Modelling of Conflict Controlled Networks

Oleksii Ignatenko
40, Glushkov Avenue, CSP 03680, Kyiv 187, Ukraine

oignat@isofts.kiev.ua

ABSTRACT

Game theoretical techniques have recently become prevalent in many engineering applications, notably in communications. While developing an information network management system often encountered a situation where one should deal with malicious intrusion attempts aimed at obstructing the routing policy work. In this case, methods of networks management based on fluid models and a discrete controlled random walk model requires certain changes. In this work we propose an approach based on conflict control point of view that could be useful for modeling of attacking actions and response behaviour of the system.

1.0 INTRODUCTION

Today network models are related to very different areas – information networks, telecommunications, gas transportation and energy systems, distributed production processes. Complex networks are everywhere. Unprecedented developing of information networks (especially the Internet) gives example of dynamic interconnected system. And this system is still much less complex then biological organisms or society of agents. For example, degree and mode of connectivity in passive agents can combine to form images resembling crystals or snowflakes. The main focus within our own bodies is far more utilitarian. Endocrine, immune, and vascular systems adjust chemical reactions to maintain equilibrium in the face of ongoing attacks from disease and diet. In biology this is called homeostasis. In regulation of a network it is called control. So, there is need for methods to model networks in order to capture essential structure, dynamics, and uncertainty. Based on these models one could explore ways to visualize network behaviour so that effective control techniques can be synthesized and evaluated. According to [1], modelling for the purposes of control and the development of control techniques for truly complex networks has become a major research activity over the past two decades.

Information network applications are especially important because they interfere with almost all sides of human activity. As a result, security and reliability of information flows directly affect the quality of service, efficiency and overall economic development of entire industries. Reliable working of the information networks has become vital for our day-to-day transactions for the most organizations. That's why the Internet becomes an attractive target for cyber crime. Financially motivated, the crime we see today becomes more distributed, sophisticated and dangerous.

A few years ago attackers widely use remotely exploiting servers identified by scanning the Internet for vulnerable network services. Significant facts of such scanning attacks were computer worms such as Code Red and SQL Slammer. Their huge scale threatens working of whole the Internet at risk; for example, SQL Slammer generated traffic sufficient to melt down backbones. Consequently, academia and industry developed effective ways to fortify the network perimeter against such attacks. Unfortunately, adversaries similarly changed tactics moving away from noisy scanning to more stealthy attacks. Not only did they change their tactics, but also their motivation. Previously, large-scale attacks were mostly expression of technical superiority. Now, cyber criminal are motivated by economic benefits. They try to not only exploit and seize control of compromised systems for as long as possible but to turn their assets into revenue.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2009	**N/A**	**-**

4. TITLE AND SUBTITLE
Modelling of Conflict Controlled Networks

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
40, Glushkov Avenue, CSP 03680, Kyiv 187, Ukraine

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA562563. RTO-MP-MSG-069 Current Uses of M&S Covering Support to Operations, Human Behaviour Representation, Irregular Warfare, Defence against Terrorism and Coalition Tactical Force Integration (Utilisation actuelle M&S couvrant le soutien aux operations, la representation du comportement humain, la guerre asymetrique, la defense contre le terrorisme et l'integration d'une force tactique de coalition). Proceedings of the NATO RTO Modelling and Simulation Group Symposium held in Brussels, Belgium on 15 and 16 October 2009., The original document contains color images.

14. ABSTRACT
Game theoretical techniques have recently become prevalent in many engineering applications, notably in communications. While developing an information network management system often encountered a situation where one should deal with malicious intrusion attempts aimed at obstructing the routing policy work. In this case, methods of networks management based on fluid models and a discrete controlled random walk model requires certain changes. In this work we propose an approach based on conflict control point of view that could be useful for modeling of attacking actions and response behaviour of the system.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**10**	

The Web offers them a powerful infrastructure to compromise computer systems. Attackers achieve this by employing the Web to serve malicious Web content capable of compromising users' computers and running special code on them. This has been enabled due to the increased complexity of Web browsers and the resulting vulnerabilities that come with complex software. For example, a modern Web browser provides a powerful computing platform with access to different scripting languages, (for example, Javascript) as well as external plugins that may not follow the same security policies applied by the browser (for example, Flash, Java). While these capabilities enable sophisticated Web applications, they also allow attackers to collect information about the target system and deliver exploits specifically tailored to a user's computer. Web attacks render perimeter defences that disallow incoming connections useless against exploitation as hackers use the browser to initiate out-bound connections to download attack payloads. This type of traffic looks almost identical to the users' normal browsing traffic and is not usually blocked by network firewalls.

That's why computer and network security nowadays has become a major priority for both network design and implementation. Network engineers use simulation tools to help them understand and develop complex system. It is an effective tool to save time and money during development and implementation. To be able to simulate complex systems, modeling is a necessary foundation. Without an accurate model of the system or process there will be no successful simulation. Simulation depends on verified and validated models.

Modeling and Simulation (M&S) tools are become standard procedure today before building computer networks to save time and money. M&S tools become more and more widespread to different areas in computer sciences as well as other fields for representing simulation of reality.

Is it possible with help from M&S to simulate computer/network security mechanism such as firewalls, Virtual Private Network (VPN), key distribution, and what are the consequences of a simulate computer network attack? If it works, what is possible to simulate with M&S tools? The possible opposite case could be; is it possible at all to simulate computer network attacks and computer/network security on a computer today with an M&S tool? An ideal scenario for M&S tool would be if it could be used to model and simulate different computer network attack methods which test computer and network security. A network engineer could predefine his/her computer network in advance in a simulation tool such as OPNET before building the computer network in reality to see what will happen to the network and/or network nodes if the network is attacked with different kind of attack techniques. The network engineer would then have a virtual model of the network inside of the simulation tool and "press a button" to see what happens when the attack strikes. The simulated network will have network nodes such as workstations (with different kinds of services and Operating Systems (OS) such as; Windows, UNIX, and Mac OS), switches, routers, firewalls, Intrusion Detection System (IDS), and servers and other types of products you will find in a typical computer network. The different simulated computer network attacks would be used as a prediction tool to see what happen when attacks occurs on the network and how good the security is in the simulated network. Which nodes in the computer network will be attacked and affected of the attack? Will the whole network go down because a strategically node goes down?

The fundamental question of issue is; is it possible to use M&S for modeling and simulation of computer/network security and computer network attacks. Network attacks are pure conflict situation, so we should turn our attention to theory of conflict between players. Game theoretical techniques have recently become prevalent in many engineering applications, notably in communications. With the emergence of cooperation as a new communication paradigm, and the need for self-organizing, decentralized, and autonomic networks, it has become imperative to seek suitable game theoretical tools that allow to analyze and to study the behavior and interactions of the nodes in future communication networks.

In general, game theory can be divided into two branches: non-cooperative and cooperative game theory. Non-cooperative game theory studies the strategic choices resulting from the interactions among competing players, where each player chooses its strategy independently for improving its own performance (utility) or reducing its losses (costs). In this context, network denial of service attacks could be considered as a contest between two players (atacker and defense system) – a game or a conflict controlled system.

2.0 CYBER CRIME. DENIAL OF SERVICE ATTACKS

The Internet (originally known as ARPANET) was first created in 1969 as a research network sponsored by the Advanced Research Projects Agency (ARPA) of the Department of Defense (DoD) in the United States of America. The original aim was to provide an open network for researchers to share their research resources. Therefore, openness and growth of the network were the design priorities while security issues less of a concern. The occurrence of the Morris Worm in 1988 marked the first major computer security incident on the Internet. However, the world was not so dependent on the Internet as it is now. The Internet was still limited to research and educational communities until the late 1990s. Hence, not much attention was paid to Internet security.

In the last decade, the phenomenal growth and success of the Internet is changing its traditional role. The Internet is no longer just a tool for the researchers. It has become the main infrastructure of the global information society. Governments use the Internet to provide information to the citizens and the world at large, and they will increasingly use the Internet to provide government services. Companies share and exchange information with their divisions, suppliers, partners and customers efficiently and seamlessly. Research and educational institutes depend more on the Internet as a platform for collaboration and as a medium for disseminating their research discoveries rapidly. Unfortunately, with the growth of the Internet, the attacks to the Internet have also increased incredibly fast. According to CERT [2], a center of Internet security expertise located in the U.S., the number of reported Internet security incidents has jumped from 6 in 1988 to 82,094 in 2002, and the estimated number of Internet security incidents in 2003 is 153,140. The growth in the number of incidents reported between 1998 to 2003 is shown in Figure 1.

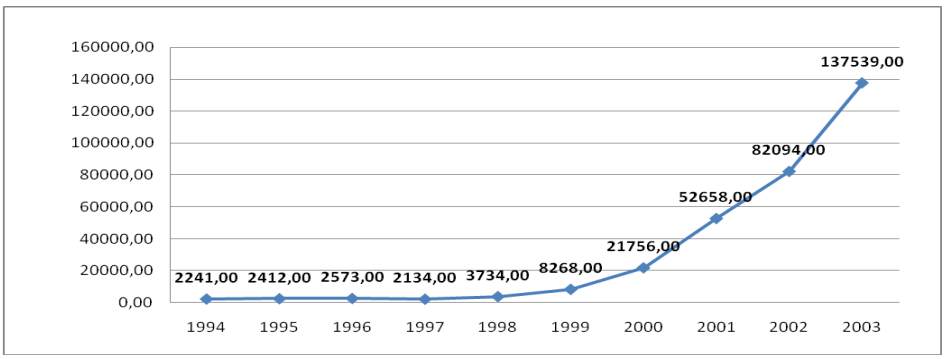

Figure 1: Number of Internet security incidents

More importantly, traditional operations in essential services, such as banking, transportation, power, medicine, and defense are being progressively replaced by cheaper, more efficient Internet-based applications. Historically, an attack to a nation's critical services involves actions that need to cross a physical boundary. These actions can be intercepted and prevented by a nation's security services. However, the global connectivity of the Internet renders physical boundaries meaningless. Internet based attacks can be launched anywhere in the world, and unfortunately no Internet based services are immune from these attacks. Therefore, the reliability and security of the Internet not only benefits on-line businesses, but is also an issue for national security.

A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be launched against both services, e.g., a web server, and networks, e.g., the network connection to a server. The impact of DoS attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business. On February 9, 2000, Yahoo, eBay, Amazon.com, E*Trade, ZDnet, Buy.com, the FBI, and several other Web sites fell victim to DoS attacks resulting in substantial damage and inconvenience [3]. As emergency and essential services become reliant on the Internet as part of their communication infrastructure, the consequences of DoS attacks could even become life-threatening. Hence, it is crucial to deter, or otherwise minimize, the damage caused by DoS attacks.

In general, a denial of service (DoS) attack is any attack which makes an on-line service (e.g., Web Service) unavailable. The attack could involve a single packet (e.g., the \land" attack) exploiting software bugs in a server, or a traffic stream with a tremendous number of packets that congest the target's server or network. We define a bandwidth attack as any attack that consumes a target's resources through a massive traffic volume. In this thesis, we focus on bandwidth attacks, and henceforth we mean bandwidth attack when we refer to denial of service attacks unless otherwise stated. The distributed denial of service (DDoS) attack is a bandwidth attack whose attack traffic comes from multiple sources. To launch a DDoS attack, an attacker usually compromises many insecure computers connected to the Internet first. Then a DDoS attack is launched from these compromised computers. The reflector attack is an attack where innocent third-parties (reflectors) are used to bounce attack traffic from the attacker to the target. A reflector can be any network device that responds to any incoming packet, for example, a web server. The attacker can make the attack traffic highly distributed by using many reflectors. The reflector attack is a type of DDoS attack.

Currently we have numerous DoS attack types. Each attack use some special exploit of Internet protocols or software weaknesses. For example, this attacks could be launched directly overwhelming by large packets (UDP, ICMP flood), using reflectors (Smurf, Fraggle), sending too long packets (Ping of Death), wrong packets (Land). Recently one can see progress in this field – new attack types cause damage to computer systems. Novel type of attack, with a low average rate, exploits the transients of a system’s dynamic behavior. The low-rate attacks introduce significant inefficiencies that tremendously reduce system capacity or service quality. In the literature, this kind of network assault is called shrew attack or Reduction of Quality (RoQ) attack. Various attacks has special characteristic. In work [4] we propose following parameter set. (Fig 2.):

- Attack type. Security experts segregate DoS attacks into two categories: distributed (attack from many sources) and non-distributed (attack from one computer).
- Attack direction. Attack directions divided on network resources and target resources.
- Attack scheme. Generally speaking, attack scheme can be direct (direct sending of malicious traffic), reflector (traffic reflects from other computers) or hidden (malicious traffic hidden in legal).
- Attack method. Method defines vulnerability that used during attack. Targeted attack uses vulnerability of software, services, and protocols. The primary goal of a consumption attack is to consume all possible available resources (usually network resources) to shut down a system. Exploitive attacks target bugs in operating systems.

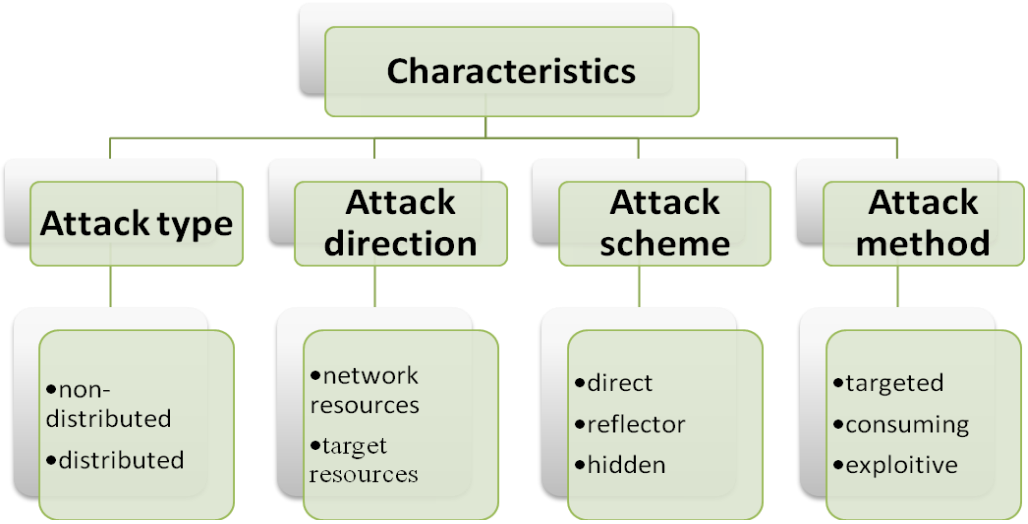

Figure 2: Network System

3.0 CONFLICT CONTROLLED NETWORKS. MODELLING AND SIMULATIONS

Network models are used to describe power grids, cellular telecommunications systems, large scale manufacturing processes, computer systems, and even systems of elevators in large office buildings. Although the applications are diverse, there are many common goals (such that, stability, performance, robustness and flexibility). Although complexity of the physical system is both intimidating and unavoidable in typical networks, for the purposes of control design it is frequently possible to construct models of reduced complexity that lead to effective control solutions for the physical system of interest. These idealized models also serve to enhance intuition regarding network behavior.

Networks considered here consist of finite set of nodes, each containing finite set of buffers. Packets arrive from outside the network to various buffers. One or more servers process packets at a given node, after which a packet either leaves the network or visits another node (Fig. 3).

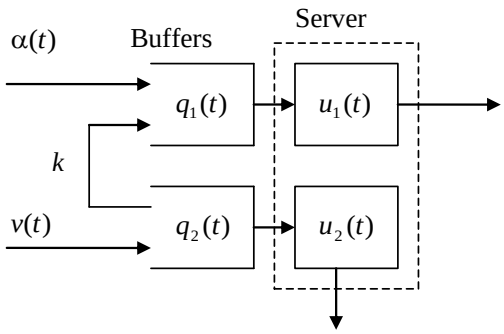

Figure 3: Network node

A general fluid model can be described by the differential equation

$$\dot{q} = Aq + \alpha(t) + Bu(t) - Cv(t), \tag{1}$$

where $q(t)$ is the n-dimensional vector of queue process, $\alpha(t): R \to R^n$ denotes the packet arrival rate, $u(t)$ - the routing policy, $v(t)$ - attack policy. Matrix A represents an inner network construction, matrix B - routing process and C describes attack process. The controlled differential equation (1) can be viewed as a state space model, as frequently used in control applications, with controls $u(t)$, $v(t)$ and independent function $\alpha(t)$. We consider model (1) as a starting point to investigate conflict problem of interaction between a routing policy and an attacker. If a successful design is obtained, we could generalize this solution on the case of Markov processes [1, 5]. The problem of finding of control $u(t)$ can be described as follows.

We choose a control function $u(t)$ in purpose of minimizing vector $q(t)$ under several special conditions (e.g. for minimal time) and any possible functions $v(t)$, $\alpha(t)$. Let us fix some function $u(t)$, then solution of (1) can be found using following formula:

$$q(t) = e^{A(t-t_0)}q(t_0) + \int_{t_0}^{t} e^{A(t-\tau)}Bu(\tau)d\tau -$$

$$-\int_{t_0}^{t} e^{A(t-\tau)}Cv(\tau)d\tau + \int_{t_0}^{t} e^{A(t-\tau)}\alpha(\tau)d\tau \tag{2}.$$

If we assume, that $A = 0$, $B = I$, $C = 0$ and $\alpha(t) = \alpha$, (2) could be rewriting as:

$$q(t) = q(t_0) + \alpha t + u(t). \tag{3}$$

This is well-known single server queue fluid model. The single server queue is a useful model for a dynamic investigation of very different systems. Now we introduce an extension of the fluid model [1] in the case of conflict process [6]. Let us consider dynamic system defined for an initial condition $q(t) = (q_1(t), q_2(t)) \in R^2$ by the system of linear equations:

$$\dot{q}_1(t) = \alpha(t) + k \cdot q_2(t) - u_1(t),$$

$$\dot{q}_2(t) = v(t) - u_2(t), \; t \geq 0. \tag{5}$$

Phase state is described by the phase vector $q(t) = (q_1(t), q_2(t)) \in R^2$, where $q_1(t) \in R_+$ is the queue length at time t. The queue length is subject to the linear phase constraint $0 \leq q_1(t) \leq q_1^{\max}$ for all $t \geq 0$.

Parameter $q_2(t) \in R_+$ is associated with the attacker player which trying to overwhelm our network (or maximize $q_1(t)$ in other words) using control parameter $v(t)$, $v(t) \geq 0$, $v(t) \leq \nu$. By choosing $v(t)$ at time t attacker sets attack power ($q_2(t)$) which is subject to the linear phase constraint $0 \leq q_2(t)$ for all $t \geq 0$.

Parameter $q_2(t)$ influences on queue $q_1(t)$ with a coefficient $k \geq 0$. The other player – defender – has a control vector $u(t) = (u_1(t), u_2(t))$. He divides his control resources between two directions: $u_1(t)$ - for service of the arrived packets, $u_2(t)$ - for counteraction of the attacker activity. Control parameter $u(t)$ is

subject of following constraints

$$u_1(t) \geq 0,\ u_2(t) \geq 0,\ u_1(t)+u_2(t) \leq \mu, \text{ for all } t \geq 0.$$

Suppose that defender has information about $\alpha(t)$, $v(t)$ and $q(t)$ at time t. Function $\alpha(\cdot): R \to R^n$ describe packets arrival service at time t. Suppose the following assumptions hold:

- $0 \leq \alpha(t) \leq \alpha_{\max}$ for all $t \geq 0$;
- $\alpha(t)$ - continuous function.
- $\int_{t_0}^{\infty} \alpha(t)dt \leq \alpha_{\text{int}}$

This model is stabilizable if $\mu \geq v$ for initial position such that $q(t_0) \leq q_{\max} - \frac{(\alpha_{\max} - \mu)\alpha_{\text{int}}}{\alpha_{\max}}$. Time optimal strategy gives by following formula

$$u(t) = (u_1(t), 0) \text{ , where } u(t) = \begin{cases} -\mu, & q(t) > 0 \\ 0, & q(t) = 0 \end{cases}.$$

To solve (10) we should find an admissible strategy $u(t, q(t), v(t))$ and moment of time T such that $q(t) = 0$ for all $t \geq T$. We denote this strategy $u(t, q(t), v(t))$ as the solution of game (5). Note that this result must be achieved over all an admissible functions $v(t)$. Let us write equations (5) in standard form. Denote $A = \begin{pmatrix} 0 & k \\ 0 & 0 \end{pmatrix}$, then

$$\dot{q}(t) = Aq(t) + \begin{pmatrix} \alpha(t) \\ v(t) \end{pmatrix} - \begin{pmatrix} u_1(t) \\ u_2(t) \end{pmatrix} \tag{6}.$$

Control sets are respectively $U = \{u \in R_+^2 : u_1 + u_2 \leq \mu\}$ and $V = \{v \in R_+^2 : v_1 \leq \alpha_{\max}, v_2 \leq \nu\}$. We solve this problem using the idea of the first direct method of Pontryagin [7, 8].

Theorem. Consider the conflict controlled system (6). If $\mu \geq v$ and $q_1(0) + \frac{k}{2}\frac{(q_2(0))^2}{\varepsilon} + \alpha_{\text{int}} \leq q_1^{\max}$, then we can construct the solution $u(t)$ and moment of time T, such that $q(t) = 0$ for $t \geq T$.

(for proof see [9])

Simulations

Let us illustrate obtained result on the example. Consider the model (5). This model was implemented in discrete event network simulation framework OMNeT++ . OMNeT++ is an object-oriented modular discrete event network simulation framework. It has a generic architecture, so it can be (and has been) used in various problem domains:

- modeling of wired and wireless communication networks
- protocol modeling

- modeling of queuing networks
- modeling of multiprocessors and other distributed hardware systems
- validating of hardware architectures
- evaluating performance aspects of complex software systems and in general, it can be used for the modeling and simulation of any system where the discrete event approach is suitable, and which can be conveniently mapped into entities communicating by exchanging messages.

OMNeT++ itself is not a simulator of anything concrete, but it rather provides infrastructure and tools for writing simulations. One of the fundamental ingredients of this infrastructure is a component architecture for simulation models. Models are assembled from reusable components termed modules. Well-written modules are truly reusable, and can be combined in various ways like LEGO blocks.

Modules can be connected with each other via gates (other systems would call them ports), and combined to form compound modules. Modules communicate through message passing, where messages may carry arbitrary data structures. Modules can may messages along predefined paths via gates and connections, or directly to their destination; the latter is useful for wireless simulations, for example. Modules may have parameters, which can be used to customize module behaviour, and/or to parameterize the model's topology. Graphical, animating user interfaces are highly useful for demonstration and debugging purposes (Figure 4.).

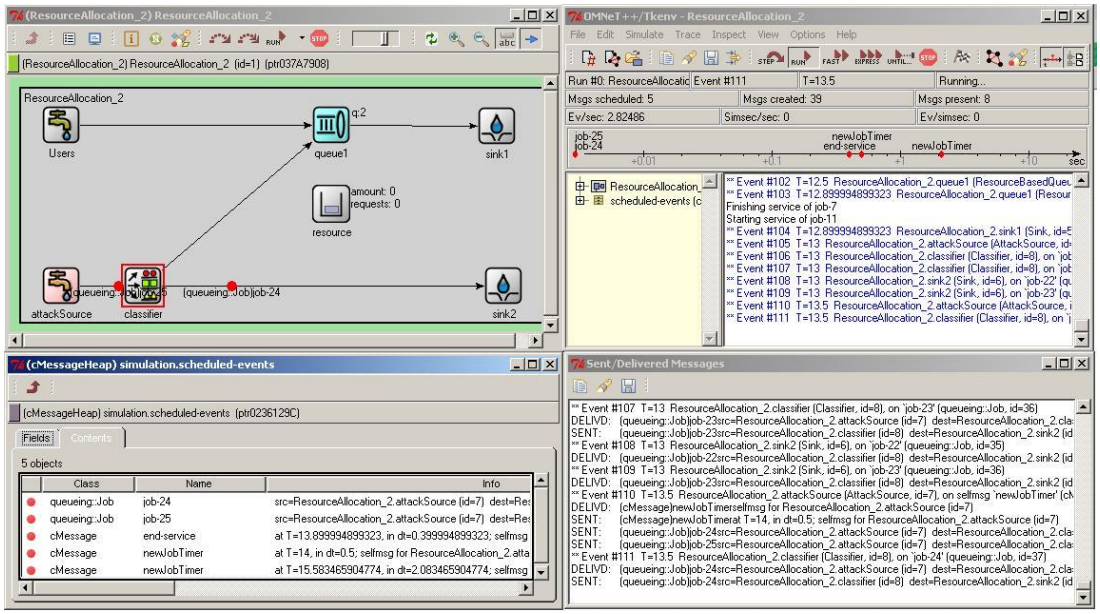

Figure 4: Network System

OMNet++ has the queue simulation library. This library includes modules for communication networks modeling. The model (5) was developed using standard and new modules (Figure 5.). It consists of users, attacking source, several queues with shared resource, classifier, router and sink nodes. Users send packets to a router. Router performs distribution among queues for processing. Queues use part of resource for working (if resource not available queue wait some time). Then packets go to DataProcessing node and left system.

Attack source node try to disrupt working. Attacker starts the flooding attack by sending identical packets to router. Defense system makes filtration and drop out fixed percent of all flooding packets.

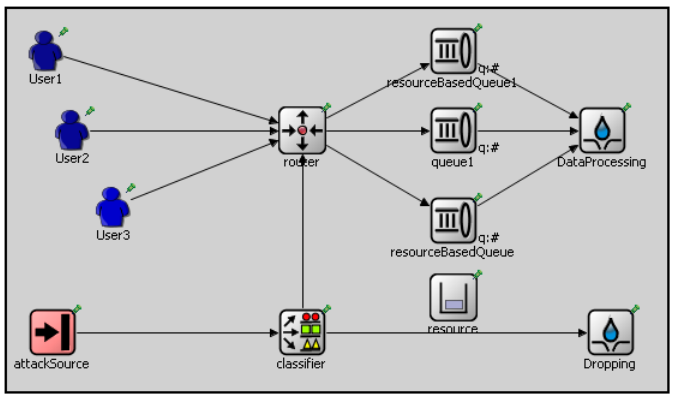

Figure 5: Model of network

Graph of packets delay rate shown on Figure 6.

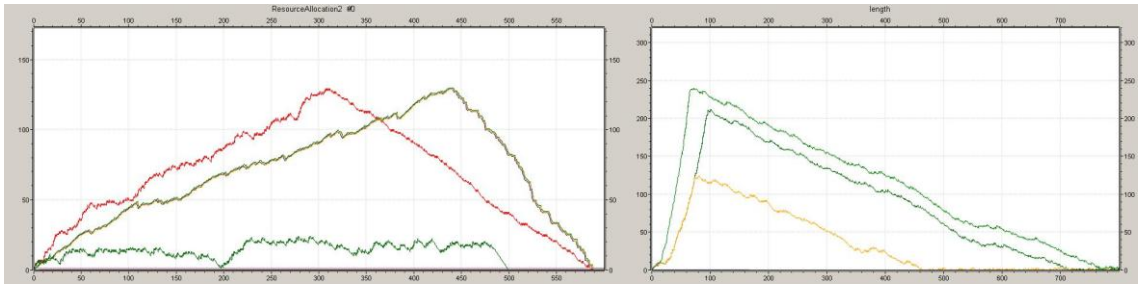

Figure 6: System dynamic

4.0 SUMMARY

"To make rapid advances in cyber security defense, we must improve the state of the art in evaluation of network security mechanisms. Evaluation is currently impeded by lack of scientific rigor, lack of relevant and representative network data, inadequate models of defense mechanisms, and inadequate models of the network and both the background and attack traffic data" [10]. Numerous features must still be implemented, verified, and validated before a serious attempt can be made for simulating computer and network security in M&S fashion. Verified and validated models of network traffic and attack traffic must be conducted to be able to make accurate simulation of a real event. Different attack models must be fabricated for verification and validation before they can be used for attack simulation.

Very important issue is a theoretical background of attack models. The most natural approach for dealing with these interconnected networks systems is theory of conflict controlled processes or game theory. Game theory provides a formal analytical framework with a set of mathematical tools to study the complex interactions among rational players. Throughout the past decades, game theory has made revolutionary impact on a large number of disciplines ranging from engineering, economics, political science, philosophy, or even psychology. In recent years, there has been a significant growth in research activities that use game theory for analyzing communication networks.

This is mainly due to:

- the need for developing autonomous, distributed, and flexible mobile networks where the network devices can make independent and rational strategic decisions;
- the need for low complexity distributed algorithms that can efficiently represent competitive or collaborative scenarios between network entities.

In this work we proposed model of network system with conflict based on the differential game theory background. This approach could be useful for modeling of attacking actions and response behaviour of the system. The model was developed and simulated using environment OMNet++. Simulations results presented on graphs.

[1] S. Meyn, “Control Techniques for Complex Networks,” Cambridge University Press, 2007.

[2] CERT/CC Statistics, URL http://www.cert.org/stats/.

[3] L. Garber. Denial-of-service attacks rip the Internet". IEEE Computer 33(4), 12-17 (2000).

[4] O. Ignatenko, P. Andon. Counteraction to denial of service attacks in Internet: approach concept // Problems of programming, 2-3, 2008, P. 564-574.

[5] D. Bertsekas, “Network optimization: continuous and discrete models”, Athena Scientific, Belmond, 1998.

[6] A.A. Chikrii, “Conflict-controlled Processes”, Kluwer Academic Publisher, Boston-London-Dordrecht, 1997.

[7] M.S. Nikolskii, “L.S. Pontryagin's First Direct Method in Differential Games”, Izdat. Gos. Univ., Moscow, 1984.

[8] L.S. Pontryagin, “Selected Scientific Papers”, Vol. 2, Nauka, Moscow, 1988.

[9] O. Ignatenko Conflict modeling of single server queue with integral constraints // PMCCS: The International Workshop on Performability Modeling of Computer and Communication Systems, Eger, Hungary, 17-18 September, 2009. (accepted)

[10] Deter/Deterlab based on emulab. A Laboratory for Security Research. Revived Mars 18, 2005 at URL: http://www.isi.deterlab.net/