Traffic Management and Access Control in Space Experiment "Kontur-2"

Vladimir Muliukha, Vladimir Zaborovsky, Alexander Ilyashenko, Alexander Silinenko
Peter the Great St.Petersburg Polytechnic University,
Russian State Scientific Center for Robotics and Technical Cybernetics
Saint-Petersburg, Russia
e-mail: vladimir@mail.neva.ru, vlad@neva.ru, ilyashenko.alex@gmail.com, avs@rtc.ru

***Abstract*—Space experiment "Kontur-2" aboard the International Space Station (ISS) is focused on the transfer of information between station and on-ground robot. Station's resources are limited, including communication ones. That is why for the space experiment "Kontur-2" it was decided to use the methods of priority traffic management. New access control mechanisms based on these methods are researched. The usage of the priority traffic processing methods allows using more efficiently the bandwidth of receiving and transmitting equipment onboard the ISS through the application of randomized push-out mechanism. The paper considers methods of dynamic traffic management and access control that are used during international space experiment "Kontur-2" performed aboard the ISS.**

Keywords-space experiment; access control; traffic management; virtual connection

I. INTRODUCTION

Access control to the network resources is an important task of the information security. Especially it is necessary for the advanced modern space applications, for example during space experiments onboard the International Space Station (ISS). Such digital resources have to be available for authorized usage by cosmonauts and the mission control center, and protected against unauthorized access. In the modern computer networks, including ISS onboard network and satellite communicational channels TCP/IP stack is used. That is why the informational interaction between nodes is occurred using application protocols over virtual transport connections.

As the result, the problem of traffic management and access control can be presented as the task of identifying the characteristics of virtual connections and traffic control using virtual connection content code. This code is calculated according to the connection content and it shows the requested quality of service (QoS). The complexity of this problem is the fact that the content code can be calculated exactly only after the virtual connection is finished. However, in this case, the access control problem cannot be solved, because the access becomes irreversible.

The paper considers methods of dynamic priority traffic management and access control methods that have been used in international space experiments performed aboard the ISS. The proposed methods are probabilistic, but they could improve the effectiveness of information traffic management by various control throughput mechanisms of such virtual connections.

To solve the problem of calculating the dynamic content code we consider to use the indicator function, whose properties depend on: the information model of the network resource and the description of the access policy, which defines the rights of users and QoS requested by virtual connection (VC).

In this paper, we propose a new approach to access control flexibility enhancement based on active queuing management mechanism and randomized preemptive procedure. In "Kontur-2" space experiment, the offered solution was implemented by the access gateway – specialized device, based on hardware firewall that realizes several functions:

1) organization of informational interaction between robotic devices;
2) communication with operator;
3) traffic management;
4) enforce security policy.

The access gateway is a two-component device. The first part is the firewall, and the second one is the security server, which generates access rules and enforces the access policy. The adaptability of the proposed mechanism improves network security, but it requires large computational resources of the access gateway. That is why the security server was realized using cloud technologies. Security server analyzes network traffic and generates access rules for firewall considering current state of connections, available resources of internal network, and access policy.

The parameters of access gateway (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 access code F and firewall has three modes in accordance to possible F (A) values (Figure 1):

- "–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. 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 VCs that have low throughput and demand low stable delivery time;
- "0" for background ones that demand high throughput and have no delivery time requirements.

 ISBN: 978-1-61208-427-5

For more accurate data sorting we propose to use multiple priority levels. In our space experiment, we consider the simplest situation with two priority levels (control commands and video data). But it may be not enough for some practice tasks so we propose some easy ways to increase the number of levels using subsets of permitted VCs (see Figure 1).

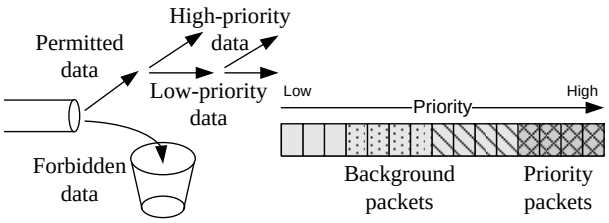

Figure 1. Multiple priority level in congested operation networks

To provide this classification procedure we have proposed active queuing management mechanism, which based on randomized preemptive control [1][2]. 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.

In this paper, we propose to use the Access Gateway with the architecture described in [1]. This architecture includes several modules: Network Monitor, Access Policy Description Module, Information Resource Module, Firewall Rules Generator and Firewall that implements the rules and manages the traffic flows.

The paper is organized as follows: Section II describes the priority queueing model and basic equations. Section III is about practical application of proposed method in space experiment "Kontur-2". Section IV concludes the paper.

II. 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.

The summarized entering stream will be the elementary with intensity $\lambda=\lambda_1+\lambda_2$. Using the Kendel notation modified by Basharin, proposed system has $\vec{M}_2/M/1/k/f_2^1$ type [3].

Problems of research priority queueing have arisen in telecommunication with the analysis of real disciplines of scheduling in operating computers. During the 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 [3], 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 [4]. The other 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.

The state graph of system $\vec{M}_2/M/1/k/f_2^1$ is presented in Figure 2.

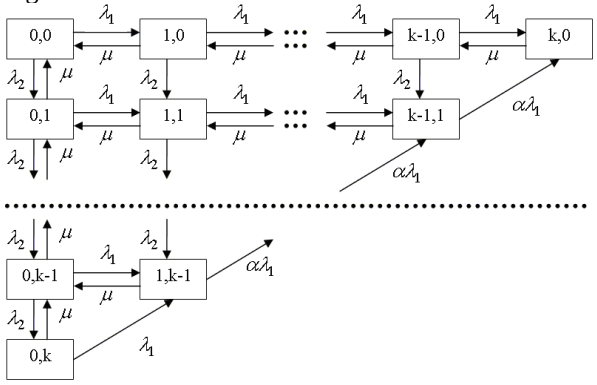

Figure 2. The state graph of $\vec{M}_2/M/1/k/f_2^1$ type system

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

$$\begin{aligned}&-[\lambda_1(1-\delta_{j,k-i})+\alpha\lambda_1(1-\delta_{i,k})\delta_{j,k-i}+(1-\alpha)\lambda_1\delta_{i,0}\delta_{j,k-i}+\\&+\lambda_2(1-\delta_{j,k-i})+\mu(1-\delta_{i,0}\delta_{j,0})]P_{i,j}+\mu P_{i+1,j}+\mu\delta_{i,0}P_{i,j+1}+\\&+\lambda_2P_{i,j-1}+\lambda_1P_{i-1,j}+\alpha\lambda_1\delta_{j,k-i}P_{i-1,j+1}+\\&+(1-\alpha)\lambda_1\delta_{j,k-i}\delta_{i,1}P_{i-1,j+1}=0,(0\le i\le k;0\le j\le k-i),\end{aligned}\quad(1)$$

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

There is a normalization condition for the system:

$$\sum_{i=0}^{k}\sum_{j=0}^{k-i}P_{ij}=1\cdot$$

At real k (big enough) this system is ill-conditioned, and its numerical solution leads to the big computing errors. We used the method of generating functions [2][3]. 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 [1]-[3], solving (1) system we receive loss probability for priority ($P_{loss}^{(1)}$) and non-priority ($P_{loss}^{(2)}$) packets:

$$P_{loss}^{(1)}=q_k+(1-\alpha)\sum_{i=1}^{k-1}p_i, \quad (2)$$

$$P_{loss}^{(2)}=r_k+\alpha\frac{\rho_1}{\rho_2}\sum_{i=1}^{k-1}p_i+\frac{\rho_1}{\rho_2}p_k \quad (3)$$

Exploring these formulas we found some useful properties of this system described in this article. 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.

In Figure 3 an expected result can be seen that the probability of losing priority packet decreases with increasing size of a buffer. Probability of loss is not decreasing 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 6 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.

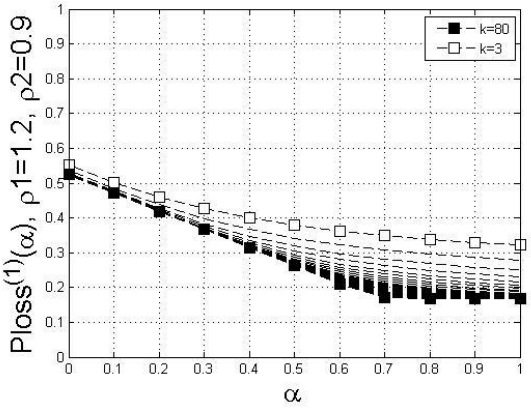

Figure 3. Loss probability of priority packets with buffer size K=3-80

Graphs of the relative throughput which is computed by formulas (4) are very important for research of processes in computer networks.

$$æ_i=1-P_{loss}^{(i)},\ (i=\overline{1,2}). \quad (4)$$

From formulas (2) and (3) 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 $\lambda_1+\lambda_2 >> \mu$.

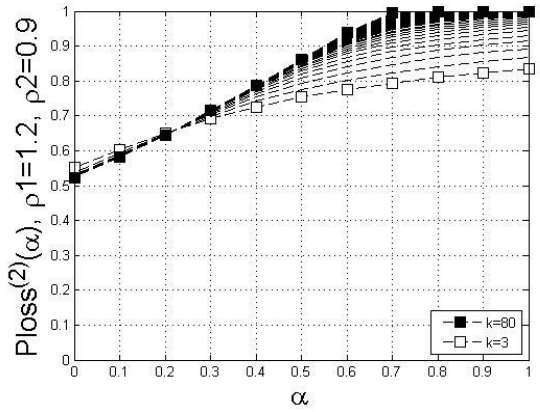

Figure 4. Loss probability of non-priority packets with buffer size K=3-80

In [2] and [3], we have calculated different variable like average queue length of priority packets and the relative time that the priority packet spend in queueing system. So the α parameter is strong enough to influence the filling of the queue.

In [3] it is shown 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 enforce requested QoS for traffic. 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 enforcing 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. 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.

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 [3] 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 .

III. PRACTICAL APPLICATION AND FUTURE DEVELOPMENT

Good example of practical application of such mechanism is the problem of controlling remote robotic object, which telemetry data and a video stream are transmitted on global networks [5]. 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.

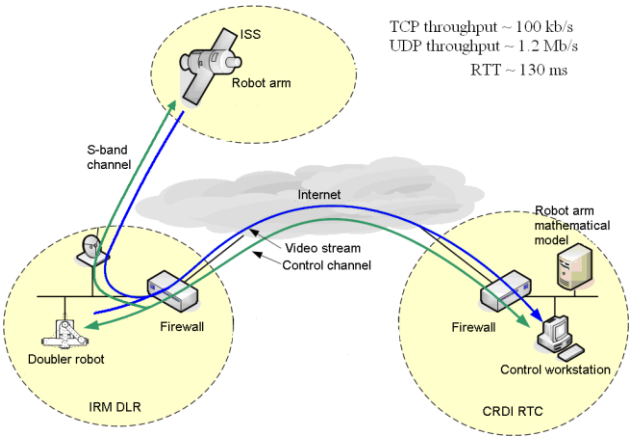

Figure 5. The scheme of space experiment "Kontur"

In a considered example from Figure 5 (ROKVISS (Robotic Component Verification on the ISS) mission and space experiment "Kontur" [6][7]), 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.

The same traffic management system is used in space experiment "Kontur-2", where the operator is onboard ISS and robotic system is on Earth surface in Saint-Petersburg, Russia and in Munich, Germany (see Figure 6).

During the space experiments "ROKVISS" and "Kontur" that were minutely considered [1][6]-[8], it was established that an important component of effective remote control for robotic object is a high degree of "dipping" of the operator in the robot's functioning environment [8]. Thus a telepresence for operator in such an environment is ensured by outputting a video stream coming from the camera of the robot into a workplace of operator-cosmonaut. Simultaneously the tactile capabilities of the robot are reproduced by the special joystick, which is connected with the operator through man-machine interfaces with the force-torque feedback. That is why the development of the space experiment "Kontur" was considered a study on the effect of weightlessness on the opportunity of operator-cosmonaut to control remote robots using force-torque joystick. The necessity to send the equipment, which will interact with the cosmonauts onboard ISS gives us new requirements for reliability and security for all systems' components, including communication channels.

An actual scientific and technical problem of the new space experiment "Kontur-2" is the creation of methods and development of the technology for remote control onsurface robots and robotics groups from orbiting spacecraft for solving planetary exploration.

The ability to effectively control robots on the surface of planets from a manned orbital spacecraft is determined by the following factors:

- reliability of telecommunication channels used for transmitting control commands, telemetry and video data between an operator and robot, their capacity for reconfiguration and scalability;
- performance of communication channels in order to minimize the delay of transmitted data;
- adequate response of the operator in weightlessness to the impact from the joystick with force-torque feedback, taking into account the time delays and discontinuity of video feedback received from the controlled robotic object.

The study of these factors significantly differs this work from the previous ones [7][9].

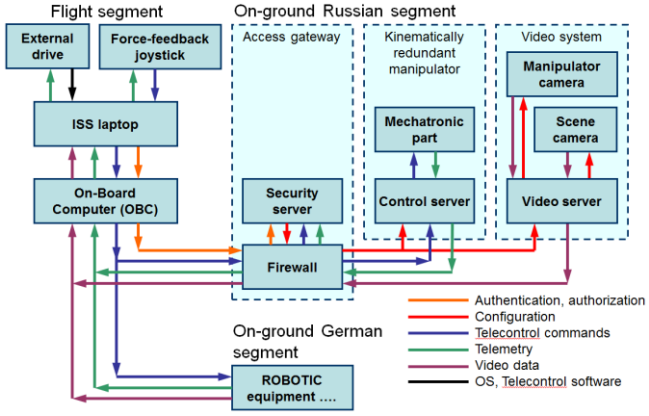

Figure 6. Functional scheme of space experiment "Kontur-2"

In future this method of preemptive access management could be used in new joint space experiment "Kontur-3" (New international space experiment) 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 robotic communication network [5]. 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

 ISBN: 978-1-61208-427-5

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. The structure of data transmission of future experiment is presented in Figure 7.

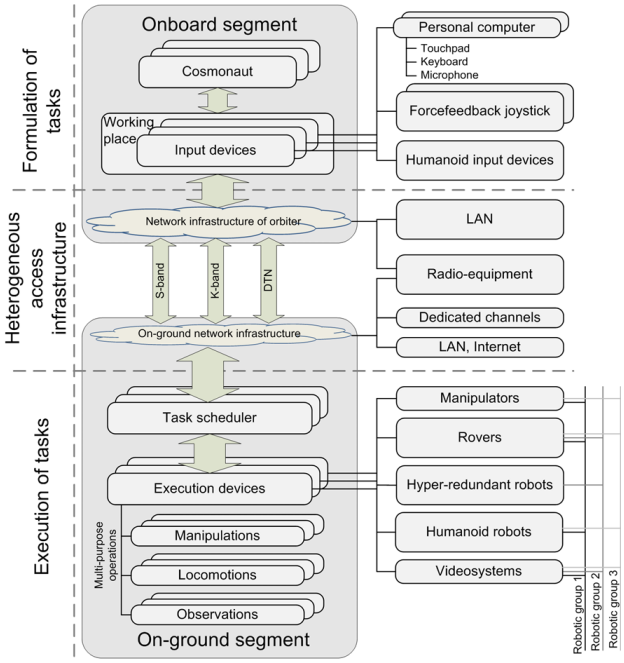

Figure 7. Data streams in future space experiment "Kontur-3"

For communication experiments, the primary focus will be on the usage of real-time duplex commanding, in combination with Delay Tolerant Network (DTN) approaches. 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.

To enforce access policy and provide information security we had to consider the use of various communication channels in future experiments. That is why the access gateway has two levels of filtering: static and dynamic. Static level allows us to control unchanging policy requirements (such as the use of white lists IP addresses and user authentication process). Dynamic control checks suspicious actions of the permitted users, as well as controls transmitted data, taking into account the used transmission channels and the QoS requirements. Some components of the system have been worked out by us in the framework of a contract with Ford Motor Company [8][10]-[12].

The basis of every robotic operation network is high-performance cloud, which is used to decompose the complex task from operator and to monitor its implementation by each robot. So robotics objects within multipurpose operation network would execute the programs and interact without human involvement. However there would be always situations when the robot could not make a decision by its own. In that case the human-operator will have two main opportunities:

1) remote telecontrol through real-time channel;
2) to send new program through DTN.

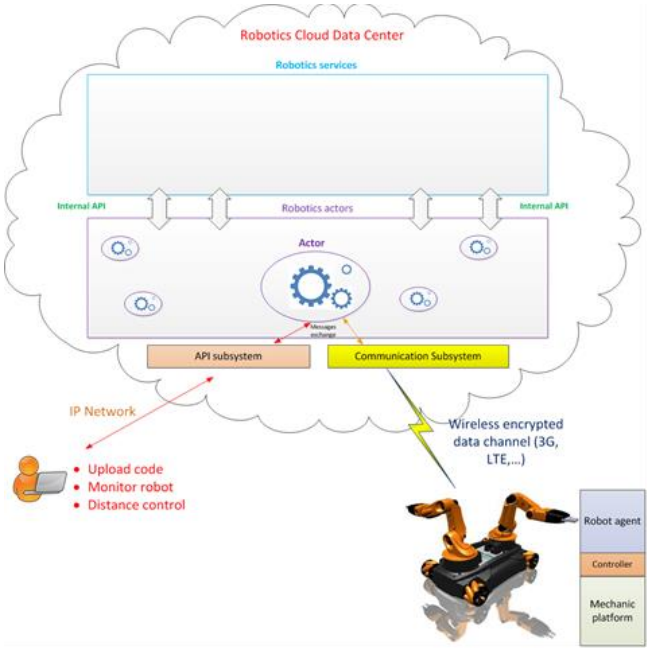

Figure 8. Robotic cloud platform with heterogeneous computing resources

Heterogeneous cloud platform provides not only remote access for computing resources or applications, but also intelligent services. Using the resources of modern cloud-based engineering centers it is possible to create equivalent social networks that bring together multiple agents to perform coordinated actions, computation, verification of test results based on the use of different materials, virtual prototyping, and data visualization. These problems, from the point of view of the computational algorithms, can be combined into chains, which form a network of operations. Their implementation is provided within a heterogeneous cloud. The components of the platform (see Figure 8), based on the OpenStack, include: IaaS cloud class segment, computing infrastructure within the cluster, the specialized high-performance hybrid system based on reconfigurable computing nodes.

Virtualization has changed the approach of deploying, managing, and using enterprise resources by providing new opportunities for consolidation and scalability of computational resources available to applications; however, this leads to the emergence of new threats posed by the complexity and dynamic nature of the process of resources provisioning. These threats can lead to the formation of cascade security violations, which traditional data protection systems are unable to deal with. The existing approaches such as “Scan and Patch” do not work in a cloud environment — network scanners cannot track changes of

 ISBN: 978-1-61208-427-5

resources configuration in real time. These approaches do not accurately identify the change in level of risk and take steps to block dynamically emerging threats.

To solve the problem of controlling access in the cloud, it is necessary to continuously monitor resources, and it cannot be achieved without the automatic generation of rules for filtering and firewall log files analysis. Information security management products in a dynamic cloud environment should include mechanisms that provide: total control over processes for deploying virtual machines; proactive scanning the virtual machines for the presence of vulnerabilities and configuration errors; tracking the migration of virtual machines and system configuration to control access to resources. Therefore, within the space experiment "Kontur-2" series of measures are set out to improve information security resources, namely:

- Enhanced Control of virtual machines. Virtual machines as active components of the service are activated in the cloud application random moments, and Administrator cannot activate or deactivate a virtual machine until the security scanner checks the configuration and evaluates the security risks.
- Automatic detection and scanning. Information security services are based on discovery of vulnerabilities in the computing environment. This discovery in turn is based on the current virtual machine configurations and on reports of potential threats that come from trusted sources, such as antivirus update servers.
- Migration of virtual machines. Proactive application migration is an effective method to control security. Each of these data will have its own priority level. The number of priorities could be increased by using the recursive application of prioritization method described above.

IV. CONCLUSION

The paper illustrates one of the possible applications of access control and traffic management approach in the tasks of robotic remote control in space experiment “Kontur-2”.

Proposed model 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 ones or background connections.

In this paper, we considered in detail the preemptive queueing mechanism, which provides a wide range packet loss probability ratio using flexible randomized push-out algorithm. The most interesting result obtained in congested network allows keeping priority VC throughput near the requested value, which is important for specific space experiment onboard ISS.

Described a practical application example of proposed model in joint space experiment “Kontur-2” onboard ISS where several types of operations are serviced by access gateway in robotic communication network.

Proposed an architecture of access gateway for robotic cloud platform with heterogeneous computing resources that expected to be used in future space experiments onboard ISS.

ACKNOWLEDGMENT

The reported study was partially supported by RFBR, research project No. 15-29-07131 ofi_m.

REFERENCES

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

[2] A. Ilyashenko, O. Zayats, V. Muliukha, and L. Laboshin, "Further Investigations of the Priority Queuing System with Preemptive Priority and Randomized Push-Out Mechanism" // Internet of Things, Smart Spaces, and Next Generation Networks and Systems, Lecture Notes in Computer Science, vol. 8638, pp.433-443.

[3] V. Muliukha, A. Ilyashenko, O. Zayats, and V. Zaborovsky, "Preemptive queueing system with randomized push-out mechanism", Communications in Nonlinear Science and Numerical Simulation, Volume 21, Issues 1–3, April 2015, pp.147-158.

[4] V. Zaborovsky, A. Gorodetsky, and V. Muljukha, "Internet Performance: TCP in Stochastic Network Environment" // Evolving Internet, 2009. INTERNET '09. First International Conference on, pp.21–26.

[5] V. Zaborovsky, O. Zayats, V. Muljukha, and A. Ilyashenko, "Cyber-Physical Approach to the Network-Centric Robot Control Problems" // Internet of Things, Smart Spaces, and Next Generation Networks and Systems, Lecture Notes in Computer Science, vol. 8638, pp.619–629.

[6] http://www.nasa.gov/mission_pages/station/research/experiments/15.html [retrieved: July, 2015].

[7] V. Zaborovsky and V. Mulukha, “Access Control in a Form of Active Queuing Management in Congested Network Environment” // Proceedings of The Tenth International Conference on Networks (ICN 2011), St. Maarten, The Netherlands Antilles, January 23-28, 2011 – Published by XPS. – 2011. – pp.12-17.

[8] V. Muliukha, V. Zaborovsky, and S. Popov, “Security of Vehicular Networks: Static and Dynamic Control of Cyber-Physical Objects” // SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies, pp.56-61.

[9] A. Albu-Schaffer, W. Bertleff, B. Rebele, B. Schafer, K. Landzettel, and G. Hirzinger, “ROKVISS - robotics component verification on ISS current experimental results on parameter identification” // IEEE International Conference Robotics and Automation. – 2006. – pp. 3879-3885

[10] L. Kurochkin, S. Popov, M. Kurochkin, V. Glazunov, “Instrumental environment of multi-protocol cloud-oriented vehicular mesh network” // ICINCO 2013 - Proceedings of the 10th International Conference on Informatics in Control, Automation and Robotics, pp. 568-574.

[11] V. S. Zaborovskiy, A. A. Lukashin, A. V. Vostrov, S. G. Popov “Adage mobile services for ITS infrastructure” // 13th International Conference on ITS Telecommunications, ITST 2013, pp. 127-132.

[12] L. Kurochkin, S. Popov, M. Kurochkin, V. Glazunov, “Hardware and software equipment for modeling of telematics components in intelligent transportation systems” // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2014, pp. 598-608.

 ISBN: 978-1-61208-427-5