UDC 004.77

DEVELOPMENT OF A METHOD FOR STUDYING TRAFFIC OF MULTISERVICE NETWORKS

Morkun V. S. – Dr. Sc., Professor, Professor at the University of Bayreuth, Bayreuth, Germany.

Hryshchenko S. M. – PhD, Senior Researcher in the Specialty Automation and Computer-Integrated Technologies State Tax University, Irpin, Ukraine.

Nizhehorodtsev V. O. – PhD, Senior Researcher in the Specialty Automation and Computer-Integrated Technologies State Tax University, Irpin, Ukraine.

Filonenko M. M. – PhD, Associate Professor Head of the Department Computer and Information Technology and Systems, State Tax University, Irpin, Ukraine.

Lagovsky V. V. – PhD, Associate Professor of the Department of Computer and Information Technologies and Systems, Head of Department Cybernetics and Applied Mathematics State Tax University, Irpin, Ukraine.

ABSTRACT

Context. The constant growth in the volume of information, the increase in the speed of information flows in digital communication networks, as before, makes the task of assessing the service stability for traffic flows an urgent one. A simple solution to ensure high service stability is to build a network of sufficient capacity for any traffic that will be thrown at it. To solve the problems of analyzing telecommunication systems, it is necessary to have appropriate models and engineering methods that allow to assess the service stability and predict the characteristics of their operation based on measurement data. In these conditions, the development of new methods for analyzing the traffic of multiservice networks that provide simplicity of calculations and their acceptable accuracy becomes especially relevant.

Objective. The purpose of this paper is to study the traffic and service stability for users.

Method. We propose a hybrid method for detecting anomalies in multiservice network traffic that uses algorithms without identification, adaptation and Mamdani fuzzy inference. The peculiarity of multiservice traffic as an object for assessing the existence of anomalies is the presence of stochastic processes in it subject to different distribution laws. For the experimental evaluation of the proposed method and algorithms, we have chosen the Poisson and Pareto distribution laws that define the limiting cases of traffic regularity. The method allows for monitoring and managing faults in a multiservice network in order to determine the causes of their occurrence. The following requirements are imposed on the developed algorithms for detecting anomalies in the traffic on multiservice networks: functioning in real or near real time; maintaining a given service stability; simplicity of implementation. The algorithms belong to the class of adaptive hybrid algorithms for identifying traffic parameters. They are used for both stationary and non-stationary traffic. Traffic is modeled as stochastic processes. Each belongs to the corresponding class, which is determined by the law of distribution of stochastic processes.

Results. Experimental evaluation of the proposed method and algorithms has shown that they allow us to estimate the trends of these stochastic processes in real time, with high accuracy and while maintaining the service stability.

Conclusions. The application of the developed method of troubleshooting management in a multiservice environment helps to improve the service stability by timely detecting problems, reducing the time of their elimination and reducing downtime, which, in turn, affects the increase in service reliability.

KEYWORDS: multiservice networks, traffic, quality, faults, method, user.

ABBREVIATIONS

MSN – multiservice networks;
SP – stochastic processes;
MSA – modified stochastic Approximation;
PGP – pseudogradient procedures.

NOMENCLATURE

a_0 – random process of average value;
σ – standard deviation;
μ – parameter;
Si – average value of traffic intensity at a given time *i*;
m_0 – initial value of the trend average;
ρ – trend correlation coefficient;
r – size of the sliding window;
R – the value of the linguistic variable assessed by the presence of anomalies;
N – sample size;
S_i – element *i* at the polls;
μ_i – algorithm parameter in the step *i*;
$M\{*\}$ – unction for calculating the mathematical expectation;
A – fuzzy threshold values determined during the training of the fuzzy inference system;
B – fuzzy threshold values determined during the training of the fuzzy inference system;
D – fuzzy threshold values determined during the training of the fuzzy inference system.

INTRODUCTION

The current level of development of the information society and intellectual spheres of human activity in modern society is based on the use of digital and telecommunication technologies. An analysis of recent research and publications on the subject shows that the use of modern information technologies has been studied by Morkun V. S., Hryshchenko S. M., Kravchenko O. M. [1–3], Leland W. E. [4] and other scientists. The constant growth in information volume and the increase in the speed of information flows digital communication networks still

DOI 10.15588/1607-3274-2023-2-13

make it an urgent task to assess the service stability of traffic flows. The task of modern telecommunication systems is to ensure a given level of service quality.

The continuous improvement of the telecommunications industry has changed both the pricing policy and the overall reduction of the data transmission load. To solve the problems of analyzing telecommunication systems, it is necessary to have appropriate models and engineering methods that allow to assess the service stability provision and predict the characteristics of their operation based on measurement data.

In these conditions, the development of new methods for analyzing the traffic of multiservice networks that ensure simplicity of calculations and their acceptable accuracy becomes especially relevant.

In packet-based multiservice communication networks, packet flows (traffic) differ significantly from the Poisson flow model, which is described by an exponential distribution function of the time interval between the arrival times of neighboring packets. Here, packet flows are formed by many different sources of requests for services provided by the network and network applications that provide video, data, broadcasting, etc. The request sources involved in the process of creating a packet stream differ significantly in their specific load intensity. The load intensity of the resulting packet stream at any given time depends on which applications are served by the request sources and the ratio of their number on different applications. The traffic structure is also affected by the technical and technological features of the service algorithms. If, for example, the service is provided by several applications, or if the protocols use retransmission of incorrectly received packets, the moments when requests for establishing communication sessions occur are highly correlated. As a result, the outgoing flows undergo significant changes during the service process and long-term dependencies in the intensity of packet arrivals appear in the final traffic. Customers are demanding more reliable performance guarantees from the network. In particular, multimedia applications often require minimal bandwidth and maximum latency to process products. The quality, reliability, and accuracy of services are the signs of control.

This is an area in which the Internet is going through a long period of renewal.

A simple solution to ensure high service stability is to build a network with enough capacity for any traffic that will be thrown at it. The name of this solution is redundant provisioning. The resulting network will carry application traffic without significant loss and, with a decent routing scheme, deliver packets with low latency. Performance doesn't get any better than that.

The object of study – is the traffic on multiservice networks.

The subject of study – multiservice networks based on the analysis of the distribution of the number of applications. To achieve this goal, the following research methods were used:

– Analysis of different views of scientists on the problem under study; –To study the state of its development; – structural and functional – To identify and characterize models and engineering methods; – Comparison – to identify the quality characteristics of service quality assurance, generalization – to determine the state of traffic research and quality assurance for users.

The purpose of the work traffic and the quality of user experience.

1 PROBLEM STATEMENT

The requirements of modern multiservice networks are constantly growing today, due to the fact that the life of a modern person is increasingly "merging" with the global Internet.

Multiservice networks allow us to receive a large number of services (IPTV, VoIP, video on demand, social networks, corporate networks, etc.) using a common infrastructure.

The development of modern multiservice computer networks is an important issue of modern society: first, multiservice computer networks are a necessary factor for human access to modern technologies that greatly facilitate life, and second, the development of multiservice networks is an important component of economic development both at the level of an individual enterprise and at the state level.

Multiservice networks have an advantage over customers in realizing the following important functions, namely:

– Provide high-quality data transmission;

– Efficient use of the bandwidth of the existing backbone communication channels;

– Building a secure data transmission scheme;

– Implementation of a unified management system for all departments and branches;

– Organizing a system of redundant data transmission channels and Internet access;

– Information resources management and centralized monitoring;

– Creation of a unified telephone network with a single address space;

– Introduction of new corporate services and applications;

– Implementation of a unified administrative and technical policy in the field of information exchange;

– Eliminating duplication of functions and increasing employee productivity and reducing costs for all communication channels;

– Increasing the organization's competitiveness;

– Increase in employee productivity.

To verify the efficiency and accuracy requirements of the proposed method and algorithm, we use as a testbed. Traffic anomalies are evaluated and identified. The A, B, and D were determined pre-variously based on the training results. The random process had an a_0=100 and σ=10. The ρ for different dependencies varied from 0.6 to 0.9999. It can be seen that at small values of the error μ, traffic estimates differ greatly from each other depending

DOI 10.15588/1607-3274-2023-2-13

on the value ρ. At large values of μ, these errors become approximately equal. The rules for setting the parameters of the modified stochastic approximation are formed. For example, when S_i = 100, σ=10 and ρ = 0.9999, the stochastic algorithm parameter is approximately 0.025. For ρ = 0.99, the parameter μ will have a value of approximately 0.12. The parameters σ and ρ are estimated in a sliding window. The correlation coefficient of the process variables in the experiments from 0.9 to 0.99999. The SP had the following parameters: initial value of the trend mean m_0 500, ρ = 0.99, size of the sliding window r = 10, μ = 0.05, σ = 100. Thus, it is necessary to verify that the proposed algorithm works almost without delays and has a high estimation accuracy. The relative error of the algorithms is 12% of the true trend value. This is a result that should be considered within the normal range, given that the algorithms work in real time, since the values obtained for the detection time range from 15 to 80 time samples. At the final stage, the developed algorithms for detecting anomalies in the traffic on multiservice networks should fully meet the requirements of efficiency and accuracy. The task of developing a method for studying the traffic of multiservice networks is considered in this article.

2 2 REVIEW OF THE LITERATURE

At the same time, there are a number of works [4–11], in which separate attempts have been made to apply methods of fuzzy knowledge processing for modeling and estimation of network traffic. However, the direct application of the results obtained in these works is not possible for MSN. This is due to the fact that the statistical properties of traffic in MSN are very different both for different operating conditions, The reason is that the statistical properties of traffic differ greatly from one operating condition to another and from one application to another in the MSN. We need an approach that provides the network with this quality in real time and can be implemented quite easily.

Various approaches to building multiservice networks and traffic analysis are reflected in the works of foreign authors Leland W. E. [4], Kosenko V., Persiyanova E., Belotskyi O., Maleieva O. [5], Kosenko V, Bugas D. [6], Xi N., Sun C., Ma J., Shen Y. [7] etc.

Controlling network operation and eliminating congestion are all part of ensuring that the required level of network quality reliability is maintained. In the absence of adequate models of network traffic, the Poisson model is often simplified for analysis and synthesis, and with a significant loss of accuracy. Forms of estimating queue sizes that were previously used are suitable exclusively for Poisson flows, and, when calculating traffic, give errors exceeding 100–200%.

Observing the flow of traffic is called traffic policy (policing and shaping).

The increase in the volume of services provided leads to the need for rapid network reorganization, the emergence of new subscribers and load redistribution. All of this necessitates a quick assessment of the required bandwidth of access interfaces.

The telecommunications community has many different definitions of MSN.

Let's consider some of them, emphasizing the shortcomings: these are networks that provide more than one service – in fact, a literal interpretation (from the simple translation of "multi" – many, "service" – service, i.e. networks that provide "many services" or, more precisely, many types of them), but at the same time quite broad, which does not allow to formulate a precise definition:

– modern transmission networks – a vague definition (it is unclear what "modern" means in this context);

– broadband transmission networks – intuitively reflects the essence of the issue, but has a number of systemic shortcomings;

– next generation communication networks (NGN – Next Generation Networks);

– networks ready to provide any telecommunications and information services.

An integral telecommunications infrastructure that has sufficient resources to support all forms of information exchange performed for the benefit of a provider or consumer of various services.

The various definitions above contain a number of shortcomings – there is none that can be considered complete and reflects the essence of the issue. Therefore, the following wording is proposed as a definition of the concept of "multiservice network": a multiservice communication network is a single telecommunications infrastructure for transferring, switching traffic of any type generated by the interaction of con-summer's and providers of communication services with controlled and guaranteed traffic parameters. This network should guarantee the specified quality of connections and services provided.

A multiservice network is an integrated telecommunications infrastructure that has sufficient resources to provide all forms of information exchange performed in the area of supplier or consumer of various services.

Modern multiservice networks can provide the following services:

1. Voice transmission based on IP telephony using IP telephones and personal computers connected to the public telephone network.

2. Videotelephony between two or more users based on an Ethernet network, which allows simultaneous transmission of audio and video information using personal computers equipped with special hardware and software.

3. Access to the databases, operating within the MSN.

4. Access to file server resources, which usually have a large amount of disk space, can store heterogeneous information and are designed to perform input and output operations. Access to file servers is regulated by the MSN administrator and may be restricted for external users.

5. A web server through which MSN users can host their own resources available to external users.

6. Access to the Internet.

DOI 10.15588/1607-3274-2023-2-13

7. An email server that is connected to the Internet and allows MSN users to interact with it using email client programs and transmit information both within and outside of MSN.

3 MATERIALS AND METHODS

Traffic refers to a digital data stream containing various types of messages that are received by the human senses (usually audio and/or video information). Data streams are transmitted over telecommunication networks to provide remote interactive services. The most common multimedia services provided to network users today are: video telephony, high-speed multimedia data transmission, IP telephony, digital television broadcasting, mobile video communications and digital video on demand.

Depending on the type of service provided, there are two main categories of traffic.

1. Real-time traffic that provides multimedia services for the transmission of information between users in real time.

2. Ordinary data traffic generated by traditional distributed services of a modern telecommunications network, such as email, file transfer, virtual terminal, remote access to databases, etc.

Examples of services that generate real-time traffic include: IP telephony, high-quality sound, videotelephony, video conferencing, remote medical services (diagnostics, monitoring, consultation), video monitoring, broadcast video, digital television, broadcasting radio and television programs.

The description and analysis of multimedia traffic in modern telecommunication networks are a complex and difficult task. The main reasons for these difficulties are

– a wide range of transmission speeds – from several Kbit/s, as in the case of telephone traffic, to hundreds of Mbit/s, when transmitting video streams;

– various statistical properties of the transmitted multimedia information flows (real-time traffic imposes strict requirements on network resources);

– a wide variety of network configurations, many technologies and transmission protocols (Gigabit Ethernet, etc.)

– multi-level processing of transmitted messages, which makes the service stability dependent on several levels of processing.

Traffic in the MSN consists of the following components: 1) multimedia traffic, which is very sensitive to delays; 2) data traffic; 3) signal information traffic; 4) e-mail traffic. In this case, the specified requirements for the service stability must be fully met. However, there are objective difficulties in the construction of the MSN control system and in the protection of network and subscriber information. These problems are caused by the complexity of the MSN structure, the diversity of the network, and the need to look at a lot of different network and information parameters. Therefore, prompt detection of network traffic anomalies is one of the key objectives of MSN management.

This article considers a new approach to traffic anomaly detection in MSN, based on the application of fuzzy logical inference. Approach to traffic anomaly detection in MSS, based on the application of fuzzy logical inference. The rules of such inference are used together with modified Identity-free algorithms.

The main theoretical contribution of the paper is are as follows. First, it substantiates a model of multiservice traffic is substantiated. Second, it provides methods and algorithms for detecting of traffic anomalies in the MSN, based on the application of fuzzy logical inference. Finally, it has been experimentally proved that the proposed algorithms The proposed algorithms have practically maximal possible speed of operation.

To develop methods for detecting anomalies in MSN traffic, we propose to develop a model of multi-service traffic. The MSN traffic model is a combination of many stochastic processes. The proposed approach to the formation of a multiservice traffic model is based on the following factors: SP distribution laws; SP stationarity; SP self-similarity; characteristics selected for SP analysis. Different distribution laws are used to model different types of traffic. For example, if the modeled traffic is “Audio” or “Video”, then it gives the effect of self-similarity, and the Pareto distribution is used to model it. If the modeled traffic is generated by SMTP/TCP protocols, then the Poisson distribution or exponential distribution is used. An important factor is stationarity and non-stationarity, it is better to solve the problem of detecting anomalies in traffic if it is stationary. It is better to analyze traffic using various characteristics of a random process. Such characteristics are the maximum, minimum, and average values of the process intensity, standard deviation, etc. The average value of the process intensity is calculated using the formula:

$$S_{mid} = \frac{1}{N}\sum_{i=1}^{N} S_i. \qquad (1)$$

The following requirements are imposed on the developed algorithms for detecting anomalies in MSN traffic: functioning in real or near real time; maintaining a given service stability; and ease of implementation. The algorithms belong to the class of adaptive hybrid algorithms for identifying traffic parameters. They are used for both stationary and non-stationary traffic. Traffic is modeled in the form of SP. Each SP belongs to the corresponding class, which is determined by the SP distribution law.

The essence of the hybrid method for detecting anomalies in MSN traffic is that, on the one hand, algorithms are used without identifying adaptation to changing SP parameters. On the other hand, fuzzy inference is used to adjust algorithm parameters and make decisions.

The use of this hybrid approach is due to the need to estimate both current point and integral traffic parameters. Estimation of integral traffic parameters is performed in a sliding window. The estimation of current point parameters is performed from point to point simultaneously with

DOI 10.15588/1607-3274-2023-2-13

the integral estimation procedure. In this case, the estimates obtained in the sliding window are used as initial values for the unidentified procedure. To perform this procedure, two algorithms are used that differ in their capabilities for SP approximation. The combination of these approaches allows both to estimate the integral properties of the SP and to track the dynamics of its behavior.

The use of fuzzy inference allows us to build parametric estimates of the algorithm parameters from a small number of observations. In this case, it becomes possible to draw fuzzy conclusions about traffic anomalies.

Let SP be given in discrete time values $ti=i$, $i=1, 2, \ldots$. The first algorithm is the algorithm MSA:

$$S_{i+1} = S_{i-1}\mu_i(S_i - S_{i-1}). \quad (2)$$

The second algorithm is used when the probability density of SP values is symmetric. It is based on the use of PGP of the form

$$S_{i+1} = S_{i-1} + \mu_i sign(S_i - S_{i-1}). \quad (3)$$

This choice of the first and second algorithms provides an assessment of the dynamic properties of the SP. Since the MSA and PGP algorithms belong to the class of non-identifying algorithms, the time for traffic analysis and anomaly detection is significantly reduced. The quadratic function in the form of:

$$M\left\{(S_1 - S_{i-1})^2\right\} \quad (4)$$

Parameter μ_i for MSA и PGP must meet the following conditions:

$$0 < \mu_1 < 1, \mu_i = \text{const}. \quad (5)$$

The peculiarity of the MSA and PGP algorithms is the fact that it is necessary to adjust the value of the μ_i for different SP being evaluated and their statistical properties. It is proposed that the procedure for adjusting these algorithms should be based on the Mamdani fuzzy inference method, according to which the identification of the parameters of the MSA and PGP algorithms is carried out using rules that have the following form in general:

$$\begin{aligned} &IF < S_i = A > AND < \sigma = B > AND \\ &< \rho = D > THEN \mu = R. \end{aligned} \quad (6)$$

The identification of anomalies in the MSN traffic is carried out on the basis of fuzzy inference of the following type:

$$\begin{aligned} &IF < S_i = A > AND, \\ &< \text{A complies with the sec} \overrightarrow{\leftarrow} \text{urity policy} > \\ &\text{THEN } R. \end{aligned} \quad (7)$$

To perform the anomaly identification procedure, it is necessary to first train the fuzzy inference system with experimental data. The experimental data is generated in advance.

When choosing the size of the sliding window, a reasonable compromise must be found between the rate of change of SP values, the size of the window, and the representativeness of the sample of SP values. This compromise is necessary to eliminate the effect of excessive smoothing of SP values.

Summarizing the nature of traffic behavior in the MSN is also based on the Mamdani method.

4 EXPERIMENTS

To experimentally test the proposed method and algorithm, we used an instrumented testbed. The testbed consists of a server and two workstations connected to a network using a router. The testbed is shown in Fig. 1.

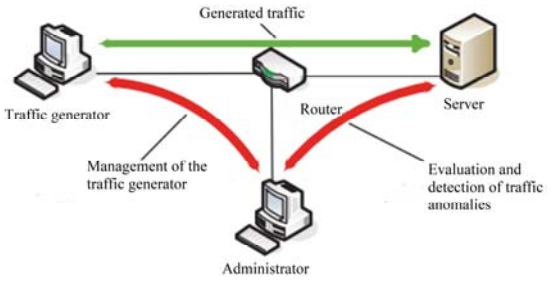

Figure 1 – Structure of the tool stand

One workstation was a traffic generator. The second station was the network administrator. The network administrator controlled the generator. The generator generated traffic with a given distribution law. At the same time, anomalies were introduced into the traffic randomly in accordance with the selected type of computer attack. The traffic passed through the router to the server. The administrator's task was to evaluate and identify traffic anomalies.

The generator generated stationary and non-stationary traffic Poisson and Pareto distributions. These distributions are the most typical for MSN. To generate anomalies, DoS attacks were used, which lead to a load on the communication channel. Non-stationary processes were modeled as multiplicative SP with deterministic and random modulating functions. The random modulating functions were first-order random autoregressive processes with different correlation coefficients. Adaptation to the parameters of the Poisson SP was performed using the MSA algorithm.) For SP with Pareto law, the algorithm of pseudogradient procedures was used.

The parameters of the adaptation algorithms were set using the following rules. The A, B, and D of these rules were determined in advance based on the training results. For this purpose, we used the experimental results presented in Fig. 2, which show the dependence of the value of the error in estimating the traffic intensity of a nonstationary SP on the value of the step coefficient of the MSA algorithm at different values of the correlation coefficient modulating the SP for Poisson traffic. The random proc-

DOI 10.15588/1607-3274-2023-2-13

ess had a_0=100, σ=10. P for different dependencies varied from 0.6 to 0.9999. It can be seen that at small values of the error μ, traffic estimates differ greatly from each other depending on the value of ρ.

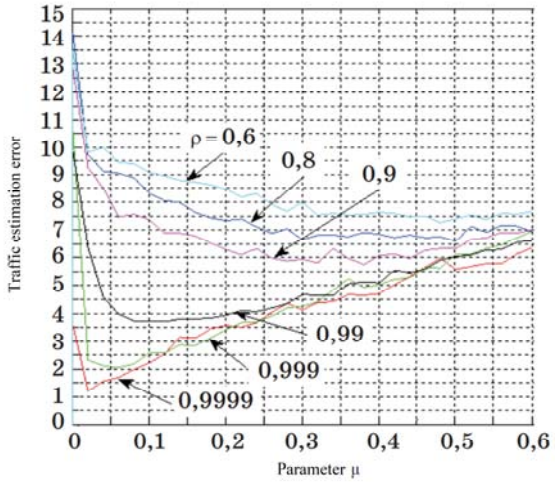

Figure 2 – Dependence of traffic estimation error on the value of the parameter

The traffic estimation error is represented vertically, and the μ is represented horizontally.

At large values of μ, these errors become approximately equal.

Based on the data presented in Fig. 2. the rules for setting the parameters of the modified stochastic approximation are formed. For example, at S_i = 100, σ=10 та ρ=0.9999 the parameter of the stochastic algorithm is approximately equal to 0.025. For ρ=0,99 the μ will have a value of approximately 0.12. The parameters σ and ρ are estimated in a sliding window.

An example of numerical modeling of an unsteady Poisson SP was analyzed in their works by scientists Ageev S. O., Sayenko I. B., Kotenko I. V. This example is shown in Fig. 3.

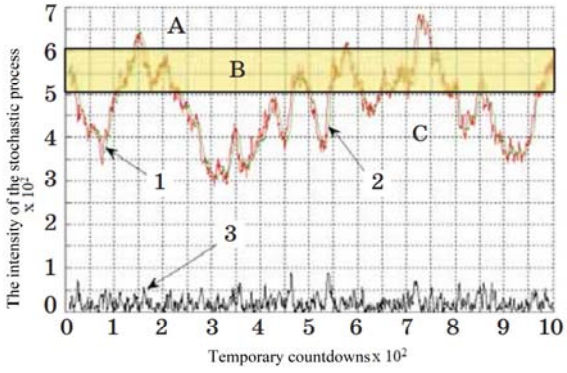

Figure 3 – Estimation of a non-stationary trend with a Poisson distribution:
1 – true trend value; 2 – trend estimate;
3 – error of trend estimate

The correlation coefficient of the process varied across experiments from 0.9 to 0.99999. SP had the following parameters: initial value of the trend mean m_0 500, ρ = 0.99, size of the sliding window r = 10, μ = 0.05, σ = 100. The proposed algorithm works almost without delays and has high estimation accuracy.

There are three zones associated with anomaly detection: Zone A indicates that there is a risk of anomalies and the risk level is unacceptable. Zone B indicates that there is a risk of anomalies and the level of risk is acceptable. There are no anomalies in the traffic located in zone C. The boundaries of zones A, B, and C is determined at the stage of pre-configuring the knowledge base of the fuzzy inference machine in accordance with the accepted security policy rules. The values of the trend estimates on the boundaries of zones A, B, and C are used to build the Mamdani rules using formula (8):

$$IF < S_1 = A > AND,$$
$$< \text{A complies with the security policy} > \text{THEN } R \qquad (8)$$

For example, the rule for concluding that there are no anomalies is as follows:

$$IF < S_i \in Zone\ C > \text{THEN}.$$

There are no traffic anomalies.

The results of estimating the parameters (Table 1) of self-similar traffic with a Pareto distribution are shown in Fig. 4 and Fig. 5.

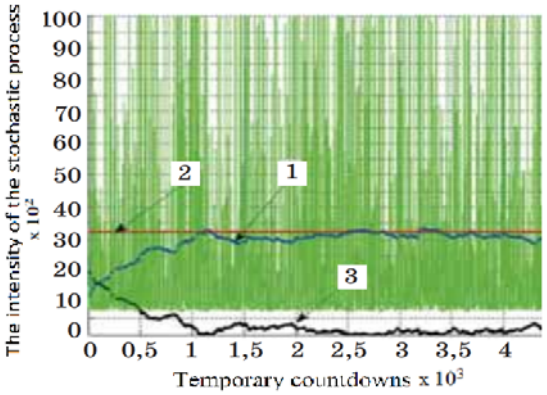

Figure 4 – Estimation of the stationary trend of self-similar traffic with distribution

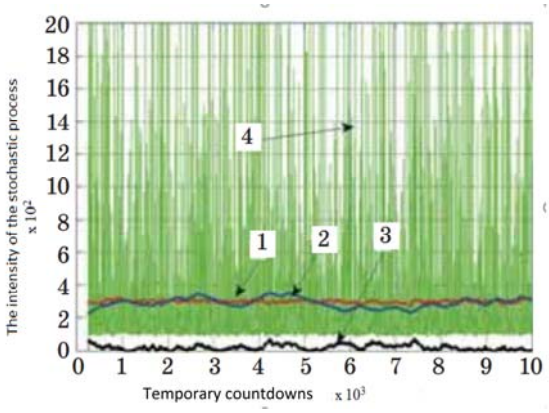

Figure 5 – Estimation of non-stationary trend of self-similar traffic with distribution

DOI 10.15588/1607-3274-2023-2-13

Table 1 – Parameters of steady-state and non-stationary process

Parameter	Stationary process	Non-stationary pr	Stationary process
Hearst parameter, H	0.85	0.75	0.85
The average value of the SP	32.5	250	32.5
Distribution parameter SP	1.3	–	1.3
Parameter of the MSN algorithm μ	0.004	0.13	0.004
Relative error of estimation, %	≤6.2	≤9.1	≤6.2

The final results of the evaluation of the developed algorithms for detecting anomalies in the traffic of the MSN for the distributions discussed above are shown in Table 2.

Table 2 – Experimental results of the algorithm evaluation

Distribution	Correlation coefficient, ρ	Average relative error of the estimate, %	Time of detection, time counts
Pareto (H 0.75)	0.99	12.0	80
	0.999	10.0	65
	0.9999	8.0	50
Poisson	0.99	8.6	27
	0.999	7.6	20
	0.9999	5.3	15

This table shows that the relative error of the algorithms is within 12% of the true trend value. This result should be considered within the normal range, given that the algorithms operate in real time, since the values obtained for the detection time range from 15 to 80 time samples. Thus, the developed algorithms for detecting anomalies in MSN traffic fully meet the requirements of efficiency and accuracy.

5 RESULTS

Different enterprises experience different types of malfunctions over time. They are primarily caused by significant losses incurred by operators due to downtime or inefficient use of network resources. Secondly, the functioning of the network depends heavily on the algorithms of the application software used in it. The term "network" here refers to the entire complex of hardware and software; and the term "network diagnostics" refers to the process of determining the causes of unsatisfactory operation of application software in this network. It is the quality of the application software in the network that is decisive from the point of view of users [8–11]. Other criteria, such as the number of data transmission errors, the degree of network resource utilization, hardware performance, etc., are secondary.

There can be several main reasons for unsatisfactory operation of application software in the network:

– damage to the cable system;

– defects in active equipment;

– overloading of network resources (communication channel and server);

– errors in the application software itself.

Often, some network defects mask others.

Thus, to reliably determine the cause of unsatisfactory operation of the application software.

Often, a network is analyzed only during periods of poor performance. In such cases, it is necessary to localize and correct existing network defects quickly. In this paper, we focus on the diagnostics of the network link layer, as this is the primary task when diagnosing a transmission network.

6 DISCUSSION

Analyzing the above, we note that a hybrid method for detecting anomalies in the MSN traffic using algorithms without identification, adaptation and fuzzy Mamdani inference is proposed. The peculiarity of multiservice traffic as an object of anomaly detection is the presence of stochastic processes in it, subject to different distribution laws. For the experimental evaluation of the proposed method and algorithms, we chose the Poisson and Pareto distribution laws that define the limiting cases of traffic regularity.

Experimental evaluation of the proposed method and algorithms has shown that they allow estimating the trends of these stochastic processes in real time, with high accuracy and with preservation of service quality.

Summarizing these situations that arise at many enterprises regarding troubleshooting, it should be noted in general that they consist of eight steps:

1. Definition of the problem;
2. Collecting the necessary information;
3. Evaluation of possible scenarios for solving the problem and determining the most likely causes of the malfunction;
4. Developing a plan for solving the problem;
5. Implementation of actions in accordance with the plan;
6. Evaluation of the results;
7. Repeating the sequence of steps if the malfunction were not eliminated;
8. Documenting the changes after successful troubleshooting.

The method allows you to monitor and manage faults in a multiservice network to determine the causes of their occurrence.

CONCLUSIONS

Summarizing the above, it is worth noting that the application of the developed method of troubleshooting management in a multiservice network helps to improve the service stability by timely detection of problems, reducing the time of their elimination and reducing downtime, which in turn affects the increase in service reliability.

The scientific novelty lies in the fact that for the first time, a method has been developed for traffic management problems and applied to traffic management tasks based on the analysis of the distribution of the number of

DOI 10.15588/1607-3274-2023-2-13

traffic management requests, which allows improving the service stability in multiservice networks.

The practical significance is that it is proposed to apply the development of the method to traffic management tasks at enterprises based on the analysis of the distribution of the number of applications.

Prospects for further research is to study and apply in practice methods to improve the service stability and reliability of services for users.

ACKNOWLEDGEMENTS

The work was carried out within the framework of the research topic of the State Tax University "The use of intellectual technologies in the analysis of economic risks of the regions of Ukraine and V4 countries" (state registration number 0121U114593).

REFERENCES

1. Morkun V. S., Morkun N. V., Hryshchenko S. M., Tron' V. V. Sintez zashemostijkogo algoritmu dlja adaptivnogo keruvannja rudozbagachennjam, *Radio Electronics, Computer Science, Control,* 2018, №3, pp. 183–190. https://doi.org/10.15588/1607-3274-2018-3-20
2. Morkun V., Kravchenko O. Trivimirnij nechitkij kontrol' ul'trazvukovogo ochishhennja, *Acta Mechanica et Automatica*, 2021, 15 (3), pp. 169–176. https://doi.org/10.2478/ama-2021-0022.
3. Morkun V., Kravchenko O. Kontrol' procesu prostorovogo ul'-trazvukovogo ochishhennja na osnovi ocinki jogo potochnogo stanu, *Druga mizhnarodna konferencija zi stalogo majbutn'ogo: ekologichni, tehnologichni, social'ni ta ekonomichni pitannja (ICSF 2021), E3S Web of Conferences 280* , 07016, 2021. https://doi.org/10.1051/e3sconf/202128007016.
4. Leland W. E., Taqqu M. S., Willinger W., and Wilson D. V. Metod for processing multiservice traffic in network node based on adaptive management of buffer resource, *On the Self-Similar Nature of Ethernet Traffic (Extended Version): IEEE/ACM Transactions on Networking,* 1994, № 2, pp. 1–15. DOI: http://dx.doi.org/10.1109/90.282603
5. Kosenko V., Persijanova Ye., Bieloc'kij O. Malieieva Metodi upravlinnja rozpodilom trafiku v informacijno-komunikacijnih merezhah sistem kritichnoї infrastrukturi, *Innovacijni tehnologiї ta naukovi rishennja dlja promislovosti*, 2017, № 2 (2), pp. 48–55. DOI: 10.30837/2522-9818.2017.2.048
6. Kosenko V., Bugas D. Effectiveness analysis of resource usage of multiservice information and telecommunication network, *Technology audit and production reserves*, 2015, Vol. 5, No. 2 (25), pp. 19–23. DOI: 10.15587/2312-8372.2015.51710
7. Xi N., Sun C., Ma J., Shen Y. Secure service composition with information flow control in service clouds, *Future Generation Computer Systems*, 2015, Vol. 49, pp. 142–148. DOI: 10.1016/j.future.2014.12.009
8. Mangili M. Martignon F., Capone A. Optimal design of Information Centric Networks Original, *Computer Networks*, 2015, Vol. 91, pp. 638–653. DOI: 10.1016/j.comnet.2015.09.003
9. Wang H., Zhang D., Shin K. G. Detecting SYN Flooding Attacks, *Proc. of IEEE INFOCOM. 2002. International Conference on Mobile Ad-Hoc and Sensor Networks MSN* 2005, Mobile Ad-hoc and Sensor Networks, 2005, pp. 443–452. DOI: 10.1007/11599463_44
10. Angrishi K. An end-to-end stochastic network calculus with effective bandwidth and effective capacity, *Computer Networks*, 2013, Vol. 57. Issue 1, pp. 78–84. DOI: 10.1016/j.comnet.2012.09.003
11. Agrawal S., Agrawal J. Survey on Anomaly Detection using Data Mining Techniques, *Procedia Computer Science*, 2015, Vol. 60, pp. 708–713 DOI: https://doi.org/10.1016/j.procs.2015.08.220

Received 15.02.2023.
Accepted 27.04.2023.

УДК 004.77

РОЗРОБКА МЕТОДУ ДОСЛІДЖЕННЯ ТРАФІКУ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Моркун В. С. – д-р техн. наук, професор, професор Байройтського університету, Байрот, Германія.

Грищенко С. М. – канд. пед. наук, старший дослідник, доцент кафедри комп'ютерних та інформаційних технологій і систем Державного податкового університету, Ірпінь, Україна.

Ніжегородцев В. О. – канд. пед. наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем Державного податкового університету, Ірпінь, Україна.

Філоненко М. М. – канд. фіз.-мат., наук, доцент. зав. кафедри комп'ютерних та інформаційних технологій і систем Державного податкового університету, Ірпінь, Україна.

Лаговський В. В. – канд. економ. наук, доц. зав. кафедри кібернетики та прикладної математики Державного податкового університету, Ірпінь, Україна.

АНОТАЦІЯ

Актуальність. Постійне зростання обсягу інформації, збільшення швидкості передачі інформаційних потоків у цифрових мережах зв'язку, як і раніше, залишається актуальним завдання оцінки якості обслуговування потоків трафіку. Простим рішенням для забезпечення високої якості обслуговування є побудова мережі достатньої потужності для будь-якого трафіку, який буде кинутий на нього. Для розв'язання проблем аналізу телекомунікаційних систем необхідно мати у своєму розпорядженні відповідні моделі та інженерні методи, що дозволяють на основі даних вимірювань оцінювати якість надання послуг та прогнозувати характеристики їх роботи. У цих умовах розробка нових методів аналізу трафіку мультисервісних мереж, що забезпечують простоту розрахунків та їхню прийнятну точність, стає особливо актуальною.

Мета роботи полягає в дослідженні трафіку та якості забезпечення для користувачів.

Метод. Запропоновано гібридний метод виявлення аномалій у трафіку мультисервісних мереж, що використовує алгоритми без ідентифікаційної адаптації та нечіткого виведення Мамдані. Особливістю мультисервісного трафіку як об'єкту оцінювання існування аномалій є наявність у ньому стохастичних процесів, підпорядкованих різним законам розподілу. Для експериментальної оцінки запропонованих методу та алгоритмів було обрано закони розподілу Пуассона та Парето, що

DOI 10.15588/1607-3274-2023-2-13

визначають граничні випадки регулярності трафіку. Метод дозволяє забезпечити контроль та управління несправностями в мультисервісній мережі з метою визначення причин їх виникнення. До розроблених алгоритмів виявлення аномалій у трафіку мультисервісних мереж пред'являються такі вимоги: функціонування як реального чи близького до реального часу; підтримка заданої якості сервісу; простота реалізації. Алгоритми належать до класу адаптивних гібридних алгоритмів ідентифікації параметрів трафіку. Вони використовуються як для стаціонарних, так і для нестаціонарних трафіків. Трафіки моделюються у вигляді стохастичних процесів. Кожен належить до відповідного класу, що визначається законом розподілу стохастичних процесів.

Результати. Експериментальна оцінка запропонованих методу та алгоритмів показала, що вони дозволяють оцінювати тренди зазначених стохастичних процесів у реальному часі, з високою точністю та зі збереженням якості обслуговування.

Висновки. Застосування розробленого методу управління усуненням несправностями в мультисервісній мережі допомагає підвищити якість обслуговування шляхом своєчасного виявлення проблем, зменшення часу їх усунення та скорочення часу простоїв, що, своєю чергою, впливає на підвищення показників надійності послуг.

КЛЮЧОВІ СЛОВА: мультисервісні мережі, трафік, якість, несправності, метод, користувач.

ЛІТЕРАТУРА

1. Моркун В. С. Синтез зашемостійкого алгоритму для адаптивного керування рудозбагаченням / В. С. Моркун, Н. В. Моркун, С. М. Грищенко, В. В. Тронь // Радіоелектроніка, інформатика, управління. – 2018. – № 3. – P. 183–190. https://doi.org/10.15588/1607-3274-2018-3-20
2. Моркун В. Тривимірний нечіткий контроль ультразвукового очищення / В. Моркун, О. Кравченко // Acta Mechanica et Automatica.– 2021. – 15 (3), – P. 169–176. https://doi.org/10.2478/ama-2021-0022.
3. Моркун В. Контроль процесу просторового ультразвукового очищення на основі оцінки його поточного стану / В. Моркун, О. Кравченко // Друга міжнародна конференція зі сталого майбутнього: екологічні, технологічні, соціальні та економічні питання (ICSF 2021). – E3S Web of Conferences 280, 07016. – 2021. https://doi.org/10.1051/e3sconf/202128007016.
4. Metod for processing multiservice traffic in network node based on adaptive management of buffer resource / [W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson] // On the Self-Similar Nature of Ethernet Traffic (Extended Version): IEEE/ACM Transactions on Networking. – 1994. – № 2, – P. 1–15. DOI: http://dx.doi.org/10.1109/90.282603
5. Косенко В. Методи управління розподілом трафіку в інформаційно-комунікаційних мережах систем критичної інфраструктури / В. Косенко, Є. Персіянова, О. Бєлоцький, О. Малєєва // Інноваційні технології та наукові рішення для промисловості. – 2017. – № 2 (2). – С. 48–55. DOI: 10.30837/2522-9818.2017.2.048
6. Kosenko V. Effectiveness analysis of resource usage of multiservice information and telecommunication network / V Kosenko, D. Bugas // Technology audit and production reserves. – 2015. – Vol. 5, No. 2 (25). – P. 19–23. DOI: 10.15587/2312-8372.2015.51710
7. Xi N. Secure service composition with information flow control in service clouds / N. Xi, C. Sun, J. Ma, Y. Shen // Future Generation Computer Systems. – 2015. – Vol. 49. – P. 142–148. DOI: 10.1016/j.future.2014.12.009
8. Mangili M. Optimal design of Information Centric Networks Original / M. Mangili, F. Martignon,. A. Capone // Computer Networks. – 2015. – Vol. 91. – P. 638–653. DOI: 10.1016/j.comnet.2015.09.003
9. Wang H. Detecting SYN Flooding Attacks / H. Wang, D. Zhang., K. G. Shin // Proc. of IEEE INFOCOM. 2002. International Conference on Mobile Ad-Hoc and Sensor Networks MSN 2005: Mobile Ad-hoc and Sensor Networks. – 2005. – P. 443–452. DOI: 10.1007/11599463_44
10. Angrishi K. An end-to-end stochastic network calculus with effective bandwidth and effective capacity / K. Angrishi // Computer Networks. – 2013. – Vol. 57, Issue 1. – P. 78–84. DOI: 10.1016/j.comnet.2012.09.003
11. Agrawal S. Survey on Anomaly Detection using Data Mining Techniques // S. Agrawal, J. Agrawal // Procedia Computer Science. – 2015. – Vol. 60. – P. 708–713 DOI: https://doi.org/10.1016/j.procs.2015.08.220

DOI 10.15588/1607-3274-2023-2-13