Reliability Challenges in Software Defined Networking

Victor Netes, Margarita Kusakina
Moscow Technical University of Communications and Informatics
Moscow, Russia
v.a.netes@mtuci.ru, margaritakus@gmail.com

***Abstract*—One of the actively developing technologies in telecommunications is Software-Defined Networking (SDN). Its usage will automate the management and administration of network equipment, greatly accelerates the organization of new services for users, and will give other advantages. A new control element, the "brain" of the SDN, is a controller that performs the functions of controlling physical devices (switches) and at the same time interacts with the application layer. One of the most important characteristics of any communication networks is reliability, and the reliability requirements are increasing with the expansion and intensification of usage of information and communication systems. This paper discusses main aspects of reliability for SDN. As the controller is a key element of the centralized network control, its failure or loss of connection with switches leads to the inability of the normal functioning of the network. Therefore, it is important to ensure the high reliability of the controller and its connections with network elements. On the example of a typical SDN network, several options for placing and linking controllers and for redundancy of connections with them are analyzed. The results of calculations show the need for redundancy of controllers and their connections with all nodes in the network.**

I. Introduction

In the recent years, one of the most discussed topics in telecommunications is Software-Defined Networking (SDN) [1]. The concept of SDN emerged in response to the growth of virtualization, mobility, the Internet of Things, etc. It is a new evolutionary concept for network architecture, which separates the control plane from the data plane. The latter in SDN forwards network traffic based on the control plane instructions.

The main advantages of SDN are as follows. Firstly, it centralized management of networking devices and provides improvements to end users. Secondly, the networks become more flexible and scalable compare to traditional ones. Lastly, it gives geographical independence in the placement of the platform.

Standardization in the field of SDN is carried out by a number of international organizations, in particular ITU-T. The ITU-T Recommendations Y.33xx are devoted to this topic. ITU-T considers SDN to be an important shift in network technologies that will enable network operators to create and manage new virtualized resources and networks without deploying new hardware technologies.

In SDN, many challenges are needed to be solved, such as the problems of scalability, virtualization, communication consistency, controller placement, and so on. One of the major challenges in SDN is reliability. As stated in the [2], in large-scale networks, reliability is a particularly important issue. As a characteristic of logically centralized control in SDN, an SDN controller tends to become a single point of failure. Therefore, it is necessary to take measures to ensure that the reliability of new technical solutions is at least as good as or better than it was before. SDN is considered as one of the most important technologies for building the network infrastructure of the digital economy [3]. However, the digital economy cannot be based on unreliable infrastructure.

The aim of this paper is to discuss main aspects of reliability in SDN and ways to ensure it. In particular, we analyze the controller placement problem, redundancy for them and connections between controllers and network elements.

The rest of the paper is organized as follows. Section II is devoted to the evolution of networks, the emergence and development of SDN; it also describes the architecture of the new paradigm, its application in 5G networks and development in Russia. Section III presents overview of reliability and two its aspects for communications networks. Section IV describes the problem of controller placement and presents the metrics used for this. Section V considers a typical SDN network on which few options of redundancy are analyzed. Concluding Section VI gives main findings and directions for future work.

II. The Concept and Use of SDN

A. Brief history and evolution

The history of SDN principles can be traced back to the separation of the control and data plane first used in the public switched telephone network as a way to simplify provisioning and management well before this architecture began to be used in data networks [4]. The use of open source software in split control/data plane architectures traces its roots to the Ethane project at Stanford's computer sciences department. Ethane's simple switch design led to the creation of protocol OpenFlow. An API for OpenFlow and the operating system for networks NOX were created in 2008.

Work on OpenFlow continued at Stanford, including with the creation of testbeds to evaluate use of the protocol in a single campus network, as well as across the WAN as a backbone for connecting multiple campuses. In academic settings there were a few research and production networks based on OpenFlow switches from NEC and Hewlett-Packard; as well as based on Quanta Computer whiteboxes, starting from about 2009.

In 2011 the Open Networking Foundation was founded to promote SDN and OpenFlow.

B. The SDN architecture

It is known that any network has control and data planes. The control plane is generally considered to be where a router or switch makes its decisions. This is software based, and uses the CPU rather than specialised hardware. The data plane (or forwarding plane) is the high speed path through the router/switch. Packets that pass through the device use the data plane.

In traditional IP networks, the control and data planes are tightly coupled, embedded in the same networking devices, and the whole structure is highly decentralized – Fig. 1.

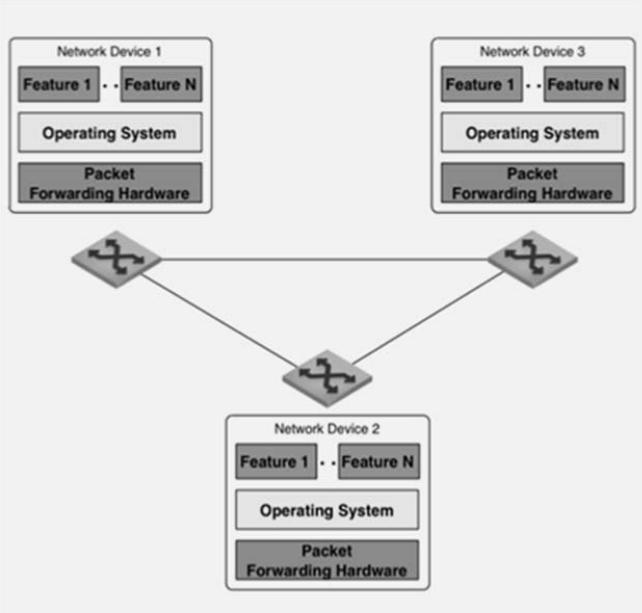

Fig. 1. Architecture of traditional IP networks

In SDN control and data planes are separated (divided between controllers and network devices), and the whole structure is centralized. The architecture of SDN consists of three layers [2] as depicted in Fig. 2. The interaction between them is realized as Applications Program Interfaces. They will be considered below in more details.

1) Application layer: The application layer is where SDN applications specify network services or business applications by defining a service-aware behavior of network resources in a programmatic manner. These applications interact with the SDN control layer via application-control interfaces (northbound interface), in order for the SDN control layer to automatically customize the behavior and the properties of network resources. The programming of an SDN application makes use of the abstracted view of the network resources provided by the SDN control layer by means of information and data models exposed via the northbound interface.

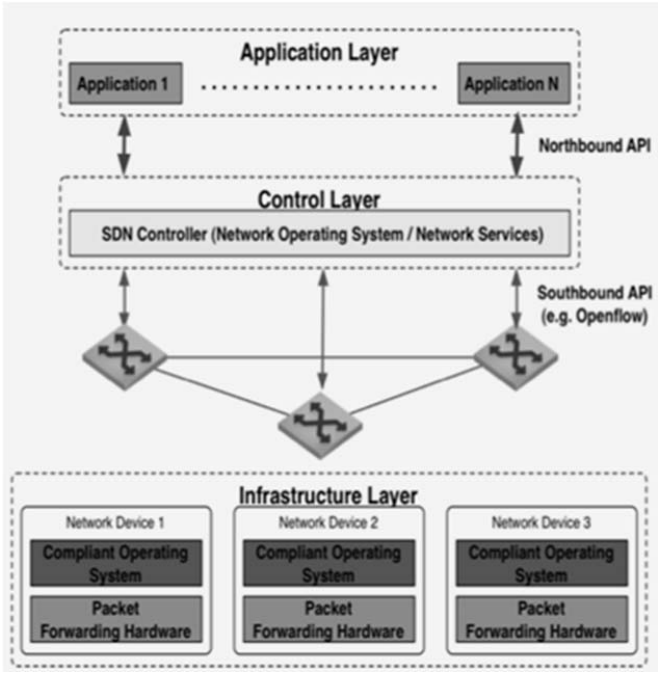

Fig. 2. Architecture of SDN

2) SDN control layer: This layer provides a means to dynamically and deterministically control the behavior of network resources (such as data transport and processing), as instructed by the application layer. The SDN applications specify how network resources should be controlled and allocated, by interacting with the SDN control layer via northbound interface. The control signaling from the SDN control layer to the network resources is then delivered via resource-control interfaces (southbound interface). The configuration and/or properties exposed to SDN applications are abstracted by means of information and data models. The level of abstraction varies according to the applications and the nature of the services to be delivered.

3) Resource layer: The resource layer is where the network elements perform the transport and the processing of data packets according to the decisions made by the SDN control layer, and which have been forwarded to the resource layer via a southbound interface.

C. Using in 5G

Another actively developing area of telecommunications is the 5th generation of mobile networks (5G). In ITU, the standard for 5G is named IMT-2020. The letters in this designation mean International Mobile Telecommunications and the numbers indicate the year when it should be completed (previously for the 3rd generation used a similar designation IMT-2000).

One of the requirements for the IMT-2020 network is that it should be designed and operated with reliability and fault tolerance [5]. At the same time, it is stipulated that reliable and

stable operation is especially important in the event of network overloads and emergencies. In addition, it is stated that the reliability and resiliency of the network should not be at risk as a result of a software or hardware upgrade.

The software is mentioned here not by chance, as one of the characteristic features of IMT-2020 is network softwarization [6]. This means an overall approach for designing, implementing, deploying, managing and maintaining network equipment and/or network components by software programming [7]. Basic technologies for network softwarization are: SDN, Network Functions Virtualization (NFV) and cloud computing [6].

Thus, the reliability of SDN has a direct impact on the reliability of 5G networks.

D. Current activities

Testing and implementation of SDN solutions is carried out by a number of American and European telecom operators: AT&T, BT, DT, Orange, Telefonica, Verizon, Vodafon, etc. (a brief overview of their activities can be found in [3]).

The largest Russian telecom operator Rostelecom is also testing SDN solutions in its laboratory. This study showed a number of problems and shortcomings that prevent the application of these solutions on a real network [3, 8]. A large part of these shortcomings are directly related to reliability. Among them are long convergence time in case of connection failure, losses of traffic when the controller is recovering from failure, etc.

Also, the development of solutions for the SDN is actively conducted in the Applied Research Center for Computer Networks (ARCCN) [9]. It is the first Russian research center created to develop technologies and products for computer networks of the new generation. ARCCN startup – RunSDN – with a complex all-in-one solution for the organization of the transport SDN network is the only Russian company that passed the competition for participation in the SDN & NFV Solutions Showcase at ONS 2017 [9].

III. EQUIPMENT AND SYSTEM RELIABILITY

A. Basic concepts and measures

In this paper, we write about reliability. However, strictly speaking, it would be more correct to use the term dependability instead. The fundamental international standard in this area is [10]. This is not by chance, since, under the agreement between International Electrotechnical Commission (IEC), International Organization for Standardization (ISO) and International Telecommunication Union (ITU) that constitute the World Standards Cooperation, it is the IEC that plays the leading role in standardizing in this area.

According to [10], dependability is defined for an item as its ability to perform as and when required. Dependability is used as a collective term for the time-related quality characteristics of an item and it includes few attributes: availability, reliability, recoverability, maintainability, and maintenance support performance.

An item in this standard is defined as a subject being considered. It may be an individual part, component, device, functional unit, equipment, subsystem, or system. The item may consist of hardware, software, people or any combination thereof. In our consideration, this term can be used both for the network as a whole and for its elements: nodes, links, terminals, etc.

In its turn, availability is ability to be in a state to perform as required. It depends upon the combined characteristics of the reliability, recoverability, and maintainability of the item, and the maintenance support performance. Reliability is ability to perform as required, without failure, for a given time interval, under given conditions.

The term dependability is used in IEC standards devoted to communication networks [11], [12] and in ITU-T Recommendation [13]. Unfortunately, quite often, instead of the term dependability, the term reliability is used in a broad sense, i.e. as a blanket term that includes abovementioned attributes [14]. Thus, in many other ITU-T Recommendations, in numerous publications, in the names of many journals, conferences, etc. there is such a word usage. To maintain consistency with them, we also write about reliability.

Besides that, the terms reliability and availability are used for quantitative measures of the appropriate attributes [10]:

- Reliability is the probability of performing as required for the given time interval, under given conditions.
- Availability is the probability that an item is in a state to perform as required at a given instant (instantaneous/point availability) or the limit, if it exists, of the instantaneous availability when the time tends to infinity (steady state / asymptotic availability). The most commonly used of them is steady state availability, which is usually called merely availability.

Both these measures are probabilistic in nature, and can be expressed as fractions or percentages, but the latter form is unsuitable for calculations. The values 0.99 (99 %), 0.999 (99.9 %), etc. are often called “two nines”, “three nines”, etc.

B. Two aspects of reliability

Usually, two aspects of reliability are considered for communication networks: equipment and system (or structural) reliability [15]. The first one depicts the reliability of equipment, which are included in network nodes. The system aspect, also called structural, shows the functioning of the network as a whole depending on the performance or failures of nodes and links.

C. Equipment reliability

Currently, the generally accepted requirement for the reliability (availability) of carrier-class network equipment is the value of 0.99999 [16], [17]. Moreover, in the future it may be expected further increase of the requirements [16].

Controller is a new type of equipment in the SDN. It is the key element of the network. Sometimes it is called the “brains” of the network, so that necessary to ensure its high reliability.

It was already mentioned, there is a threat that the controller will become a single point of failure [2]. As noted in [2], the SDN controller may be replicated to improve reliability. In addition, the use of only one controller is not desirable keeping in mind to ensure network survivability, i.e. the ability to continue to function during and after a natural or man-made disturbance. All this leads to the idea of redundancy for controllers with geographical separation of their locations (georedundancy).

Two approaches are possible for organizing the controller. Firstly, it can be made as a traditional standalone specialized equipment; secondly, it is possible to virtualize its functionality by placing the controller in the cloud, i. e. in the data center, resulting in a symbiosis of technologies SDN and Network Function Virtualization (NFV).

If the controller is implemented in a traditional way and is placed in a node, it is closer to the network elements, which means that lower latency is provided. If it is implemented in the data center, the reliability will be higher, but in this case there is a greater distance from the network elements. This results not only in higher latency, but also less reliable communication between the controller and managed network elements. In this case, it should be taken into account general considerations about the reliability of cloud services [18], [19].

D. System reliability

New tasks related to system reliability in SDN network include selection of the number and locations of controllers, distribution of controlled network elements between them, organization of communication between controllers and network elements, etc.

The SDN provides new opportunities to ensure reliability through self-recovery and automatic redistribution of traffic flows (re-routing). These are provided by the protocol OpenFlow itself by finding a new route, but it is undesirable to overload the backup path links. Rational organization of such re-routing requires solving the above-mentioned tasks.

IV. CONTROLLER PLACEMENT FOR SDN

The issues of controller placement are investigated in a number of papers [20], [21], [22], etc. In particular, [21] considers the problem, the solution of which provides: finding the minimum number of controllers in the network, the choice of locations of controllers among candidate nodes, the distribution of controlled network elements between controllers, the reassignment of controllers in case of failures with minimal deterioration. This takes into account the limitations on packet transmission latency between the controller and the equipment and between controllers, as well as the limitations due to the need for load balancing between controllers. In case of controller failure, for backup one the above conditions should be maintained with minimal losses.

When solving the problem of controller placement, various metrics can be used. The most popular among them are the minimum – average latency (1) and the minimum – worst-case latency (2) [22], defined respectively by the following formulas:

$$L_{avg}(S) = \frac{1}{n}\sum_{v\in V} \min_{s\in S} d(v,s), \quad (1)$$

$$L_{wc}(S) = \max_{v\in V} \min_{s\in S} d(v,s), \quad (2)$$

where S is the set of nodes in which controllers are placed; V is the set of nodes in which network equipment are placed; n is the number of nodes in the set V; d is the latency between indicated nodes.

These problems are reduced to the well-known in graph theory problems of finding medians and centers respectively [23], [24]. They are used in various applications. For example, the median might be a good place to locate a mall: the average driving distance is minimized; the center is for emergency facility location: the response time must be minimized in the worst case. The problems of placing several medians and centers are also known. The p-median problem is to locate p facilities on a network so as to minimize the average distance from one of the demand points to one of the p facilities. The p-center problem is to locate p facilities on a network so as to minimize the largest distance from a demand point to its nearest facility. In the considered situation, the facilities are SDN-controllers and the demand points are switches in network nodes.

These works has focused on optimization in terms of the latency, which is the sum of the delays on all links in the minimal path between considered nodes:

$$d(v,s) = \sum_{(i,j)\in P} d_{ij}, \quad (3)$$

where d_{ij} is the delay in the link between nodes i and j; P is the set of links that make the path between nodes v and s.

In these tasks, we consider a weighted graph in which to the arcs are assigned "weights" representing their lengths or delays. However, we can apply these results to reliability. The considered approach can be used to optimize reliability using the following idea from [24]. In the shortest path problems, the sum of the weights of the arcs forming the path was taken as the path length. Consider now the case where the weight of an arc represents its reliability. The reliability of the path P is calculated by the formula

$$r(P) = \prod_{(i,j)\in P} r_{ij}, \quad (4)$$

where r_{ij} is the reliability of the arc (i,j).

The problem of finding the most reliable path can be reduced to the problem of the shortest path, taking as the weight of the arc (i,j) value $c_{ij} = -\log r_{ij}$. Taking the logarithm from both parts of the equality (4), we obtain

$$\log r(P) = \sum_{(i,j)\in P} \log r_{ij}.$$

Thus, for c_{ij} there is additivity, as in (3). It can be seen that the shortest path with the weight matrix $\|c_{ij}\|$ will be the most

reliable path with the matrix $||r_{ij}||$, and the reliability of this path is equal to the anti-logarithm of its length.

Therefore, by modifying the metrics (1) and (2) in this way, it is possible to find the location of the controllers, providing maximum reliability of their communication with other nodes (on average or for the worst case respectively).

V. Redundancy in SDN

Redundancy is one of the most important methods to ensure reliability. Consider its application for SDN networks on a typical example.

As mentioned above, the operation of communication between the node and SDN controller (in figures SDNC) is necessary for the normal operation of the switch. The reliability of the SDN switch, together with the controller and the means of communication between them, should not be lower than that of a traditional switch.

As an example, take a SDN network, which shown in Fig. 3. Its structure is chosen by analogy with the network considered in [25], where the national backbone network in Norway was taken. The network under consideration consists of 11 nodes located in four major cities of the European part of Russia: Moscow (MSK), Saint Petersburg (SPB), Nizhny Novgorod (NN) and Rostov-on-Don (RoD). The nodes contain switches. Traffic from cities goes through access networks with connections to two, three or four nodes in the city.

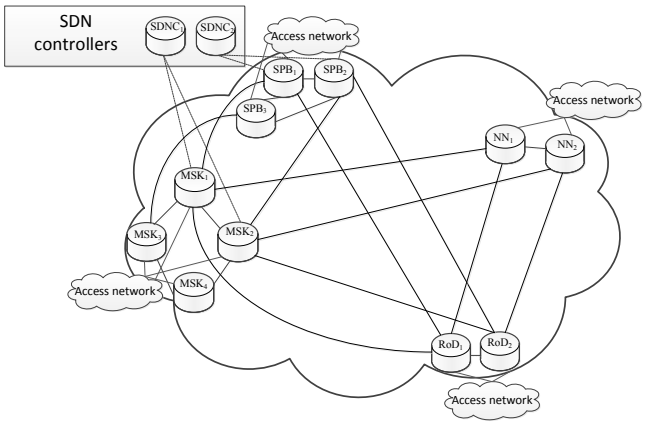

Fig. 3. Topology of the considered network

Consider the node in Rostov-on-Don, as it is the most remote from the cities where the controllers are located, and hence the reliability for it will be lower.

Three options for the location and connection of controllers were considered:

- In the network there is one controller connected to one of the nodes in the city (in Moscow); only its communication with the node in another city has redundancy (Fig. 4).
- The same controller is connected to two nodes in the same city; each of connections is duplicated separately with nodes in the other two cities, similar to the previous case (Fig. 5).
- In the network there are two controllers located in different cities (Moscow and St. Petersburg); each connection is duplicated (Fig. 6).

The calculations were made based on availability of the equipment in the nodes and links. In general, the calculations are carried out in accordance with the input data and method described in [26]. The availability of SDN controllers and all nodes were taken equal to 0.99999 ("five nines"). The details can be found in [27]. The calculation results are given in the Table I.

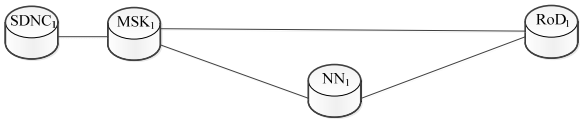

Fig. 4. The topology of the network fragment with a single SDN controller connected to a single node

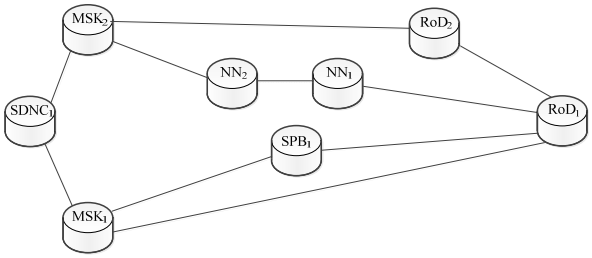

Fig. 5. The topology of the network fragment connecting one SDN controller to two nodes in the same city

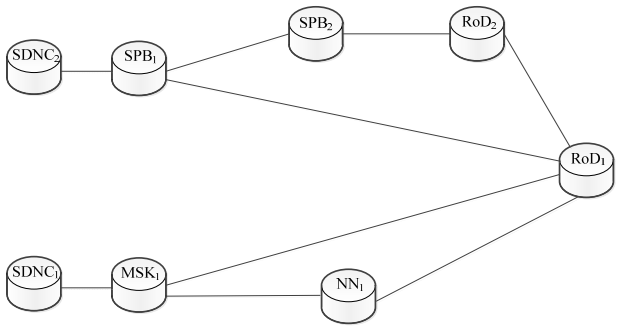

Fig. 6. The topology of the network fragment with two SDN controllers in different cities

TABLE I. The availability of different options to connect the controllers SDN

SDN controller(s) connection variant	Availability	Unavailability	Average downtime, min/year
One controller connected to one node	0.999965	$3.5 \cdot 10^{-5}$	18.40
One controller connected to two nodes in the same city	0.999979	$2.1 \cdot 10^{-5}$	11.04
Two controllers connected to two nodes in different cities	0.999989	$1.1 \cdot 10^{-5}$	5.78

Comparison of the results shows that the second variant has a downtime of more than 1.5 times less than the first, and the third variant has it more than 3 times less than the first. At the same time, only the network topology with two SDN controllers in different cities and the redundancy for paths from each node allows to obtain availability close to the required value of "five nines".

The calculation results show the need for redundancy of controllers and their connections with all the nodes in the network.

VI. Conclusion

The main findings of this paper are the following: the huge role of information and communication technologies in the life of modern society makes reliability a very important factor for communication networks; this fully applies to SDN networks that form the basis for the digital economy and 5G; achieving high reliability in SDN requires redundancy, in particular, for controllers and network connections with them; the cost of this redundancy must be taken into account when conducting a feasibility study for cloud services.

Future work could be devoted to the development of methods for calculation and evaluation of network end-to-end reliability. Typically, in such calculations, the states of network elements (nodes and links) are assumed to be statistically independent. In the case of SDN, this assumption is not justified because operability of multiple switches may depend on the same controllers. Besides that, the same links can be used for communication of terminals among themselves and for communication of switches with controllers. This creates a serious problem that needs to be addressed.

References

[1] P. Goranson, C. Black, T. Culver, *Software Defined Networks: A Comprehensive Approach.* Cambridge: Elsevier, 2017.

[2] ITU-T Recommendation Y.3300 (06/2014). *Framework of software-defined networking.*

[3] V.A. Efimushkin, T.V. Ledovskikh, A.B. Ivanov, V.A. Shalaginov, "The role of SDN/NFV technologies in the digital economy infrastructure. Experience of testing and implementation", *Elektrosviaz,* 2018, No 3, pp. 27-36 (in Russian).

[4] Software-Defined Networking, Web: https://en.wikipedia.org/wiki/Software-defined_networking#History.

[5] ITU-T Recommendation Y.3101 (01/2018). *Requirements of the IMT-2020 Network.*

[6] Recommendation ITU-T Y.3150 (01/2018). *High-Level Technical Characteristics of Network Softwarization for IMT-2020.*

[7] Recommendation ITU-T Y.3100 (09/2017). *Terms and Definitions for IMT-2020 Network.*

[8] V. Shalaginov, "Pilot tests of SDN solutions of communication operator data networks", *in Proc. of the XI Internat. Conf. of "Information Society Technologies".* Moscow: Media Publisher, 2017, pp. 425-426 (in Russian).

[9] Internet Technologies of the New Generation, Web: http://en.arccn.ru/media/ons2017.

[10] IEC 60050-192:2015. *International Electrotechnical Vocabulary – Part 192: Dependability.*

[11] IEC 61907:2009. *Communication Network Dependability Engineering.*

[12] IEC 62673:2013: *Methodology for Communication Network Dependability Assessment and Assurance.*

[13] ITU-T Recommendation E.862 (06/92). *Dependability Planning of Telecommunication Networks.*

[14] T. Van Hardeveld, International Perspectives on Reliability, Web: https://reliabilityweb.com/articles/entry/international_perspectives_on_reliability.

[15] *Theory of Communication Networks,* Editor V.N. Rogisky. Moscow: Radio i Sviaz, 1981 (in Russian).

[16] N.A. Sokolov, *The Planning of Telecommunication Network.* St. Petersburg: Technology of Telecommunications, 2012 (in Russian).

[17] A. Goldstein, B. Goldstein, *Softswitch.* St. Petersburg: BHV-St. Petersburg, 2006 (in Russian).

[18] V.A. Netes, "Virtualization, cloud services and dependability", *Vestnik Sviazy,* 2016, No 8, pp. 7-9 (in Russian).

[19] V. Netes, "End-to-end availability of cloud services" *in Proc. of the 22st Conf. of Open Innovations Association FRUCT,* Jyvaskyla, Finland, 15-18 May 2018, pp. 198-203.

[20] M. Ulema "Vulnerabilities and opportunities in SDN, NFV, and NGSON", *in IEEE CQR 2014 Internat. Workshop. Emerging Technology Reliability Roundtable.* Tucson, Arizona, USA, May 2014, pp. 24–27.

[21] N. Perrot, T. Reynaud. "Optimal placement of controllers in a resilient SDN Architecture", *in Proc. of the 12th Internat. Conf. on the Design of Reliable Communication Networks (DRCN 2016).* Paris, France, March 2016. pp. 145–151.

[22] B. Heller, R. Sherwood, N. McKeowin. "The controller placement problem", *in SIGCOM HotSGN 2012,* Stanford University, Web: http://www.sharecourse.net/sharecourse/upload/quiz/13/21/909838c7e75f081c3ac73dcb0545cf13.pdf.

[23] H. Frank, I.T. Frisch, *Communication, Transmission, and Transportation Networks.* Reading: Addison Wesley, 1971.

[24] N. Christofides, *Graph Theory: an Algorithmic Approach.* London, New York: Academic Press, 1975.

[25] G. Nencioni, B.E. Helvik, A.J. Gonzalezy, P.E. Heegaard, A. Kamisinski, "Impact of SDN Controllers Deployment on Network Availability", Department of Telematics, Norwegian University of Science and Technology, Trondheim, Norway, 2017.

[26] V.P. Shuvalov, M.M. Egunov, E.A. Minina, *Assurance of Reliability Measures for Telecommunication Systems and Networks.* Moscow: Goryachay Liniya – Telecom. 2015 (in Russian).

[27] V.A. Netes, M.S. Kusakina, "Reliability of communication between controllers and switches in SDN", *Vestniik Sviazy,* 2018, No 9. pp. 10-13 (in Russian).