ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

A Mathematical Model for Determining Traffic Anomalies in Computer Data Networks with Discrete Characteristics

Ismailov Otabek M.

Assistant Professor,Department of "Computer systems", Tashkent University of Information Technologies Named After Muhammad Al-Khwarizmi, Tashkent, Uzbekistan

ABSTRACT: This article is devoted to the study of several methods in the identification of anomalies in the time series, which consists in the detection and processing of deviations in the data streams obtained during technological processes.
The object under study is a local-computing or backbone (main) network with a discrete data stream. The purpose of the study is to obtain information about the fractal characteristics of network traffic, which is necessary for the development of design models and optimization, as well as the improvement of technologies to ensure the smooth operation of the network. To identify and predict possible anomalies in the network. The paper analyzes a number of scientific papers aimed at studying the fractal properties and characteristics of network traffic. On the basis of the analysis performed in this paper, an improved method is proposed for calculating network traffic in networks with a discrete data flow by searching and comparing data on the flow in the main and local communication channels. The proposed mathematical model and algorithm for fractal analysis of network traffic will effectively identify deviations in traffic. Detection of anomalies in network traffic allows you to prevent cyber attacks, abnormal situations and accidents in the early stages of ISCIC. All this indicates the relevance of research in this area.

KEY WORDS: Identification of Anomalies, Mathematical Models, Time Series, Network Traffic, Cyberattacks.

I.INTRODUCTION

To date, the problem of ensuring the safety of integrated control systems for production complexes (ICSPC) is a very urgent task. Ensuring the protection and uninterrupted functioning of the ICSPC is connected with a number of organizational and technical measures. Research into the information security of computing systems has shown that one of the main factors of the violation of security and information integrity, in the multi-tiered architecture of the ICSPC, is seen in the identification of incidents in the operation of the hardware and software systems and the users' work in the system.

Systematic monitoring of the state of the data transmission channels of the ICSPC is implemented with the aim of timely detection and adaptive impact on the attacks. At the same time, the main task of data link monitoring systems is the timely detection, identification, detailed analysis of network incidents with the establishment of its causes and sources. On a rogue day, there are two ways to analyze network traffic: signature-based method and anomaly-based method [1]

II. SIGNIFICANCE OF THE SYSTEM

The paper mainly focuses on the study of several methods for identifying anomalies in the time series. The study of literature survey is presented in section III, Methodology is explained in section IV, section V covers experimental results of the study, and section VI discusses the future study and Conclusion.

III. LITERATURE SURVEY

Scientific research on the development of theoretical and practical methodologies for the analysis of network traffic and the detection of anomalies are reflected in the works of many foreign and domestic scientists.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

1. Signature-based method – R. N. Selin, R. Lippmann, R. Kwitt, A. Ghosh, E. Eskin, N. Cristianini, Mohammed Salem, Helen Amstrong and etc.;

2. Anomaly-based method – V. A. Artamonov, D. Y. Gamayunov, Paul Barford, Jeffery Kline, Hyun Joo Kim, Pedro Casas and etc. [2].

The concept of the signature method is to describe the attack in the form of a signature and search for this signature in the network (network traffic, log, etc.).Signature method allows reliable diagnostics of the used tool or technology of attack and prevents a large number of false messages. However, this method requires a mandatory updating of the database to obtain signatures of new or changes to existing attacks [3].

In this regard, recently the research and practical implementation of systems based on the method of detection of anomalies has been increased, the concept of which presupposes the detection of unusual behavior of the information system. This is achieved by collecting information about the normal functioning of the network for a certain period of time, and based on the accumulated information; the activity profile of the system is built. Analysis of the most works such as Loban I.A. « Statistical analysis of network traffic », « Causes and sources of network anomalies. » "The young scientist." till Zhumai I.N. « Analysis of methods for modeling network traffic » etc.showed that at present there are two main approaches in the description and forecasting of traffic in computer networks, each of which has its advantages and disadvantages. In this case, if one of the methods is based on the use of probabilistic characteristics of network traffic, the other uses the fractality of processes in networks. The mathematical apparatus for describing the processes of modeling network traffic can be different[4-25].

In particular, in paper of I.M. Azhmukhamedov, A.N. Marenkov, called «Determination of anomalies in the volume of network traffic based on the apparatus of fuzzy sets.» the authors carried out the analysis and statistical forecast of network packets in order to detect malicious progam in traffic. If there is a discrepancy between the forecast and the actual data, the system solution (conclusion) is an "anomaly." The apparatus of fuzzy sets is used in the work. (Kabildzhanov AS) [15].

In Analysis of the self-similarity of trafficweb-resource, the author proves that network traffic has the property of self-similarity, and the method of heavy tail. Reduces the data array by 5, 10, 15 times by averaging. (there is a column for heavy tails) [16].

The paper :FuadWehbe, S.A. (2014). Plants. Journal of the Kharkov National University of Radio electronics "Radiotekhnika" is devoted to the study of the self-similarity of traffic. Simulation modeling is used in the NS-2 environment. (virtual environment-the degree of chaotization of the system (traffic) and the quality of the transmitted information) [17].

This article of Kesiyan Grant Arutovich, UrtenovMahametHuseevich, ShahmeliikyanTimurArkadevich called «Analysis of methods for generating time series with long-term correlation structure. Scientific Journal of KubSU »generates time series with a simultaneous correlation structure. A comparative analysis of six methods for modeling fractally differentiated noise is made, among them: direct method of determination, Hosking method, Davis and Hart method, circulant embedding method, Paxson method and spectral modeling method. In addition, the analysis algorithms are presented and a method for estimating the Hurst parameter, which is the main quality criterion when comparing the above methods for modeling fractally differentiated noise, is selected. Based on the results of the comparative analysis, the table of results of comparison of methods is given[18].

The paper of A.G. Lozhkovsky, V.A. Kaptur, O.V. Verbanov, V.M. Kolchar, «Mathematical model of packet traffic.» is devoted to the study of mathematical modeling, which allows to adequately describe traffic in multiservice networks [19]. When simulating traffic, the mathematical apparatus of the Poisson distribution is used, which gives not the best (inefficient) results.

Studies of traffic design methods in computer networks are described in [20]. In this paper, network traffic is considered as a Poisson process. In the study of traffic, the authors are based on the self-similarity of traffic.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

The issues of network traffic management based on the identification of anomalies were considered in [2]. The general ideology of forecasting systems and the decision making as described in«Determination of anomalies in the volume of network traffic based on the apparatus of fuzzy sets » of I.M. Azhmukhamedov, A.N. Marenkov are described [15]. A scheme and a technique for processing and comparing data, searching for cycles, predicting, searching for and evaluating anomalies are described.

The scheme of the algorithm of traffic control is described. The system is checked at the visual level Scan 3.3. andNSanditor Network Security Auditor.

Along with the foregoing, the papers of Loban,I.A. «Statistical analysis of network traffic.», «Causes and sources of network anomalies», «Overview of methods for detecting anomalies in data streams.», «Analysis and classification of methods for detecting network attacks.», «Development of a network traffic anomaly detection system.», «Search and estimation of network traffic anomalies based on cyclic analysis.» and «Modeling of network traffic and forecasting using the ARIMA model» are also devoted to an overview of existing methods and algorithms for detecting anomalies of network traffic in order to structure the available data and subsequent selection of means for the development of an anomaly identification system in large data streams [26,4-6,10,11,13].

At the same time, recent research shows that the analysis of network traffic in computer, industrial and telecommunication networks of data transmission shows that it has the property of scale invariance, that is, they possess the self-similarity property [4, 7, 22, 27]. As you know, self-similar traffic has a special structure, which persists on many scales - in implementation there is always a certain amount of very large emissions with a relatively small average traffic level. This phenomenon significantly degrades the characteristics (increases losses, delays, jitter of packets) while passing through self-similar traffic through network nodes. It is for this reason that the development of mathematical models and algorithms of anomaly processes in the network should take into account the characteristics of traffic and the formation of universal systems for efficient processing.

IV. METHODOLOGY

The metastatic model and the algorithm for determining traffic anomalies in computational data networks with discrete characteristics can be formulated as follows. Suppose that there is data in the form of a table:

Table 1

t	**D_1**	**K_1**	**D_2**	**K_2**	**….**	**D_m**	**K_m**
t_1	$D_1(t_1)$	$K_1(t_1)$	$D_2(t_1)$	$K_2(t_1)$		$D_m(t_1)$	$K_m(t_1)$
t_2	$D_1(t_2)$	$K_1(t_2)$	$D_2(t_2)$	$K_2(t_2)$		$D_m(t_2)$	$K_m(t_2)$
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
t_n	$D_1(t_n)$	$K_1(t_n)$	$D_2(t_m)$	$K_2(t_n)$	.	$D_m(t_n)$	$K_m(t_n)$

$t_i, (i = \overline{1,n})$ – *time*

$D_i(t_j)$ – *traffic at* t_j *-time of i-day*

$K_i(t_j)$ –*quantity of worked computers at* t_j *-time of i-day*

$\lambda = (\lambda^1, \lambda^2, ..., \lambda^N)$, $\lambda^j \in \{0,1\}$, $j = 1, N$ forming vector; here $\sum_{j=1}^{N} \lambda^j = \ell$

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

$$\vec{a}_i = \left(\frac{D_i(t_{p_1})}{K_i(t_{p_1})}, \frac{D_i(t_{p_2})}{K_i(t_{p_2})}, \dots, \frac{D_i(t_{p_h})}{K_i(t_{p_h})} \right)$$

$$\vec{b}_j = \left(\frac{D_j(t_{f_1})}{K_j(t_{f_1})}, \frac{D_j(t_{f_2})}{K_j(t_{f_2})}, \dots, \frac{D_j(t_{f_h})}{K_j(t_{f_h})} \right)$$

$$N_a = \frac{(a_i, \lambda)}{(b_j, \lambda)} \tag{1}$$

We order the ratio of the components of the vectors u as follows

$$\frac{a_1}{b_1} \geq \frac{a_2}{b_2} \geq \dots\dots \geq \frac{a_N}{b_N}. \tag{2}$$

1. Anomaly is possible in the first l components.

$$\text{then } \lambda = \left(\underbrace{1,1,1,\dots,1}_{\ell}, \underbrace{0,0,0,\dots,0}_{N-\ell} \right).$$

For functional (1) next problem will be solved

$$\begin{cases} I(\lambda) = \dfrac{(a,\lambda)}{(b,\lambda)} \to \max; \\ \lambda \in \Lambda^{\ell}, \end{cases} \tag{3}$$

We introduce the following notation:

$$A = \sum_{i=1}^{l} a_i \,, B = \sum_{i=1}^{l} b_i \,, \begin{cases} \Delta a_{ij} = a_j - a_i \\ \Delta b_{ij} = b_j - b_i, i = \overline{1,l}, i = \overline{l+1, N} \end{cases} \lambda^0 = \left(\underbrace{1,1,\dots 1}_{l\,ma}, \underbrace{0,0,\dots,0}_{N-l\,ma} \right).$$

Let there be given real numbers a, b and $c \geq 0,\ d > 0\ (a + c \geq 0, b + d > 0)$. Then one of the following inequalities holds:

1. If $\begin{cases} a > 0 \\ b > 0 \end{cases}$ и $\frac{c}{d} > \frac{a}{b}$, then the following inequalities hold $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.
2. If $\begin{cases} a > 0 \\ b > 0 \end{cases}$ и $\frac{c}{d} < \frac{a}{b}$, then the following inequalities hold $\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}$.
3. If $\begin{cases} a < 0 \\ b < 0 \end{cases}$ и $\frac{c}{d} < \frac{a}{b}$, then the following inequalities hold $\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}$.
4. If $\begin{cases} a < 0 \\ b < 0 \end{cases}$ и $\frac{c}{d} > \frac{a}{b}$, then the following inequalities hold $\frac{a}{b} < \frac{a+c}{b+d} > \frac{c}{d}$.
5. If $\begin{cases} a \geq 0 \\ b \leq 0 \end{cases}$, then the following inequalities hold $\frac{a+c}{b+d} \geq \frac{c}{d}$.
6. If $\begin{cases} a \leq 0 \\ b \geq 0 \end{cases}$, then the following inequalities hold $\frac{a+c}{b+d} \leq \frac{c}{d}$.

Evidence for the validity of the above inequalities is not given due to their simplicity.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

If in the inequalities we will accept $a=\Delta a_{ij}, b=\Delta b_{ij}, c=A, d=B$, then for $\forall i, j\ \left(i=\overline{1,\ell},\ j=\overline{\ell+1,N}\right)$ will be $\begin{cases} A+\Delta a_{ij}\geq 0, \\ B+\Delta b_{ij}>0 \end{cases}$, and one of these inequalities holds.

*Theorem 1.*In order that the vector $\lambda^0=\left(\underbrace{1,1,\ldots 1}_{l\,ma},\underbrace{0,0,\ldots,0}_{N-l\,ma}\right)$, chosen with the help of an ordered sequence (2), was the optimal solution for problem (3),

It is necessary and sufficient that there should be no $a=\Delta a_{ij}$, $b=\Delta b_{ij}$, satisfying the conditions of inequalities 1 and 4.

Proof.

Sufficiency: Let it be chosen $\forall\lambda\in\Lambda^l$. Then expression $\begin{cases} A^*=(a,\lambda)=\sum\limits_{i=1}^{N}a_i\lambda_i, \\ B^*=(b,\lambda)=\sum\limits_{i=1}^{N}b_i\lambda_i \end{cases}$ can be reduced to the form

$$\begin{cases} A^*=A+\sum\limits_{t=1}^{p}\Delta a_{fk}^{(k)} \\ B^*=B+\sum\limits_{t=1}^{p}\Delta b_{fk}^{(k)} \end{cases}.$$

To save l- informative vector λ value f and k defined with next way:

1. If $\lambda_i=0$ and $\lambda_j=1$, then $f=j$ and $k=i\ \left(i=\overline{1,l},\ j=\overline{l+1,\ N}\right)$.

2. If $\lambda_i=1$ and $\lambda_j=0$, then $f=i$ and $k=j\ \left(i=\overline{1,l},\ j=\overline{l+1,\ N}\right)$.

For A^* и B^* equality will be $\begin{cases} A^*=A+A_1+A_2+A_3+A_4+A_5+A_6 \\ B^*=B+B_1+B_2+B_3+B_4+B_5+B_6 \end{cases}$.

Here A_k и B_k – sums of Δa_{ij} and Δb_{ij}, satisfying conditions of $k\left(k=\overline{1,\ 6}\right)$ inequality.

From inequality 6 follows $\dfrac{A_1+A_2+A_3+A_4+A_5+A_6}{B_1+B_2+B_3+B_4+B_5+B_6}\leq\dfrac{A_1+A_2+A_3+A_4+A_5}{B_1+B_2+B_3+B_4+B_5}$.

Since condition (2) performed , then A_5 and B_5 equal to zero. From conditions of theorem follows, that A_2, B_2 and A_4, B_4 equal to zero.

It follows, that $\begin{cases} A^*=A+A_1+A_3 \\ B^*=B+B_1+B_3 \end{cases}$.

Since the corresponding summable elements of the sums A_3 and B_3 satisfy condition 3, then $\begin{cases} A_3<0 \\ B_3<0 \end{cases}$, from which it follows that $\dfrac{A}{B}<\dfrac{A_3}{B_3}$. From inequality 3 it follows that $\dfrac{A+A_3}{B+B_3}<\dfrac{A}{B}$.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 11, November 2018

Since the corresponding summable elements of the sums A_1 and B_1 satisfy condition of inequality 1, then $\begin{cases} A_1 > 0 \\ B_1 > 0 \end{cases}$, from which it follows that $\frac{A}{B} > \frac{A_1}{B_1}$. From inequality 1 it follows that $\frac{A+A_1}{B+B_1} < \frac{A}{B}$.

From $\frac{A}{B} < \frac{A_3}{B_3}$ и $\frac{A+A_1}{B+B_1} < \frac{A}{B}$ it follows, that

$$\frac{A+A_1}{B+B_1} < \frac{A}{B} < \frac{A_3}{B_3}. \tag{4}$$

Since $\begin{cases} A_3 < 0 \\ B_3 < 0 \end{cases}$, from inequality $\frac{A+A_1}{B+B_1} < \frac{A_3}{B_3}$ and inequality 3 follows, that

$$\frac{A+A_1+A_3}{B+B_1+B_3} < \frac{A+A_1}{B+B_1}. \tag{5}$$

It follows from (5) and (4) that $\frac{A+A_1+A_3}{B+B_1+B_3} < \frac{A}{B}$.

Necessity: Assume that there are such Δa_{ij} and Δb_{ij}, which satisfy the inequalities 2 or 4. It follows from these inequalities that $\frac{A+A_2+A_4}{B+B_2+B_4} > \frac{A}{B}$.

Since the corresponding summable elements of the sums A_2 and B_2 satisfy the conditions of inequality 2, then $\begin{cases} A_2 > 0 \\ B_2 > 0 \end{cases}$, from which it follows that $\frac{A}{B} < \frac{A_2}{B_2}$. From inequality 2 it follows that $\frac{A+A_2}{B+B_2} > \frac{A}{B}$.

Since the corresponding summable elements of the sums A_4 and B_4 satisfy the conditions of inequality 4, then $\begin{cases} A_4 < 0 \\ B_4 < 0 \end{cases}$, from which it follows that $\frac{A}{B} > \frac{A_4}{B_4}$. From inequality 4 it follows that $\frac{A+A_4}{B+B_4} > \frac{A}{B}$.

From the inequalities $\frac{A}{B} < \frac{A_2}{B_2}$ и $\frac{A}{B} > \frac{A_4}{B_4}$ follows that

$$\frac{A_4}{B_4} < \frac{A}{B} < \frac{A_2}{B_2}. \tag{6}$$

Since $\begin{cases} A_4 < 0 \\ B_4 < 0 \end{cases}$, From the inequalities $\frac{A_4}{B_4} < \frac{A_2}{B_2}$ and inequality 4 it follows that

$$\frac{A_2+A_4}{B_2+B_4} > \frac{A_2}{B_2} > \frac{A}{B}. \tag{7}$$

Since $\begin{cases} A > 0 \\ B > 0 \end{cases}$, From the inequalities $\frac{A_2+A_4}{B_2+B_4} > \frac{A}{B}$ and inequality 4 it follows that $\frac{A_2+A_4}{B_2+B_4} > \frac{A+A_2+A_4}{B+B_2+B_4} > \frac{A}{B}$.

As a result, since $\frac{A}{B} < \frac{A+A_2+A_4}{B+B_2+B_4}$, value of the functional $I(\lambda) = \frac{A}{B}$, corresponding to the selected vector

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 11, November 2018

$\lambda^0 = \left(\underbrace{1,1,1,\ldots,1}_{l}, \underbrace{0,0,0,\ldots,0}_{N-l} \right)$, is not optimal.

The theorem is proved.

Suppose vector $\lambda = \left(\underbrace{1,1,1,\ldots,1}_{\ell}, \underbrace{0,0,0,\ldots,0}_{N-\ell} \right)$ – the solution obtained by the ordering method is not an optimal solution of problem (3). Then, to determine the optimal solution of problem (3), transformations are performed on the basis of inequalities 2 and 4.

The transformation process is performed as long as there are Δa_{ij} and Δb_{ij}, satisfying the conditions of inequalities 2 and 4. If there are no Δa_{ij} and Δb_{ij}, satisfying the conditions of inequalities 2 and 4, it follows from Theorem 1 that the solution obtained is optimal.

In this method, the value of the functional and the components of the vector are formed on the basis of inequalities.

Suppose that for Δa_{ij} and Δb_{ij} the condition of one of the inequalities 2 and 4 is valid.

Then it follows from the results of the inequalities that $\frac{A+\Delta a_{ij}}{B+\Delta b_{ij}} > \frac{A}{B}$, values of *iиj* vector component λ will be changed with places also functional, corresponds to λ, will be equal $\frac{A+\Delta a_{ij}}{B+\Delta b_{ij}}$.

We denote the algorithm based on this method by A4, and it consists of the following steps.

Step 1. Set the initial value to the vector $\lambda = \{\underbrace{1,1,\ldots,1}_{\ell}, \underbrace{0,0,\ldots,0}_{N-\ell}\}$.

Step 2. Values are calculated A and B, means that $A = (a, \lambda)$, $B = (b, \lambda)$.

Step 3. $i = 1$, $j = N$; $A_1 = A, B_1 = B$.

Step 4. Values are calculated Δa_{ij} and Δb_{ij}.

Step 5.The conditions for satisfying the inequality 4. If Δa_{ij} and Δb_{ij} satisfy the conditions of inequality 4, then, by the results of the inequality, transformations are carried out, i.e. values *i* and *j* vector component λ change places, calculated $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$, and go to step 7, otherwise - to the next step.

Step 6. The conditions for satisfaction of inequality 2 are checked. If Δa_{ij} and Δb_{ij} satisfy the conditions of inequality 2, then, by the results of the inequality, transformations are carried out, i.e. values *i* and *j* vector component λ change places, calculated $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$, and the next step is made.

Step 7. The condition is checked $j > \ell$. If $j > \ell$, then $j = j - 1$ and go to step 4, otherwise - to the next step.

Step 8. The condition is checked $i < \ell$. If $i < \ell$, then $i = i + 1$ and go to step 4, otherwise - to the next step.

Step 9. The conditions are checked $A_1 = A$ and $B_1 = B$. If $A_1 = A$ and $B_1 = B$, then λ – the optimal solution, and the algorithm stops, otherwise the transition to step 3 is carried out.

Letsselect $\forall \lambda \in \Lambda^l$.

Theorem 2. In order that the chosen vector λ is an optimal solution of problem (3), it is necessary and sufficient that there exist $a = \Delta a_{ij}$, $b = \Delta b_{ij}$ $\left(i = \overline{1,l},\ j = \overline{l+1,N}\right)$, satisfying the conditions of inequalities 2, 4, and 5.

Proof.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

Sufficiency: Let it be chosen $\forall\lambda\in\Lambda^l$. Then the expressions $\begin{cases}A^*=(a,\lambda)=\sum\limits_{i=1}^{N}a_i\lambda_i\\ B^*=(b,\lambda)=\sum\limits_{i=1}^{N}b_i\lambda_i\end{cases}$ can be reduced to the form

$$\begin{cases}A^*=A+\sum\limits_{t=1}^{p}\Delta a_{fk}^{(k)}\\ B^*=B+\sum\limits_{t=1}^{p}\Delta b_{fk}^{(k)}\end{cases}.$$

To save l- informative vector λ values f and k are defined as follows:

1. If $\lambda_i=0$ and $\lambda_j=1$, then $f=j$ and $k=i\left(i=\overline{1,l},\ j=\overline{l+1,\ N}\right)$.

2. If $\lambda_i=1$ and $\lambda_j=0$, then $f=i$ and $k=j\left(i=\overline{1,l},\ j=\overline{l+1,\ N}\right)$.

For $A*$ and $B*$ follows $\begin{cases}A^*=A+A_1+A_2+A_3+A_4+A_5+A_6\\ B^*=B+B_1+B_2+B_3+B_4+B_5+B_6\end{cases}$.

Here A_k and B_k – sums of Δa_{ij} and Δb_{ij}, satisfying conditions of $k\left(k=\overline{1,\ 6}\right)$ inequalities.

From inequality 6 follows $\dfrac{A_1+A_2+A_3+A_4+A_5+A_6}{B_1+B_2+B_3+B_4+B_5+B_6}\le\dfrac{A_1+A_2+A_3+A_4+A_5}{B_1+B_2+B_3+B_4+B_5}$.

It follows from the hypothesis of the theorem that the sums A_2, B_2 A_4, B_4 и A_5, B_5 equal to zero.

It follows that $\begin{cases}A^*=A+A_1+A_3\\ B^*=B+B_1+B_3\end{cases}$.

Since the corresponding summable elements of the sums A_3 and B_3 satisfy the inequality 3, then $\begin{cases}A_3<0\\ B_3<0\end{cases}$, from which it follows that $\dfrac{A}{B}<\dfrac{A_3}{B_3}$. From inequality 3 it follows that $\dfrac{A+A_3}{B+B_3}<\dfrac{A}{B}$.

Since the corresponding summable elements of the sums A_1 and B_1 satisfy the inequality 1, then $\begin{cases}A_1>0\\ B_1>0\end{cases}$, from which it follows that $\dfrac{A}{B}>\dfrac{A_1}{B_1}$. From inequality 1 it follows that $\dfrac{A+A_1}{B+B_1}<\dfrac{A}{B}$.

From the inequalities $\dfrac{A}{B}<\dfrac{A_3}{B_3}$ и $\dfrac{A+A_1}{B+B_1}<\dfrac{A}{B}$ follows that

$$\frac{A+A_1}{B+B_1}<\frac{A}{B}<\frac{A_3}{B_3}. \tag{8}$$

Since $\begin{cases}A_3<0\\ B_3<0\end{cases}$, From the inequalities $\dfrac{A+A_1}{B+B_1}<\dfrac{A_3}{B_3}$ and inequality 3 it follows that

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 11, November 2018

$$\frac{A+A_1+A_3}{B+B_1+B_3}<\frac{A+A_1}{B+B_1}. \qquad (9)$$

From (8) and (9) it follows that $\frac{A+A_1+A_3}{B+B_1+B_3}<\frac{A}{B}$.

Necessity: suppose that there are such Δa_{ij} and Δb_{ij}, which satisfy the inequalities 2, 4 or 4. It follows from inequalities 2, 4 or 5 that $\frac{A+A_2+A_4+A_5}{B+B_2+B_4+B_5}>\frac{A}{B}$.

Since the corresponding summable elements of the sums A_2 and B_2 satisfy the conditions of inequality 2, then $\begin{cases}A_2>0\\B_2>0\end{cases}$, from which it follows that $\frac{A}{B}<\frac{A_2}{B_2}$. From inequality 2 it follows that $\frac{A+A_2}{B+B_2}>\frac{A}{B}$.

Since the corresponding summable elements of the sums A_4 and B_4 satisfy the conditions of inequality 4, then $\begin{cases}A_4<0\\B_4<0\end{cases}$, from which it follows that $\frac{A}{B}>\frac{A_4}{B_4}$. From inequality 4 it follows that $\frac{A+A_4}{B+B_4}>\frac{A}{B}$.

From the inequalities $\frac{A}{B}<\frac{A_2}{B_2}$ и $\frac{A}{B}>\frac{A_4}{B_4}$ follows that

$$\frac{A_4}{B_4}<\frac{A}{B}<\frac{A_2}{B_2}. \qquad (10)$$

Since $\begin{cases}A_4<0\\B_4<0\end{cases}$, From the inequalities $\frac{A_4}{B_4}<\frac{A_2}{B_2}$ and inequality 4 it follows that

$$\frac{A_2+A_4}{B_2+B_4}>\frac{A_2}{B_2}>\frac{A}{B}. \qquad (11)$$

Since $\begin{cases}A>0\\B>0\end{cases}$, From the inequalities $\frac{A_2+A_4}{B_2+B_4}>\frac{A}{B}$ and inequality 1 it follows that $\frac{A_2+A_4}{B_2+B_4}>\frac{A+A_2+A_4}{B+B_2+B_4}>\frac{A}{B}$.

Since each corresponding element of sets A_5 and B_5 satisfies the conditions of the inequality 5, then the inequality $\frac{A+A_2+A_4+A_5}{B+B_2+B_4+B_5}>\frac{A+A_2+A_4}{B+B_2+B_4}>\frac{A}{B}$.

As a result, since $\frac{A+A_2+A_4+A_5}{B+B_2+B_4+B_5}>\frac{A}{B}$, value of the functional $I(\lambda)=\frac{A}{B}$, corresponding to the selected vector λ, is not optimal.
The theorem is proved.

V. EXPERIMENTAL RESULTS

If the vector λ is not a solution of problem (3), then transformations are performed on the basis of inequalities 2, 4 and 5. The transformation process is performed as long as there are Δa_{ij} and Δb_{ij}, satisfying the conditions of inequalities

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 11, November 2018

2, 4, and 5. If there are no more Δa_{ij} and Δb_{ij}, satisfying the conditions of inequalities 2, 4, and 5, it follows from Theorem 2 that the solution obtained is optimal.

In this method, the value of the functional is computed and the components of the vector λ in the following way.

Suppose that for Δa_{ij} and Δb_{ij} the condition of one of the inequalities 2, 4 or 5 is valid. Then it follows from the results of the inequalities that $\frac{A+\Delta a_{ij}}{B+\Delta b_{ij}} > \frac{A}{B}$. Values of *i* and *j* vector component λ change with places.

The transformation process is performed as long as the conditions of Theorem 2 are satisfied.

The algorithm corresponding to this method consists of the following steps.

Step 1. Set the initial value to the vector $\lambda = \{\underbrace{1,1,\ldots,1}_{\ell}, 0, 0, \ldots 0\}$.

Step 2. The values of A and B are calculated, i.e. $A = (a, \lambda)$, $B = (b, \lambda)$.

Step 3. $i = 1$, $j = N$; $A_1 = A, B_1 = B$.

Step 4. Values are calculated Δa_{ij} and Δb_{ij}.

Step 5. The conditions for satisfying inequality 4 are checked. If Δa_{ij} and Δb_{ij} satisfy the conditions of inequality 4, then, from the results of the inequality, the values of *i* and *j* vector component λ change places, calculated $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$, and go to step 8, otherwise - to the next step.

Step 6. The conditions for satisfaction of inequality 2 are checked. If Δa_{ij} and Δb_{ij} satisfy the conditions of inequality 2, then, from the results of the inequality, the values of *iandj* vector component λ change places, calculated $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$, and go to step 8, otherwise - to the next step.

Step 7. The conditions for satisfying the inequality 5 are checked. If Δa_{ij} and Δb_{ij} satisfy the conditions of inequality 5, then, by the results of the inequality, transformations are carried out, i.e. values of *i* and *j* vector component λ change places, calculated $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$, and go to step 8, otherwise - to the next step.

Step 8. The condition is checked $j > \ell$. If $j > \ell$, then $j = j - 1$ and go to step 5, otherwise - to the next step.

Step 9. The condition is checked $i < \ell$. If $i < \ell$, then $i = i + 1$ and go to step 5, otherwise - to the next step.

Step 10. Conditions rechecked $A_1 = A$ and $B_1 = B$. If $A_1 = A$ and $B_1 = B$, then λ – the optimal solution, and the algorithm stops, otherwise the transition to step 3 is carried out.

VI. CONCLUSION AND FUTURE WORK

To date, modern society can not be imagined without a developed information infrastructure that meets its needs. Designing fault-tolerant telecommunication systems and networks that provide services with specified levels of data processing quality is a complex scientific and technical problem. In this regard, further research in solving the problems of modeling network traffic to optimize their flow will be continued. Conducted in this paper, studies have shown that the network traffic of computer networks have the nature of self-similarity. However, fractality with a discrete property is observed in the object under study. The aforementioned approaches and methods for analyzing network traffic are not efficient enough to identify traffic anomalies in networks with a discrete stream. Therefore, the method proposed in this paper allows us to more effectively identify anomalies in the time series, which consists in the detection and processing of deviations in the data streams obtained during the technological processes. The developed mathematical model of the fractal analysis of network traffic by iterating through the data will make it possible to predict the possible volume of traffic in the near future period in real time. The implementation of the proposed algorithm for detecting traffic anomalies in networks with a discrete data flow allows you to design the functioning of the means of ensuring the smooth operation of the network, as well as to prevent many cyber attacks, abnormal situations and accidents at early stages in local-computer networks.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

REFERENCES

[1] IDS / IPS - Intrusion Detection and Prevention Systems. URL: http: //www.netconfig.ru/server/ids-ips. (Date of last review: 06.04.2016).
[2] Marienkov Alexander Nikolaevich. Traffic control of a computer network on the basis of identification of anomalies. The dissertation author's abstract on competition of a scientific degree of the candidate of technical sciences. Astrakhan, 2012.
[3] D. J. Brown, B. Suckow, and T. Wang.A survey of intrusion detection systems. Department of Computer Science, University of California, San Diego, CA, United States. 2002. URL: http: //charlotte.ucsdu/classes/fa01/cse221/projects/group10.pdf. (Date of last review: 06.04.2016).
[4] Loban,I.A. Statistical analysis of network traffic. http://elib.bsu.by/bitstream/123456789/95143/1/203-207.pdf. - Date of last review: July 10, 2018.
[5] OladkoVladlenaSergeevna. Candidate of Technical Sciences, Associate Professor; MikovaSofyaYurievna, student; Nesterenko Maxim Alekseevich, student; SadovnikEvgenyAlexandrovich, student of Volgograd State University. *Causes and sources of network anomalies. "The young scientist."*, 2015. No. 22 (102). pp. 158-161.
[6] V.P. Shkodirev, K.I. Yagafarov, V.A. Bashtovenko, E.E. Ilyin. Overview of methods for detecting anomalies in data streams. http://ceur-ws.org/Vol-1864/paper_33.pdf. - Viewed: 10/07/2018.
[7] http://ita.ee.lbl.gov/ -Internet traffic archive. - Date of last review: July 10, 2018.
[8] Petrov, V.V. (2003). Statistical analysis of network traffic. MPEI, IRE, Moscow, Krasnokazarmennaya 13, December 2003, p.47
[9] Mikova, S.Yu.,Oladko, V.S., Nesterenko, M.A. Approach to the classification of network traffic anomalies. *International scientific journal "Innovation Science"*, 2015. № 11/2015. pp. 78-80.
[10] Branitsky, A.A., Kotenko, I.V. Analysis and classification of methods for detecting network attacks, Proceedings of SPIIRAS, 2016. Issue 2 (45), pp. 207-244. All-Russian mathematical portal Math-Net.Ru. www.proceedings.spiiras.nw.ru.
[11] Levonevsky, D.K., Fatkieva, R.R. Development of a network traffic anomaly detection system. *Scientific Bulletin of the NSTU "Modern Information Technologies"*, 2014. volume 56, No. 3, pp. 108-114.
[12] Maksimenko, G.A. Method for detecting anomalies of data streams in all regions, Information Processing Systems, 2009. Issue 7 (81). pp.33-37.
[13] I.M. Azhmukhamedov, A.N. Marienkov. Search and estimation of network traffic anomalies based on cyclic analysis. Electronic scientific journal "The Engineering Herald of the Don", 2007-2015, https://cyberleninka.ru/article/v/poisk-i-otsenka-anomaliy-setevogo-trafika-na-osnove-tsiklicheskogo-analiza. - Date of last review: July 10, 2018.
[14] Ivan Khozyainov. Cyber-oracle: search for anomalies in monitoring data using a neural network. https://habr.com/company/itsumma/blog/341598/. - Date of last review: July 10, 2018.
[15] I.M. Azhmukhamedov, A.N. Marenkov. Determination of anomalies in the volume of network traffic based on the apparatus of fuzzy sets. *Vestnik ASTU*, 2011 .No. 1 (51). pp. 48-50.
[16] Analysis of the self-similarity of trafficweb-resource http://www.kp.karelia.ru. Date of last review: July 10, 2018.
[17] FuadWehbe, S.A. Plants. *Journal of the Kharkov National University of Radioelectronics "Radiotekhnika"*, 2014 .No. 176. pp.229-234.
[18] Kesiyan Grant Arutovich, UrtenovMahametHuseevich, ShahmeliikyanTimurArkadevich. Analysis of methods for generating time series with long-term correlation structure. *Scientific Journal of KubSU*, 2011. No. 74 (10), pp.1-11.
[19] A.G. Lozhkovsky, V.A. Kaptur, O.V. Verbanov, V.M. Kolchar, Mathematical model of packet traffic.
[20] Batyr, S.S., Stupak, G.V., Traffic forecasting methods in computer networks
[21] V. Yu. Aksenov, V. N. Dmitriev. Algorithm for fractal analysis of time series in sensor network monitoring systems. *Lead ASTU*. 2012 .№1, pp. 91-96.
[22] D.V. Belkov, E.N. Edemskaya, L.V. Nezamova. Statistical analysis of network traffic. *НауковіпраціДонНТУ*, 2011. No13 (185), pp.66-75.
[23] K.M. Rukkas, Yu.V. Solyanik, K.A. Ovchinnikov, OlotuOluvatosin David. Electronic scientific specialized publication-journal "Problems of Telecommunications". 2014 .No. 1 (13), pp. 84-95. http://pt.journal.kh.ua
[24] Shelukhin, O.I., Antonyan, A.A. Analysis of changes in the fractal properties of telecommunication traffic caused by abnormal intrusions. T-Comm.2014 .№6, pp.61-64.
[25] Zhumai I.N. Analysis of methods for modeling network traffic. Almaty. 2014 .pp.106.
[26] Grebennikov, A.V. Modeling of network traffic and forecasting using the ARIMA model. Grebennikov, Yu.A. Kryukov, D.V. Chernyagin // *5 Electronic Journal "System Analysis in Science and Education"*, 2011 .No. 1, pp. 1-11.
[27] Numerical Method [Electronic resource] - Mode of access: http://numericalmethod.com/blog/. - Date of access: 04/13/2013.

AUTHOR'S BIOGRAPHY

Ismailova Otabek Mirhalilovich

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

O.M.Ismailov, born in 1973, native of Tashkent, Uzbek, higher education, in 1994 graduated from Tashkent State Technical University with a degree in Automated Systems for Processing and Information Management. Candidate of Technical Sciences (Doctor of Philosophy).

He has been working in the MFA system since 1994. He has held the positions of attache, 3-secretary of the International Information Department, 2-secretary, 1-secretary, head of department, head of communications, computer systems and the Internet. In 2002-2006. He worked as the head of the Embassy of the Republic of Uzbekistan in Egypt, 2013-2015. - 2-secretary - head of the consular department of the Embassy of the Republic of Uzbekistan in Japan.

Conducts research activities, has more than 30 scientific papers.
He is fluent in Uzbek, Russian and English.