# *Access Control in a Form of Active Queuing Management in Congested Network Environment*

Vladimir Zaborovsky
St. Petersburg state Polytechnical University
Saint-Petersburg, Russia
e-mail: vlad@neva.ru

Vladimir Mulukha
St. Petersburg state Polytechnical University
Saint-Petersburg, Russia
e-mail: vladimir@mail.neva.ru

***Abstract* — Internet processes information in the form of distributed digital resources, which have to be available for authorized use and protected against unauthorized access. The implementation of these requirements is not a simple task because there are many ways to its realization in the modern multiserviced and congested networks. In this case many well-known solutions of the past became inappropriate because of traffic fractal statistics, which are caused by persistent packet dynamics of transport protocols and loss of available throughput. Therefore we offer the new approach to raise access control functionality, taking into account models of transport protocols in congested network environment, characteristics of virtual channel throughput and features of active queuing management mechanism that based on randomized preemptive procedure.**

***Keywords* — *access control, authorized use, virtual connection, priority queueing management, randomized push-out mechanism***

## I. Introduction

Internet as a global information infrastructure is used widely for business, education and research. This infrastructure keeps information in the form of distributed digital resources that have to be available for authorized use, and protected against unauthorized access. However, the implication of these requirements is not a simple task due to many elements and many ways of realization. Therefore solutions of the past have become inappropriate because of traffic fractal statistics, which are caused by persistent packet dynamics and correspondent loss of virtual channel available throughput. In this paper we propose a new approach to access control flexibility enhancement based on active queuing management mechanism and randomized preemptive procedure. The offered solution can be implemented by a firewall and can be applied in the existing network environments.

To reach this purpose we propose: 1) the new classification of virtual connections (VC) based on security characteristics and throughput requirements; 2) VC model, which takes into account fractal characteristics of packet flows; 3) randomized preemptive queuing management mechanism in congested networks. We use a combined method of VCs throughput management that unites principles of feedback and program control within a framework for Policy-based Admission Control (Fig. 1):

- Policy Decision Point (PDP).
- Policy Enforcement Point (PEP) – security-critical component, which protects the resources and enforces the PDP's decision.
- Policy Administration Point (PAP).

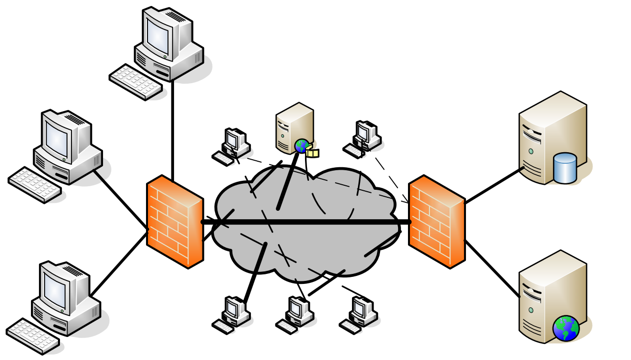

Figure 1. Firewall as a central component of access policy enforcement

In this framework firewall combines PDP and PEP by controlling access request and enforcing access decisions in real-time. In this case, access control can be considered as the throughput control of VC. So, access to the specific network resource is prohibited if the corresponding VC between the user and resource has no available throughput. Therefore from PAP firewall receives two types of access policy rules: packet filtering rules and data flow rules.

The parameters of firewall rules depend on the set of network environment and/or protocols characteristics *A*. This set can be divided on two classes with different access conditions. In proposed approach the classification decision is based on indicator function *F* and firewall has two modes in accordance to possible *F (A)* values:

- 0, if the data flow is forbidden according to the access policy (filtering rules);
- 1, if the data flow is permitted.

Forbidden mode means that access denied by PAP. Then the subset of permitted flows is divided into new two subsets:

- priority ones that have low throughput and demand low stable delivery time;
- background ones that demand high throughput and has no delivery time requirements.

To provide this classification procedure we proposed active queuing management mechanism, which based on randomized preemptive control. Therefore in the firewall the data flow throughput and time that packets spend in queue (minimum value for priority permitted flows and infinity for denied) are the functions of randomized control parameter $\alpha$. Each of the firewall rules has a set of attributes: identifiers of subject and object and the access

ISBN:978-1-61208-113-7

rights from one to another. In the modern network environment access rules have much more attributes that need to identify two subsets of permitted flows. Therefore the actual problem of access control within framework for Policy-based Admission Control is the flexible configuration of firewall rules, which considers dynamics of network environment including specific congested conditions. In this paper we introduce active queuing management mechanism for access control policy enforcement based on randomized preemptive procedure and network environment characteristics.

The paper is organized as follows: In Section II we suggest new classification of virtual connections. In Section III the model of virtual connection is presented. The Section IV and V are the theoretical parts of the paper where the mathematical model and basic equations are analyzed and estimated. The Section VI is about practical usage of proposed method.

## II. Virtual connection classification

In this paper we use the term "access management" as the combine of access control and traffic management. Access control is the basic technical method of information security in the computer networks. It is providing confidentiality by blocking the denied data flows, availability by permitting legal connections and integrity by reducing the risk of data modification or destruction. Confidentiality, integrity and availability are the core principles of information security. Access control is based on subject-object model, where subjects are the entities that can perform actions in the system and influence the environment condition and objects are the entities representing passive elements between which access need to be controlled. Data flows between objects and subjects named virtual connections (VC). In this paper Virtual Connection is the type of information interaction between applications on object and subject by means of formation one-way or duplex packet stream, and also the logical organization of the network resources necessary for such interaction.

Computer network can be considered as the set of such VC. In classical subject-object model the set of VC is divided into two subsets:

- Non forbidden connections that do not harm the protected information;
- Forbidden connections that can low the confidentiality, integrity or availability of protected information.

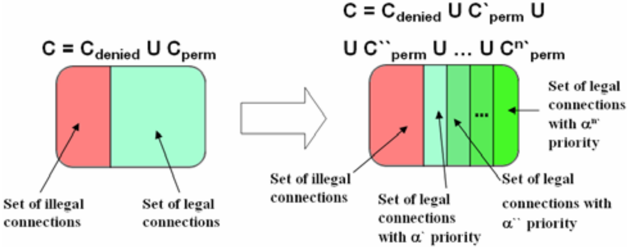
C = C$_{denied}$ U C$_{perm}$
C = C$_{denied}$ U C`$_{perm}$ U
U C``$_{perm}$ U … U C$^{n`}$$_{perm}$
Set of illegal connections
Set of legal connections
Set of illegal connections
Set of legal connections with α` priority
Set of legal connections with α`` priority
Set of legal connections with α$^{n`}$ priority
...

Figure 2. Virtual connections classification model.

We consider spreading the set of legal connections into several subsets by priority characteristics. In this paper we present the simplest example with two subsets:

- Non forbidden priority connections;
- Non forbidden non priority or background connections.

On Fig. 2 there is graphical interpretation of considered classification.

## III. Virtual connection model

The modeling of the VC behavior has received considerable attention in recent years. In this paper we present a simple model of VC. Each connection can be described by several parameters:

$$Vc(S,O,Th,Type,Fr)$$

where $S,O$ are the subject and object of information interaction, $Th$ – virtual connection throughput, $Type$ – the resource requirements, $Fr$ – fractal nature of VC.

From this point of view we suggest to divide set of virtual connections into two subsets:

- Fractal natured virtual connections based on transport protocols with feedback (TCP connections)
- Data flows without fractal properties like UDP data streams

Researches have shown that fractal properties of VC influence its throughput. For calculation the average throughput of TCP connection it is necessary to create a model of connection with fractal properties.

In this paper we suggest to use a simple discrete time model of TCP connection: at each discreet time moments "*k*" TCP throughput "*Th*" can be describes by formulas:

$$X_{k+1} = R(A, X_k, \xi_k) X_k, \quad Th_k = F(X_k),$$

where *X* – congestion window, which size measures in conventional unit, *A* – vector of the protocol deterministic characteristics; ξ - stochastic variable describes by density distribution function [3][4]

$$R(A, X_k, \xi_k) = \begin{cases} 1; \xi_k = 0, X_k = C \\ 1/2; \xi_k = 1 \\ 1/X_k; \xi_k = 2 \\ 2; \xi_k = 0, X_k < C, X_k < S \\ (X_k + 1)/X_k; \xi_k = 0, X_k < C, X_k > S \end{cases}$$

where C is TCP receive window size, S – threshhold.

As it is known from an example of Cantor set the fractal properties appears at loss of the set's part. Fractal properties of TCP-connection characterize the throughput losses because of feedback mechanism. On Fig. 3 there are shown the throughput losses because of CWND adaptation mechanism.

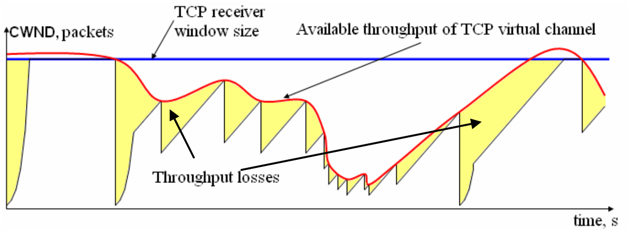

Figure 3. TCP throughput losses because of CWND mechanism.

We suggest using different algorithms to calculate the throughput of VC with fractal properties and without ones.

For the connections without fractal properties we will use the simple formula:

$$Th = Th_0 \cdot (1 - p) ,$$

where $Th_0$ is the connection throughput from the stream source and $p$ is the packet loss probability.

For TCP connections we use the well-known formula:

$$Th = \min(\frac{C}{RTT}; \frac{1}{RTT \cdot \sqrt{\frac{2}{3}p}}) ,$$

where $C$ is TCP receive window size, $RTT$ is round trip time and $p$ is the packet loss probability (loss rate). The graph of this function for $C$ = 100 packets and RTT=110 ms is shown on Fig. 4.

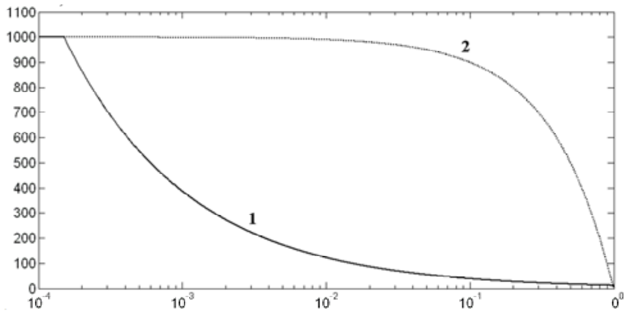

Figure 4. Dependence of TCP throughput on packet loss probability for TCP connections.

## IV. Model of network envirinment

According to the VC models written above we consider the preemptive priority queueing system with two types of customers. First type of customers has priority over the second one. The customers of the type 1 (2) arrive into the buffer according to the Poisson process with rate $\lambda_1$ ($\lambda_2$). The service time has the exponential distribution with the same rate $\mu$ for each type. The service times are independent of the arrival processes. The buffer has a finite size $k$ ($1 < k < \infty$) and it is shared by both types of customers. The absolute priority in service is given to the customers of the first type. Unlike typical priority queueing considered system is supplied by the randomized push-out mechanism that helps precisely and accurate to manage customers of both types. If the buffer is full, a new coming customer of the first type can push out of the buffer a customer of type 2 with the probability $\alpha$. We have to mention that if $\alpha$ =1 we retrieve the standard non-randomized push-out.

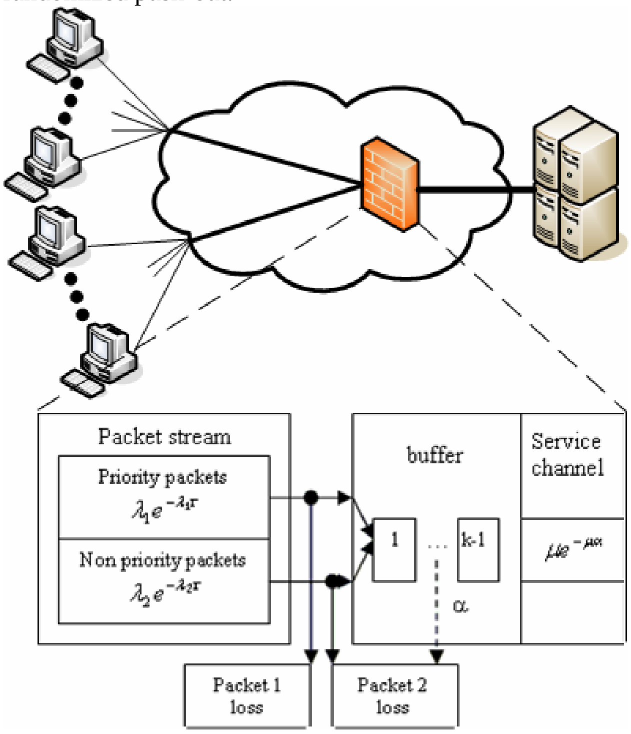

Figure 5. Priority queueing schema $\vec{M}_2 / M / 1 / k / f_2^1$ of telematics network devide.

The scheme described priority queueing is resulted on Fig. 5. The priority queueing without the push-out mechanism ($\alpha = 0$) and with the determined push-out mechanism ($\alpha = 1$) are well-studied. The concept of the randomized push-out mechanism with reference to network and telecommunication problems is offered in [1] where this mechanism was combined with relative priority, instead of absolute, as in our case.

The summarized entering stream represented on Fig. 5 will be the elementary with intensity $\lambda = \lambda_1 + \lambda_2$. The priority queueing represented on Fig. 5, is $\vec{M}_2 / M / 1 / k / f_2^1$ type by Kendall's notation.

Problems of research priority queueing have arisen in telecommunication with the analysis of real disciplines of scheduling in operating computers. Last years a similar sort of queueing model, and also their various generalisations are widely used at the theoretical analysis of Internet systems.

As shown in [1], the probability pushing out mechanism is more convenient and effective in comparison with other mathematical models of pushing out considered in the literature. It adequately describes real processes of the network traffic and is simple enough from the mathematical point of view. The randomized push-out mechanism helps precisely traffic management and security. The another control and security factor is the telematics device buffer size. It can be varied to increase the throughput of necessary connections and reduce throughput of suspicious ones.

## V. MAIN EQUATIONS

The state graph of system $\vec{M}_2 / M / 1 / k / f_2^1$ is presented on Fig. 6.

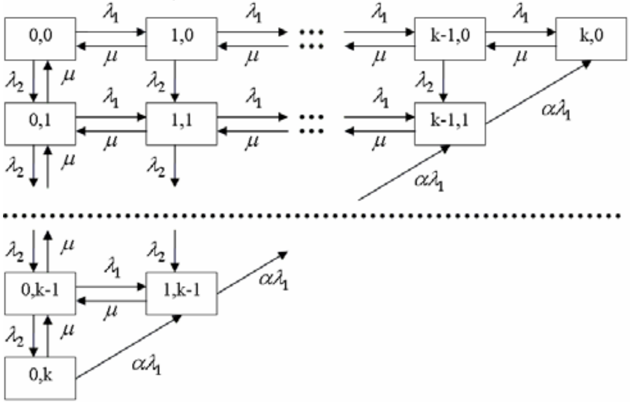

Figure 6. The state graph of $\vec{M}_2 / M / 1 / k / f_2^1$ type system.

Making by usual Kolmogorov's rules set of equations with the help of state graph we will receive:

$$-[\lambda_1(1-\delta_{j,k-i}) + \alpha\lambda_1(1-\delta_{j,k})\delta_{j,k-i} + \lambda_2(1-\delta_{j,k-i}) +$$
$$+\mu(1-\delta_{i,0}\delta_{j,0})]p_{ij} + \mu p_{i+1,j} + \mu\delta_{i,0}p_{i,j+1} + \lambda_2 p_{i,j-1} + \quad (1)$$
$$+\lambda_1 p_{i-1,j} + \alpha\lambda_1\delta_{j,k-i}p_{i-1,j+1} = 0, (i=\overline{0,k};\ j=\overline{0,k-i}),$$

where $\delta_{i,j}$ is the delta-symbol.

There is a normalization condition for the system:

$$\sum_{i=0}^{k}\sum_{j=0}^{k-i} p_{ij} = 1 .$$

At real $k$ (big enough) this system is ill-conditioned, and its numerical solution leads to the big computing errors. In this paper we use the method of generating functions [1] in its classical variant offered by H.White, L.S.Christie and F.F.Stephan with reference to $\vec{M}_2 / M / 1 / f_2$ type systems.

Solving (1) system we receive some auxiliary variables [4]

$$p_i = p_{k-i,i}, \quad (i=\overline{0,k}),$$

$$q_{k-j} = (1-\alpha)\sum_{i=1}^{j} p_i\rho_1^{i-j} + q_k\rho_1^{-j}, \quad (j=\overline{1,k}),$$

$$r_n = \frac{(1-\rho)\rho^n}{(1-\rho^{k+1})}, \ (n=\overline{0,k}) .$$

When using them we can receive loss probability for priority ( $P_{loss}^{(1)}$ ) and non-priority ( $P_{loss}^{(2)}$ ) packets:

$$P_{loss}^{(1)} = q_k + (1-\alpha)\sum_{i=1}^{k-1} p_i ,$$

$$P_{loss}^{(2)} = r_k + \alpha\frac{\rho_1}{\rho_2}\sum_{i=1}^{k} p_i . + \frac{\rho_1}{\rho_2} p_k$$

By these formulas we received some graphs for different rate of input streams of relative throughput of this type (Fig 7,8)

$$æ_i = 1 - P_{loss}^{(i)}, \ (i=\overline{1,2}) .$$

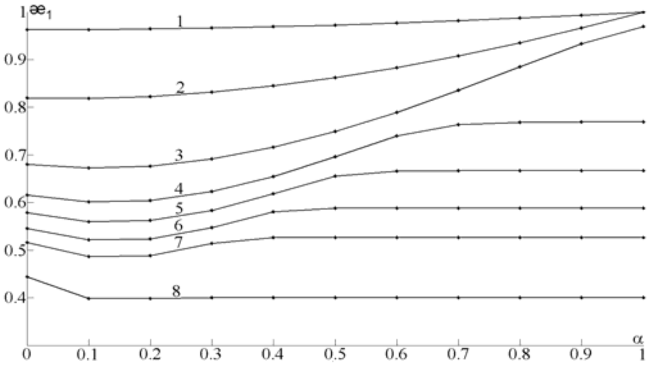

Figure 7. Relative throughput of priority packets for strongly congested transport virtual channel with $\rho_2 = 1{,}5$ and different values $\rho_1$: 1 – $\rho_1 = 0{,}1$ ; 2 – $\rho_1 = 0{,}5$ ; 3 – $\rho_1 = 1{,}0$ ; 4 – $\rho_1 = 1{,}3$ ; 5 – $\rho_1 = 1{,}5$ ; 6 – $\rho_1 = 1{,}7$ ; 7 – $\rho_1 = 1{,}9$ ; 8 – $\rho_1 = 2{,}5$ . The same legend is used by all Figures.

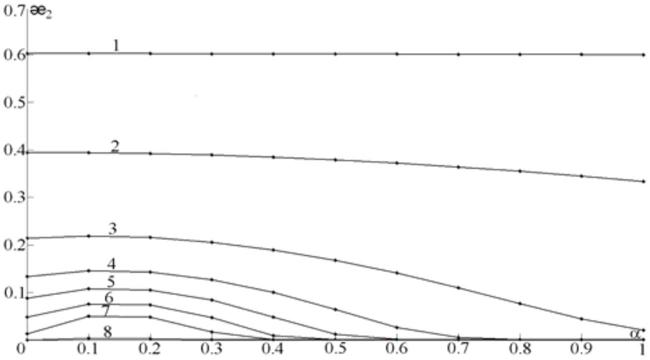

Figure 8. Relative throughput of non-priority packets

From Fig. 7 and 8 we can see, that by choosing parameter $\alpha$ , we can change æ<sub></sub>i in very wide range. For some $\rho_1$ values variable æi changes from 0.6 to 1 while $\lambda_1 + \lambda_2 >> \mu$ . There is an extremum on the most of the curves at $\alpha = 0{,}1 - 0{,}2$ . It means that increasing the push-out probability of non priority packets thus we reduce probability of their loss in the strongly congested networks. It can be explained by the fact that various mechanisms work in the absence of push-out mechanism ( $\alpha = 0$ ) and while $\alpha > 0$ .

The relative time that the priority packet spend in queueing can be calculated by Little's Formula (Fig 9,10):

$$\theta_i = \frac{\bar{s}_i}{\bar{\tau}_i} = \frac{\bar{n}_{load}^{(i)}}{(1-\bar{P}_{loss}^{(i)})} + \rho_i, \ \bar{\tau}_i = \frac{1}{\lambda_i}, \ (i=\overline{1,2}).$$

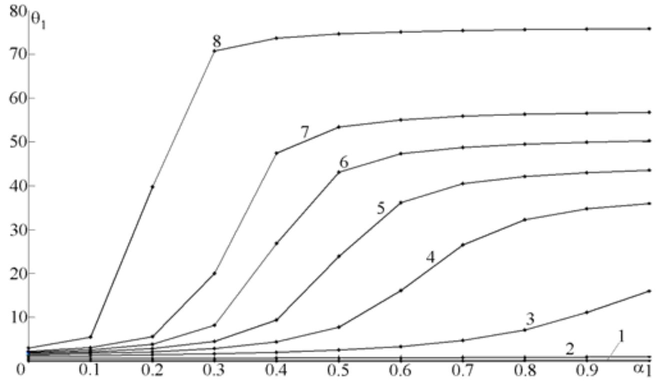

Figure 9. The time that priority packet spend in queueing

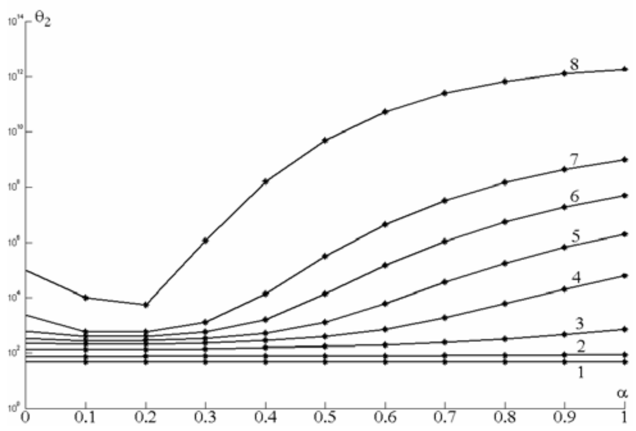

Figure 10. The time that non-priority packet spend in queueing

Fig 9,10 show that proposed queueing mechanism provide a wide range of control feature by randomized push-out parameter α and buffer size k. According to the packet's mark (Forbidden, Priority, Background) the period that packet spend in queue can vary from 1 to $10^{14}$ times, which can be used to control access to information resource providing confidentiality.

For highly congested network the priority type is much less important, than the push-out mechanism and the value of $\alpha$ parameter. The push-out mechanism allows to enforce access policy using traffic priority mechanism.

By choosing $\alpha$ parameter we can change the time that packets spend in the firewall buffer, which allows to limit access possibilities of background traffic and to block forbidden packets. So by decreasing the priority of background VCs and increasing the push-out probability $\alpha$ we can reduce the VC throughput to low level without interrupting it.

The most wide range of control can be reached in intermediate environment conditions when linear law of the losses has already been broken, but the saturation zone has not been reached yet. Numerical experiment [4] has been made to detect conditions in which $\rho_1$ varied over a wide range from 0,1 to 2,5, and $\rho_2 = 1{,}5$ .

## VI. Practical usage and future development.

Good example of opportunity to use such mechanism is the problem of controlling removed robotic object, which telemetry data and a video stream are transmitted on global networks. In this case control commands are transmitted by TCP, and a video stream data are transmitted by UDP. A mean values of throughput of our robotic object: throughput of TCP channel (control and telemetry packets) ~100Kb/s, throughput of UDP video stream ~1,2Mb/s.

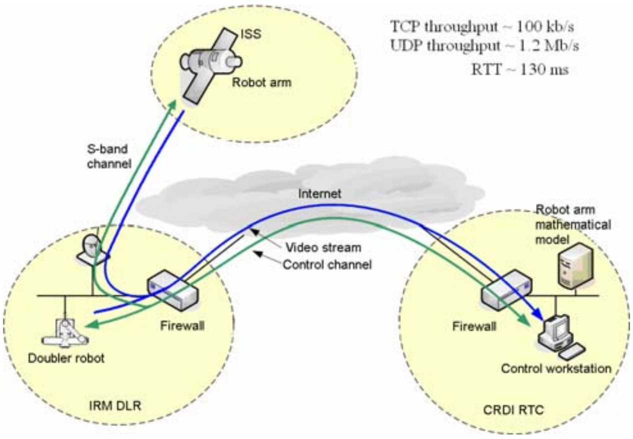

Figure 11. The scheme of space experiment "Contour"

In a considered example on Fig. 11 (ROKVISS mission [5]), the choice of a priority of service and loss-probability of a priority packet $\alpha$ allows to balance such indicators of functioning of a network, as loss-probability of control packets $p_{loss}^{(1)}$ and quality of video stream for various conditions of a network environment. The parameter $\alpha$ can vary for delay minimization in a control system's feedback.

The given problem is important for interactive control of remote real-time dynamic objects, in a case when the complex computer network is the component of a feedback control contour, therefore minimization of losses and feedback delays, is the important parameter characterizing an effectiveness of control system.

In future this method of preemptive access management could be used to mature the DTN technology for space exploration missions and communications architecture for example for robots control on planet's surface from orbital station through the network environment with unstable throughputs and unpredictable packet delays.

Of course in this case two types of priority are not enough for enforce access policy in multiservice network environment, but the recurrent mode of proposed procedure can increase the number of priority VC subsets.

## VII. CONCLUSION.

1. The offered access control approach allows more deeply and more detailed understanding of requirements of access policy in the form of firewall configuration rules.

2. Proposed model based on DiffServ approach considers computer network as the set of VCs, which throughput is easy controlled by proposed classification procedure and algorithm that divides the set of non forbidden VCs in two subsets: non forbidden priority connections and non forbidden non priority or background connections.

3. Introduced VC model takes into account several parameters such as: dynamic and statistics characteristics including fractal properties of VC with feedback throughput control like TCP.

4. Considered preemptive queueing mechanism can be viewed as a background for DiffServ access control because it provides a wide range packet loss probability ratio using flexible randomized push-out algorithm.

5. Proposed push-out algorithm based on selecting priority parameter controls packet loss probability taking into account restricted capacity of packet buffer in DiffServ access point. The most interesting result obtained in congested network allows to keep priority VC throughput near the requested value, which is important for specific space experiment with robotics arm on ISS board.

## REFERENCES

[1] Avrachenkov K.E., Vilchevsky N.O., and Shevljakov G.L. Priority queueing with finite buffer size and randomized push-out mechanism // Proceedings of the ACM international conference on measurement and modeling of computer (SIGMETRIC 2003). San Diego: 2003, p. 324-335.

[2] Vladimir Zaborovsky, Aleksander Gorodetsky, and Vladimir Muljukha «Internet Performance: TCP in Stochastic Network Environment», Proceedings of The First International Conference on Evolving Internet INTERNET 2009, 23-29 August 2009, Cannes/La Bocca, France, Session «INTERNET 1: Internet Performance», Published by IEEE Computer Society, 2009, p.447-452

[3] V. Zaborovsky and A. Titov «Specialized Solutions for Improvement of Firewall Performance and Conformity to Security Policy», Proceedings of The 2009 International Conference on Security and Management, Volume II, Las Vegas, Nevada, USA, July 13-16, 2009, Published by CSREA Press, USA 2009, p.603-608

[4] Zaborovsky V., Zayats O., and Muljukha V. Priority Queuing with Finite Buffer Size and Randomized Push-out Mechanism // Proceedings of the Ninth International Conference on Networks ICN 2010 Menuires, France 2010 p.316-321.

[5] http://www.dlr.de/en/desktopdefault.aspx/tabid-727