Access Control in a Form of Active Queuing Management in Multipurpose Operation Networks

Vladimir Zaborovsky*, Vladimir Mulyukha**, Alexander Ilyashenko***, Oleg Zayats
St. Petersburg state Polytechnical University
Saint-Petersburg, Russia
e-mail: vlad@neva.ru*, vladimir@mail.neva.ru**, ilyashenko.alex@gmail.com***

***Abstract* — Internet processes information in the form of distributed digital resources, which have to be available for authorized usage and protected against unauthorized access. The implementation of these requirements is not a simple task because there are many ways for its realization in the modern congested multipurpose operation networks. The problem of access control can be presented as the task of identifying the characteristics of virtual connections by calculating the appropriate access code. The paper considers the aspects of the filtering algorithms that reduce the computational requirements of the access code and the dynamic priority processing of the packets in the buffer firewall.**

Keywords-access control, virtual connection, priority queueing management, randomized push-out mechanism

I. INTRODUCTION

Access control to the network resources is an important task of the information security. Distributed digital resources that have to be available for authorized usage, and protected against unauthorized access. In the modern computer networks, informational interaction is occurred using application protocols over virtual transport connections. As the result, the problem of access control can be presented as the task of identifying the characteristics of virtual connections by calculating the appropriate access code.

The complexity of this problem is the fact that the access code can be calculated exactly only after the virtual connection is finished. However, in this case, the access control problem can't be solved, because the access becomes irreversible.

The information protection in computer systems has been discussed for almost 50 years. However, the well-known methods of protection of the local data from a remote attacker don't take into account the specifics of modern computer networks such as:

- Territorial distribution and concurrency;
- The dual nature of access control procedures that doesn't allow to form a "security perimeter" as a static requirement concerning network services;
- Non-locality of network resources and characteristics;
- A semantic gap between security policy description and firewall configuration parameters.

The paper considers the problem of computing the access code for virtual connections passing through the corporate firewall based on the analysis of the packets that form the virtual connections. The estimates of the result are probabilistic, but they could improve the effectiveness of information security introducing various mechanisms to control throughput of such virtual connections.

We propose a formalism in which virtual connections are considered as network "meso" objects and packets are the "micro" ones.

Properties of "meso" objects, such as its throughput, could be changed according to the security policy and the characteristics of the "micro" objects, which are determined while passing through the firewall.

The proposed formalism is applied to the management task of the local user access to the external information resources, which are considered as network "macro" objects. To solve the problem of calculating the dynamic code we suggest using the indicator function, whose properties depend on the information model of the macro object and on the description of the access policy, which defines the rights of users and measured data of packets generated by virtual connection.

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. The adaptability of the proposed mechanism improves network security, but it requires large computational resources of the firewall. The paper suggests the aspects of the filtering algorithms that reduce the computational requirements of the access code and the dynamic priority processing of the packets in the buffer firewall.

In order to realize information security in multipurpose operation networks we propose: 1) the new classification of virtual connections (VC) based on access code: security VC characteristics and throughput requirements; 2) VC model, which takes into account fractal characteristics of packet flows; 3) randomized preemptive queuing management mechanism in congested operation 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).

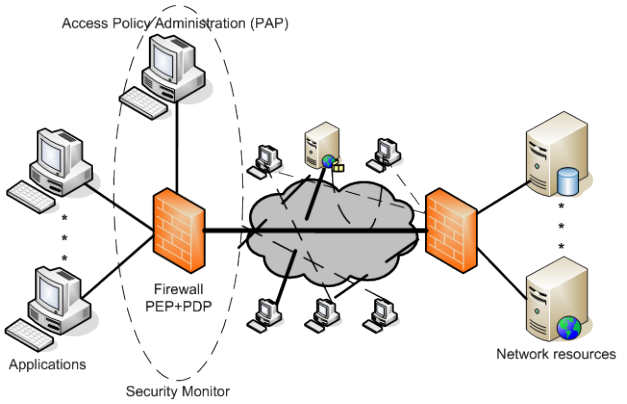

Figure 1. Firewall as a central component of access policy enforcement

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 when 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 in two classes with different access conditions. In proposed approach, the classification decision is based on access code *F* and firewall has three modes according to possible *F (A)* values (Fig. 2):

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

The state of the virtual connection is controlled throughout its lifetime, since the value of access code for "meso" object could change while receiving new "micro" objects.

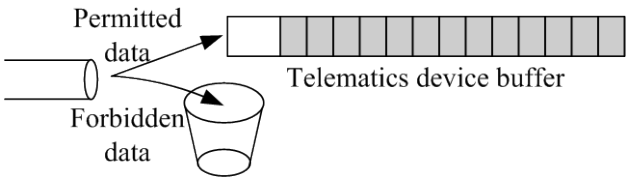

Figure 2. Data flows devision in firewall

When the network environment is congested or when VCs have different QoS requirements the subset of permitted connection has to be divided into new subsets with different access codes:

- "1" for prior "meso" objects that have low throughput and demand low stable delivery time;
- "0" for background ones that demand high throughput and have no delivery time requirements.

For more accurate data sorting we propose to use multiple priority levels. In this paper we consider the simplest situation with two priority levels. It is not enough for practice tasks so we propose some easy ways to increase the number of levels using subsets of permitted VCs (Fig. 3).

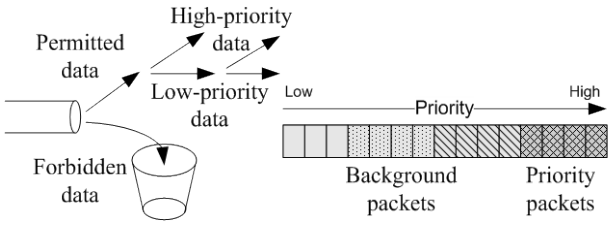

Figure 3. Multiple priority level in congested operation networks

In order to provide this classification procedure we proposed active queuing management mechanism, which is 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 α. Each of the firewall rules has a set of attributes, access code: identifiers of subject and object and the access 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.

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

II. Security Monitor Architecture

Computer network security is a main issue of modern information infrastructure. This infrastructure stores information in the form of distributed digital resources, which have to be protected against unauthorized access. However, the implementations of this statement are far from

simple due to the dynamic nature of the network environment and users activity [1].

The virtual connection can be described entirely only when it is closed, but in this case, it will not allow us to provide the required level of information security. While we receive information from the VC, there is always the non-zero probability that the VC's properties have been wrongly estimated. In this paper, we consider the architecture of security telematics device that have to decrease this probability using multiple sources of information:

- current data about network traffic that the firewall receives from packet headers fields;
- current data about network environment and users from IDS and special user-activity monitor;
- prior data from informational resource model about expected traffic properties.

So below we describe a new approach to configure the security network appliances, which allows an administrator to overcome the semantic gap between security policy requirements, the ability to configure the firewall filtering rules [2] and to decrease the wrong VC's properties estimation probability. The architecture of the proposed system is presented in Fig. 4.

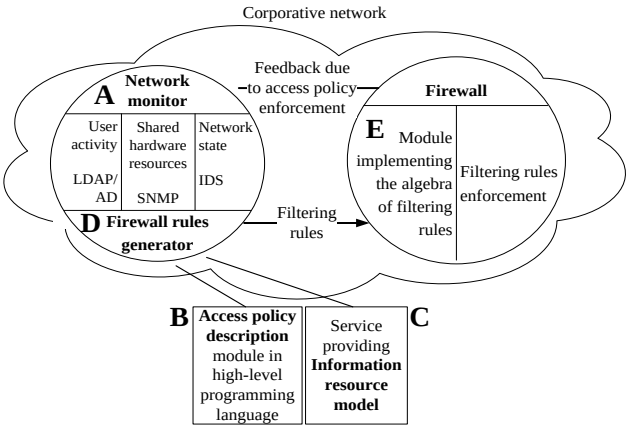

Figure 4. Security monitor architecture

where:

A. Network monitor

Network monitor controls the whole system. Network environment state consists of three main parts:

- "User activity" is the information about what computer is currently used by which user. This information can be obtained from Microsoft Active Directory (AD) by means of LDAP protocol.
- "Shared hardware resources" is the information about network infrastructure and shared internal resources that can be described by network environment state vector Xk
- "Network state" is the information about external network channel received from Intrusion Detection Systems (IDS).

B. Access policy description module

Filtering rules of a firewall in itself are a formalized expression of an access policy. An access policy may simply specify some restrictions, e.g., "Mr. Black shouldn't work with Youtube" without the refinement of the nature of "Mr. Black" and "work" [2],[3].

There is a common structure of access policy requirements, which uses the notions of subject, action and object. Thus, the informally described requirement "Mr. Black shouldn't work with Youtube" can be formally represented as the combination of the subject "Mr. Black", the action "read", the object "www.youtube.com" and the decision "prohibit". This base can also be augmented by a context, which specifies various additional requirements restricting the cases of rule's application, e.g.: time, previous actions of the subject, attributes' values of the subject or object, etc.

However, access rules, which are based on the notions of subject, action and object are not sufficient alone to implement complex real-world policies. As a result, new approaches have been developed. One of them, Role Based Access Control (RBAC) [4], uses the notion of role. A role replaces a subject in access rules and it's more invariant. Identical roles may be used in multiple information systems while subjects are specific to a particular system. As an example, remember the roles of a system administrator and unprivileged user that are commonly used while configuring various systems. Administrator-subjects (persons) may be added or removed while an administrator-role and its rules are not changing.

However, every role must be associated with some subjects as only rules with subjects can be finally enforced. During policy specification roles must be created firstly, then access rules must be specified with references to these roles, then the roles must be associated with subjects.

The OrBAC [5] model expands the traditional model of Role Based Access Control. It brings in the new notions of activity, view and abstract context. An activity is to replace an action, i.e., its meaning is analogous to the meaning of a role for a subject. A view is to replace an object. "Entertainment resources" can be an example of view, and "read" or "write" can be examples of an activity. Thus, the notions of role, activity, view and abstract context finally make up an abstract level of an access policy. OrBAC model allows to specify the access rules only on an abstract level using the abstract notions. Those are called the abstract rules. For instance, an abstract rule "user is prohibited to read entertainment resources", where "user" is a role, "read" is an activity, and "entertainment resources" is a view. The rules for subjects, actions and objects are called concrete access rules.

To specify an OrBAC policy, a common language, XACML (eXtensible Access Control Markup Language) was introduced. The language maintains the generality of policy's specification while OrBAC provides additional notions for convenient editing.

C. Firewall rules generator

There is a feature common for all firewalls: they execute an access policy. In common representation, the main function of access control device (ACD) is to decide whether a subject should be permitted to perform an action with an object. A common access rule "Mr. Black is prohibited to read www.youtube.com".

As was mentioned above, "Mr. Black" is a subject, "HTTP service on www.youtube.com" is an object, and reading is an action. So the configuration of ACD consists of common access rules that reference the subjects, actions and objects.

Although a firewall as an ACD must be configured with common access rules, each implementation uses its own specific configuration language. The language is often hardware dependent, reflecting the features of firewall's internal architecture, and usually being represented by a set of firewall rules. Each rule has references to host addresses and other network configuration parameters. An example of the verbal description of a firewall rule may go as follows:

Host with IP address 10.0.0.10 is prohibited to establish TCP connections on HTTP port of host with IP address 208.65.153.238.

The main complexity of this approach is to find out how such elementary firewall rules could be obtained from common access rules.

Each firewall vendor reasonably aims at increasing its sales appeal while offering various tools for convenient editing of firewall rules. However, so far the problem of obtaining firewall rules from common access rules is not resolved in general. Moreover, this problem has not been paid much attention to.

The most obvious issue concerning this problem is that additional information beyond access rules is necessary in order to obtain the firewall rules. This information concerns the configuration of network services and the parameters of network protocols that are used for data exchange – "network configuration". In general, it can be stored among the descriptions of subjects, actions and objects. An example:

Mr.Black: host with IP-address = 10.0.0.10;
www.youtube.com: HTTP service (port 80) on host with IP-address = 208.65.153.238.

Thus, the final firewall rules can be obtained by addition of the object descriptions to the access rules. It should be noted that even for small and especially for medium and large enterprises it is necessary to store and manage the network configuration separately from the security policy. The suggested approach allows us to achieve this goal: the security officer can edit the access rules with reference to real objects while the network administrator can edit the parameters of the network objects [2].

It should also be noted that there is no need to specify any fixed rules regarding association of the network parameters with the objects. For instance, HTTP port may be a parameter of an object or it may be a parameter of an action. A criterion is that the most natural representation of access policy must be achieved.

While generating the rules, the parameters of network objects can be automatically retrieved from various data catalogs. DNS is the best example of a world-wide catalog, which stores the network addresses. Microsoft offers the network administrators the powerful means, Active Directory, to store information about users. Integration with the above mentioned technologies greatly simplifies the work of a security officer as he has only to specify the correct name of an object while forming firewall rules.

D. Information resource model

Interaction between subject and object in computer network can be presented as a set of virtual connections. Virtual connections can be classified as technological virtual connections (TVC) or information virtual connections (IVC). (see Fig. 5).

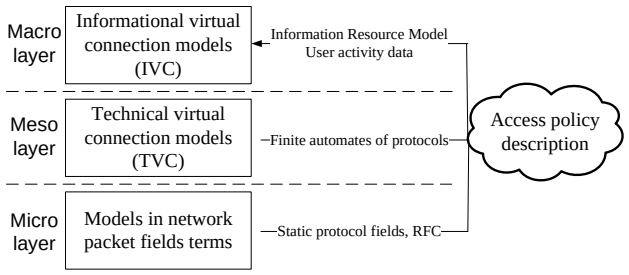

Figure 5. Layers of access control policies.

To implement the policy of access control, the filtering rules are decomposed in the form of TVC and IVC. These filtering rules can be configured for different levels of the data flow description based on the network packet fields at the levels of channel, transport, and application protocols.

At different layers of access control policy model, the filtering rules have to take into account various parameters of network environment and objects. At the packet filter layer, a firewall considers standards static protocol fields described by RFC. At the layer of TVC, firewall enforces the stateful inspection using finite automata describing states of transport layer protocols. On the upper layer of IVC firewall must consider a-priori information about subject and object of network interaction [6].

As was mentioned above, the information about subject can be obtained from catalog services by LDAP protocol, e.g. Microsoft Active Directory.

According to existing approach [7] a resource model can be presented in:

1) logical aspect – an N-dimensional resource space model [8];
2) representation aspect - the definition based on standard high-level description languages like XML or OWL [9];
3) location aspect – the physical storage model of the resource including resource address.

All these approaches describe the network resource as a whole but don't take into account the specific access control task. Any remote network resource can be fully classified when the connection between this resource and local user would be closed. So it is necessary to control all virtual connections in real time while monitoring traffic for security purpose.

In this paper, we propose to implement a special service external to the firewall that would collect, store and renew information about remote network objects. It should automatically create information resource model, describing all informational virtual connections that have to be established to receive this resource. This service should periodically renew information about resource to keep it alive.

Firewall should cooperate with this external service to receive information resource model and enforce access policy requirements.

E. Algebra of filtering rules

As was mentioned above, the information security is defined by an access policy that consists of access rules. Each of these rules has an access code, a set of attributes; the basic ones among them are identifiers of subject and object and the rights of access from one to another. In TCP/IP-based distributed systems, access rules have additional attributes that help to identify flows of packets (sessions) between the client and network application server. Generally these attributes identify the network subjects and objects at different layers of TCP/IP interaction model: MAC-addresses at link layer, IP-addresses at network layer, port numbers at transport layer and some parameters of application protocols.

The access policy in large distributed informational system consists of a huge number of rules that are stored and executed in different access control appliances. The generation of the access policy for such appliances is not very difficult: information must be made available for authorized use, while sensitive data must be protected against unauthorized access. However, its implementation and correct usage is a complex process that is error-prone. Therefore the actual problem of rule generation is representation, analysis and optimization of access policy for large distributed network systems with lots of firewall filtering rules. In our papers, we proposed an approach to description, testing and verification of access policy by the means of specific algebra with carrier being the set of firewall filtering rules. According to proposed approach we define a ring as algebraic structure over set of filtering rules or R [10].

III. VIRTUAL CONNECTION CLASSIFICATION

In this paper, we use the term "access management" as the combination 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 streams, 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. As it was mentioned before, the 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 VCs. In classical subject-object model the set of VCs is divided into two subsets by security characteristic:

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

From another point of view the set of VCs can be divided into several subsets by the type of transmittable information and its quality of service request:

- priority ones, which demand low stable delivery time;
- non-priority ones, which demand high throughput and have no delivery time requirements.

The last subset of non-priority VCs also could be divided into several subsets with different priority levels. So in this paper, we present the simplest example with three subsets:

1) priority non forbidden connections;
2) background non forbidden connections;
3) forbidden connections.

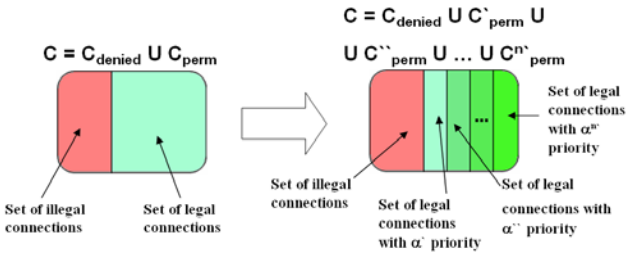

Figure 6. Virtual connections classification model

As it was described there are always type I and type II classification errors, but using additional information in proposed architecture of security monitor we are trying to minimize them.

On Fig. 6 there is graphical interpretation of considered classification.

IV. 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 by Fr characteristic:

- 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 VCs 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 described by density distribution function [1],[11]

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

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

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. 7 there are shown the throughput losses because of CWND adaptation mechanism.

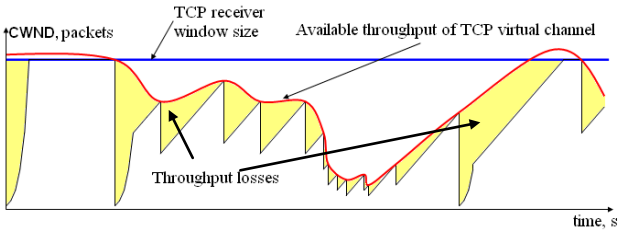

Figure 7. TCP throughput losses because of CWND mechanism

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

For the connections of type 2 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 (type 1) we use the well-known formula:

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

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=100 ms is shown on Fig. 8.

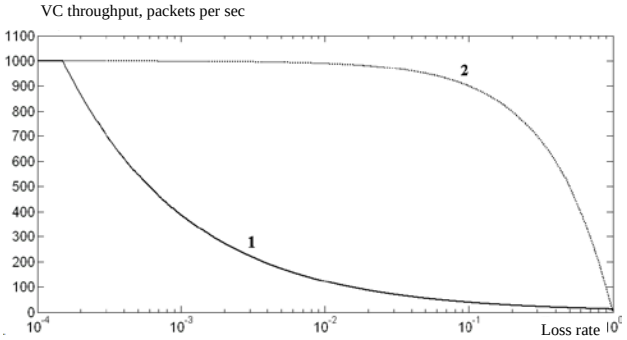

Figure 8. Dependence of TCP throughput on packet loss probability for TCP connections

V. MODEL OF NETWORK ENVIRONMENT

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 λ_1 (λ_2). The service time has the exponential distribution with the same rate μ 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 α. We have to mention that if $\alpha = 1$ we retrieve the standard non-randomized push-out.

The scheme described priority queueing is resulted on Fig. 9. 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 [12] where this mechanism was combined with relative priority, instead of absolute, as in our case.

The summarized entering stream represented on Fig. 9 will be the elementary with intensity: $\lambda = \lambda_1 + \lambda_2$. If we'll trace only the general number of packets in system, then simplified one-data-flow model would be $M/M/1/k$ type. In the modified by G.P.Basharin Kendel notation, the general structure of a label and sense of its separate positions remains, however in each position the vectorial symbolic is used [13]. There is an additional symbol f_i^j, where i specifies priority type (0 – without a priority, 1 – relative, 2 – absolute), and j specifies a type of the pushing out mechanism (0 – without pushing out, 2 – the determined pushing out). So $j = 1$ wasn't used. In [12], authors offer to use this value for the randomized push-out mechanism, as an intermediate between variants $j = 0$ and $j = 2$. So, using this new notation, system represented on Fig. 9 has $\vec{M}_2 / M / 1 / k / f_2^1$ type.

The history of one-channel two data-flow priority systems research includes already more than half a century, however, as far as we know, there is only one work [12] where the randomized push-out mechanism have been studied (in a combination with the relative priority for queueing $\vec{M}_2 / M / 1 / k / f_1^1$ type). At the same time, for the typical models with the push-out mechanism ($j = 0$ and $j = 2$) the problem is solved basically.

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 generalizations are widely used at the theoretical analysis of Internet systems.

As has been shown in [12], 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. 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.

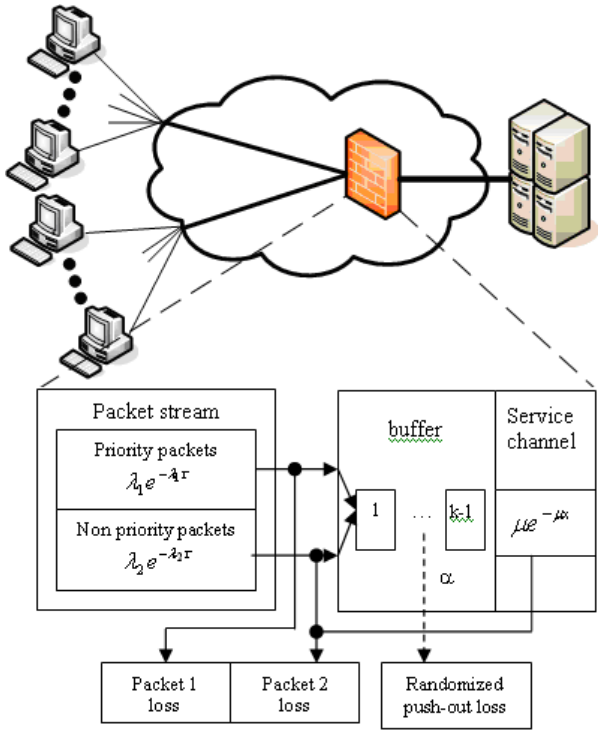

Figure 9. Priority queueing schema $\vec{M}_2 / M / 1 / k / f_2^1$ of telematics network devide

VI. MAIN EQUATIONS

The state graph of system $\vec{M}_2 / M / 1 / k / f_2^1$ is presented on Fig. 10.

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

$$
\begin{aligned}
&-[\lambda_1(1-\delta_{j,k-i}) + \alpha\lambda_1(1-\delta_{i,k})\delta_{j,k-i} + (1-\alpha)\lambda_1\delta_{i,0}\delta_{j,k-i} + \\
&+\lambda_2(1-\delta_{j,k-i}) + \mu(1-\delta_{i,0}\delta_{j,0})]P_{i,j} + \mu P_{i+1,j} + \mu\delta_{i,0}P_{i,j+1} + \\
&+\lambda_2 P_{i,j-1} + \lambda_1 P_{i-1,j} + \alpha\lambda_1\delta_{j,k-i}P_{i-1,j+1} + \\
&+(1-\alpha)\lambda_1\delta_{j,k-i}\delta_{i,1}P_{i-1,j+1} = 0, (0 \le i \le k; 0 \le j \le k-i),
\end{aligned}
\quad (1)
$$

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

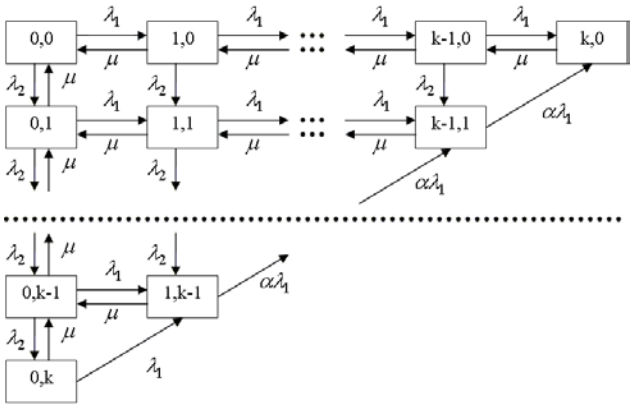

Figure 10. The state graph of $\vec{M}_2 / M /1/ k / f_2^1$ type system

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 [12] in its classical variant offered by H.White, L.S.Christie [14] and F.F.Stephan [15] with reference to $\vec{M}_2 / M /1/ f_2$ type systems. According to generating function method and normalization condition we have:

$$G(u,v) = \sum_{i=0}^{k}\sum_{j=0}^{k-i} P_{i,j} u^i v^j, \; G(1,1) = \sum_{i=0}^{k}\sum_{j=0}^{k-i} P_{i,j} = 1.$$

And after several transformations result equation for generating function will be:

$$[\lambda_1 u(1-u) + \lambda_2 u(1-v) + \mu(u-1)]vG(u,v) =$$
$$= \mu(u-v)G(0,v) + \mu u(v-1)G(0,0) +$$
$$+\alpha\lambda_1 u^{k+1}(v-u)P_{k,0} + [\alpha\lambda_1(u-v) +$$
$$+\lambda_1(1-u)v + \lambda_2(1-v)v]u\sum_{i=0}^{k} P_{i,k-i}u^i v^{k-i} +$$
$$+(1-\alpha)\lambda_1 P_{0,k} v^k u(u-v).$$

Solving this equation and (1) system we receive some auxiliary variables:

$$p_i = P_{k-i,i}, \; (i = \overline{0,k}),$$

$$q_{k-j} = (1-\alpha)\sum_{i=1}^{j} p_i \rho_1^{i-j} + p_0 \rho_1^{-j} - (1-\alpha)p_k \delta_{j,k}, (j = \overline{0,k}),$$

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

$$G(u,v) = \frac{(u-v)G(0,v) + u(u-1)G(0,0)}{v\rho_1(u-u_1)(u-u_2)} +$$
$$+\frac{\alpha\rho_1 u^{k+1}(v-u)P_{k,0} + (1-\alpha)\rho_1 P_{0,k} v^k u(u-v)}{v\rho_1(u-u_1)(u-u_2)} +$$
$$+\frac{[\alpha\rho_1(u-v) + \rho_1(1-u)v + \rho_2(1-v)v]u\sum_{i=0}^{k} P_{i,k-i}u^i v^{k-i}}{v\rho_1(u-u_1)(u-u_2)}.$$

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

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

Exploring these formulas we found some useful properties of this system described in this article. One of them presented on Fig.11, 12. When incoming stream of priority packets getting more intensive, system starts to prohibit admission of non-priority packets. While the total flow rate is less than unity ($\rho_1 + \rho_2 \le 1$), the probability of loss is equal to zero. This means that the system is fully copes with the load (see Fig.11). In Figure 12, the graph does not start from zero because the system is initially overloaded with non-priority packets. Same effect and in this case.

On Fig. 13 an expected result can be seen that the probability of losing priority packet decreases with increasing size of a buffer, but not as much as has been expected. Probability of loss is decreasing not more than 5% for small values of α. Therefore, only for large probability values increasing buffer size effectively influences the losses. For priority stream influence of this effect is the same for all values of alpha, but for non-priority packets the situation is different. Figure 14 shows that it is sometimes advantageous to have a buffer of smaller size. With a small buffer probability of be pushed out much lower, what explains this effect.

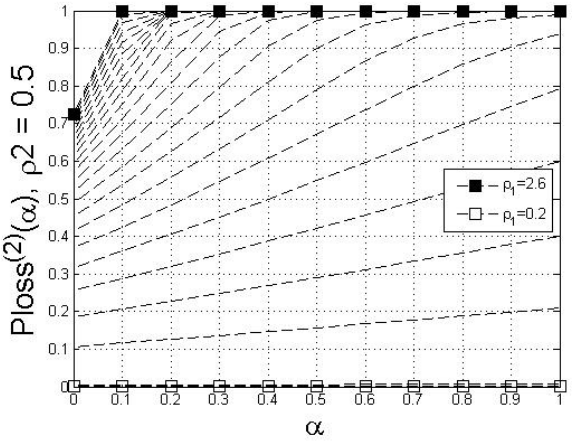

Figure 11. Loss probability of non-priority packets with 0.1 step for $0.2 \le \rho_1 \le 2.6$, buffer size 31 and weak non-priority stream

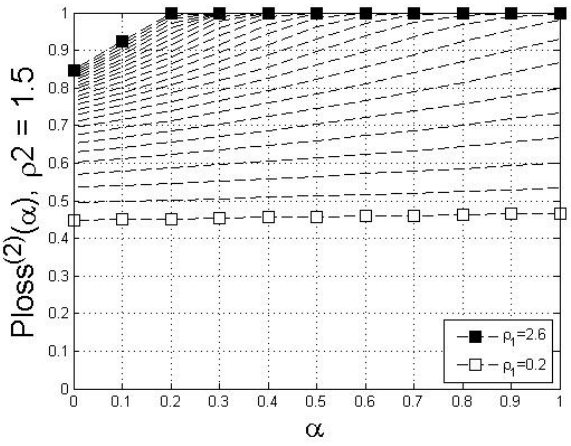

Figure 12. Loss probability of non-priority packets with 0.1 step for $0.2 \le \rho_1 \le 2.6$, buffer size 31 and more ntensive non-priority stream

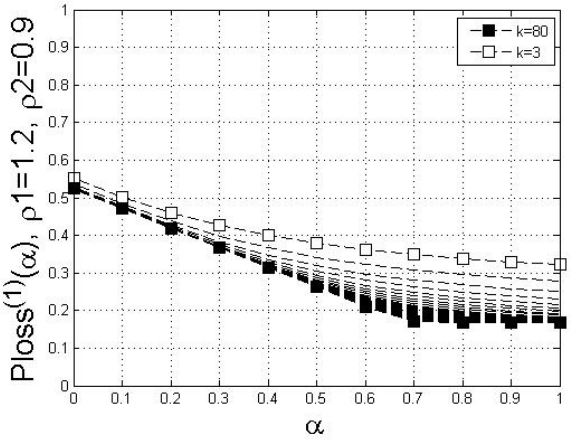

Figure 13. Loss probability of priority packets with buffer size K=3-80

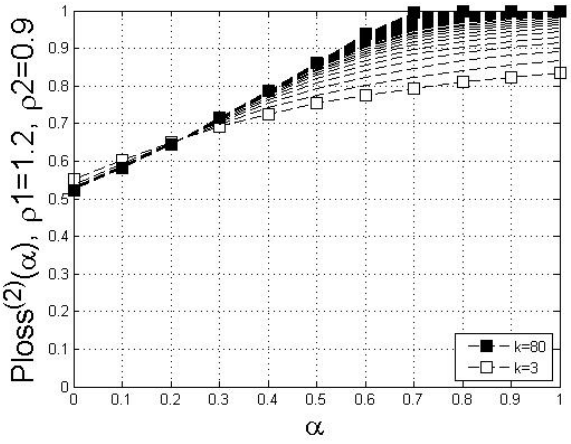

Figure 14. Loss probability of non-priority packets with buffer size K=3-80

Graphs on Fig.11, 12 are inverted images of the graphs of the relative throughput, which is computed by formulas (2) and are very important for research of processes in computer networks.

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

From Fig. 11 and 12 we can see, that by choosing parameter α, we can change $P_{loss}^{(2)}$ in very wide range. For some ρ_1 values variable $æ_i$ changes from 0.7 to 1 while $\lambda_1 + \lambda_2 >> \mu$.

Next interesting variable is average queue length of priority packets (see Fig.15, 16, 17), computing as (3). While the system is not loaded, the average queue length is zero, as shown in the bottom of the chart (see Fig. 13). But once the system begins to fill, then average queue length begins to grow rapidly. And as seen in the Figures 15, 16, 17, that by using the α be strong enough to influence the filling of the queue. In some cases, change the setting at 0.1 entails the complete filling of the queue.

$$\overline{n_{oч}}^{(1)} = \sum_{i=1}^{k}(i-1)q_i = \overline{n}^{(1)} - \sum_{i=1}^{k} q_i = \overline{n}^{(1)} - (1-q_0). \quad (3)$$

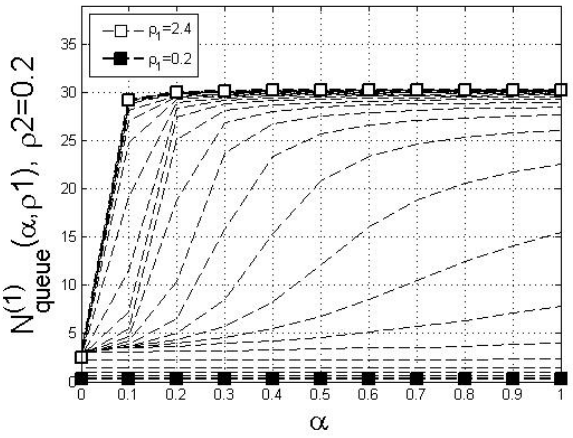

Figure 15. Average priority queue length with low intensity of second stream with buffer size 31

The relative time that the priority packet spend in queueing can be calculated by Little's Formula (Fig 18,19,20) [16]:

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

Fig 18, 19, 20 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.

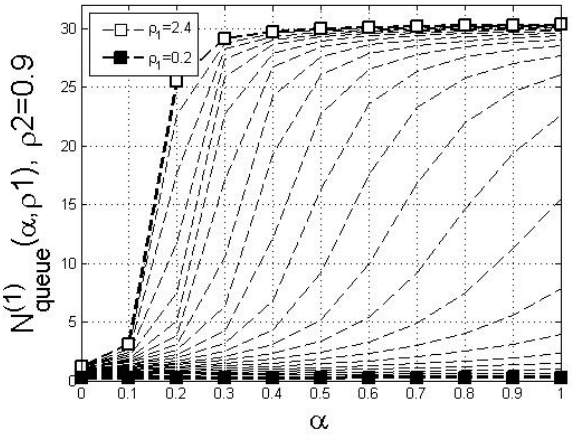

Figure 16. Average priority queue length with medium intensity of second stream with buffer size 31

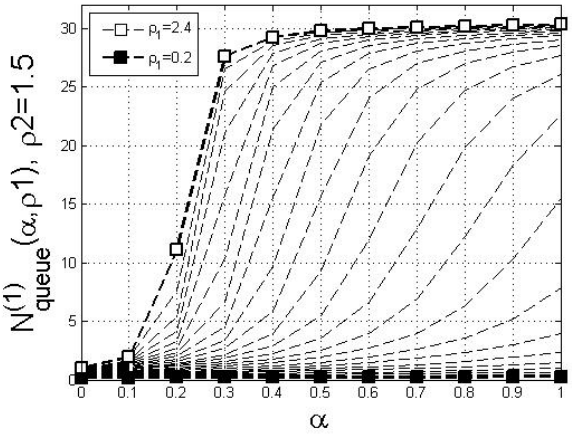

Figure 17. Average priority queue length with high intensity of second stream with buffer size 31

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

By choosing α 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 α we can reduce the VC throughput to low level without interrupting it.

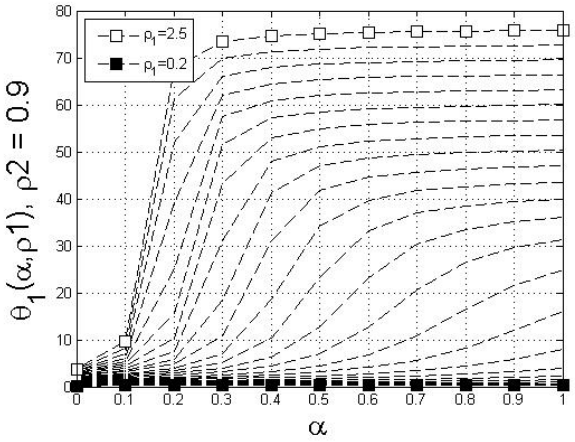

Figure 18. The time that priority packet spend in queueing

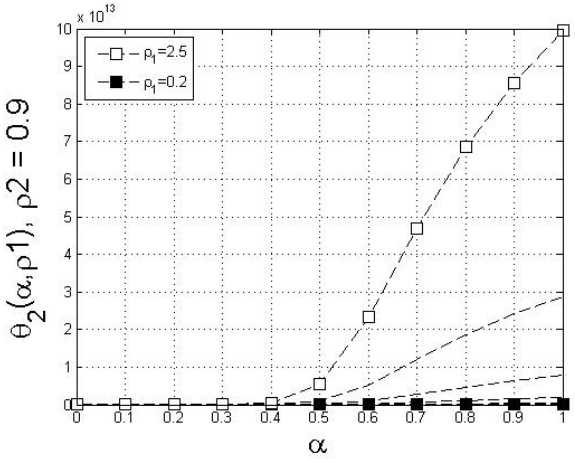

Figure 19. The time that non-priority packet spend in queueing

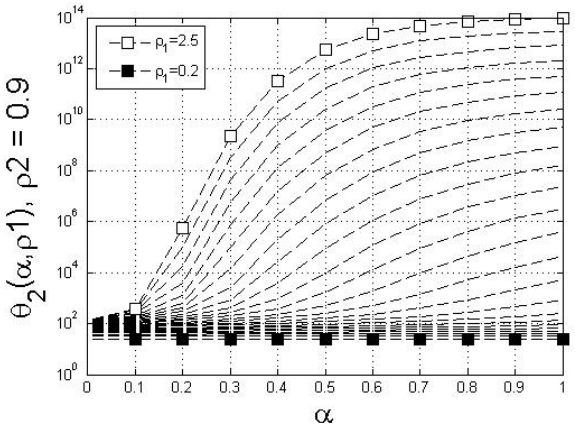

Figure 20. The time that non-priority packet spend in queueing built in logarithmic y scale

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 [17] has been made to detect conditions in which ρ_1 varied over a wide range from 0,1 to 2,5, and few fixed values for ρ_2.

VII. 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.

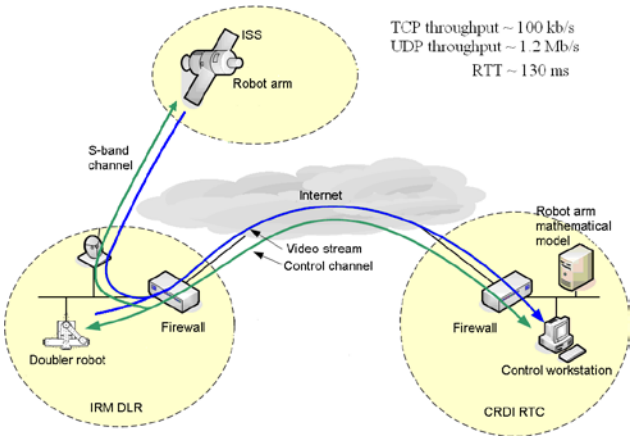

Figure 21. The scheme of space experiment "Contour"

In a considered example on Fig. 21 (ROKVISS mission [18]), the choice of a priority of service and loss-probability of a priority packet α 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 α 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 in new joint space experiment METERON-R (Multi-purpose Experimental TElecommunication Robotic Operations Network - Russia) that will be carried out on ground and on-board the ISS, in order to research efficiency and security of robotic operations in space and ground environments, including the configuration of robotic control systems as a part of multipurpose operations network (Fig. 22). The joint experiments will focus on the analysis of how well astronauts can operate complex robotic systems based on operation networks with mobility and manipulation capability from within the highly constrained ISS and micro-gravity environment. Multiple human-robot interfaces will be used in combination, while simulating realistic robotic remote operations with round-trip time communication conditions representative of future human planet exploration missions.

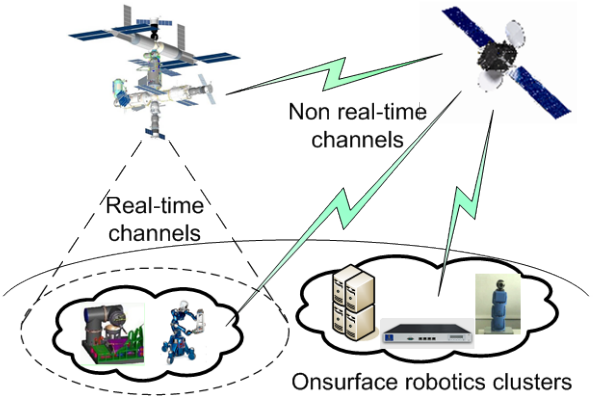

Figure 22. The scheme of space experiment "METERON-R"

For communication experiments, the primary focus will be on the usage of real-time duplex commanding, in combination with Delay Tolerant Network (DTN) approaches and Inmarsat channel. Real-time channel will have low delay (15-20 ms) and high throughput (4 Mb/s), but the connection would be established only when the space station is in the radio-optical range (7-10 min). DTN channels have high delay and low throughput, but function for 24/7. Inmarsat channel characteristics are between real-time and DTN and they are much depend on quantity of retransmission satellites.

Robotics objects within multipurpose operation network would execute the programs and interact without human involvement. However there would be always situations when the robot couldn't make a decision by its own. In that case, the human-operator will have several opportunities:

1) remote telecontrol through real-time channel;
2) to send several commands or additional data through Inmarsat channel;
3) to send new program through DTN.

Each of these data will have its own priority level. So in this case, two types of priority are not enough for traffic management in multipurpose operation network environment, but the recurrent mode of proposed procedure can increase the number of priority VCs subsets.

VIII. 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. In multipurpose operation networks, we propose a new formalism in which the distributed digital resources are considered as “macro” objects, virtual connections are the network "meso" ones and packets are the “micro” objects. Proposed formalism allows to enforce security policy and provides authorized usage and protection against unauthorized access.

3. 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.

4. 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.

5. 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.

6. 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.

7. We described the future usage of proposed formalism in joint space experiment where several types of operations are serviced by security monitor in multipurpose operation network.

REFERENCES

[1] Zaborovsky V. and Mulukha V. Access Control in a Form of Active Queuing Management in Congested Network Environment // Proceedings of the Tenth International Conference on Networks, ICN 2011 pp.12-17.

[2] Zaborovsky V. and Titov A. Specialized Solutions for Improvement of Firewall Performance and Conformity to Security Policy, Proceedings of The 2009 International Conference on Security and Management, Volume II, Published by CSREA Press, USA 2009, p.603-608

[3] Titov A. and Zaborovsky V. Firewall Configuration Based on Specifications of Access Policy and Network Environment // Proceedings of the 2010 International Conference on Security & Management. July 12-15, 2010.

[4] Ferraiolo D.F. and Kuhn. D.R. Role-Based Access Control. 15th National Computer Security Conference. (October 1992), pp. 554–563. (http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf)

[5] http://orbac.org/index.php?page=orbac&lang=en

[6] Zaborovsky V., Lukashin A., and Kupreenko S. Multicore platform for high performance firewalls. High performance systems // Materials of VII International conference – Taganrog, Russia.

[7] Zhuge H., The Web Resource Space Model, Berlin, Germany: Springer-Verlag, 2007

[8] Zhuge H., Resource Space Grid: Model, Method and Platform, Concurrency and Computation: Practice and Experience, vol. 16, no. 14, pp. 1385-1413, 2004

[9] Martin D., Burstein M., J. Hobbs, O. Lassila. et al. (November 2004) “OWL-S: Semantic Markup for Web Services,” [Online]. Available: http://www.w3.org/Submission/OWL-S/.

[10] Silinenko A. Access control in IP networks based on virtual connection state models: PhD. Thesis 05.13.19: / SPbSTU, Russia, 2010.

[11] 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, Published by IEEE Computer Society, 2009, p.447-452

[12] 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.

[13] Basharin G. P. A single server with a finite queue and items of different types // Teor. Veroyatnost. i Primenen., 1965, Volume 10, Issue 2, Pages 282–296

[14] White H. and Christie L.S. Queueing with preemptive priorities or with breakdown // Operations research, 1958, vol. 6, no. 1, p. 79-95.

[15] Stephan F.F. Two queues under preemptive priority with Poisson arrival and servive rates // Operations research, 1958, vol. 6, no.3, p. 399-418

[16] L. Kleinrock. Queueing Systems Volume I-II, 1976.

[17] 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, p.316-321.

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