



RESEARCH ARTICLE

Performance of Multi-Service Telecommunication Systems Using the Architectural Concept of Future Networks

Geleceğin Ağlarının Mimari Konseptini Kullanan Çok Servisli Telekomünikasyon Sistemlerinin Performansı

Bayram Ganimatoglu Ibrahimov¹ , Yalchin Sabiroglu Isayev² ,
Mustafa Emre Aydemir^{3*} 

¹ Azerbaijan Technical University, Department of Electronics Engineering, G. Javid Avenue, 25, Baku, Azerbaijan,

² Military Academy of the Armed Forces of Azerbaijan. Baku, Azerbaijan

³ İstanbul Esenyurt University, Department of Electrical and Electronics Engineering, Esenyurt, İstanbul Turkey

Received: November 12, 2021

Revised: September 18, 2022

Accepted: October 10, 2022

Abstract

In this study, the performance indicators of Multiservice Telecommunication Systems (MTS) based on Future Networks (FN) using Software-Defined Networking (SDN) technologies are analyzed. In SDN, the network management enables a dynamic and programmatically efficient network configuration to improve network performance and monitoring, thus making it more like cloud computing than traditional network management approach. Based on the study of MTS using the architectural concepts of Future networks, a mathematical model of SDN's is proposed. Analytical expressions have been obtained that make it possible to evaluate the indicators of service quality, information security and fault tolerance of the system in the provision of multimedia services.

Keywords: Future Networks, SDN, Reliability, Performance, Resiliency, Firewalls, Quality of Service, Open Flow Switch, Security Threat, DDoS Attack.

Özet

Bu çalışmada, SDN (Software Defined Networking, Yazılım Tanımlı Ağ Oluşturma) teknolojilerini kullanan Gelecek Yazılım ağlarına (FN, Future Networks) dayalı çok servisli telekomünikasyon sistemlerinin (Multiple System Telecom. Service, MTS) performans göstergeleri analiz edilmektedir. SDN'de ağ yönetimi, ağ performansını ve izlemeyi iyileştirmek için dinamik ve programlı olarak verimli bir ağ yapılandırması sağlar, böylece onu geleneksel ağ yönetimi yaklaşımından daha çok bulut bilişim gibi yapar. Gelecek ağlarının mimari kavramlarını kullanan MTS çalışmasına dayanarak, SDN'lerin matematiksel bir modeli önerilmiştir. Multimedya hizmetlerinin sunumunda sistemin hizmet kalitesi, bilgi güvenliği ve hata toleransı göstergelerinin değerlendirilmesini mümkün kılan analitik ifadeler elde edilmiştir.

Anahtar Kelimeler: Geleceğin Ağları, SDN, Güvenilirlik, Performans, Esneklik, Güvenlik Duvarları, Hizmet Kalitesi, Açık Akış Anahtarı, Güvenlik Tehdidi, DDoS Saldırısı.

1. INTRODUCTION

One of the important directions for achieving the goals of the digital economy in many countries is the construction of a developed unified info-communication space and a unified multi-operator environment based on the architectural concepts of Future

*Corresponding Author

E-mail: mustafaaydemir@esenyurt.edu.tr

networks, which provide modernization at a wide level of subscriber and network access networks and transport communication networks using new ICTs.

Research shows [1-3] that the info-communication support of the digital economy and the discrepancy between the capabilities of public communication networks based on NGN (Next Generation Network) led to the emergence of a fundamentally new approach to building MTS based on FN, using new technologies.

Future networks (FN), as well as NGN networks, are based on the principle of "Many multimedia services - one network", which are based on technology - SDN, virtualization of network functions and a multimedia communication subsystem IMS (IP multimedia subsystem) with the help of which a single info-communication space and a single multi-operator environment [4-7].

Based on the analysis, it has been established that among the above technologies, SDN technology occupies an important place, which implies a new approach to building MTS and organizing network interaction. Here, the control levels of the future generation network and multifunctional terminal devices for data transmission are separated, and the functions of the control levels are implemented by a separate switching node interacting with network devices [2, 8-11].

Consequently, the creation of MTS of the next generation FN based on SDN technologies requires considering the factors - the threat to information security, the quality of service (QoS) indicator and the fault tolerance of the system [4, 12-15].

In connection with the current situation, the task of developing methods of analysis and forming a correct assessment of performance indicators of future generation MTS based on SDN technologies is very urgent.

2. GENERAL STATEMENT OF THE PROBLEM AND CONSTRUCTION OF A MATHEMATICAL MODEL

Based on the study of MTS based on SDN technologies in the provision of multimedia services, it has been established that insufficient attention has been paid to the issues of ensuring information protection and guaranteed quality of service for useful and service traffic flows [1, 4-7]. In addition, in [7, 8], how non-functional requirements for the operation of MTS, methods of maintaining system fault tolerance under the influence of DDoS (Distributed Denial of Service) and DoS (Denial of Service) and ensuring the required level of system performance indicators are not precisely defined.

To solve the above problems and considering the importance of the interaction of MTS software and hardware based on the FN concept, a mathematical model (MM) of software-defined networks is proposed.

The proposed MM more accurately consider the telecommunication processes occurring in the studied MTS based on the FN architectural concept using SDN technology, which is a multi-channel queuing system (QS) of the general type $M / G / N_k / N_b$ s with some assumptions. Suppose that the incoming flow of claims to the system is a stationary Poisson flow with the parameter λ_i , the service duration of the i -th traffic has a

distribution function $B(t)$ with times $B(i)$. We assume that at the nodes of SDN networks the number of waiting places is limited to N_{buffer} storage under critical load $\rho_i \leq 1, i = \overline{1, K}$.

The mathematical formulation of the problem of the proposed MM of SDN networks for assessing the performance indicators of the MTS $D(\lambda_i)$ depending on the intensity λ_i of the incoming i -th traffic packet flow when using the architectural concept of FN is described by the following objective functions:

$$E_{performance.} = W[Argmax(D(\lambda_i)), i = \overline{1, K}], \quad (1)$$

under the following restrictions

$$E[T_{st.}(\lambda_i)] \leq T_{st.adm.}(\lambda_i), P_i(t) \leq P_{i.adm.}(t), C_{i.ap} \leq C_{i.ap.adm}, \quad i = \overline{1, K} \quad (2)$$

where $P_i(t)$ - is the probability of no-failure operation of the SDN network when servicing the i -th packet flow, $i = \overline{1, K}$; $C_{i.ap}$ - the cost of hardware and software for SDN networks, $i = \overline{1, K}$; $E[T_{st.}(\lambda_i)]$ - average stay time of the i -th packet flow in SDN networks, $i = \overline{1, K}$; $P_{i.adm.}(t)$, $C_{i.ap.adm.}$, $T_{st.adm.}(\lambda_i)$ - accordingly, the admissible value of the probability of network uptime, the cost of hardware and software, average stay time of the i -th packet flow, $i = \overline{1, K}$.

Expressions (1) and (2) define the essence of the new approach under consideration, based on which MM is proposed to assess the performance indicators of MTS based on FN using SDN technologies in the provision of multimedia services.

It should be noted that based on (1) and (2), the proposed MM of SDN networks take into account effective methods of protecting information security threats from illegal users, system fault tolerance and QoS boundary indicators of service and useful traffic packet flows. The purpose of this work is to study and analyze performance indicators of multiservice telecommunication systems using the architectural concept of FN with the use of SDN technologies in the provision of multimedia services.

3. ANALYSIS OF INFORMATION SECURITY THREATS IN SDN NETWORKS

It is known [1-4] that the studied SDN network contains the same information security risk factors that exist on traditional NGN-based communication networks. Therefore, this paper discusses the new security risks that SDN technologies bring using the OpenFlow protocols.

The rules for communication between the switch and the SDN controller are set by the OpenFlow protocol. The biggest vulnerability in the MTS network lies in the connection from the network element-SDN switch to the SDN controller. This is the main problem of all virtualization systems in general; there must be a separate channel for the transmission of service traffic. In this case, encryption of this channel is important, but not fully capable of protecting against DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks. The latter is a tool for cyberattacks and threats.

Let's say that the SDN network can be used by an attacker for DDoS / DoS attacks on the controller by sending many requests for calculating routes, which is described by the penalty function. The penalty function for DDoS / DoS attacks on an SDN network controller is expressed as follows:

$$\Phi_{p.f.}(\lambda) = \sum_{i=1}^K \alpha_i \cdot \lambda_i \cdot T_i, \quad \rho_i \leq 1, i = \overline{1, K}, \quad (3)$$

where λ_i - is the speed of the incoming i -th stream of the traffic packet, $i = \overline{1, K}$; T_i is the delay time of the i -th traffic packet flow and depends on the speed of the controller and the traffic service rule by the switch; α_i - penalty coefficient, which determines the delay time when processing the i -th packet stream, $i = \overline{1, K}$.

For the continuous functioning of the system and the security of the transmission of traffic packets streams in the nodes of SDN networks, it is necessary to use firewalls. However, the participation of firewalls in communication networks increases the traffic transmission time and the load factor of the nodes of the SDN network switch when servicing the traffic flow. Considering MM in the form of a general QS M /G/ Nk /Nbs the system load factor when servicing the i -th traffic flow is expressed as follows:

$$\rho_i = \lambda_i \cdot L_n / N_k \cdot C_{i,max} \quad i = \overline{1, K} \quad (4)$$

where L_n - is the average length of served traffic in firewalls; $C_{i,max}$ the maximum value of the network bandwidth when servicing the i -th traffic flow.

Considering the system configuration and information security risk indicators, it is possible to determine the main bottlenecks in the functioning of SDN networks using controllers and OpenFlow switches with which you can prevent possible DDoS / DoS attacks:

- Switch overload using Open-Switches.
- Exhaustion of controller resources in the SDN network.
- Routing table overflow using OpenFlow switches.

Considering the performance of the SDN network $D(\lambda_i)$ and above, the formulated main tasks for preventing possible DDoS / DoS attacks (3) will take the following form:

$$\Phi_{p.f.}(\lambda) = \sum_{i=1}^K [\alpha_i / D(\lambda_i)] \cdot \frac{\rho_i}{B(i)}, \quad \rho_i \leq 1, \quad i = \overline{1, K} \quad (5)$$

where $B(i)$ - is the transmission time of the i -th traffic packet flow and characterizes the i -th moment of traffic servicing time.

Expression (5) characterizes the indicators of information security threat in SDN networks, which can be used to prevent possible DDoS / DoS attacks. In addition, (5) determines the average queue length in SDN network nodes using controllers and OpenFlow switches, which allows to formulate optimization problems of minimizing DDoS / DoS attacks on a controller by an attacker and minimizing the average number of active SDN network nodes.

4. RESEARCH OF FAULT TOLERANCE OF FUNCTIONING OF SDN NETWORK NODES

To provide multimedia services in MTS based on the future network, it is necessary to ensure the possibility of continuous operation of the SDN network and the security of transmission of useful and service traffic, as well as the fault tolerance of the system [7].

Considering the distributed architecture of MTS using SDN technologies, in which attacks can be carried out at various points on the network boundaries, technical difficulties arise in ensuring the security of such systems. Firewalls are one way to protect SDN. The effectiveness of information protection of traffic processing centers is largely determined by the choice of means of ensuring fault tolerance of firewalls.

Consider the options for a fault-tolerant system, including N_k groups as part of firewalls, each of which serves traffic to one group of servers and is defined as follows [7, 8]:

$$P_{fire.}(t) = \prod_{i=1}^K [P_i(t)]^{N_k}, \quad i = \overline{1, K}, \quad (6)$$

where $P_i(t)$ is the uptime probability (UP) of firewall SDN networks and is expressed as follows:

$$P_i(t) = 1 - [1 - p_i(t)]^{N_k}, \quad p_i(t) = \exp(-\Lambda_i \cdot t), \quad i = \overline{1, K}, \quad (7)$$

where Λ_i - is the failure rate of level nodes (1 / s) of the input switches and firewalls, $i = \overline{1, K}$.

Expressions (6) and (7) characterize the fault tolerance of the functioning of the systems and show that an increase in the number of firewalls leads to improved performance and increased security of the next generation MTS using SDN technologies.

The main task of firewalls is to protect switching equipment from DDoS / DoS and unauthorized access. In addition, firewalls in MTS are often called traffic filters, since their main task is not to pass traffic packets that do not meet certain criteria.

The study of the influence of firewalls on the total time of the session control procedure, the estimate of the average time and the proportion of traffic filtering time in firewalls, given in the article [5], show that the participation of firewalls in the network increases the time of data transmission, but at the same time provides filtering and control of passing through it network traffic.

Consequently, the procedure for filtering useful and service traffic, considered on the example of a firewall, occurs in stages, with the participation of such units inside the firewalls as the buffer storage (BS) of the input and output interface, the ring receiving and transmitting buffer of the controller memory, the central processing unit, the operational memory [5].

5. RESEARCH AND ASSESSMENT OF PROBABILISTIC-TEMPORAL CHARACTERISTICS OF SDN NETWORKS

The investigated SDN network is presented as a queuing system (QS), which consists of three systems - BS of the input interface, BS to the ring receiving system, systems serving streams of service and payload traffic packets, and outgoing systems [5, 11, 12]. In this case, the first and second systems filter traffic packets according to the rules of firewalls.

Based on the general queuing system $M/G/N_k/N_{bs}$ under the influence of DDoS / DoS attacks on the buffer storage of the SDN controller, the probability of blocking in the switching nodes of SDN networks is calculated by [7, 11].

Expression (8) in SDN networks means that traffic packets cannot be received by the system, since the storage buffer of the SDN ne is full due to the impact of DDoS / DoS attacks.

From the general queuing system $M/G/N_k/N_{bs}$ it follows that the system is for the final queue $N_{bs} < \infty$ (due to the finite capacity of the BS system)

Thus, considering the probability P_0 , in a system with a limited queue, expression (6) takes the following form:

$$P_B = \frac{1-\rho}{1-\rho \cdot \rho^{N_{bs}}} \cdot \rho^{N_{bs}} = P_0 \cdot \rho^{N_{bs}}, \rho < 1, \tag{8}$$

One of the most important QS indicators of the general type $M/G/N_k/N_{bs}$ is the average queue length and, based on the Little formula, is determined by the following expression [9, 11]:

$$E[L_{ave.}(\lambda)] = \sum_{i=1}^{N_{bs}} (i-1)P_i = (\rho \cdot T_{at}) \cdot E[T_{exp.}] \tag{9}$$

where $E[T_{exp.}]$ - average waiting time in the queue; T_{at} - average traffic transmission time.

Figure 1 shows a graphical dependence of the average queue length in QS on the load factor of the SDN network for a given system throughput C_{max} and overhead rates.

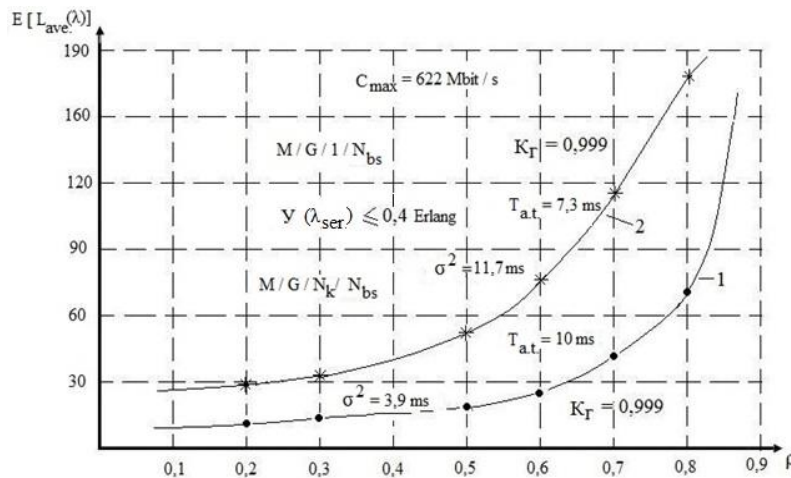


Figure 1. Graph of the dependence of the average packet queue length on the load factor of the SDN network nodes (1 - $M/G/N_k/N_{bs}$; 2 - $M/G/1/N_{bs}$).

The analysis of the graphical dependence shows that in the case of an improvement in the performance indicators of MTS, with an increase in the load factor of the SDN network, which meets the requirements of fault tolerance of the system operation and the effective use of the SDN switch and controller, leads to an increase in the average queue length in the nodes of the SDN network for a given C_{max} Mbit/s, $T_{a.t.} = (7,0, \dots, 10)$ ms, $\sigma = (3, \dots, 12)$ ms, $K_{\Gamma} = 0,999, Y(\lambda_{ser.}) \leq 0,40$ and $C_V^2 = 0,5, \dots, 1,0$. Noticeable change begins with the values $\rho \geq 0,60$.

One of the key indicators of the probabilistic temporal characteristics of SDN networks when using traffic filtering in firewalls and when establishing a multimedia session is the average time spent by packets in QS $E[T_{s.p.}(\lambda)]$. From the Polyachek-Khinchin formula, it is found as:

$$E[T_{s.p.}(\lambda)] = \frac{B^{(1)}}{1-\rho} - B^{(1)} \frac{\rho(1-C_V^2)}{2(1-\rho)} \quad (10)$$

where C_V^2 – the coefficient of variation of the packet service duration and is equal to $C_V^2 = \sigma^2 / T_{a.p.}^2$; μ^{-1} – average service time of a traffic packet; $B^{(1)}$ – the first moment in time of packet servicing.

Expressions (7)-(10) determine the probabilistic-temporal characteristics of SDN network nodes and are an indicator of the quality of service of QoS traffic packets.

As a result of the study, a formula was obtained that allows us to estimate the average service time of traffic packets of different types in the nodes of the SDN network and is the boundary indicators of the quality-of-service (QoS).

Thus, the study and system analysis of MTS based on the FN architectural concept using SDN technology show that, with their high performance, information security and fault tolerance, they should have a low system cost, which necessitates their optimization.

6. CONCLUSION

System and technical analysis of MTS based on the architectural concept of FN, MM proposed a software-defined network using firewalls in the form of QS, considering the risks of information security threats during DDoS / DoS attacks, probabilistic and temporal characteristics of useful and service traffic, and indicators of fault tolerance of the system.

As a result of MM research, analytical expressions were obtained to assess the probabilistic and temporal characteristics of SDN networks based on a switch controller using OpenFlow protocols, firewall penalty functions for filtering multimedia traffic with the necessary parameters and uptime probability of SDN network nodes, ensuring guaranteed quality of QoS services regulated by in ITU-T recommendations, Y.3000 series.

REFERENCES

- [1] R.L. Smelyanskiy, *Software-Defined Networks*, Open Systems, vol.4, 23–26 (2012).
- [2] V.A. Efimushkin and others, *The role of SDN / NFV technologies in the infrastructure of the digital economy*, Telecommunications, vol.3, 27–36 (2018).

- [3] A.V. Roslyakov, S.V. Vanyashin, Future networks, (2015), Samara.
- [4] B.G. Ibrahimov, Analysis of multiservice telecommunication networks of the next generation based on the architectural concept of SDN & NFV and IMS, (2018), Scholarly notes, vol.3. AzTU, pp.34-38.
- [5] K.E. Samuilov, A.Y. Botvinko, E.R. Zaripova, Estimating the time to establish a session between users in the presence of a firewall, (2016), RUDN Bulletin. vol.1. pp.59 – 66.
- [6] S.S. Loginov, About Control Layers in a Software Defined Network (SDN), (2017), Comm: Telecommunications and Transport. vol.11. pp.50-55.
- [7] B.G. Ibrahimov, R.T. Humbatov, A.H. Hasanov, R.F. Ibrahimov, *Cryptographic methods and means protection transmitted information in telecommunication systems*, International Journal of Electronics & Communication., **6(4)** 16 –20 (2018).
- [8] M. Romanov, Fault Tolerant Security, (2007), Storage News. vol.2, pp. 20–24.
- [9] B.G. Ibrahimov, A.H. Hasanov, Research of the quality of functioning multiservice communication networks when establishing a multimedia session, Computer and Information systems and technologies, (2021), Kharkiv, pp.55-60.
- [10] A.N. Sokolov, N.A. Sokolov, Single line queuing systems , (2010), Telecom, pp.112-116.
- [11] B.G. Ibrahimov, R.T. Gumbatov, A.A. Alieva, R.F. Approaches to the analysis of performance indicators of multiservice telecommunication networks based on SDN technology, (2021), Information Technology, vol. 27, pp. 419–424.
- [12] B.G. Ibrahimov, A.A. Alieva, F.V. Mamedova, Analysis of performance indicators of multiservice telecommunication networks based on innovative technologies, Collection of scientific articles International scientific and technical and scientific-methodical conference, Actual problems of information telecommunications in science and education., (2021), vol.1, pp.40 – 44.
- [13] D.A. Pokamestov, Ya.V. Kryukov, E.V. Rogozhnikov, S.A. Novichkov, D.A. Lakontsev, Model for estimating the throughput of 5G NR backhaul networks, Comm: Telecommunications and Transport. vol. 15, (2021), pp. 11-16.
- [14] A. S. Tanenbaum, H. Bos, Modern Operating Systems, 2015, Pearson.
- [15] G. Weiss, Scheduling and Control of Queueing Networks, 2021, Cambridge University Press.

To Cite This Article: B. G. Ibrahimov et. al, *Performance of Multi-Service Telecommunication Systems Using the Architectural Concept of Future Networks*, Journal of Aeronautics and Space Technologies **16(1)**, 41-49 (2023).

VITAE

Bayram Ganimatoglu Ibrahimov is Professor of the Department of Telecommunications and Information Security at the Azerbaijan Technical University in Baku. He holds a PhD in Telecommunication Systems, Networks and Devices. His research interests are in the areas of theoretical foundations of telecommunications, queuing theory, multiservice communication networks, optical telecommunication technologies, and information security. He has published a number of research papers in peer-reviewed international journals such as T-Comm, Telecommunications and Transport, Herald of Computer and

Information Technologies, International Journal of Engineering Sciences & Research Technology, American Journal of Networks and Communications, International Journal of Electronics & Communication”, “Automatic Control and Computer Sciences”. He is a member of the editorial board of the journal "T-Comm, Telecommunications and Transport" of the Moscow Technical University of Communications and Informatics and the journal "Reliability and Quality of Complex Systems" of the Penza State Technical University.

Yalchin Sabiroglu Isayev is Head of the Department of Air Defense of the Azerbaijan Military School named after Heydar Aliyev in the city of Baku. He holds an associate professor's degree in military science and homeland security, as well as bachelor's and master's degrees in radio engineering and telecommunications. His research interests are in the areas of theoretical foundations of telecommunications, queuing theory, multiservice communication networks, optical telecommunication technologies, and information security. He has published several research papers in peer-reviewed international journals such as "T-Comm, Telecommunications and Transport", "Bulletin of Computer and Information Technologies"

Mustafa Emre Aydemir is a full time Professor of Electrical and Electronics Engineering at Istanbul Esenyurt University. He holds a PhD degree in Electromagnetic Compatibility from Istanbul Technical University. His research interests are optimization and embedded systems. He has published several research papers in refereed international journals such as “International Journal of Electronics and Communications” and “Turkish Journal of Electrical Engineering & Computer Sciences”