Security of Vehicular Networks: Static and Dynamic Control of Cyber-Physical Objects

Vladimir Muliukha, Vladimir Zaborovsky, Sergey Popov

Telematics department St.Petersburg Polytechnic University
Saint-Petersburg, Russia
Email: vladimir@mail.neva.ru, vlad@neva.ru, popovserge@spbstu.ru

***Abstract*—The modern vehicle has long ceased to be a pure mechanical device. Each year data-processing component of the car is becoming more important. Considering the vehicle as the dynamic cyber-physical object in non-deterministic environment, we propose to use the methods of cloud services information security to solve the problem of access control to the cars telematics network. We propose to use a real-time control for each of these aspects, which is a complex technical challenge with static and dynamic interactions. The paper proposes a solution for implementing access control for vehicular networks. It is done by firewalls using dynamic access approach, based on virtual connections management, and algebra of filtering rules with mechanism of traffic filtering in "stealth" mode. The proposed security monitor architecture allows to enforce dynamic access policy depending on static set of firewall filtering rules and current condition of virtual connections and network environment.**

Keywords–Security; Vehicular network; Cyber-physics objects; Dynamic access control; Virtual connections.

I. INTRODUCTION

Information systems are deeper entering our lives, integrating with various purely physical systems. For example, a modern car is no longer a mechanical device. After enabling cyber component to all internal circuits and vehicular communications, it can be assigned to the new class – Cyberphysical objects. And each year this "cyber" component of the car is becoming more and more important.

In order to simplify the driving, more and more systems in the car become automated. Lots of the remaining mechanical systems in a modern car are controlled by computer via the Controller Area Network (CAN), but not directly by the driver. According to the researches, modern vehicles comprise up to 60-70 Electrical Control Units (ECUs). The ECUs serve a multitude of purposes like monitoring and controlling the different subsystems of a car [1][2].

Many of ECUs are connected together by the controller area network bus. Now, CAN is the most frequently used protocol in automotive networks, other protocols, designed to fit specific uses may also be used, such as Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST) or FlexRay [1]. Such bus and ECUs form telematics network and serve as information and communication system of the modern vehicle. In modern vehicles, most of important functions are realized by telematics network. It measures vehicle's speed and revolutions per minute or informs the driver and other systems when an accident is about to occur and so on.

The world's largest automobile manufacturers are developing further, integrating in modern vehicles, more and more software and hardware to provide the owner and the driver of the car a maximum number of different digital services, including the remote ones.

According to the joint project of the Ford Motors Company and Saint-Petersburg State Polytechnical University, we suggest that in the near future, all new cars should be integrated into a single information service network and should be able to communicate with other cars and external sources, via USB, Bluetooth, WiFi, 3Gm and Long-Term Evolution (LTE) networks.

Digital revolution allows vehicles to significantly extend their functionality. Security means have to evolve together with cars. From 1960s to 2010s, vehicular security devices developed from mechanical through electromechanical and electronical to software based systems [3]. In the next few years, the car will be part of a single information and service space – cyber-physical object operating in the information space, which will result in a new class of security threats.

For several years, experts concerned with vehicular information security by hacking CAN network and replacing data from controllers. But, while maintaining speed and trends for Automotive Research in the near future, the hacking would be done remotely. This can lead to very bad consequences from data theft to a carjacking or damage the vehicle itself.

Thus, the issue of cars information security as the new class of cyber-physical systems that combine mechanical and electronic components is one of the most important issues of the vehicular networks.

The article describes cars as the new class of systems that combine the mechanical part and logical information, so-called cyber-physical objects. The security of information services for networks of cyber-physical objects is based on the access control technology.

The paper is organized as follows: In Section II, we consider the vehicle as the cyber-physical object. In Section III, we discuss security aspects of mobile cyber-physical networks using cloud computing security approaches. Section IV contains main aspects of the dynamic access control enforcement in computer networks. And in Section V, we suggest an architecture of a secure cloud computing environment. Section VI concludes the paper.

 ISBN: 978-1-61208-376-6

II. VEHICLES AS THE CYBER-PHYSICAL OBJECTS

In the near future, new generation of vehicles will be created. Such cars would be able to receive, store, and transmit information about their surrounding environment, which will be used during their operations. Information will be transmitted between such objects, between car and information center and also between the vehicle and the driver.

In our work, for the formalization of vehicular networks we use Cyber-Physical (CPh) approach, which extends the range of engineering and physical methods for a design of complex technical objects by researching the informational aspects of communication and interaction between objects and with an external environment.

The selection of CPh systems as a special class of designed objects is due to the necessity of integrating various components responsible for Computing, Communications, and Control (3C) processes. Although in modern science there are different approaches to the use of information aspects of the physical objects, but only within cybernetics, such approaches have had structural engineering applications. The conceptual distinction between closed and open systems in terms of information and computational aspects requires the use of new models, which take into account the characteristics of information processes that are generated during the driving of the vehicle and are available for monitoring, processing, and transmission via computer network.

According to Figure 1, a CPh model of a vehicular control system can be represented as a set of components, including following units: information about the characteristics of the environment (Observation), analysis of the parameters of the current state for the controlled object via CAN or telematics network (Orientation), decision-making according to the formal purpose of functioning (Decision), organization and implementation of the actions that are required to achieve the goal (Action). The interaction of these blocks using information exchange channels allows us to consider this network structure as a universal platform. Such platform allows us to use various approaches, including new algorithms and feedback mechanisms for the goals restrictions entropy reduction or the reduction of the internal processes dissipation.

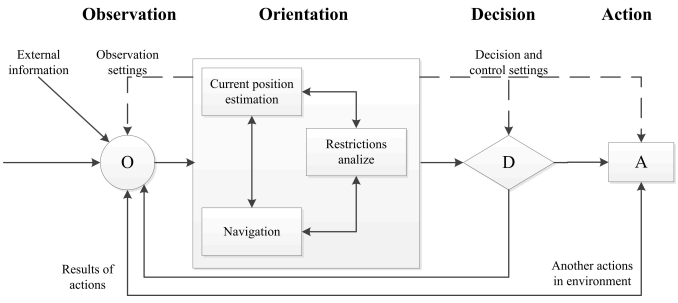

Figure 1. Cyber-physical model of vehicular control system.

Centric solutions allow using universal means for the organization of information exchange to integrate different technologies for the both observed and observable components of the control system. The main differences between these observed and observable components are the property ”part whole” (for observed components) and the ratio ”system environment” (for the observable ones). The parameters and the structure of such control system can quickly be adjusted according to the current information about the internal state of the object and the characteristics of the environment, which are in a form of digital data. Reported features open up the new prospects for the development of intelligent vehicular cyber-physical systems that will become in the near future an integral part of the human environment in the information space ”Internet of Things.” According to the estimates [4], network-centric cyber-objects in the global information space of the Internet will fundamentally change the social and productive components of people’s lives. That will accelerate of the knowledge accumulation and the intellectualization for all aspects of the human activity. However, this process requires not only innovative engineering ideas, but also the development of scientific concepts uniting universal scientific paradigm. Within this paradigm, for every CPh object like car, the information should be considered as a fundamental concept of objective reality, in which physical reality has ”digital” basis and therefore is computable. The idea of integrating the physical concepts with the theory of computation has led to the new conceptual schema for nature descriptions, known as ”it from bit” [5]. In this scheme, all physical objects, processes, and phenomena of nature, which are available to be read and understood by a person, are inherently informational and therefore they are isomorphic to some digital computing devices. Within this paradigm information acts as an objective attribute of matter that characterizes the fundamental distinctiveness of the potential states of the real object. The distinctiveness, according to the Landauers principle [6], is an energy factor of the objects states and that is why it gives an explanation of what are the states and how they are perceived by other objects. This distinctiveness appears while creating the systems that are capable to ensure the autonomy of the existence during the interaction with the external environment by the self-reproduction of its characteristics. It should be noted that on the way to the wide-spread use of ”digital reality” for the control problems, there are some limitations that reflect the requirements for the existence of the special state of physical objects reflecting its changes as a result of the information exchange processes. So, cyber-physical approach now often used to describe the properties of the so-called non-Hamiltonian systems in which the processes of self-organization are described by dissipative evolution of the density states matrix. However, the cyber-physical methodology may be successfully used to create complex robotic systems, the components which are capable for reconfiguration as the result of transmitting and processing digital data or metadata. The control and security tasks that are considered in this paper cover the actual scope of the cyber-physical approach, which is the basis of cloud computing technology and develop the methodology of cybernetics in the direction of the metadata control.

III. SECURITY ASPECTS OF CYBER-PHYSICS SYSTEMS

Modern technical systems have clear boundaries separating them from the environment or other objects and systems.

Therefore, the description of the processes in such systems is local and the change of its state can be described by the laws of physics, which are, in its most general form, the deterministic form of the laws of conservation, for example, energy, mass, momentum, etc. The mathematical formalization

 ISBN: 978-1-61208-376-6

of these laws allows to computationally determine the motion parameters of the physical systems, using position data on the initial condition, the forces in the system and the properties of the external environment. Although the classical methodology of modern physics, based on abstraction of "closed system" is significantly modified by studying the mechanisms of dissipation in the so-called "open systems", but such an aspect of reality as the information is still not used to build the control models and to describe the properties of complex physical objects. In the modern world, where the influence of the Internet, supercomputers, and global information systems on all aspects of the human activity becomes dominant, accounting an impact of information on physical objects cannot be ignored, for example, while realizing sustainability due to the information exchange processes. The use of cyber-physical methods becomes especially important while studying the properties of systems, known as the "Internet of Things" [6][7], in which robots, network cyber-objects, and people interact with each other by sharing data in the single information space for the characterization of which are used such concepts as "integrity", "structure", "purposeful behavior", "feedback", "balance", "adaptability", etc.

The scientific bases for the control of such systems were called Data Science. The term "Big Data" describes the process of integration technologies for digital data processing from the external physical or virtual environment, which are used to extract useful information for control purposes. However, the realization of the Data Science potential in robotics requires the creation of new methods for use the information in control processes, based on sending data in real time at the localization point of moving objects (the concept of "Data in motion").

In general, the "Big Data" are characterized by a combination of four main components (four "V"): volume, variety, velocity, and value. The general "V" is visibility of data and it is also a key defining characteristic of Big Data.

As a result, "Big Data" in modern science has become a synonymous for the complexity of the system control tasks, combining such factors of the physical processes that characterize the volume, velocity, variety, and value of data generated by them.

The security of CPh systems like vehicles is more complex task than access control in stationary local network. The cars move constantly changing the network configuration. Security policy enforcement requires data about permissions and prohibitions, as well as the current localization of the car and the route to it. Thus, while ensuring the information security of the vehicular network, we have to consider the static and dynamic aspects. This task is very similar to the information security of cloud services, where is regular migration of virtual machines from one physical platform to another to optimize the structure of the cloud and a hardware load balance.

The virtual computing environment allows us to create applications' service-oriented network of virtual devices. Any vehicle involved in the information exchange has its own virtual "avatar" in a high cloud environment. This virtual "avatar" of the car has all the information from the real object and the data obtained from other "avatars" in a virtual environment. Information exchange and required calculations are done in the secure virtual environment.

Localization of computing and data collected can accelerate the process of information processing and decision making. After that, the data is transmitted to the driver on the car for a final decision.

IV. Dynamic access policy using firewall filtering rules

The implementations of vehicular network security are far from simple due to the dynamic nature of network environment and users activity [7][8][9].

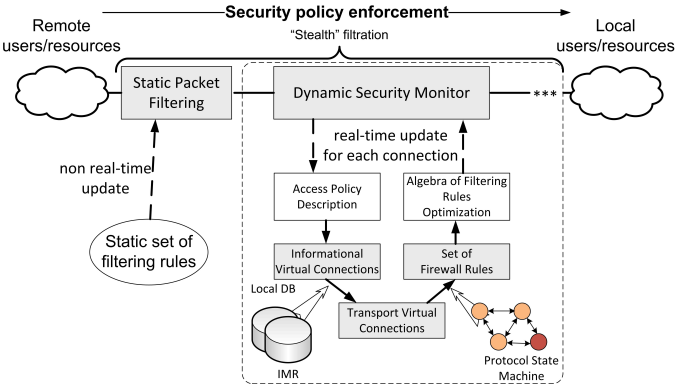

Figure 2. Security conveyor architecture.

Specific threats for the vehicular network are attacks affecting data integrity and availability of the car systems. An attacker often prefers not to steal any information out of the car but to modify it, thus tricking the various systems of the auto. Attack on availability can significantly hamper the work of the car, cutting off some of its devices from the information exchange process.

This specificity requires the use of specialized protective equipment. The main thread is while attacking the integrity of the information, the attacker can spoof the signals from the remote control signal, for example, acting as the owner and steal the vehicle.

In vehicular network, every second, hundreds of users and telematics devices establish new virtual connections [10] with distant resources and services. According to the mandatory security policy, if we have N users, M resources and these numbers are big, than we have to create a huge access N*M matrix. And each element of this matrix will be a vector of parameters and attributes, describing one virtual connection. Vehicles and resources of course can be grouped according to their rights and context, but in either case such matrix is too big to be processed efficiently in real-time.

We propose the architecture of security conveyor (see Figure 2), which consists of several filtering stages. At the first stage when a connection is established there is a classical static packet filter, which reject prior harmful traffic that corresponds local telematics devices of the car. The second stage enforces more accurate dynamic aspect of the access policy. Doing it the dynamic firewall have to take into account that the network resources can change their context any moment without informing our security conveyor. That is why we propose to use some prior information about remote users and resources in firewall to enforce security policy. Such information should be received from databases and services outside of our security monitor.

 ISBN: 978-1-61208-376-6

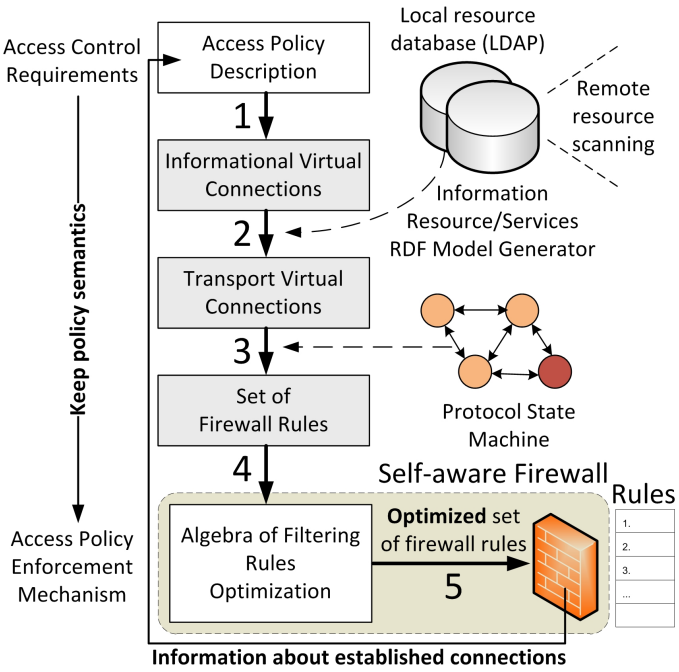

Figure 3. Dynamic access control approach.

In computer networks, information is transmitted in the form of packets. Each of these packets has some part of message in it. All network devices such as vehicular transmitters and firewalls have to operate with these packets. According to Figure 3, every access rule can be considered as one or more informational virtual connections (1) specifying action as ”access”, ”read”, ”write”, and so on. Then, we have to determine what does this record mean to telematics devices, how can the vehicle and requested information resource be described. To answer these questions, our security monitor has to use some prior outside information from specialized databases and services (2). Using such information we receive one or more Technological Virtual Connections (TVCs) from initial informational virtual connections [10]. Then, all these TVCs rules should be transformed into the requirement to the packet filter. At this stage, we use different transport protocols state machines to receive information about packet sequences (3). If all these procedures will be applied to each established virtual connection well receive huge amount of filtering rules. That is why at the next stage, we propose to optimize the set of filtering rules using specialized algebra of filtering rules (4) [11]. Only optimized set of filtering rules can be processed in real-time by firewall to enforce access policy (5).

V. Architecture of a Secure Cloud Computing Environment

During the researches at the Telematics department of SPbSPU, we proposed architecture of a secure cloud computing environment. This architecture considers dynamic nature of cloud environment and is suitable for description of vehicular networks.

A distributed computing environment (cloud system) consists of the following software and hardware components:

1) Virtualization nodes;
2) Storage of virtual machines and user data;
3) Cluster controller;
4) Cloud controller.

The distributed computing environment intended for solving scientific and engineering problems is a set of various computing resources, such as virtual machines, and has the following features [12]:

1) The environment is used by a wide range of users, who are solving problems of different classes;
2) Virtual machines of different user groups can operate within one hypervisor;
3) Wide range of software components (Computer-Aided Design (CAD)/Computer-Aided Engineering (CAE) applications, development tools) and operating systems is used;
4) Different hardware configurations are used, including virtual multicore computing machines and virtual machines, which allow performing computations using the streaming technology Compute Unified Device Architecture (CUDA).

Virtualization node is the hypervisor software which runs on powerful multicore computing node. In virtualization, the domain level 0 (dom0 in terms of hypervisor XEN or service console in terms of other hypervisors) and virtual computing machines (domain level U, domU) operate.

For information security and Access Control (AC) between the virtual machines that operate under a single hypervisor, the internal (”virtual”) traffic and the external traffic (incoming from other hypervisors and from public networks) must be controlled. The solution of the access control problem could be achieved through the integration of a virtual firewall into the hypervisor; this firewall would functions under the hypervisor, but separately from the user virtual machines. The virtual firewall domain can be defined as ”security domain” (domS). Invisible traffic filtering is an important aspect of the network monitoring; the firewall must not change the topology of the hypervisor network subsystem. This can be achieved by using ”Stealth” [12] technology, which is a packet traffic control invisible to other network components.

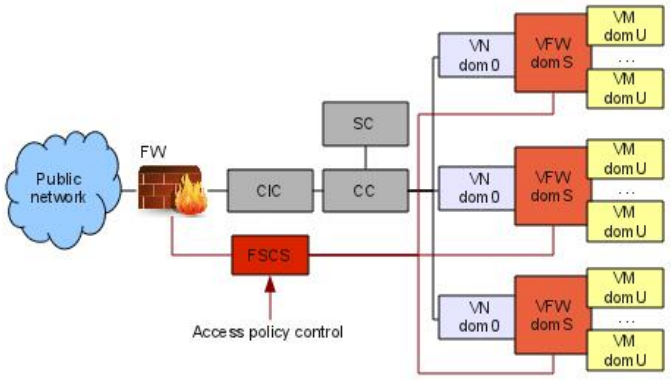

Figure 4. Secure cloud architecture.

Figure 4 shows the common architecture of a distributed cloud system with integrated AC components. The following abbreviations are used: hardware FireWall (FW); Virtual FireWall (VFW); the Central Control System of all Firewalls in

the cloud (FSCS); Virtual Machine (VM); CLoud Controller (ClC); Cluster Controller (CC); Storage Controller (SC).

The FSCS distributes the access control policies to all firewalls in the system. When the information security policy changes, new access rules are replicated to all components. The security domain isolates virtual machines from the hypervisor, which prevents the possibility of attack against the hypervisor inside the cloud. The hardware firewall isolates the private cloud components from the external threats.

The joint use of hardware and software firewall and intrusion detection system, based on the prediction of the driver's and vehicular's behavior and the vehicular network state will reduce the risks of invasion in a car network. Using a virtual machine "avatar" in a cloud computing environment, allows a better control of the processes of information exchange and the current status of all road users.

The task of finding an optimal allocation of virtual machines to minimize the number of nodes used by the cloud system is similar to the N–dimensional problem of packing containers (Bin Packing Problem), where N corresponds to the number of virtual machine's selected characteristics taken into account in the allocation. In [13], specialists of our department proposed a new approach for virtual machines distribution. A new virtual machines scheduler is able to place a virtual machine on the optimal compute node and migrate it to another node if resource consumption state has been changed. In [13], the proposed algorithm allows to optimize the structure of high-performance computing cloud system, facilitates localization of data and computing resources, and reduces the time required to provide a user requested services.

Cloud can improve system performance through the use of parallelization technology. When a large multi–node cluster needs to access large amounts of data, task scheduling becomes a challenge. Apache Hadoop is a cluster computing framework for distributed data analytics. However, the performance of each job depends on the characteristics of the underlying cluster and mapping tasks onto Central Processing Unit (CPU) cores and Graphics Processing Unit (GPU) devices provides significant challenges. Spark provide interesting advantages to the typical Hadoop platform [14]. Spark is an open source cluster computing system provides primitives for in–memory cluster computing. Job can load data into memory and query it repeatedly much quicker than with disk–based systems.To make programming faster, Spark integrates into the Scala language. Scala is statically typed high–level programming language designed to express common programming patterns in a concise, elegant, and type–safe way. Scala runs on the Java Virtual Machine (JVM) so it integrates features of object–oriented and functional languages. Spark is built around distributed datasets that support types of parallel operations: transformations, which are lazy and yield another distributed dataset (e.g., map, filter, and join), and actions, which force the computation of a dataset and return a result (e.g., count) [15]. In our work, we propose to use Deep Content Inspection (DCI) that reconstructs, decompresses, and decodes network traffic packets into their constituting application level objects. DCI examines the entire object and detects any malicious or non-compliant intent.

While solving information security problems for vehicular networks, we rely on our expertise in the field of robots control, for example during the space experiment "Kontur-2" [16]. Using DCI for network traffic monitoring enables us to provide the required level of security for on-surface robots, and traffic prioritization methods in packets processing allow us to provide the required level of Quality Of Service (QoS) [17] [18].

VI. Conclusion

Considering the vehicle as the dynamic cyber-physical object in non-deterministic environment, we propose to use the methods of cloud services information security to solve the problem of access control to the cars telematics network.

Vehicular security devices developed from mechanical through electromechanical and electronical to software based systems.

From the viewpoint of information security, the vehicle can be regarded as the dynamic virtual machine in the cloud environment.

In this paper, we propose an architecture of a secure cloud computing environment, which involves the use of static and dynamic access control methods.

It is necessary to mention that proposed solution doesnt solve all security problems of vehicular networks. The model described above can be merged easily with other methods of security control, for example with encryption or obfuscation. The prototype of the proposed system is currently developing for the Ford Motors Company at the Telematics department of the Saint-Petersburg State Polytechnical University.

Acknowledgment

This paper funded by RFBR grant 13-07-12106 and is done in the framework of the project with the Ford Motor Company.

References

[1] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Security of embedded automotive networks: state of the art and a research proposal," in SAFECOMP 2013 - Workshop CARS (2nd Workshop on Critical Automotive applications : Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security, Toulouse, France, 2013, J. Fabre, P. Quéré, and M. Trapp, Eds. HAL, 2013. [Online]. Available: http://hal.archives-ouvertes.fr/SAFECOMP2013-CARS/hal-00848234

[2] B. Donohue, "Hacking the Modern Automobile," 2013, URL: http://blog.kaspersky.com/car-hacking/ [accessed: 2014-10-01].

[3] A. Weimerskirch, "Automotive Data Security," 2012, URL: http://www.sae.org/events/gim/presentations/2012/ weimerskirch_escrypt.pdf [accessed: 2014-10-01].

[4] A. L. Fradkov, Cybernetical Physics: Principles and Examples. Nauka, Saint-Petersburg, Russia, 2003, ISBN: 5-02-025028-7.

[5] J. A. Wheeler, "Information, physics, quantum: the search for links," in Proceedings of the 3rd International Symposium Foundations of Quantum Mechanics in the Light of New Technology, Kokubunji, Tokyo, Japan, August 28-31, 1989, N. B. Gakkai, Ed. Hitachi, Ltd., 1989, pp. 354–368.

[6] G. Niemeyer and J.-J. E. Slotine, "Telemanipulation with time delays," The International Journal of Robotics Research, vol. 23, no. 9, 2004, pp. 873–890. [Online]. Available: http://ijr.sagepub.com/content/23/9/873.abstract

[7] V. Zaborovsky, O. Zayats, and V. Mulukha, "Priority queueing with finite buffer size and randomized push-out mechanism," in Networks (ICN), 2010 Ninth International Conference on, April 2010, pp. 316–320.

[8] V. Zaborovsky and V. Mulukha, "Access control in a form of active queuing management in congested network environment," in Networks (ICN), 2011 Tenth International Conference on, 2011, pp. 12–17.

 ISBN: 978-1-61208-376-6

[9] V. Zaborovsky, A. Gorodetsky, and V. Muljukha, “Internet performance: Tcp in stochastic network environment,” in Evolving Internet, 2009. INTERNET ’09. First International Conference on, Aug 2009, pp. 21–26.

[10] V. Zaborovsky, V. Mulukha, A. Silinenko, and S. Kupreenko, “Dynamic firewall configuration: Security system architecture and algebra of the filtering rules,” in Evolving Internet, 2011. INTERNET ’11. Third International Conference on, Jun 2011, pp. 40–45.

[11] V. Zaborovsky, V. Mulukha, and A. Silinenko, “Access control model and algebra of firewall rules,” in WORLDCOMP11: Proceedings of the 2011 International Conference on Security and Management (SAM2011). CSREA Press, Jul 2011, pp. 115–120.

[12] V. Zaborovsky, A. Lukashin, S. Kupreenko, and V. Mulukha, “Dynamic access control in cloud services,” in Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on, Oct 2011, pp. 1400–1404.

[13] A. Lukashin and A. Lukashin, “Resource scheduler based on multi-agent model and intelligent control system for openstack,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ser. Lecture Notes in Computer Science, S. Balandin, S. Andreev, and Y. Koucheryavy, Eds. Springer International Publishing, 2014, vol. 8638, pp. 556–566.

[14] T. Kumawat, P. K. Sharma, D. Verma, K. Joshi, and K. Vijeta, “Implementation of spark cluster technique with scala,” in International Journal of Scientific and Research Publications (IJSRP), vol. 2, 2012. [Online]. Available: http://www.ijsrp.org/research-paper-1112/ijsrp-p1181.pdf [accessed: 2014-10-01]

[15] A. Lukashin, L. Laboshin, V. Zaborovsky, and V. Mulukha, “Distributed packet trace processing method for information security analysis,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ser. Lecture Notes in Computer Science, S. Balandin, S. Andreev, and Y. Koucheryavy, Eds. Springer International Publishing, 2014, vol. 8638, pp. 535–543.

[16] V. Zaborovsky, M. Guk, V. Muliukha, and A. Ilyashenko, “Cyber-physical approach to the network-centric robot control problems,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ser. Lecture Notes in Computer Science, S. Balandin, S. Andreev, and Y. Koucheryavy, Eds. Springer International Publishing, 2014, vol. 8638, pp. 619–629.

[17] A. Ilyashenko, O. Zayats, V. Muliukha, and L. Laboshin, “Further investigations of the priority queuing system with preemptive priority and randomized push-out mechanism,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems, ser. Lecture Notes in Computer Science, S. Balandin, S. Andreev, and Y. Koucheryavy, Eds. Springer International Publishing, 2014, vol. 8638, pp. 433–443.

[18] V. Muliukha, A. Ilyashenko, O. Zayats, and V. Zaborovsky, “Preemptive queueing system with randomized push-out mechanism,” Communications in Nonlinear Science and Numerical Simulation, 2014, p. in print. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1007570414004031