Heterogeneous Virtual Intelligent Transport Systems and Services in Cloud Environments

Vladimir Zaborovsky, Vladimir Muliukha, Sergey Popov, Alexey Lukashin
Telematics department, St. Petersburg State Polytechnical University
Saint-Petersburg, Russia
e-mail: vlad@neva.ru, vladimir@mail.neva.ru, popovserge@spbstu.ru, lukash@neva.ru

***Abstract* — Modern Intelligent Transport Systems (ITS) are based on specific services that are hosted at network edges. These services are created using in-vehicle computing appliances, private cloud infrastructure and global information resources. According to the proposed approach all vehicles are considered as a mobile part of a low level operation network that provides low latency and requested quality of service (QoS) characteristics for the intelligent transport communication and information systems. Moreover, some of the discussed decisions support multiprotocol interactions and provide predictable real time performance so they can be used for different kinds of industrial, transport and robotics applications. ITS supplemented by low level operation network expands opportunities for a practical implementation of the emerging technologies for the Internet of Things (IoT). Due to the wide functional abilities the proposed approach is suitable for Big Data and on-demand high performance applications. Some aspects of these services develop the ideas of IBM "Smarter Planet" initiative and CISCO' Fog Computing. Researched model of multiprotocol node may be seamlessly integrated into an existing ITS cloud infrastructure using virtual firewall appliances to provide bilateral access control between vehicles that belong to MESH network and IaaS segments' resources, which support high performance computing and even supercomputers services.**

Keywords – Intelligent Transport Systems; Cloud Services; MESH; Multiprotocol Node; Security Services

I. INTRODUCTION

There are few approaches with potential to improve reliability and security of Intelligent Transport Systems (ITS) using possibilities to merge local resources of vehicle and different kinds of global cloud oriented services. Some aspects of these services develop the ideas of IBM "Smarter Planet" [1] initiative and CISCO' Fog Computing [2]. Emergence is achieved by the integration of three key technologies into reconfigurable and scalable service infrastructure: information, computer and communications. Such combination process is not a trivial task, especially in the case of transport systems, which support interaction of moving objects. The advantage of this technological approach is to expand online services to the drivers and passengers, to increase logistics efficiency and security of transport operations, as well as to prevent some road accidents. In this context, main challenge concerning research and design for the new generation of ITS is associated with a collaborative decision of the fundamental problem – organization of a real time access to big data from a moving car [3]. All aspects of this problem have a common background that are closely associated with communication technology tasks, namely [4]:

Connecting a user to local and global data. The volume of data, to which the vehicle has an access, is a critical parameter of ITS. This requirement depends on a hierarchical structure of the territorially distributed communication system, the local part of which receives time-critical operational data and processes it by the end-users' computers, and the second one belongs to a global cloud-oriented distributed information service housing at the data center far from the edge of ITS infrastructure.

Distributing processing tasks between a vehicle and cloud backbone resources. A computing platform extends capabilities of ITS services by sharing a processing operation with data between mobile real time vehicles' appliances and high performance massive scale resources of global information network or private cloud backbone.

Support bilateral mobile vehicle interaction. Variability due to the mobility is the key feature of ITS, that should be taken into account to improve performance, security and privacy issues by controlling data flows at the networks' edge points and by integrating multiprotocol vehicles' gateway with distributed communication infrastructure.

Seamless integration with security services. Information security requires seamless integration of data and communication services. This can be reached by using specific solution based on the stealth firewall technology for vehicle telematics hardware appliances and IaaS components of cloud environment.

Taking into account all aspects mentioned above we consider new services for Vehicle Controls Systems (VCS) that are hosted at any edge of ITS network infrastructure. These services expand the range of automotive protocols supported by vehicle embedded computing appliances, as well as available via MESH network private cloud resources and global public information systems. From the system point of view new services can be divided into three main categories: 1) communication services, which support real-time requirements; 2) access control between vehicle and high performance data processing resources; 3) high capacity storage systems that are available to VCS and belong to ITS cloud environment. Discussed approach can be implemented not only within ITS but also for various applications including emergency departments, regional data centers and Internet of Things (IoT).

The paper is organized as follows: in Section II, we introduce basic requirements for a new generation of ITS, describe characteristics, architecture and data structure of new proposed services; then, in Section III, we propose a model of ITS network edge that is the key component of mobile transport MESH network; we move on with information

 ISBN: 978-1-61208-318-6

security and access control services based on stealth firewalls in Section IV and conclude with Section V, in which we briefly present the main results of our work.

II. ITS AND CLOUD TECHNOLOGY

One of the promising technologies for vehicles' infrastructure management is cloud computing [5]. This technology allows us to take into account the territorial distribution and dynamic nature of the transport systems while improving their sustainability and scalability. The synergistic effect of the cloud technology implementation include a number of advantages, namely:

- Improvement of the dynamic characteristic of the MESH network at physical and data links layers;
- Expansion of available information and computing services;
- Spreading end-user's requests between several access points and applications to reduce response time and to increase semantic significance of the responses.

The main technological challenge concerns the way of how to allocate widely spread services and provides their availability to the end-user. One of the perspective ways to solve the problems mentioned above is to use cloud-oriented approach, which can be extended for mobility application due to the delay tolerance and secure infrastructure services (see Fig. 1).

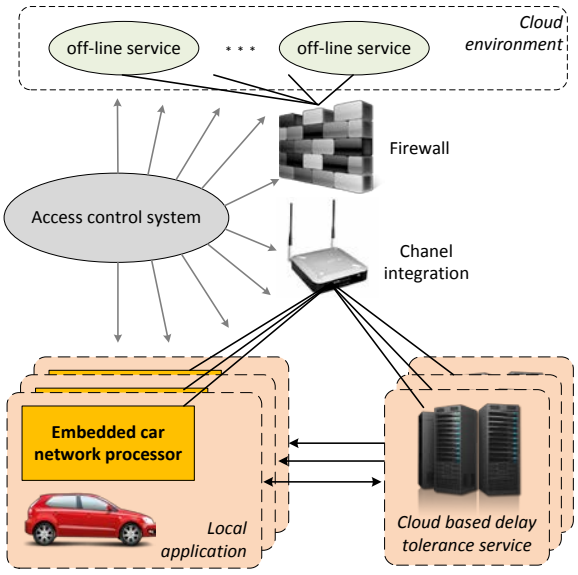

Figure 1. ITS system structure.

Each vehicle appears as a source of information in the cloud environment and for other vehicles simultaneously. The vehicle control system itself has a non-zero probability of crash or failure. However, data flows from vehicle via wireless media are susceptible to interferences that can disrupt connection and interaction of network notes and service components. In this case, the reasonable effectiveness criterion of the tasks listed above is the probability of the message delivery within a given time interval from the source to the destination in the cloud environment [6]. Delivery probability is a controlled parameter, which is a function of the cloud resources needed to process service requests. For example, fault tolerant implementation of supervisory tasks, such as route planning or vehicle speed control can be realized with the requested level of delivery probability by using the distributed cloud computing system. Furthermore, service agents, which interact with a vehicle applications and run on a remote Virtual Machine (VM) can improve or even optimize vehicle performance by analyzing historical driving patterns along the same route.

The concept of a virtual machine in the cloud architecture and MESH network architecture, that we propose, provides the implementation of the fault-tolerant, powerful and flexible tool for managing traffic services, roads infrastructure, and vehicle data. The implementation of our concept, which is based on the access control between vehicles' appliances and cloud services can be realized using existing wireless and wired connections of various technologies.

We consider a set of objects, a model of which is an extended network socket abstraction:

$$\mathrm{M^o} = \{\mathrm{name, IP, port}\}, \quad (1)$$

where *name* is a name of the service provided, *IP* is an address of the facility, and *port* is an applications' port, which is used for the transport layer interconnections.

On the set of objects M^o we introduce a number of services:

$$\mathrm{M^s} = \{\mathrm{name}, \{\langle \mathrm{p_i, type} \rangle\}\}, \quad (2)$$

where "*name*" is the name of the service, $\{p_i\}$ is a set of the typed parameters with the attributes type.

Consider the map $T = M^0 \circ M^S$, formed by the ratio $\Lambda(t)$ for different moments of time $t = t_0, \dots, t_n$, which determines the availability of the service for the subjects of the information exchange.

Then, oriented dynamic multigraph $G = (V, E)$, where V is a set of vertices, consisting of the named services from M^s, and E is a set of edges determining the sequence of services, characterizes the availability of the chosen sequence of services $\{m_1^s, \dots, m_n^s\} \in V$.

In turn, each vertex of the multigraph is a directed dynamic graph

$$\mathrm{g = (v, e)}, \quad (3)$$

where v is a set of service parameters of $\{p_i\}$, and e is a set of edges, that determine the acceptability of the given sequence of operations for the selected parameter $\{p_i\}$.

Within proposed hierarchy of models an admissibility of operations is characterized by quantifying estimation of relationships $\lambda_i(t)$, chosen from the set of all estimators of operations $\{\lambda\}$.

In this case, the task of choosing m^o from the set $\{M^o\}$ to obtain a sequence of services $\{m_1^s, \dots, m_n^s\}$ with parameters $\{\{p_1\}, \dots, \{p_n\}\}$ from $\{M^s\}$ can be formulated as the problem of finding a path of the dynamic multigraph G:

$$\exists\, (\mathrm{E_1 \dots E_n}) \in \mathrm{E}, \exists\, \{\mathrm{e_1, \dots, e_{1n}}\} \in \mathrm{e}\, |(\mathrm{E_1 \dots E_n}) = \\ = \{\mathrm{m_1^s \dots m_n^s}\} \vee \forall \mathrm{e_i} = \mathrm{p_i}\,. \quad (4)$$

Equation (4) can be solved by the modified Dijkstra's routing algorithm [3], in which for each moment is given the

 ISBN: 978-1-61208-318-6

vector of parameters, that takes into account both the information and the geographical connections of cyber-objects.

There are three ways to implement secure communications between vehicle and cloud services: vehicle-to-vehicle (V2V), vehicle-to-communication infrastructure (V2I), vehicle-to-cloud (V2C). For the first one, we need to use MESH topology [4], in the second case – multiprotocol telematics appliances, and the last way could be realized using reconfigurable wireless networks. Merger of all these technologies provide solid background for a bilateral information interaction between all parts of ITS. That leads to simultaneous use of various technologies for communication channels to improve accessibility of cloud services, which require integration of data communications to the shared wireless multiprotocol network.

Classical algorithms of MESH networks allow searching of the single route to the unique pre-known user. In the case of the cloud-oriented services and vehicles' appliances, while routing each time, a network node has to make a choice of the most perspective next hop from several alternatives. It is necessary to find available destination nodes with access to a cloud and to evaluate perspective of communication through them.

Fig. 2 shows the formation of functional virtual networks based on the multiprotocol MESH network of emergency services vehicles. Red background shows a virtual network of ambulance cars that provide an emergency aid service; blue one presents a virtual network of police cars.

Figure 2. Functional virtual networks of emergency services vehicles.

Local vehicles appliances communicate via MESH network with single vehicles (V2V component) and cloud services (V2I and V2C components) as they need. Communication with the cloud environment can be implemented in two ways: by the vehicle with communication equipment and by the stationary point. The vehicle located out of stationary communication area can access the cloud resources through a vehicle relay network. The network provides a bidirectional message transfer between the vehicle and the cloud environment.

The most important task for such network construction is the choice of communication protocols to increase message transfer adequacy. An estimation of message delivery time to the cloud services and back to MESH network users depends on a vehicle's traffic intensity, a level of communication network load, an interface availability and its composition in each vehicles.

A set of interfaces that allows being a user of Long Term Evolution (LTE) and MESH networks concurrently or MESH only (communication between vehicles only) should be installed in vehicles (network node). This new double-interface node (LTE, 802.11s) serves as a gateway providing communication between the MESH network and the cloud environment through LTE.

Data transfer protocol and an intensity of transfer determine message transfer adequacy, design and actual communication speed, mean latency of message delivery between vehicles' appliances and cloud environment.

The main features of the virtual communication network shown in the Fig. 2 are the following:

- Short lifetime of the static vehicles' MESH;
- A necessity of message transfer via MESH to the node that has an access to the cloud-oriented environment;
- Seamless integration with security services using cloud-oriented firewalls.

III. IMPLEMENTATION OF NEW MULTIPROTOCOL TECHNOLOGY IN FUTURE ITS

We need to realize multiprotocol support for message and data delivery within restricted time interval using different kinds of telecommunication protocols for fully use of cloud-based infrastructure to provide different vehicle's services, especially critical tasks. These aspects are the key requirements for future ITS that should operate with mobile objects and stationary components of infrastructure.

The implementation of such future ITS can be realized using network access mobile devices with reconfigurable multi-frequency radio connections that are simultaneously compatible with wireless interfaces (Fig. 3).

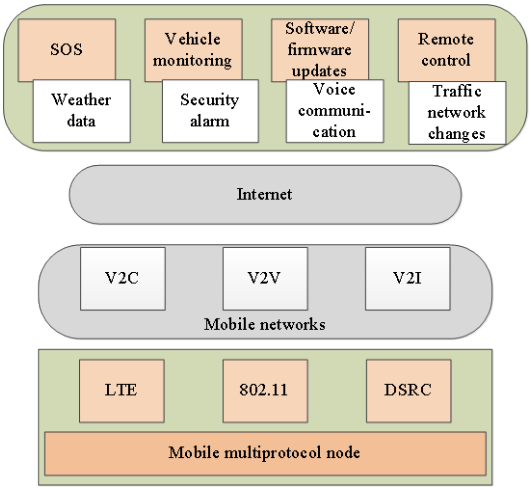

Figure 3. Multiprotocol node supporting ITS services.

The support of information interactions mentioned above requires designing a new generation of multi-protocol routers for Dedicated short-range communications (DSRC), LTE, MESH, and Wi-Fi networks. Such routers should generate optimal paths taking into account the nominal and available bandwidth as well as current delays while delivering data packets or control information. These routers should have a well-defined relationship between: 1) data rate and the available throughput of virtual channel, 2) routing policy and current network topology, and 3) routing algorithms and characteristics of transport, network, and data link layer protocols.

Creating a mathematical model of such future ITS is complicated by the large number of interdependent variables. In our work, we have used simulation methods and Network

 ISBN: 978-1-61208-318-6

Simulator 3 (NS-3) [7] for verification of the proposed approaches. The NS-3 simulator version 3.16 does not have a premade solution for creation of a multiprotocol node that serves as a gateway between different wireless technologies. Building of simulation model for mobile communication network requires realization of a multiprotocol node model that functions as message router between MESH communication networks and stationary infrastructure [4]. Realization of the multiprotocol node was made on the base of a "spot-to-spot" virtual point that enables intermediate interaction between interfaces. The following modules of NS-3 were used to implement the model with the multiprotocol node:

- 802.11s interface model. Implementation allows us to use the Hybrid Wireless Mesh Protocol (HWMP) route protocol in proactive and reactive modes, in addition we use Optimized Link-State Routing (OLSR), Ad hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector routing (DSDV) protocols for wireless MESH networks;
- Implementation of routing protocol models in wireless networks HWMP, OLSR, AODV, DSDV;
- FlowMonitor is a module of network traffic statistics collecting and processing;
- WireShark is an analyzer of computer network traffic;
- NS-3-highway-mobility is a model of vehicular traffic.

The simulation model allows to combine different routing protocols, network interfaces, and vehicles' traffic models. Simulation result is the set of xml-files generated by FlowMonitor module.

For experimental researches there was developed a specialized packet technology to initialize model's parameters and to realize the change of parameters during the experiment. These parameters are: vehicle's speed or trajectory change, routing protocol, transport layer protocol, connection throughput, number of nodes in the network, number of nodes transmitting data simultaneously, size of packets, packet loss rate in the communication channel [4]. While modeling for each node in the network the following characteristics are registered: packet's send and receive timestamp, packet loss rate, packet size, source and destination IP addresses. Output stores as the xml-files for future analysis. A simulation process with prescribed parameters allows researching the most dynamic periods of the MESH network existence (short time of the network static life, wide range of network traffic intensities, high intensity of route relocation).

Various sets of initialize parameters allow us to analyze different kinds of MESH and cloud-oriented states. For example, an estimation of security level for data transfer, actual speed of data transfer supported by the network, and average time of connection between the network mobile node and cloud-oriented environment.

In our researches, we have done two types of experiments:

1. Influence of the routing protocols on data transmission rate. We have considered OLSR [8], DSDV [9], AODV [10], and HWMP [11] routing protocols. As a source we've used UDP traffic with 8, 32, 64, 128, 512, 1024, 2048 Kb/s throughput. There was only one node with LTE interface.

The best results with high intensity flows are shown by AODV, DSDV protocols. To transfer short messengers with low intensity it is better to use HWMP.

2. Influence of vehicle traffic characteristics on the packet loss rate

2.1. HWMP, OLSR, AODV, and DSDV routing protocols were used. Network bandwidth was 8 – 2048 Kb/s. There was one node with LTE interface. Packet size was 1024 bytes. A number of vehicles was 8 or 16 for 800 meters of the road. Traffic speed was from 10 to 100 miles per hour (MPH). An actual packet loss rate was determined by Wireshark.

The reliability of message delivery was evaluated in a high dynamics of the network structure. Changes occurred at least once per second. Under these conditions, the intensity of the routing protocols was high and the packet loss rate was significant.

Fig. 4 shows the packet loss rate transmitted from the network 802.11s node to the cloud from the protocols used by the wireless routing and data transfer speed. Packet loss rate ranges from 7 to 46 percent. Packet losses increase with increasing transmission speed. By increasing the transmission speed twice, packet loss increases three times due to the broadcast routing requests. The greatest losses occur while using OLSR protocol.

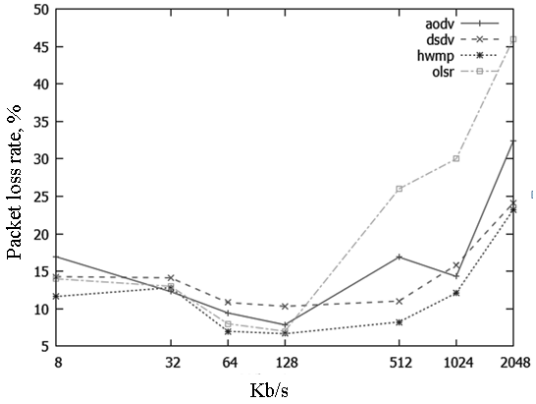

Figure 4. Packet loss rate from data transmission rate.

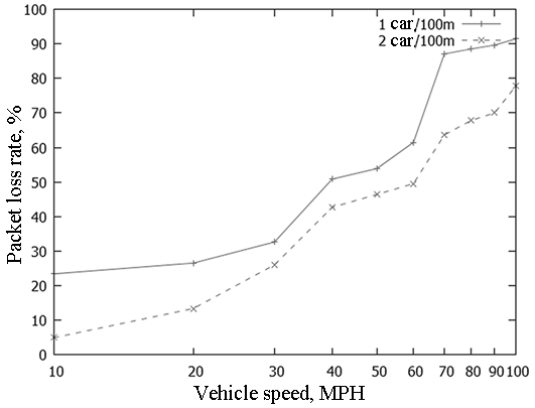

Figure 5. Packet loss rate from vehicle speed

2.2 Fig. 5 shows that for one or two vehicles that car moves at a speed of 100 MPH packet loss rate is 78-92%. The reason is that vehicles are in radio visibility zone for very short time, which is not enough to establish connection with the cloud environment. By increasing the number of cars on the road, we would decrease the packet loss rate.

 ISBN: 978-1-61208-318-6

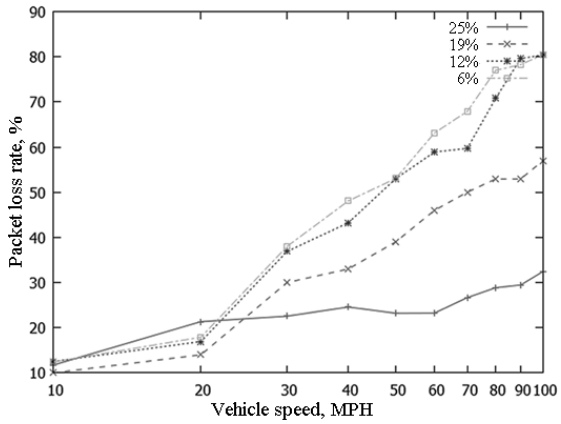

Figure 6. Packet loss rate while transmitting emergency message.

Fig. 6 shows the packet loss rate while transmitting emergency message from the vehicle on the strait road 800 meters long. Packet size is 1024 bytes. Number of cars is 16. Vehicle speed ranges from 10 to 100 MPH. The number of nodes with LTE interface is 1, 2, 3, and 4 (which corresponds to 6%, 12%, 19%, and 25% of all cars).

According to the received results (Fig. 6) packet loss rate is greater than 40%, while there are less than 25% of cars have LTE and speed is greater than 50 MPH. In this case, it is better to use alternative communication channels between vehicle and cloud environment.

IV. SECURITY SERVICES FOR CLOUD-ORIENTED ITS INFRASTRUCTURE

Now, we will discuss the organization of bilateral access control provided for the mobile and fixed components of the ITS. Due to the dynamic nature of cloud environment, we propose to realize the services' integration by using the expanding to cloud applications an existing version of the patented (US 7281129, RF 2214623) firewall decision. This approach allows dynamic changing access rules and operates in so called addressless or stealth modes using security policy semantic as an invariant for any interconnection between vehicles and ITS resources. An operational form of the proposed service can be represented as a set of traffic filters applied to each virtual connection.

The development of cloud computing environment requires new approaches to provide information security [12]. These requirements come from the need to consider the dynamic nature of the processes allocation of computing and network resources in the configuration of a virtual machines, which are the basic components of modern service infrastructure. In this section, we discuss an approach to the firewalls' configuration, by which are implemented control access policies to the cloud resources. Semantics of filtering rules and semantics of access policy must match or be close in a sense of chosen criteria to fulfill the requirements of information security for all possible configurations of cloud environment. Since the parameters of virtual machines that implement the application services are allocated dynamically the active filtering rules should also be changed during operation. In these circumstances, the traditional manual control settings of firewall rules in according to the access policy become impossible.

In such a dynamic environment as IaaS, the most stable part of the information relations is specifications of access policy. These specifications are special type of metadata that reflect the semantics of access strategy. Clearly, this strategy is not changing depending on the dynamic reconfiguration of available resources, so it can be regarded as a functional invariant of cloud services. Therefore, it is especially important to develop methods of automatic configuration of filtering rules and adaptation their parameters to the current state of cloud infrastructure, which can be viewed as carrier of the mentioned above invariant [6]. The formal model of cloud environment includes several parameters, namely:

$$\theta = \langle U, R, P, C \rangle, \quad (5)$$

where $U = \{u_i\}$, $i = 1 \ldots n$ is a set of cloud system's users. R is a set of roles $R = \{r_j\}$, $j = 1 \ldots m$. And each role is a set of privileges: $r_j = \{p_k\}$, $k = 1 \ldots l$, $r_j \subset P$, C – is a set of user sessions, which are presented by virtual connections between data source and destination in a cloud, P – set of privileges in the following form: $p_k = \{u, rul\}$, where $u \in U$ is a user of a cloud system, who is running information service (e.g., web application); $rul = \{r_g\}$, $g = 1 \ldots h$ – is a set of rules, which identify network application. The rule consist of the following parameters: $r = \langle transport, port, protocol, ext \rangle$, where *transport* is a transport layer protocol (e.g., tcp or udp), *port* – is a number of tcp or udp port, *protocol* – is an application layer protocol, *ext* – are additional parameters for application protocol.

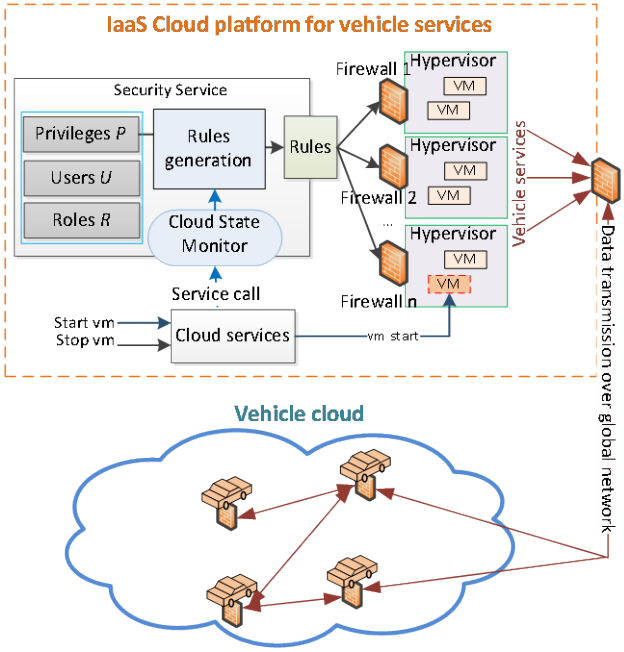

Figure 7. Security platform for cloud oriented ITS.

The example P is formed by the following parameters: *{user:*"Ivan", [{*transport:*"TCP", *port:*"80", *protocol:*"HTTP", *ext:*[{*method:*"GET"}]}]}. This privilege allows access to web servers, which are running on port number 80 using HTTP protocol and HTTP method GET to virtual machines that below to the user named Ivan. In order to continue our formalization, the state of cloud system is presented in the following form:

$$State = \{vm_i\}, i = 1..n, State \subset VM \times U, \quad (6)$$

where *U* is a set of cloud users, *VM* – is a set of IP addresses of running virtual machines in a cloud. *State* is a set of addresses of running virtual machines with labels of users who started virtual instance.

It is necessary to reconfigure security system each time when the *State* of a cloud system changes. Proposed security system consists of a group of firewalls and the security service, which is integrated with the cloud controller (see Fig. 7). This approach allows translating RBAC model of security policy to the set of filtering rules according to the state of cloud environment. As explained above when the *State* changes all firewalls on a mobile and fixed parts of ITS receive a message "new virtual machine with privileges *P* started" or "virtual machine with privileges *P* stopped" from cloud controller and then generate new filtering rules while keeping semantics of security policy.

To provide a consistent set of rules we consider operation $gen(a_s, a_o, p)$, which translates privilege delegated to virtual machine with ip address a_s into the object (vehicle service), which is running in virtual machine with ip address a_o:

$$(\mathrm{p} = \langle \mathrm{u_s}, \{\mathrm{rul_i}\}\rangle) \xrightarrow{\mathrm{gen}} \{\langle \mathrm{a_s}, \mathrm{a_o}, \mathrm{rul_i}\rangle\}, \mathrm{i} = 1..\mathrm{n}, \qquad (7)$$

All services are related with specific virtual machines and when a user requests new service ITS launches a new virtual machine and its security subsystem, inspects user's privileges, and generates filtering rules, which are running in another virtual machine. A stealth mode allows implementing the information protection system in a form of dedicated security domain. This domain can be quickly adapted to the current state of the network infrastructure and scaled if necessary to achieve seamless integration without reconfiguration of current ITS routing policy.

The proposed IaaS computing platform with integrated security is implemented in telematics department of the Saint-Petersburg State Polytechnical University and operates for ITS and other services. This platform is built using OpenStack services with custom proprietary software components. The platform installation is fully automated by Chef scripts and it is possible to install all services in a few hours on standard hardware. Our secure cloud computing test bench is available at the following address: http://cloudlet.stu.neva.ru.

V. CONCLUSION

The results of this research can be summarized as a perspective way to expand opportunity for practical implementation of future ITS within concepts "Internet of Things" and "Smarter Planet".

We have proposed a formalization of the routing problem that provides the opportunity to develop a constructive multi-functional hierarchical model of ITS, which could implement different classes of vehicle's services, including transfer of the special class of emergency messages.

As the part of our work, we have developed a simulation method allowing to combine the hierarchical network model with a specific structure of the urban transport network to select the optimal parameters of telematics services in the virtual network nodes for the delivery of emergency messages. The paper presents the results of the routing protocols' choice using simulation modeling in NS-3.

The proposed decisions can be used to reduce traffic congestion and emergency incidents, to support multi-protocol interactions, and to provide predictable real-time performance for different kinds of end-user applications, that needs to:

- Sharing data between mobile objects and fixed infrastructure nodes;
- Routing messages in multiprotocol mode;
- Delivering urgent and delay tolerance information;
- Integrating security services between ITS applications.

Information exchange technologies developed in this work are implemented in the international space experiment "Kontur-2" on board the ISS [13].

Our future research will be focused on applying a cloud computing paradigm to develop adequate to the times communication services and safer requirements for the future generation of ITS.

ACKNOWLEDGMENT

This paper funded by Russian Ministry of Education and Science and RFBR grant 13-07-12106. This research was supported by a grant from the Ford Motor Company.

REFERENCES

[1] http://www.ibm.com/smarterplanet/now [retrieved: Jan 2014].

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things", Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, MCC '12, New York, NY, USA, 2012. ACM, pp. 13-16.

[3] V. Zaborovski, M. Chuvatov, Ol. Gusikhin, A. Makkiya, and D. Hatton, "Heterogeneous Multiprotocol Vehicle Controls Systems in Cloud Computing Environment", In 10th International Conference on Informatics in Control, Automation and Robotics (ICINCO), SciTePress, 2013, pp. 555-561.

[4] M. Kurochkin,V. Glazunov, L. Kurochkin, and S. Popov, "Instrumental environment of multi-protocol cloud-oriented vehicular mesh network", In 10th International Conference on Informatics in Control, Automation and Robotics (ICINCO), SciTePress, 2013, pp. 568-574.

[5] S. Bitam and A. Mellouk, "Its-cloud: Cloud computing for intelligent transportation system", In Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 2054-2059.

[6] V. Zaborovsky, O. Zayats, V. Mulukha, "Priority Queueing With Finite Buffer Size and Randomized Push-out Mechanism", Proceedings of The Ninth International Conference on Networks (ICN 2010), IEEE Computer Society, 2010, pp. 316-320.

[7] http://www.nsnam.org/ [retrieved: Jan 2014].

[8] http://www.ietf.org/rfc/rfc3626.txt [retrieved: Jan 2014].

[9] Perkins Charles E., Bhagwat Pravin: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, London England UK, SIGCOMM 94-8/94.

[10] http://www.ietf.org/rfc/rfc3561.txt [retrieved: Jan 2014].

[11] S.M.S. Bari , F. Anwar, M.H. Masud, "Performance Study of Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN Mesh Networks", In International Conference on Computer and Communication Engineering (ICCCE), 2012, pp. 712-716.

[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, pp. 1400-1404.

[13] V. Zaborovsky, A. Kondratiev, V. Muliukha, A. Silinenko, A. Ilyashenko, M. Filippov, "Remote Control Robotic Systems in "Kontur" Space Experiments", Informatics, Telecommunication and Control, Politechnical University, Saint-Petersburg, Russia 6(162), 2012, pp. 23-32 (in Russian).

 ISBN: 978-1-61208-318-6