

# Telematics Approach to Fine Access Policy Enforcement: Rules Configuration Algebra and Randomized Priority Queueing Management

Vladimir Zaborovsky, Oleg Zayats, Vladimir Mulukha, Alexander Silinenko

St. Petersburg state Polytechnical University, R&D Institute for Robotics and Technical Cybernetics  
Saint-Petersburg, Russia

**Abstract.** Internet is a global information infrastructure that keeps information in the form of distributed digital resources which have to be available for authorized usage, while sensitive data should be reliably protected against unauthorized access. Implementation of these requirements is not simple task because security policy has many elements and many ways of realization. That is why in the multiservice network environment many well-known solutions of the past have become inadequate. Therefore we have offered the new approach to raise accuracy of implementation of access policy. The idea of this approach is based on combining: 1) formal methods that are used to define security requirement, 2) firewall configuration rules in the form of mathematical expressions, and 3) methods of fine tuning of telematics channel throughput which is based on randomized queueing management mechanism. With the help of algebra of configuration rules we develop methods to standardize and optimize the firewall configuration while the preemptive priority queueing mechanism enforce adaptive feature of security system. Proposed approach based on theoretical results that correspond to IETF Framework for Policy-based Admission Control.

**Keywords** — access policy, algebra of filtering rules, traffic security, priority queueing management, randomized push-out mechanism

## I. INTRODUCTION AND THEORETICAL BACKGROUND

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 must be available for authorized use, while sensitive data which have be protected against unauthorized access. However, the implications of this statement are far from simple due to security policy has many elements and many ways of enforcement. Therefore many well-known solutions of the past have become increasingly inadequate. For this reason we require more deeply and more detailed understanding of requirements of Policy Decision point (PDP) and Policy Enforcement point (PEP) which defines security appliances configuration rules [1]. The main purpose of security appliances or firewalls development is to increase their performance and accuracy realization of access policy requirements by means of traffic management (queueing), configuration methods (formal algebra) and environment characteristics identification algorithm or indicator functions. To reach this purpose it is necessary to choose a model of security appliances with customized management parameters which have to be adjusted in accordance of access policy. Nowadays there are some

ways to solve this task. The standard in this area is eXtensible Access Control Markup Language (XACML) that based on IETF Framework for Policy-based Admission Control, which components include:

- Policy Decision Point (PDP) – XACML solution that makes the access decisions.
- Policy Enforcement Point (PEP) – the most security-critical component, which protects the resources and enforces the PDP's decision.
- Policy Administration Point (PAP) – the XACML-policy editor.

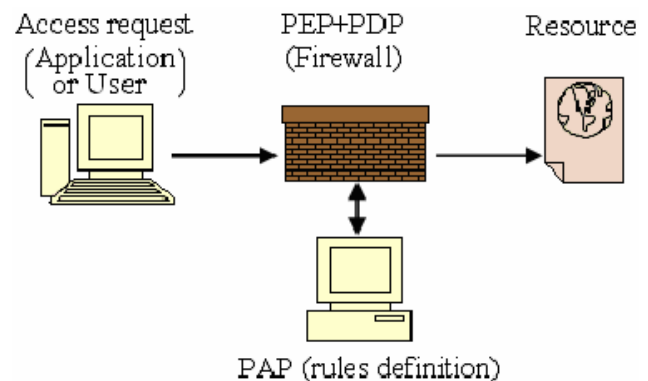


Figure 1. Firewall as a central component of access policy enforcement

In modern computer networks firewall combines PDP and PEP controlling access request and enforcing access decisions in real-time. In this case traffic can be considered as a huge number of data flows from various applications and/or users (Fig. 1). The firewall applies filtering rules for each data flow therefore its performance is strictly depends on the number of rules. To increase firewall performance PAP has to form minimal number of filtering rules that enforce the access policy.

Number of rules can vary depends on environment condition which identifies by means of indicator function. In according to telematics approach this function  $F$  has three values:

- -1, if the data flow is denied according to the access policy (filtering rules);
- 0, if the solution is "suspicious" and it requires additional time for access decision;
- 1, if the data flow is permitted.

When  $F = 0$  proposed novelty consists that the data stream is not discarded completely, its status is marked as "suspicious" and this flow receives some part

of available bandwidth (Fig. 2). Thus this part varies in interval  $0 < \alpha < 1$  and may be considered as randomized parameter of queuing management.

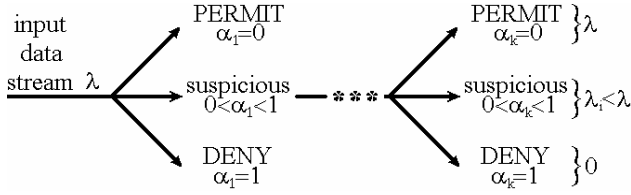


Figure 2. Stage-by-stage (from 1 to k) access decision

In such PDP the traffic throughput and time that packets spend in queue (minimum value - for PERMIT mark and infinity - for DENY) are the functions of randomized parameter  $\alpha$ .

Network environment security condition defines by an access policy requirements enforced using firewall configuration rules. Each of these rules has a set of attributes: identifiers of subject and object and the rights of access from one to another. In TCP/IP network environment access rules have much more attributes that need to identify characteristics of packet flows between users and network res

36ources. This attributes belong to different layers of network interaction model such as: MAC-addresses on link layer, IP-addresses on network layer, port numbers on transport layer and some parameters of application protocols.

The access policy in the modern corporative network usually consists of a huge number of rules for security appliances that forms in PAP. Preparation of access rules is a complex process that carries many errors. Therefore the actual problem is analyze, verification and optimization of access rules set for different types of network environments.

The well-known approach to solve these tasks is based on eXtensible Access Control Markup Language which gives a wide spectrum of methods for design PDP and PEP configurations. But this language has no embedded options to verify rule-combining algorithm or evaluation of individual rules in firewall configuration in the terms of performance attributes. XACML has syntactic and semantic complexity which restricts its usage and complicates application of formal verification methods. Therefore it is necessary to have theoretically well-founded security appliance or firewall configuration approach which allows to realize access policy requirements, and also to optimize number and to verify a correctness of filtering rules.

The paper is organized as follows: In Section II and III algebra of filtering rules and the usage of new approach are presented. The Section IV and V are the theoretical parts of the paper where the mathematical model and basic equations are analyzed and estimated.

## II. ALGEBRA OF FILTERING RULES

In accordance to ideas which have been discussed above we can define algebraic structure over set of

filtering rules namely  $R$ . This algebra consists of following operations over the  $R$  elements:

1. Commutativity of addition:  $\forall a, b \in R \quad a + b = b + a$ .
2. Associativity of addition:  $\forall a, b, c \in R \quad a + (b + c) = (a + b) + c$ .
3. Zero element of addition:  $\forall a \in R \exists 0 \in R: a + 0 = 0 + a = a$ .
4. Inverse element of addition:  $\forall a \in R \exists b \in R: a + b = b + a = 0$ .
5. Associativity of multiplication:  $\forall a, b, c \in R \quad a \times (b \times c) = (a \times b) \times c$ .
6. Distributivity:  $\forall a, b, c \in R \begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}$
7. Identity element:  $\forall a \in R \exists 1 \in R: a \times 1 = 1 \times a = a$ .
8. Commutativity of multiplication:  $\forall a, b \in R \quad a \times b = b \times a$ .

Now let's define the algebra of filtering rules as  $\mathcal{R} = \langle R, \Sigma \rangle$ , where  $R$  – the set of filtering rules,  $\Sigma$  – the set of possible operations over the elements of  $R$ . The set of filtering rules  $R = \{r_j, j = \overline{1, |R|}\}$  – the carrier set of algebra  $\mathcal{R}$ . Every rule  $r_j = \{X_1, \dots, X_N, A_1, \dots, A_M\}_j$  consists of vector  $X_j$  of parameters and vector  $A_j$  of attributes. The example of elements of  $X_j$ :  $X_{j1}$  – the set of clients IP-addresses,  $X_{j2}$  – the set of servers TCP-ports. The rules attributes defines a behavior of access control system that must be applied to corresponding flow of packets (session). For example,  $A_{j1}$  – the mandatory attribute that defines the action of access control system over packets;  $A_{j1}=0$  means that packets must be dropped (access deny),  $A_{j1}=1$  means that packets must be passed to receiver (access allow). The sets of possible values for parameters and attributes vectors specifies as sets  $DX_1, \dots, DX_N$  and  $DA_1, \dots, DA_M$  in accordance with semantics of every parameter and attribute. For carrier set  $R$  is right the following expression (here “ $\times$ ” is symbol of Cartesian product):

$$R \subset DX_1 \times DX_2 \times \dots \times DX_N \times DA_1 \times DA_2 \times \dots \times DA_M$$

The set  $\Sigma = \{\phi_1, \phi_2\}$  defines the operations that possible over filtering rules, where  $\phi_1$  – operation of addition,  $\phi_2$  – operation of multiplication.

The operation of addition for filtering rules defines by following expressions:

$$r_3 = r_1 + r_2 = \{X_{11}, X_{12}, \dots, X_{1N}, A_{11}, A_{12}, \dots, A_{1M}\} + \{X_{21}, X_{22}, \dots, X_{2N}, A_{21}, A_{22}, \dots, A_{2M}\} \\ r_3 = \begin{cases} \{X_{11} \cup X_{21}, \dots, X_{1N} \cup X_{2N}, A_{11} \vee A_{21}, A_{12} \cup \\ \cup A_{22}, \dots, A_{1M} \cup A_{2M}\}, \text{ if } A_{11} = A_{21}; \\ \{X_{11} \Delta X_{21}, \dots, X_{1N} \Delta X_{2N}, A_{11} \wedge \\ \wedge A_{21}, A_{12} \Delta A_{22}, \dots, A_{1M} \Delta A_{2M}\}, \text{ if } A_{11} \neq A_{21}, \end{cases}$$

where  $A_{i1}$  – the attribute “the action of rule”,  $\cup$  – union of sets,  $\Delta$  – symmetrical difference of sets,  $\vee$  and  $\wedge$  – logical disjunction and conjunction respectively. In other words the sum of two filtering rules is

- 1) union of sets of the same name parameters and attributes if the attribute “the action of rule” is equivalent in both rules;
- 2) symmetrical difference of sets of the same name parameters and attributes if the attribute “the action of rule” is different in summand rules.

The operation of multiplication for filtering rules defines by following expressions:

$$r_3 = r_1 \times r_2 = \{X_{11}, X_{12}, \dots, X_{1N}, A_{11}, A_{12}, \dots, A_{1M}\} \times \{X_{21}, X_{22}, \dots, X_{2N}, A_{21}, A_{22}, \dots, A_{2M}\}$$

$$r_3 = \{X_{11} \cap X_{21}, X_{12} \cap X_{22}, \dots, X_{1N} \cap X_{2N}, A_{11} \wedge A_{21}, A_{12} \wedge A_{22}, \dots, A_{1M} \wedge A_{2M}\},$$

where  $\cap$  – intersection of sets. In other words the product of two filtering rules is intersection of sets of the same name parameters and attributes; attribute “the action of rule” for result rule is a conjunction of corresponding attributes of initial rules.

Zero  $0_r$ , identity  $1_r$  and inverse  $-r$  elements of  $R$  are specifies by following expressions:

$$0_r = \{\emptyset, \emptyset, \dots, \emptyset, A_1, \emptyset, \dots, \emptyset\}, A_1 = 0$$

$$1_r = \{DX_1, DX_2, \dots, DX_N, A_1, DA_2, \dots, DA_M\}, A_1 = 1$$

$$-r = \{X_1, X_2, \dots, X_N, \bar{A}_1, A_2, \dots, A_M\},$$

where  $\bar{A}_1$  – logical inversion of  $A_1$

The described algebra is distributive commutative ring with identity element that means execution of corresponding axioms.

### III. FIREWALL CONFIGURATION USING PROPOSED ALGEBRA

Let’s specify the element of set  $R$  as  $r = \{X_1, X_2, A_1\}$  where  $X_1$  – subset of source IP-addresses,  $DX_1 = [0.0.0.0, 255.255.255.255]$ ;  $X_2$  – subset of destination IP-addresses,  $DX_2 = [0.0.0.0, 255.255.255.255]$ ;  $A_1$  – attribute “the action of rule”,  $DA_1 = \{0,1\}$ , 0 denies access, 1 allows access. It is necessary to define the full and consistent access policy that allows establishing of sessions from Internal network (see schema on Fig.3, a) to External subnetworks  $0.0.0.0 - 9.255.255.255$ ,  $20.0.0.0 - 49.255.255.255$  and from External subnetworks  $40.0.0.0 - 49.255.255.255$  to the whole Internal network.

For this task a convenient method of representation of access policy is 2-dimensional space  $x_1x_2$ . Every point of this space specifies by the coordinates  $(x_1, x_2)$ . The set of points  $(x_1, x_2)$  specifies by Cartesian product of sets  $DX_1$  and  $DX_2$  (see on Fig.3, b).

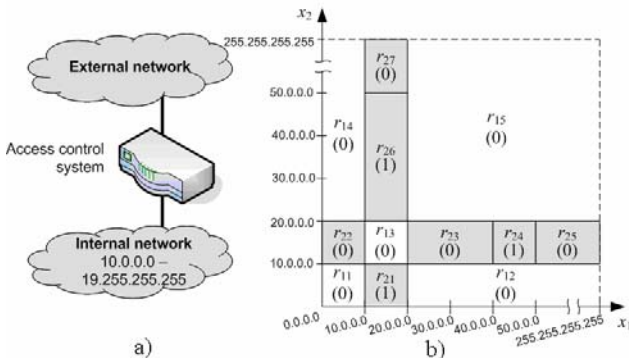


Figure 3. Access control system based on firewall (a) and access policy as a space of firewall parameters (b)

Definition 1. The access policy is full if filtering rules specify the whole of space of parameters:

$$\forall x_1 \in DX_1, x_2 \in DX_2, \dots, x_N \in DX_N (x_1, x_2, \dots, x_N) \in \bigcup_{i=1}^{|R|} (X_{i1}, X_{i2}, \dots, X_{iN})$$

Definition 2. The access policy is consistent if any point of space of parameters belongs only to own filtering rule:

$$\bigcap_{i=1}^{|R|} (X_{i1}, X_{i2}, \dots, X_{iN}) = \emptyset$$

Obviously that for schema on Fig. 3 there are some forbidden areas as incorrect from the point of view of IP-network functionality. The following rules describes such areas (on Fig. 9,b this areas has white color):

$$r_{11} = \{0.0.0.0 - 9.255.255.255; 0.0.0.0 - 9.255.255.255; 0\};$$

$$r_{12} = \{20.0.0.0 - 255.255.255.255; 0.0.0.0 - 9.255.255.255; 0\};$$

$$r_{13} = \{10.0.0.0 - 19.255.255.255; 10.0.0.0 - 19.255.255.255; 0\};$$

$$r_{14} = \{0.0.0.0 - 9.255.255.255; 20.0.0.0 - 255.255.255.255; 0\};$$

$$r_{15} = \{20.0.0.0 - 255.255.255.255; 20.0.0.0 - 255.255.255.255; 0\}.$$

Let’s optimize this set of rules by applying of algebra’s addition operation for rules  $r_{11}$  and  $r_{14}$ ,  $r_{12}$  and  $r_{15}$ :

$$r_{17} = r_{11} + r_{14} = \{0.0.0.0 - 9.255.255.255; 0.0.0.0 - 9.255.255.255, 20.0.0.0 - 255.255.255.255; 0\};$$

$$r_{18} = r_{12} + r_{15} = \{20.0.0.0 - 255.255.255.255; 0.0.0.0 - 9.255.255.255, 20.0.0.0 - 255.255.255.255; 0\}.$$

For other areas (it has gray color on Fig. 3,b) it is necessary to specify the filtering rules in accordance of task conditions:

$$r_{21} = \{10.0.0.0 - 19.255.255.255; 0.0.0.0 - 9.255.255.255; 1\};$$

$$r_{22} = \{0.0.0.0 - 9.255.255.255; 10.0.0.0 - 19.255.255.255; 0\};$$

$$r_{23} = \{20.0.0.0 - 39.255.255.255; 10.0.0.0 - 19.255.255.255; 0\};$$

$$r_{24} = \{40.0.0.0 - 49.255.255.255; 10.0.0.0 - 19.255.255.255; 1\};$$

$$r_{25} = \{50.0.0.0 - 255.255.255.255; 10.0.0.0 - 19.255.255.255; 0\};$$

$$r_{26} = \{10.0.0.0 - 19.255.255.255; 20.0.0.0 - 49.255.255.255; 1\};$$

$$r_{27} = \{10.0.0.0 - 19.255.255.255; 50.0.0.0 - 255.255.255.255; 0\}.$$

These rules may be optimized also by applying of algebra’s addition operation:

$$r_{28} = r_{21} + r_{26} = \{10.0.0.0 - 19.255.255.255; 0.0.0.0 - 9.255.255.255, 20.0.0.0 - 49.255.255.255; 1\};$$

$$r_{29} = r_{22} + r_{23} = \{0.0.0.0 - 9.255.255.255, 20.0.0.0 - 39.255.255.255; 10.0.0.0 - 19.255.255.255; 0\}.$$

As a result the access policy describes by following filtering rule set:

$$R = \{r_{13}, r_{17}, r_{18}, r_{24}, r_{25}, r_{27}, r_{28}, r_{29}\}.$$

Dimension of  $R$  is the main attribute that describes firewall performance characteristics. Usage of the algebraic operations of addition and multiplication allows to reduce dimension  $R$  and by this way to increase firewall performance while saving requirements of the specific security policy. However the correctness of each rule depends on an environment condition which can vary in real time. Therefore static description of access policy by means of proposed algebra is not enough and according to the telematics approach it is necessary to consider an environment condition with statistical parameters. Development of randomized model of the network environment considering these requirements, allows to

raise accuracy of the description of an access policy by means of filtering rules.

#### IV. MODEL OF NETWORK ENVIRONMENT

Here 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.

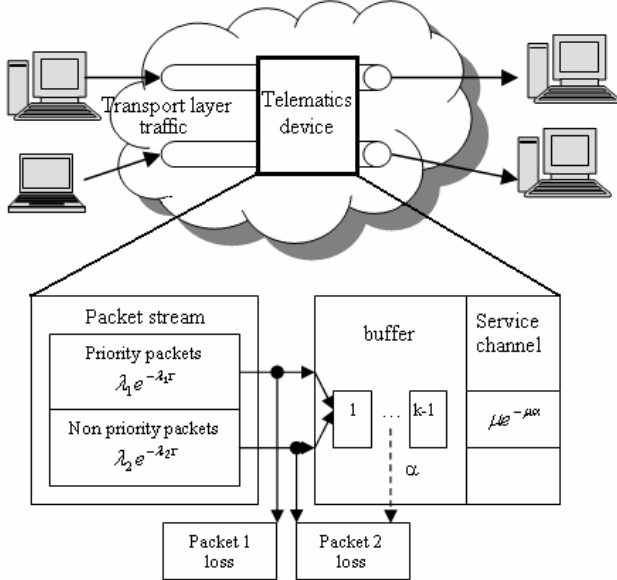


Figure 4. Priority queueing schema  $\bar{M}_2 / M / 1 / k / f_2^1$  of telematics network device.

The scheme described priority queueing is resulted on Fig. 4. 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. 4 will be the elementary with intensity  $\lambda = \lambda_1 + \lambda_2$ . The priority queueing represented on Fig. 4, is  $\bar{M}_2 / M / 1 / k / f_2^1$  type by Kendall's notation.

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 [2] where the randomized push-out mechanism have been studied (in a combination with the relative priority for queueing  $\bar{M}_2 / M / 1 / k / f_1^1$  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 generalisations are widely used at the theoretical analysis of Internet systems.

As shown in [2], 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  $\bar{M}_2 / M / 1 / k / f_2^1$  is presented on Fig. 5.

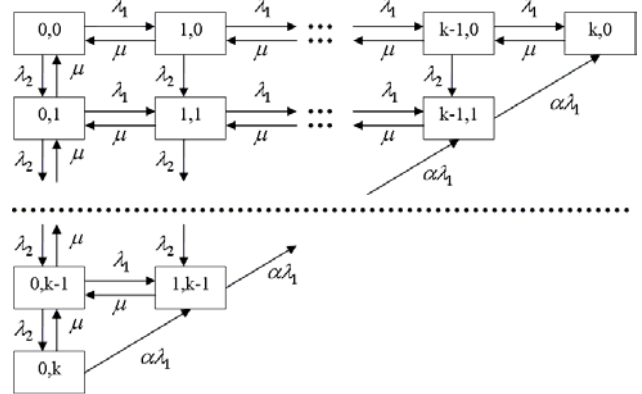


Figure 5. The state graph of  $\bar{M}_2 / M / 1 / k / f_2^1$  type system.

Making by usual Kolmogorov's rules [3] set of equations with the help of state graph we will receive:

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

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 [2] in its classical variant offered by

H.White, L.S.Christie and F.F.Stephan with reference to  $\bar{M}_2 / M / 1 / f_2$  type systems [4,5].

Solving (1) system we receive some auxiliary variables

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

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

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

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 6,7)

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

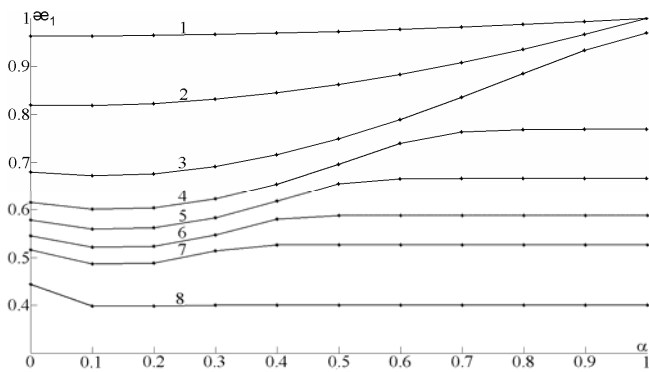


Figure 6. Relative throughput of priority packets for strongly loaded transport virtual channel with  $\rho_2 = 1,5$  and different values  $\rho_1$ :

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.

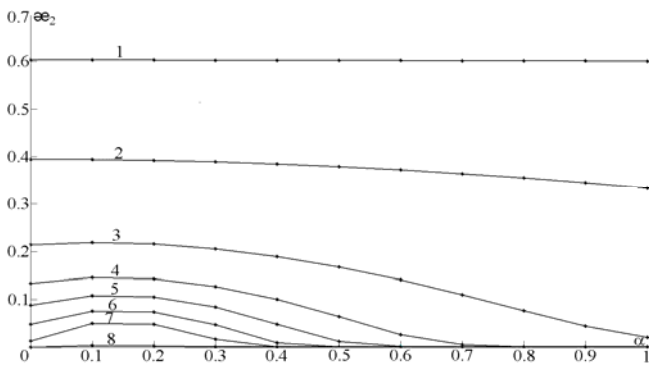


Figure 7. Relative throughput of non-priority packets

From Fig. 6 and 7 we can see, that choosing parameter  $\alpha$ , we can influence on  $\alpha_i$  in very wide limits.

For some values  $\rho_1$  the range of changes of  $\alpha_i$  will be 0.6-1 at  $\lambda_1 + \lambda_2 \gg \mu$ . On schedules the extremum is obviously visible at values  $\alpha = 0,1-0,2$ , it means that increasing probability of replacement of not priority packets, we thus reduce probability of their loss in the strongly loaded networks. It is possible to explain it by that in the absence of replacement mechanism ( $\alpha = 0$ ) and at  $\alpha > 0$  various mechanisms work. There are an absolute throughput of i-packet type  $\lambda_i (1 - P_{loss}^{(i)})$ .

The relative time that the priority packet spend in queueing by Little's Formula (Fig 8,9).

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

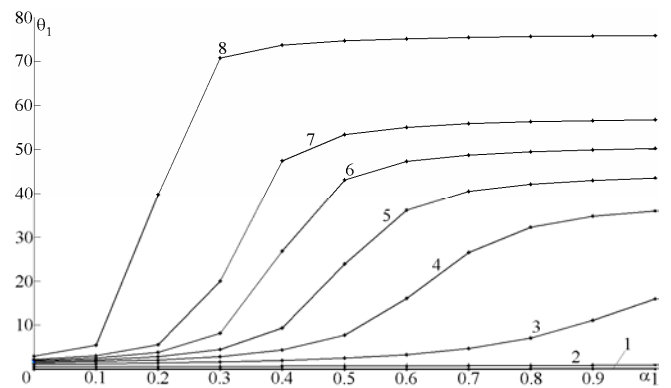


Figure 8. The time that priority packet spend in queueing

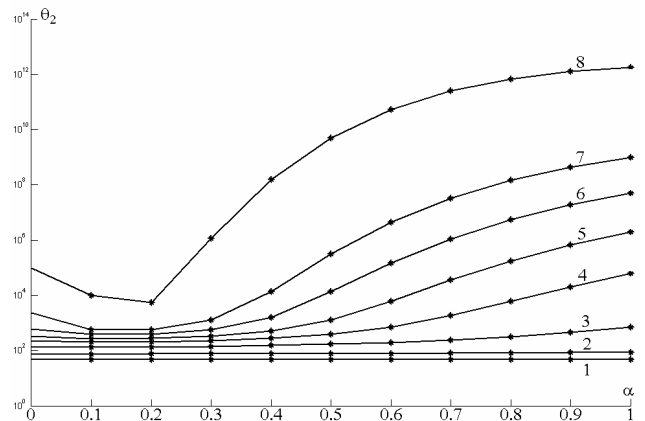


Figure 9. The time that non-priority packet spend in queueing

Fig 8,9 show that proposed queueing mechanism provide a wide range of control feature by randomized push-out parameter  $\alpha$  and buffer size  $k$ . In accordance to packet mark (PERMIT, DENY, suspicious) period that packet is in queue vary from 1 to  $10^{14}$  times which can be used to control access to information resource.

It is important to notice, that dependence received  $\alpha_i$  numerical by, it is very close to linear for both types of packets. In practice of engineering calculations at the weak priority traffic linear approximation is comprehensible  $\rho_1/\rho_2$ .

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

By choosing  $\alpha$  we can change the time that packets spend in the firewall buffer that allows to limit access possibilities of suspicious packets and to block packets with mark DENY. So by decreasing the priority of suspicious connections and increasing the push-out probability  $\alpha$  we can reduce the connection 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 [6] has been made to detect conditions in which  $\rho_1$  varied over a wide range from 0,1 to 2,5, and  $\rho_2 = 1,5$ .

Of course, two types of priority are not enough for apply corporate access policy in multiservice network environment, but step-by-step scheme depicted on Fig. 2 can be used to increase accuracy of traffic control based on consecutive application of developed algebra operations.

## VI. CONCLUSION.

1. The offered access control approach allows more deeply and more detailed understanding of requirements of Policy Decision and Policy Enforcement points which defines security appliances configuration rules.

2. Proposed algebra or formal mathematical description of security policy conditions for distributed network systems is the powerful analytical tool to create, verify and optimize the set of firewall configuration rules.

3. Number of firewall configuration rules vary depends on environment condition which identifies by means of indicator function  $F$  with three states, one of which is used to choose traffic flow priority parameter  $\alpha$ .

4. Proposed queueing mechanism provide a wide range control feature by randomized push-out parameter  $\alpha$  which can be used to manage access to information resources based on consecutive application of developed algebra operations.

5. Selecting priority parameter which corresponds to push-out probability of a packet from the buffer, we can change time that packets spend in the buffer of firewall which allows to control access possibility of suspicious packets and to block packets with mark DENY. In this case by decreasing the priority of suspicious connections and increasing  $\alpha$  we can reduce the connection throughput without interrupting it.

## REFERENCES

- [1] eXtensible Access Control Markup Language (XACML) Committee Specification. OASIS Open, 2003. <http://www.oasis-open.org/committees/xacml/>
- [2] Avrachenkov K.E., Vilchevsky N.O., 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
- [3] L. Kleinrock. Queueing Systems Volume I-II, 1976.
- [4] White H., Christie L.S. Queueing with preemptive priorities or with breakdown // Operations research, 1958, vol. 6, no. 1, p. 79-95.
- [5] Stephan F.F. Two queues under preemptive priority with Poisson arrival and service rates // Operations research, 1958, vol. 6, no.3, p. 399-418.
- [6] Zaborovsky V., Zayats O., Muljukha V. Priority Queueing with Finite Buffer Size and Randomized Push-out Mechanism // Proceedings of the Ninth International Conference on Networks ICN 2010 Mennieres, France 2010 p.316-321.