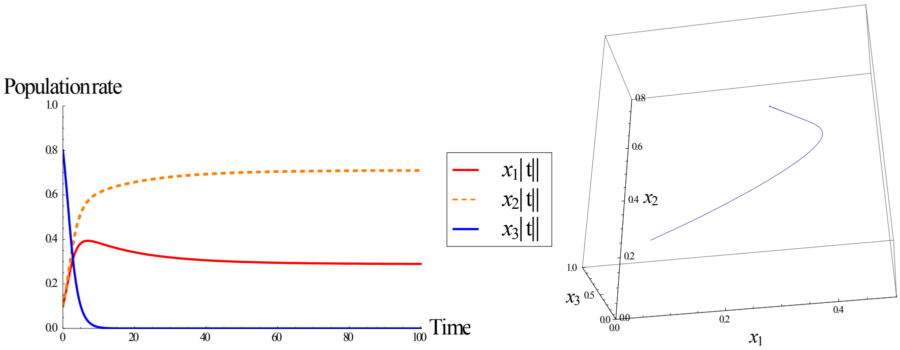

Fig. 2. $x_1(t)$, $x_2(t)$, $x_3(t)$ **- shares of population**

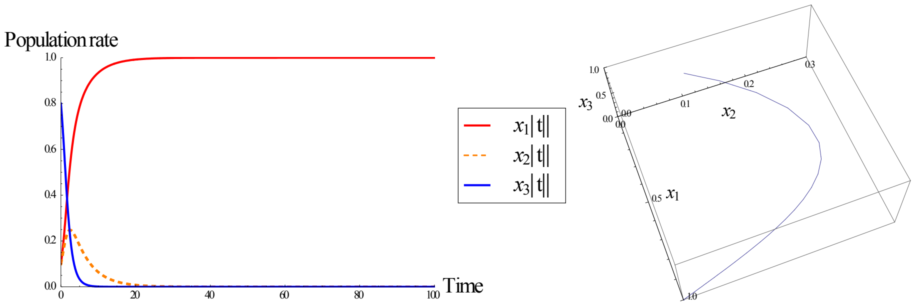

Fig. 3. $x_1(t)$, $x_2(t)$, $x_3(t)$

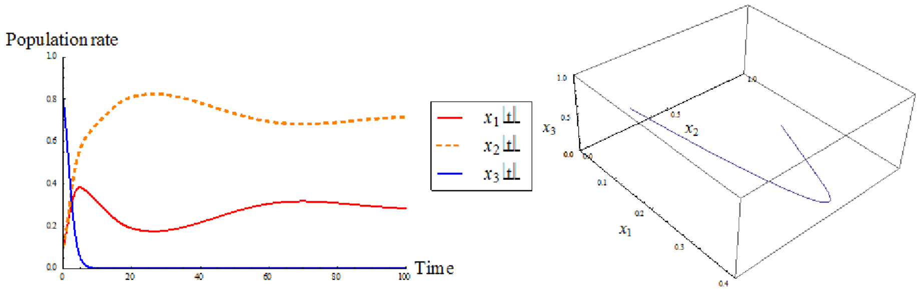

Fig. 4. $x_1(t)$, $x_2(t)$, $x_3(t)$

Attack modeling

To test theoretic model described above, a simulation model was developed under NS-3 Network Simulator package. The specifics of the model, as well as simulation results, are described below.

For the purposes of testing, a simple topology consisting of four nodes was built (Fig. 5) – the nodes represent sender, router, receiver and attacker.

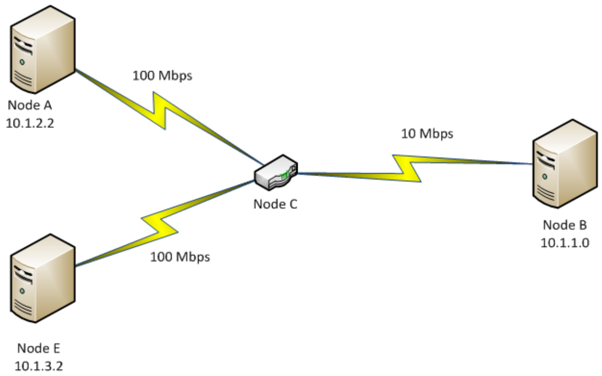

Fig. 5. Testbed topology.

The basic workflow is as follows: the sender (Node A) uploads a large file to some storage, controlled by file server (Node B), that resides in a different subnet. Thus, a large volume of traffic is generated and routed between the adjacent subnets by router (Node C). Then an attacker from the sender's subnet steps in (Node E). His goal is to disrupt a client-server operations by performing a denial-of-service attack, but, as router comes equipped with basic flood-detection capabilities, attacker won't be able to perform a full-scale UDP or ICMP DoS attack, and has to resort to different means.

He chooses a particularly stealthy approach known as low-rate TCP denial-of-service attack, which exploits the weakness of TCP retransmission mechanism to cause a significant service degradation or even a full outage. The idea is the following: as TCP employs an exponential backoff technique for retransmission of packets presumed to be lost, it is enough for an attacker to cause a short-term service outage with traffic spike and then maintain this state by sending the same spikes on the exact moments the client attempts to retransmit a packet. In more detail, if the client detects a packet loss at time t, it is enough for an attacker to perform short-term DoS in moments t+RTO, (t+RTO)+2*RTO, ((t+RTO)+2*RTO)+4*RTO and so on, where RTO is a value of TCP retransmission timeout. Moreover, lots of TCP implementations have the default RTO value of 1 second, which makes the described attack feasible even for networks with large amount of clients, as they are likely to have close RTO values.

The setup of NS-3 model is as follows: at time 0 the client at Node A establishes the connection with the server at Node B and starts sending data using TCP. Then, at 20 seconds from the beginning of a simulation, an attacker at Node E kicks in, periodically sending 30 traffic spikes of predefined length, separated by periods of silence. We denote the period between traffic spikes as T, and the length of the spike itself as τ. Obviously, different values and ratio between T and τ would yield different results in terms of attack success, with most prominent being achieved as T nears RTO. Depicted on Fig. 6 are sample graphs of client congestion windows dynamics under different values of T with τ being the same value of 0.1.

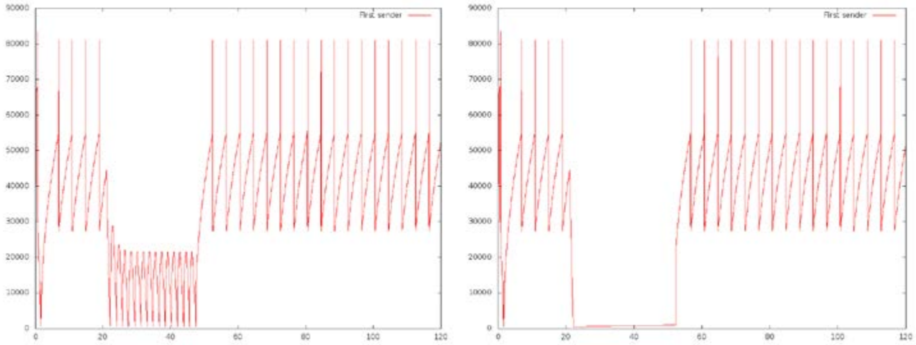

Fig. 6. Congestion window dynamics at T = 0.9 and T = 1.

As shown on graphs, the least goodput (and the most successful denial-of-service) is achieved with T being equal to default RTO value, which is consistent with theoretically predicted results.

Further, we investigate a client throughput change during attacks with different T values. The resulting graph, presented at Fig. 7, shows the performance degradation of client on 10 Mbps link under different attacks with the same total amount of traffic sent.

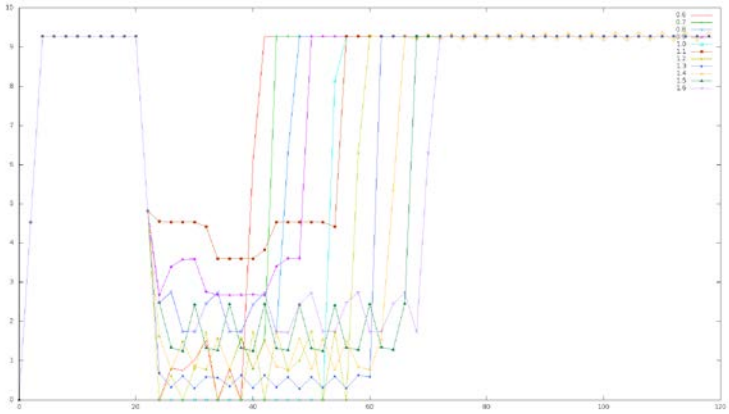

Fig. 7. Client throughput depending on attack parameters

6.0 CONCLUSIONS

In this paper, we have presented an overview of approaches to deal with security problems using a game-theoretic framework. The general objective was to identify and address the security and efficiency problems, where game theory can be applied to model and evaluate security problems and consequently used to design efficient network control solution. The application of game theory is an emerging field in network security, with only a few papers published so far.

Game theory provides a (parametric) model, which is refined and calculated using statistical data from real network. This model is actually a set of three layers of models, discovering system's dynamic and users' behavior from different angles. The first layer is a game between user and network. Solution is the protocol – strategy of user data flow. The second later is a game among users. Each user tries to receive maximal resource. This is non-cooperative game. Rational behavior leads to the Nash equilibrium (through its computing can be very complex). Network tries to balance users and achieve effective NE. System allocation algorithms efficiency is measured by PoA or PoS metrics. The last layer is a game with attacker. Attacker wants to disrupt network and prevent users from receiving any resources. This is game with pure conflict (zero-sum game). Analysis of resulting NE gives us metric to measure strength of attack and detect weaknesses of system.

7.0 REFERENCES

1. Sandberg, Henrik, Saurabh Amin, and K. Johansson. "Cyberphysical Security in Networked Control Systems: An Introduction to the Issue." Control Systems, IEEE 35.1 (2015): 20-23.

2. Shakkottai, Srinivas, Srinivas Govindaraju Shakkottai, and Rayadurgam Srikant. Network optimization and control. Now Publishers Inc, 2008.

3. Kelly, Frank P., Aman K. Maulloo, and David KH Tan. "Rate control for communication networks: shadow prices, proportional fairness and stability." Journal of the Operational Research society (1998): 237-252.

4. Manshaei, Mohammad Hossein, et al. "Game theory meets network security and privacy." ACM Computing Surveys (CSUR) 45.3 (2013): 25.

5. Liang, Xiannuan, and Yang Xiao. "Game theory for network security." Communications Surveys & Tutorials, IEEE 15.1 (2013): 472-486.

6. La, Richard J. "Role of network topology in cybersecurity." Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on. IEEE, 2014.

7. Kelly, Frank P., Aman K. Maulloo, and David KH Tan. "Rate control for communication networks: shadow prices, proportional fairness and stability." Journal of the Operational Research society (1998): 237-252.

8. Mo J., Walrand J. Fair end-to-end window-based congestion control // IEEE/ACM Trans-actions on Networking. – 2000. – 8. – P. 556 – 567.

9. Paganini F., Doyle J.C., Low S.H. Scalable laws for stable network congestion control // Proc. of IEEE Conference on Decision and Control. – 2001. – 1. – P. 185 – 190.

10. Low S.H., Srikant R. A Mathematical Framework for Designing a Low-Loss, Low-Delay Internet // Network and Spatial Economics. – 2004. – 4 (1). – P. 75 – 102.

11. Altman E. et al. The evolution of transport protocols: An evolutionary game perspective //Computer Networks. – 2009. – T. 53. – №. 10. – C. 1751-1759.

12. Smith, John Maynard. Evolution and the Theory of Games. Cambridge university press, 1982.

13. E. Altman, N. Bonneau, M. Debbah, G. Caire, An evolutionary game perspective to ALOHA with power control, in: Proceedings of the 19th International Teletraffic Con-gress, Beijing, 29 August–2

September, 2005.

14. Papadimitriou, Christos. "Algorithms, games, and the internet." Proceedings of the thirty-third annual ACM symposium on Theory of computing. ACM, 2001.

15. Han, Zhu, et al. Game theory in wireless and communication networks. Cambridge Uni-versity Press, 2012.

16. Ignatenko, Oleksii, and Oleksandr Synetskyi. "Evolutionary Game of N Competing AIMD Connections." Information and Communication Technologies in Education, Research, and Industrial Applications. Springer International Publishing, 2014. 325-342.

17. Andon, F. I., and O. P. Ignatenko. "Modeling conflict processes on the internet." Cybernetics and Systems Analysis 49.4 (2013): 616-623.