UDC 004.624+519.21 **doi: 10.32620/reks.2025.3.17**

Kyrylo RUKKAS[1], Anastasiia MOROZOVA[1], Ievgen MENIAILOV[1], Myroslav MOMOT[2]

[1] ***V. N. Karazin Kharkiv National University, Kharkiv, Ukraine***
[2] ***National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine***

ANALYSIS OF PACKET LOSS PROBABILITY MODELS IN A ROUTER BUFFER BASED ON TRAFFIC FRACTALITY

The subject *of this study is various types of network traffic in modern computer networks with a complex structure and a certain degree of self-similarity. Efficient use of network resources and ensuring the quality of service to subscribers are important tasks of computer networks. The probability of losing a message due to buffer storage device overflow is an important parameter in determining the quality of service (QoS). The mathematical model should be used to estimate this parameter. Recent advancements have resulted in many different models of packet loss probability in a router buffer. However, many models do not consider the traffic characteristics of various modern applications and protocols. The traffic in modern computer networks has a complex structure and often has a certain degree of self-similarity. Currently, a large number of models are available for estimating the probability of packet loss due to buffer overflow.* ***The goal*** *of this work is to perform a comparative analysis of such models and provide recommendations for their use and to estimate the influence of network traffic fractality on the probability of packet loss in a router due to buffer overflow.* ***The tasks to be solved are*** *as follows: 1) to conduct an analysis of analytical models that describe the packet loss probability in a router considering the influence of fractality and without it; 2) to construct the dependencies of the packet loss probability in the router on the data transmission channel load for different buffer capacity values, the Hurst exponent, and traffic deviation; and 3) to describe the dependences of the packet loss probability on the buffer capacity for different channel load values.* ***Comparative*** *analysis of various methods of fractal traffic modeling and simulation with different storage capacity, Hurst exponent, deviation coefficients, and channel load factor values is used.* ***The following results were obtained:*** *1) The M/M/1 queuing system model gives the most optimistic estimate. This estimate can be used as a lower bound for the message loss probability for a given buffer capacity and a channel load factor; 2) the highest message loss probability was observed when using queuing systems with a Hurst exponent of 0.95; 3) the packet loss probability also increased with an increasing traffic fractality and deviation coefficient; 4) the influence of fractality decreased with an increase in the buffer capacity was found; 5) an objective estimation of the message loss probability due to a router buffer overflow can only be made by considering the nature of the traffic.* ***Conclusions****. The main contribution of this research is that various types of network traffic have a fractal nature, and the traditional methods of route service specification, such as traffic using the M/M/1 queuing model, give more errors. Because of the research conducted to reduce the impact of traffic fractality, increasing the capacity of buffer storage devices is necessary.*

Keywords: *network; packet; packet loss probability; routing; buffer; traffic fractality; Hurst Exponent.*

1. Introduction

1.1. Motivation

Computer networks are the main component of modern information systems. Efficient use of network resources and ensuring the quality of service to subscribers are important tasks of computer networks. The probability of losing a message due to buffer storage device overflow is an important parameter in determining service quality. The mathematical model should be used to estimate this parameter.

Recent advancements have resulted in many different models of packet loss probability in a router buffer. However, many models do not consider the traffic characteristics of various modern applications and protocols. The traffic in modern computer networks has a complex structure and often has a certain degree of self-similarity. Currently, a large number of models are available for estimating the probability of packet loss due to buffer overflow. This paper aims to conduct a comparative analysis of such models and recommendations for their use.

1.2. State of the Art

Research [1] has shown that different types of Internet traffic have different degrees of self-similarity. Another study by Dymora et al. [2] demonstrated that self-similar traffic occurs in the Internet of Things. Millán et al. [3] demonstrated that traffic in local networks is also fractal.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Analysis of real data traffic in existing and future computer networks has shown the incorrectness of using Poisson models to determine their probabilistic-time characteristics [1].

In the study [4], an approach that allows one to demonstrate that the self-similarity of networks is defined by the patterns of intersection between dense network communities is presented. Using this natural and intrinsic to the network's framework, fractal networks can be rigorously defined and their properties linked.

The most common traffic models are described in detail in the study [5]. Traffic models enable network designers to make assumptions about the networks being designed based on experience and enable performance prediction for future requirements.

The TCP connection arrival process is asymptotically self-similar. The self-similarity of such an arrival process implies that the use of standard models in evaluating the performance of resource allocation methods can yield misleading results. Therefore, the TCP connection is characterized by interarrival times using heavy-tailed distributions. Such distributions, especially the Weibull distributions, yield a better model than exponential models for the interarrival times of the TCP connections [6].

A previous study [7] aimed to observe network traffic and determine whether there are long-term dependencies in all network working times and above-hour intervals. The results confirmed that the traffic has a self-similar nature to the degree of self-similarity in the range of 0.5 to 1. The parameter H is larger when network use is higher and the self-similarity property in the network traffic dominates the network performance.

A previous study [8] demonstrated that methods for computing network characteristics (such as network throughput and delivery time) based on Markov models give unreasonably optimistic estimates. This leads to underestimation of the load and, consequently, the impossibility of providing the required quality of service.

This study [9] analyzed traffic flows in high-speed computer networks using a minimum quantity of time series points that must contain estimates of the Hurst exponent. An experiment using estimators applied to a time series provides an accurate determination of the Hurst exponent.

The paper [10] provided a comprehensive overview of approaches to Synthetic network traffic generation It covers essential aspects, such as data types, generation models, and evaluation methods, including traditional statistical methods and deep learning-based techniques. This study also addresses the issues of generating realistic fractal traffic models for simulations and evaluating new modeling methods that may better reflect real network behavior than classical M/M/1 models.

In the study [11], an innovative feature selection (FS) method was proposed to filter out Distributed Denial of Service (DDoS) attacks in software-defined networks (SDN) using machine learning. Traffic characteristics (including potential fractal properties) can be used to improve the reliability and efficiency of attack detection. It considers how traffic fractal properties can be indicators of DDoS attacks and how SDN can be used to detect and prevent them.

The paper [12] investigated the impact of Wireless Mesh Networks (WMNs) topology on performance metrics, including latency, throughput, and reliability, across a range of fractal dimensions. This study contains comparative evaluations against classical random, small-world network models. In this study, we show how the fractality of the topology affects traffic characteristics such as throughput, latency, jitter, and packet delivery ratio. A comparative analysis is conducted against classical random networks, small-world, and scale-free network models.

A previous study [13] proposed a method that predicts router load by analyzing the fractal dimension of network traffic to reduce the probability of packet loss. This study investigates the impact of different traffic fractal dimensions on the probability of packet loss and the quality of service at high traffic intensity. Fractal traffic analysis significantly reduces the number of lost packets compared to the existing method without prediction.

Thus, recent advancements have resulted in many different models and methods for computing network metrics and characteristics, which consider network traffic self-similarity and fractality. However, a current task is a comparative analysis of such models and recommendations for their use, as well as estimating the influence of network traffic fractality on the packet loss probability in a router due to buffer overflow.

1.3. Objectives and Approach

This study aims to estimate the influence of network traffic fractality on the probability of packet loss in a router due to buffer overflow. In accordance with the research goal, the following tasks must be solved:

1. Analyze analytical models that describe the packet loss probability in a router.

2. To simulate the estimation of the dependences of the probability of packet loss on different factors, which are described in analytical models considering the network traffic fractality.

3. To develop recommendations for using different packet loss probability models in a router.

The article is organized as follows:

Section 2 describes the problem of estimating the influence of network traffic fractality on the packet loss probability in a router due to buffer overflow, as well as the assumptions and developing the methodology for solving research tasks.

Section 3 analyzes analytical models that describe the packet loss probability in a router, considering the influence of fractality.

Section 4 provides experiments and illustrative examples of the dependence of the probability of packet loss on the load factor for different buffer capacity, channel load (utility), and Hurst Exponent sizes.

Section 5 contains a discussion of the obtained results and recommendations.

Section 6 concludes the article by summarizing the conclusions and describing further research and development directions.

2. Methodology

Traditionally, various types of Queuing Theory models are used to simulate router operations. The M/M/1 system with a limited queue length is the simplest mathematical routing model. It assumes an exponential distribution of the packet delivery and processing times. This model describes the simplest data flows that do not always correspond to reality. The analytical expressions of this model allow for obtaining specific values for the queue waiting time and packet loss probability.

The G/G/1 model is more general and flexible. This model does not impose strict restrictions on packet delivery distribution and processing times. It allows considering traffic variability through deviation coefficients (C_λ^2, C_μ^2). Using G/G/1 allows moving from unrealistic scenarios to real network conditions, where traffic does not always correspond to exponential distributions.

Modern network traffic (HTTP, video, IoT, P2P) has a self-similarity and fractal nature. Therefore, recently developed models allow the fractality of traffic to be considered against traditional models of queuing theory. Some models allow the fractality of traffic to be considered using the Hurst exponent. Another approach is to use special distribution laws of packet arrival (Pareto, Weibull) instead of the exponential distribution. Such distributions more accurately describe the fractal structure of the router's input packet flow.

The influence of network traffic fractality on the probability of packet loss due to buffer overflow in a router is estimated. The basic estimation algorithm can be divided into several stages.

The first stage involves the analysis of analytical models that describe the packet loss probability in a router using the Queuing Systems (QS) model M/M/1, G/G/1, and additionally considering the influence of fractality using the self-similarity parameter (Hurst Exponent). In this stage, the most commonly used distributions for fractal traffic modeling and their characteristics, such as the Mathematical expectation and variance, are considered.

The second stage proposes a loss probability formula for a G/M/1 system.

The next stage is to explore the dependencies of the packet loss probability in the router on the data transmission channel load for different buffer capacity, the Hurst exponent, and traffic deviation values. In this stage, various types of traffic in modern computer networks are investigated, and the values of the Hurst Exponent for most applications are assumed.

In the last stage, the simulation is conducted to estimate the dependence of the probability of packet loss on storage capacity, Hurst Exponent, deviation coefficients, and data transmission channel load factor.

The following sections present a comparative analysis of various methods of fractal traffic modeling and simulation with different storage capacity, Hurst Exponent, deviation coefficients, and channel load factor values.

3. Packet loss probability models

Currently, the main model is the Queuing Systems (QS) model M/M/1, which assumes that the time of arrival and processing requests are exponentially distributed [14].

$$P_{loss} = \frac{1-\rho}{1-\rho^{W+1}} * \rho^{W}, \quad (1)$$

where $\rho = \frac{\lambda}{\mu} < 1$ – service channel load factor;

λ – input flow intensity;

μ – output flow intensity;

W – storage capacity measured in packets.

A general expression for the probability of packet loss in the G/G/1 system was obtained in the study [2].

$$P_{loss} = \frac{1-\rho}{1-\rho^{(W+1)^{\frac{2}{(C_\lambda^2+C_\mu^2)}}}} * \rho^{W^{\frac{2}{(C_\lambda^2+C_\mu^2)}}} \quad (2)$$

where $C_\lambda^2 = (\frac{\delta[\lambda]}{M[\lambda]})^2$ – squared deviation coefficient of the input flow;

$C_\mu^2 = (\frac{\delta[\mu]}{M[\mu]})^2$ – squared deviation coefficient of the output flow.

If the input and output flows are exponentially distributed, then $C_\lambda^2 = C_\mu^2 = 1$, which means that expression (2) is transformed into expression (1) for the M/M/1 system. Millán et al [3] proposed estimating the packet loss probability using the self-similarity parameter (Hurst Exponent). The expression for the probability of loss is defined as follows:

$$P_{loss} = \frac{1-\rho}{1-\rho^{(W+1)^{2(1-H)}}} * \rho^{W^{2(1-H)}} \quad (3)$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

If Hurst Exponent H=0.5, then the process doesn't have a fractal property. In this case, expression (3) is transformed into expression (1). If Hurst Exponent H=1, then the process is completely self-similar and has a fractal property.

The characteristics of some distributions are shown in Table 1. The Pareto distribution is the most commonly used distribution for fractal traffic modeling. The advantage of this distribution is its ability to determine the fractal traffic using its parameters. The disadvantage is that it has infinite variance, which means that input traffic is highly variable. Therefore, this distribution cannot be used.

Table 1

Characteristics of some distributions

Distribution	Mathematical expectation	Variance
Pareto	$\frac{\alpha * \beta}{\alpha - 1}$ for $\alpha < 1$, doesn't exist	$\frac{\alpha * \beta^2}{(\alpha - 1) * (\alpha - 2)}$ for $\alpha < 2$ variance doesn't exist
Weibull	$\beta * \Gamma\left(\frac{\alpha + 2}{\alpha}\right)$	$\beta^2 * [\Gamma\left(\frac{\alpha + 2}{\alpha}\right) - \Gamma^2\left(\frac{\alpha + 1}{\alpha}\right)]$
Log-normal	$e^{\alpha + \frac{\beta}{2}}$	$e^{\beta^2 + 2 * \alpha} * (e^{\beta^2} - 1)$
Gamma	$\alpha * \beta$	$\alpha * \beta^2$

Alongside the Pareto distribution, the Weibull distribution is most often used in fractal traffic modeling. The probability distribution for the Weibull distribution is defined as follows:

$$F(x) = 1 - e^{-(\frac{x}{\beta})^{\alpha}}, \quad (4)$$

where α, β – scale parameter and the shape parameter of the distribution.

The study [6] demonstrated that traffic models with long-term dependence (in particular, models based on fractal Brownian motion) lead to an asymptotic distribution of Weibull-type tail probabilities:

$$P(x < B) \sim e^{-(\gamma B)^{2-2H}}, \quad (5)$$

where γ – constant value;

$P(x < b)$ – the probability that the parameter x (for example, the queue length) is greater than the parameter B;

H – is the Hurst Exponent (self-similarity parameter). The Hurst Exponent H represents a measure of the statistical phenomenon stability or the long-term dependence over time. The value $H = 5.0$ indicates that there isn't long-term dependence. The closer the value of H is to 1, the higher the degree of stability of the long-term dependence. Research on the various types of traffic in modern computer networks assumes values of the Hurst Exponent for most applications between 0.5 and 1 ($0.5 < H < 1.0$) [14].

Based on expression (2) the parameter α of the Weibull distribution can be expressed through the Hurst Exponent as follows:

$$\alpha = 2 - 2H \quad (6)$$

Therefore, during the investigation of a queuing system (G/G/1) with priorities and fractal input traffic, the parameter α of the Weibull distribution will be in the interval $0 < \alpha < 1$.

The following formula can be used to calculate the probability of loss when using ATM technology.

$$P_{loss} = \frac{d}{\beta * (\beta - 1)} * \lambda^{\beta} (\lambda_{\Sigma} * \tau)^{1+\beta}) W^{1-\beta} \quad (7)$$

where β – parameter related to the Hurst Exponent by the following way $\beta = 3 - 2H$;

τ – average transmission time from one source;

λ – flow intensity of one source;

λ_{Σ} – cumulative flow intensity from several sources;

d – normalizing coefficient.

This formula is empirical, and its application is limited to ATM technology. For G/M/1 type QS models with the input flow described by the Gamma with the distribution parameter 0.5, the following loss probability formula is proposed for such a system [6]:

$$P_{loss} = \frac{\left(1 - \frac{\rho}{4} - \sqrt{\left(\frac{\rho^2}{16} + \frac{\rho}{2}\right)}\right)}{1 - \left(\frac{\rho}{4} + \sqrt{\left(\frac{\rho^2}{16} + \frac{\rho}{2}\right)}\right)^{W+2}} * \left(\frac{\rho}{4} + \sqrt{\left(\frac{\rho^2}{16} + \frac{\rho}{2}\right)}\right)^{W+1} \quad (8)$$

4. Simulation results

To conduct the research, the dependencies $P_{loss} = f(\rho)$ were constructed (using formulas (1), (2), (3)) for different values of $W = \{5,10,15,20\}$ taking into account different values of the Hurst Exponent $H = \{0.6, 0.8, 0.95\}$ and for different deviation coefficients $C = \{4,20\}$ (shown in Fig. 1). The dependencies $P_{loss} = f(W)$ were also constructed for different values of $\rho = \{0.2,0.4,0.5,0.6\}$ (shown in Fig. 2).

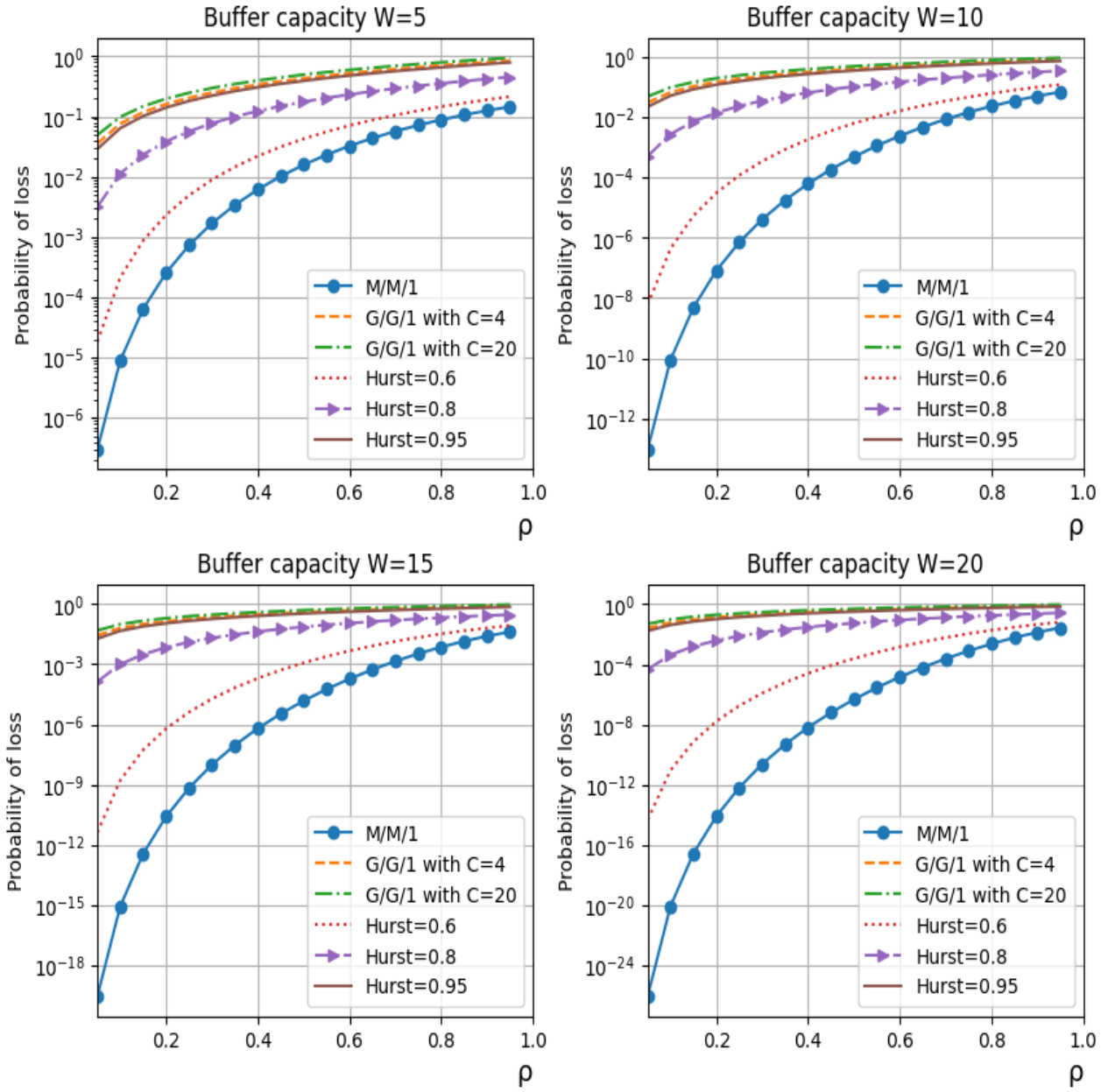

Fig. 1. Dependences of the probability of packet loss on the load factor $P_{loss} = f(\rho)$ for different sizes of the buffer capacity

A program in Python was written to obtain dependency graphs. The NumPy and Matplotlib libraries were used for numerical computation and chart visualization.

The most optimistic estimation is given by formula (1) for the QS model M/M/1, which follows from the above dependencies. This evaluation can be used as a lower bound for the message loss probability for a given buffer capacity W and channel load factor ρ. The highest message loss probability is observed when using QS with a Hurst parameter of 0.95. Increasing the traffic fractality and deviation coefficient increases the packet loss probability P_{loss}. The influence of fractality decreases as the buffer capacity increases.

The given graphs show that an objective evaluation of the packet loss probability due to buffer storage overflow can only be made by considering the nature of the traffic. Otherwise, this probability can be determined with a large degree of error. Based on the type of traffic and its fractality in accordance with Table 2 and Formula 2, the range of packet loss probability can be determined.

Each type of traffic has its own degree of fractality (Table 2).

The main types of network traffic have a Hurst Exponent greater than 0.6 (Table 2). For such traffic, the probability of message loss should be determined using formula (3).

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

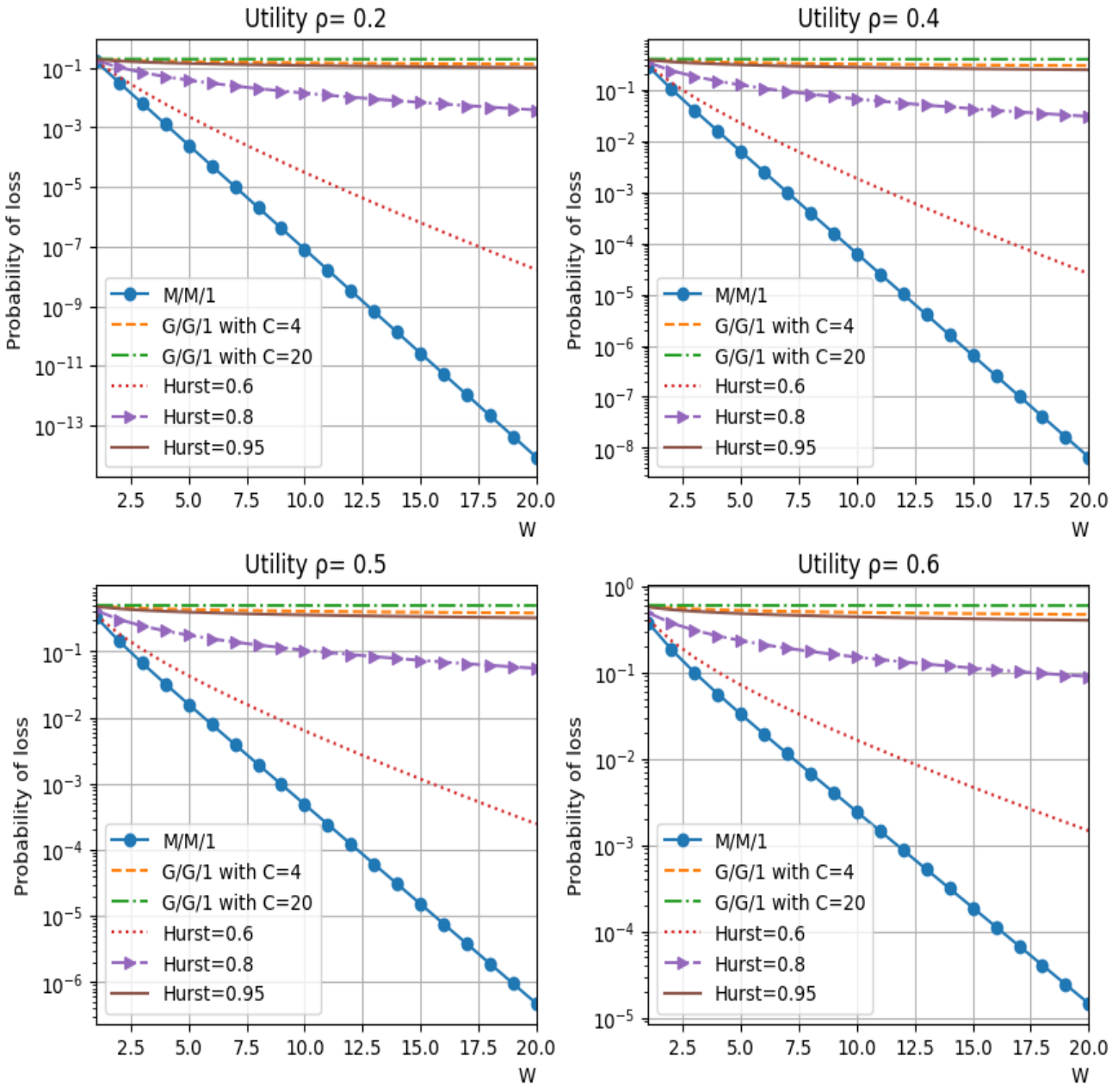

Fig. 2. Dependence of the probability of packet loss on the buffer capacity $P_{loss} = f(W)$ for different channel loads (utility)

Table 2

Fractality of different traffic types

Types of traffic	Degree of traffic fractality (H)
Ethternet	0.6-0.9
Industry Ethernet	0.6-0.8
IoT	0.5-0.7
HTTP	0.75-0.92
Video	0.6-0.9
Audio	0.6-0.9
P2P	0.6-0.9

5. Case study

To verify the obtained results, a simulation model was developed that simulates a three-way computer network (Fig. 3). The simulation used a topology comprising three parallel paths, each with routers of the same performance and data transmission channels of equal bandwidth. The same amount of RAM is allocated to all flows in all routers. This model is used for the parallel transmission of three data flows. An input flow is transmitted along each path with the same intensity but with different

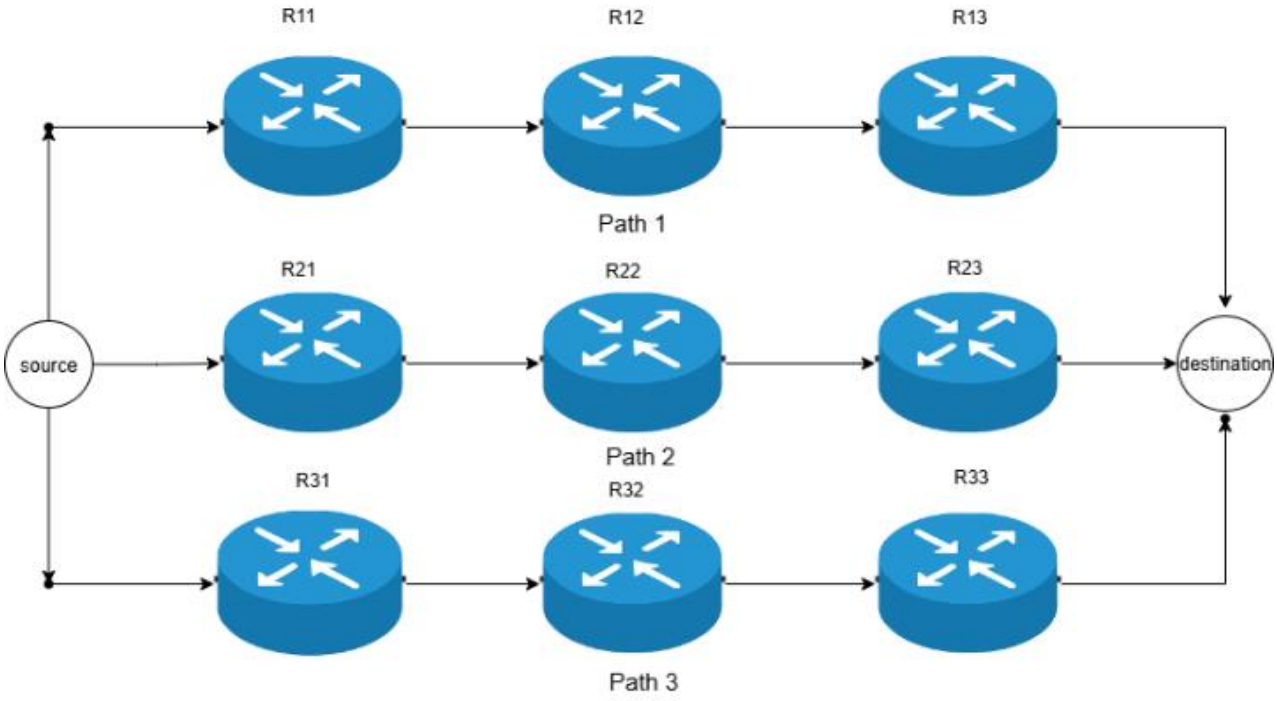

Fig. 3. Computer network scheme

fractality (traffic burstiness). The first input flow simulates the non-phractal traffic and is described by the application receipt exponential law. The second and third flows simulate fractal traffic with varying degrees of fractals.

The simulation results are as follows. With a buffer size of 3 on each router equal to 3 (shown in Fig.4), the percentage of packet losses for normal traffic increases slightly with increasing inbound traffic intensity. With a small fractality (C=2.14), the percentage of transmission losses along a route consisting of three routers increases much faster. For high fractal traffic (C=5.1), the percentage of losses grows much faster.

Figure 5 shows that the loss percentage is significantly lower for all types of traffic with a router buffer

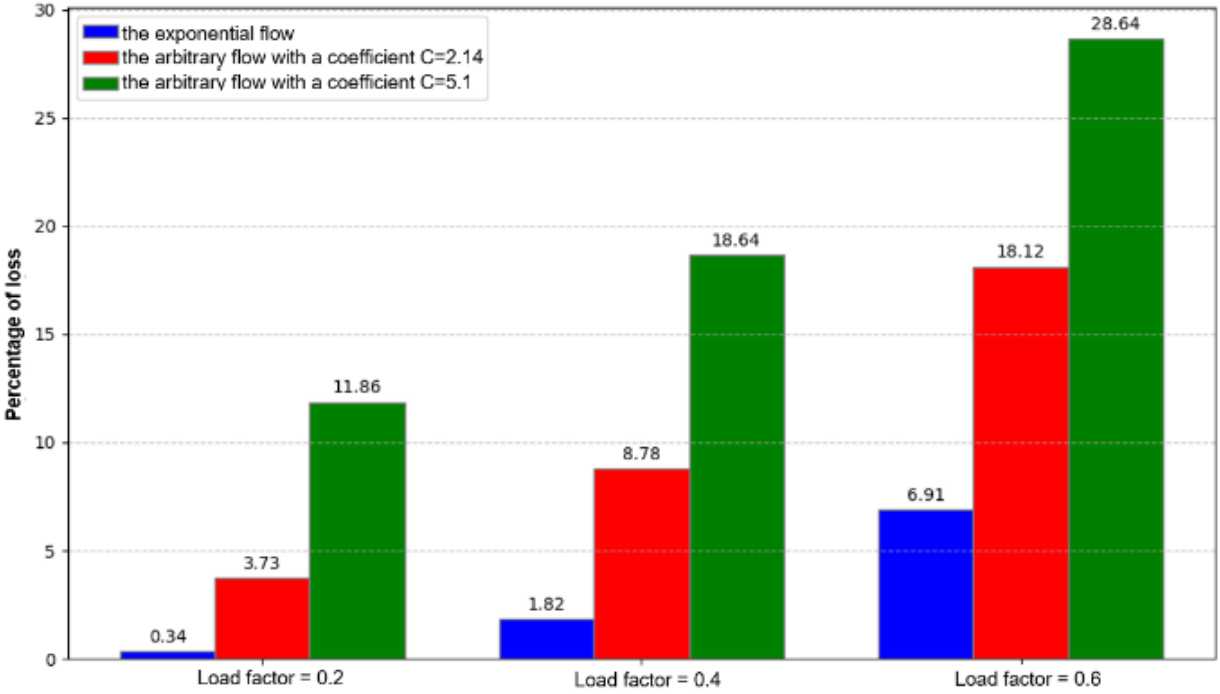

Fig. 4. The dependency of the percentage loss on the load factor at buffer size equal to 3

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

size equal to 5. Figure 6 shows that with a buffer size of 7, the loss rate increases more slowly than with a buffer size of 5 and significantly less than with a buffer size of 3.

From the graphs shown, it can be concluded that a significantly larger buffer volume must be allocated than in the case of transmission of non-fractal traffic to reduce the percentage of losses during fractal traffic transfer. This confirms the theoretical results obtained above.

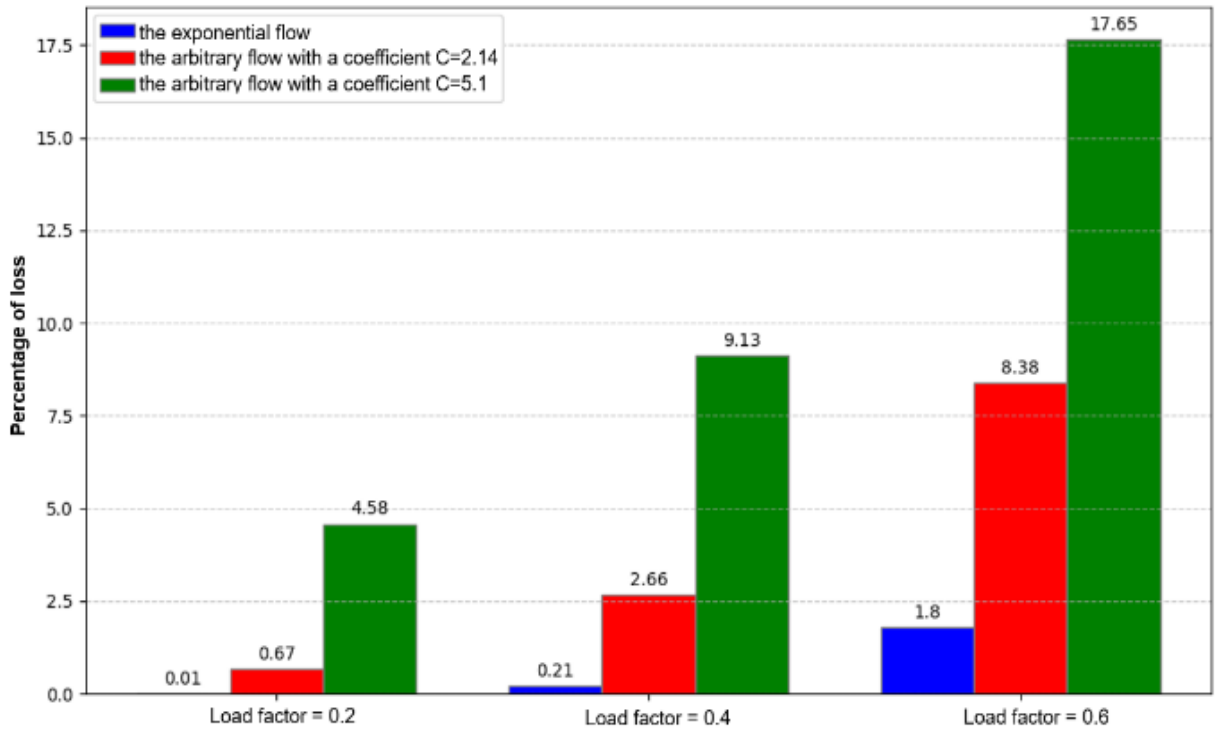

Fig. 5. The dependency of the percentage loss on the load factor at buffer size equal to 5

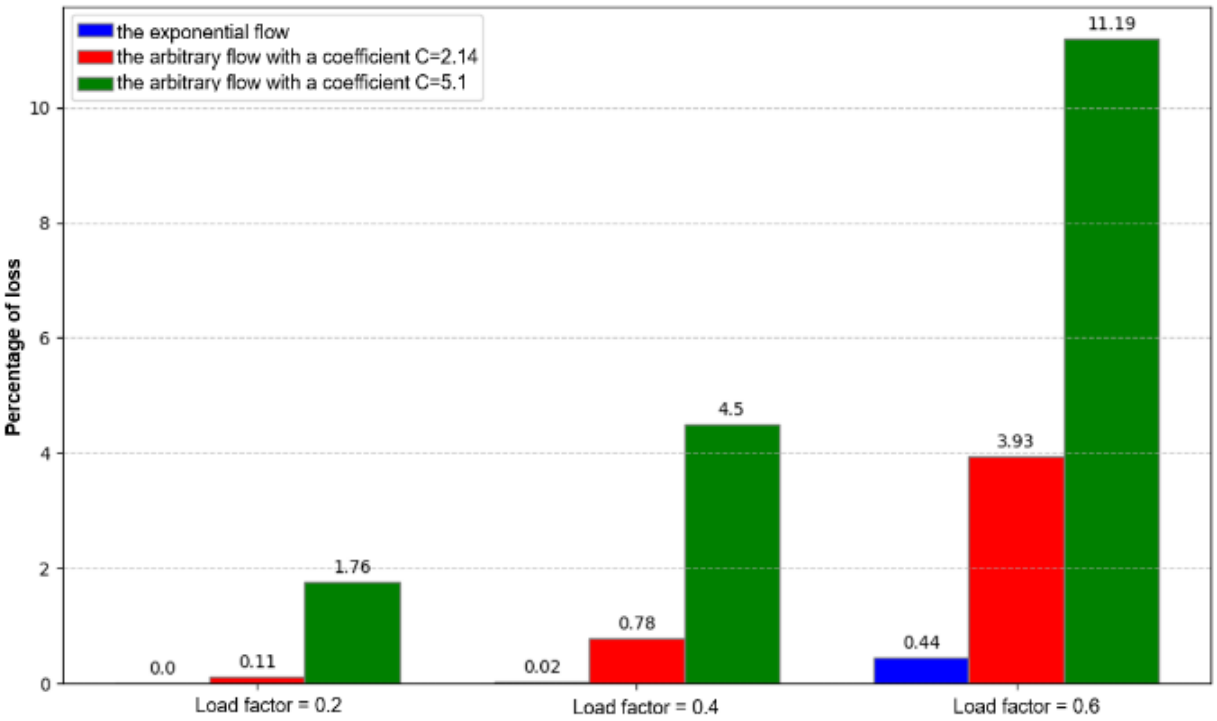

Fig. 6. The dependency of the percentage loss on the load factor at buffer size equal to 7

6. Discussion

According to the experimental results, when comparing the packet loss probability models in a router based on traffic fractality and the dependences of the packet loss probability on the load factor for different buffer capacity, channel load (utility), and Hurst Exponent sizes, we can conclude that:

- the most optimistic estimate is given by the M/M/1 queuing system model. This estimate can be used as a lower bound for the probability of message loss.

- the highest message loss probability was observed when queuing systems with a Hurst exponent of 0.95 were used. This can be explained by the fact that increasing traffic fractality also increases the packet loss probability.

- the influence of fractality decreases with an increase in the buffer capacity.

To determine the probability of packet loss on the router depending on the volume of the storage device and the load factor of the transmission channel, using the fractality values for different types of traffic and formula (3) is recommended.

The proposed model can also be used to solve the inverse problem to calculate the minimum required capacity of the storage device based on the channel load factor and the requirements for the probability of packet loss. In the case that the measurement of traffic fractality is not possible, formula (2) is recommended to calculate the capacity of the storage device for the router.

7. Conclusions and Further Research

A comparative analysis of packet loss probability models in a router based on traffic fractality is presented.

The dependencies of the probability of packet loss $P_{loss}=f(\rho)$ and $P_{loss}=f(W)$ were constructed, and recommendations for these mathematical models were developed.

The present work has shown that various types of network traffic have a fractal nature. This study highlights that the traditional methods of route service specification, such as traffic using the M/M/1 queuing model, give more errors.

Increasing traffic fractality and deviation coefficient increases the probability of message loss. The influence of fractality decreases as the buffer capacity increases.

The given $P_{loss}=f(\rho)$ and $P_{loss}=f(W)$ graphs show that an objective evaluation of the packet loss probability due to buffer storage overflow can only be made by considering the traffic type and its fractality. Otherwise, this probability can be determined with a large degree of error. To reduce the impact of traffic fractality, it is necessary to increase the capacity of buffer storage devices.

The proposed models and dependencies enable the selection of the router buffer size to achieve the required packet loss probability, considering the intensity and traffic fractality. To achieve this, the traffic intensity and its fractal nature must be estimated. The traffic fractality can be obtained based on the type of traffic (see Table 2) or by special measurements of the Hurst exponent.

The main scientific novelty and special scientific contribution of this study are as follows:

1. Evidence and quantification of the fractal nature of modern network traffic. This study empirically and analytically demonstrates that various types of network traffic in modern computer networks (e.g., Ethernet, IndustrialEthernet, IoT, HTTP, Video, Audio, and P2P) have a fractal nature and a significant degree of self-similarity, which is confirmed by the values of the Hurst exponent ($H> 0.6$ for most types of traffic). This is a fundamental difference from the traditional assumptions about the Poisson traffic.

2. Identification of inaccuracies of traditional Queuing System models. This study shows that using the classical M/M/1 Queuing Model to estimate the probability of packet loss in a router buffer leads to significantly underestimated (too "optimistic") and therefore erroneous results under fractal traffic conditions. This emphasizes the need to rethink traditional approaches to network design and management.

3. The impact of fractality and the deviation coefficient are quantified. In this paper, we constructed graphical dependencies based on the proposed models. These dependencies clearly demonstrate that the probability of packet loss increases significantly with an increase in traffic fractality (when the Hurst exponent tends to 1) and the deviation coefficient. These results allow for a quantitative estimation of packet loss probability and waiting time for different types of traffic.

4. Influence of fractality on the buffer capacity. The main practical result is that the impact of traffic fractality on the probability of packet loss decreases with increasing buffer storage capacity. This provides a straightforward engineering solution for minimizing the negative effects of fractality.

5. Rationale for the need to consider the nature of network traffic for an objective assessment. The paper emphasizes that an objective assessment of the probability of packet loss due to a router buffer overflow is possible only if the nature of the traffic (i.e., its type and degree of fractality) is considered. Failure to consider these characteristics leads to high calculation errors.

6. Specification of the practical recommendations. Based on the analysis and simulations, the authors offer specific recommendations on the use of formula (3) to determine the probability of packet loss, considering fractality. They also highlight the need to increase buffer capacity to reduce the impact of traffic fractality.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

In addition, a methodology is proposed for solving the inverse problem, i.e., calculating the minimum required buffer capacity based on the requirements for the packet loss probability and the channel load factor.

Thus, the novelty and contribution of the paper are the comprehensive approach to the packet loss problem. Unlike many previous works, the proposed approach not only recognizes the existence of fractal traffic but also quantitatively studies its impact on the performance of router buffers, while offering practical recommendations for designing more reliable and efficient networks.

Future research directions:

- the formation of a model of packet loss probability in a router buffer for different internetworking technologies other than ATM and analysis of the impact of different network technologies (e.g., software-defined networking (SDN), network function virtualization (NFV)) on the management of fractal traffic and packet loss;

- research on the consequences of fractal traffic for Quality of Service (QoS) guarantees - affect delay, jitter, and other QoS metrics;

- research on the potential connection between fractal traffic characteristics and Distributed Denial of Service (DDoS) attacks;

- research on network topology's influence on the propagation of fractal traffic characteristics and its impact on packet loss at individual routers.

Contribution of the authors: Conceptualization, methodology, packet loss probability models – **Kyrylo Rukkas;** simulation of the dependencies of packet loss on the load factor $P_{loss}=f(\rho)$ for different sizes of the buffer capacity – **Anastasiia Morozova;** simulation of the dependencies of packet loss on the buffer capacity $P_{loss}=f(W)$ for different channel load (utility) – **Ievgen Meniailov**; formation of different values (of the Hurst Exponent, deviation coefficients, buffer capacity, load factor) for simulation – **Myroslav Momot**.

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This study was conducted without any financial support.

Data Availability

The manuscript contains no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All the authors have read and agreed to the published version of this manuscript.

References

1. Millán, G., Lefranc, G., Osorio-Comparán, R., & Lomas-Barrie, V. Time series analysis of computer network traffic in a dedicated link aggregation. *Preprint for IEEE Transactions on Information Theory 2021*. 7 p. DOI: 10.48550/arXiv.2107.05484.

2. Dymora, P., & Mazurek, M. Influence of model and traffic pattern on determining the self-similarity in IP networks. *Applied sciences,* 2021, vol. 11, iss. 1, article 190. DOI: 10.3390/app11010190.

3. Millán, G., & Lefranc, G. Presentation of an estimator for the Hurst parameter for a self-similar process representing the traffic in IEEE 802.3 networks. *International Journal of Computers, Communications & Control (IJCCC),* 2009, vol. 4, no. 2, pp. 137-147. DOI:10.15837/ijccc.2009.2.2421.

4. Bunimovich, L., & Skums, P. Fractal networks: Topology, dimension, and complexity. *Chaos*, 2024, vol. 34, iss. 4, article 042101. ISSN: 1054-1500. DOI: 10.1063/5.0200632.

5. Mohammed, A. M., & Agamy, A. F. A survey on the common network traffic source models. *International Journal of Computer Networks (IJCN)*, 2011, vol. 3, iss. 2, pp. 103-115. Available at: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCN-136 (accessed 20.01.2025).

6. Melo, E. F., & de Oliveira, H. M. An overview of self-similar traffic: its implications in the network design. *Revista de Tecnologia da Informação e Comunicação*, 2020, vol. 9, no. 1, pp. 38-46. DOI: 10.48550/arXiv.2005.02858.

7. Dymora, P., Mazurek, M., & Strzalka, D. Computer network traffic analysis with the use of statistical self-similarity factor. *Annales Universitatis Maiae Curie-Sklodowska*, *Sectio AI Informatica*, 2013, vol. 13, no. 1, pp. 69-81. DOI:10.2478/v10065-012-0040-0.

8. Bhoi, R., & Mishra, S. Analysis and fractal behavior of network traffic data based on topology. *International Journal of Engineering Science Invention*, 2017, vol. 6, iss. 10, no. 1, pp. 66-69. Available at: http://www.ijesi.org/papers/Vol(6)10/Version-1/K0610016669.pdf (accessed 20.01.2025).

9. Millan, G., Osorio-Comparan, R., & Lefranc, G. Preliminaries on the accurate estimation of the hurst exponent using time series. *Proceedings of 2021 IEEE International Conference on Automation/24th Congress of the Chilean Association of Automatic Control,*

(ICA - ACCA), 2021, article 9465274. DOI: 10.1109/ICAACCA51523.2021.9465274.

10. Sivaroopan, N., Silva, K., Madarasingha, C., Dahanayaka, T., Jourjon, G., Jayasumana, A., & Thilakarathna, K. A Comprehensive survey on network traffic synthesis: from statistical models to deep learning. *arXiv e-prints*, 2025. 33 p. DOI: 10.48550/arXiv.2507.01976.

11. Han, D., Li, H., Fu, X., & Zhou, S. Traffic feature selection and distributed denial of service attack detection in software-defined networks based on machine learning. *Sensors*, 2024, vol. 24, article no. 4344. 22 p. DOI:10.3390/s24134344.

12. Zaidyn, M., Akhtanov, S., Turlykozhayeva, D., Temesheva, S., Akhmetali, A., Skabylov, A., & Ussipov, N. Fractality of wireless mesh networks: dimensional effects on network performance. *arXiv e-prints*, 2025. 11 p. DOI: 10.48550/arXiv.2506.19366.

13. Meleshko, Y., Drieieva, H., Drieiev, O., Yakymenko, M., Mikhav, V., & Shymko, S. A method of routing of fractal-like traffic with prediction of router load for reduce the probability of network packet loss. *Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems (CoLInS)*, 2023, vol. 3 pp. 434-448. Available at: https://ceur-ws.org/Vol-3403/paper34.pdf (accessed 20.01.2025).

14. Castellanos-López, S. L., Cruz-Perez, F. A., Rivero Ángeles, M. E., & Hernandez-Valdez, G. Count and Teletraffic Analysis of G/M/1 Queueing Systems with Log-Normal Interarrival Time of Bursty IoT Traffic. *IEEE Access*, 2025, vol. 13, pp. 50611-50634. DOI: 10.1109/ACCESS.2025.3543460.

Received 16.02.2025, Accepted 25.08.2025

АНАЛІЗ МОДЕЛЕЙ ЙМОВІРНОСТІ ВТРАТИ ПАКЕТІВ У БУФЕРІ МАРШРУТИЗАТОРА З УРАХУВАННЯМ ФРАКТАЛЬНОСТІ ТРАФІКУ

К. М. Руккас, А. Г. Морозова, Є. С. Меняйлов, М. О. Момот

Предметом дослідження є різноманітні види мережевого трафіку в сучасних комп’ютерних мережах, який має складну структуру і часто має певний ступінь самоподібності. Ефективне використання ресурсів мережі та забезпечення якості обслуговування абонентів є важливими завданнями комп'ютерних мереж. Імовірність втрати повідомлення через переповнення буфера запам'ятовуючих пристроїв є важливим параметром у визначенні якості обслуговування. Для оцінки цього параметра слід використовувати математичну модель. Останні досягнення містять багато різних моделей ймовірності втрати пакетів у буфері маршрутизатора. Однак багато моделей не враховують характеристики трафіку різних сучасних програм і протоколів. Трафік в сучасних комп'ютерних мережах має складну структуру і часто має певну ступінь самоподібності. В даний час існує велика кількість моделей для оцінки ймовірності втрати пакетів через переповнення буфера. Метою даної роботи є порівняльний аналіз таких моделей та рекомендації щодо їх використання та оцінка впливу фрактальності мережевого трафіку на ймовірність втрати пакетів у маршрутизаторі через переповнення буфера. Завдання, які вирішуються: 1) провести аналіз аналітичних моделей, що описують ймовірність втрати пакетів у маршрутизаторі як з урахуванням впливу фрактальності, так і без неї; 2) побудувати залежності ймовірності втрати пакетів у маршрутизаторі від завантаженості каналу передачі даних для різних значень ємності буфера, показника Херста та відхилення трафіку; 3) описати залежності ймовірності втрати пакетів від ємності буфера для різних значень завантаження каналу. Використані методи порівняльного аналізу різних методів фрактального моделювання трафіку та симуляції з різними значеннями ємності зберігання, показника Херста, коефіцієнтів відхилення та коефіцієнта завантаження каналу. Були отримані наступні результати: 1) найбільш оптимістичну оцінку дає модель системи масового обслуговування M/M/1; цю оцінку можна використовувати як нижчу межу для ймовірності втрати повідомлення для заданої ємності буфера та коефіцієнта завантаження каналу; 2) найвища ймовірність втрати повідомлення спостерігалася при використанні систем масового обслуговування з показником Херста 0,95; 3) у статті було показано, що зі збільшенням фрактальності трафіку та коефіцієнта відхилення ймовірність втрати пакетів також зростає; 4) виявлено, що вплив фрактальності зменшується зі збільшенням буферної ємності; 5) об’єктивна оцінка ймовірності втрати повідомлення через переповнення буфера маршрутизатора може бути зроблена лише з урахуванням характеру показаного трафіку. Висновки. Основний внесок цього дослідження полягає в тому, що різні типи мережевого трафіку мають фрактальну природу, а традиційні методи специфікації маршрутних послуг такий трафік з використанням моделі масового обслуговування M/M/1 дає більше помилок. В результаті проведених досліджень з метою зменшення впливу фрактальності трафіку необхідно збільшити ємність буферних накопичувачів.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Ключові слова: мережа; пакет; ймовірність втрати пакета; маршрутизація; буфер; фрактальність трафіку; показник Херста.

Руккас Кирило Маркович – д-р техн. наук, доц., проф. каф. теоретичної та прикладної інформатики, Харківський національний університет ім. В. Н. Каразіна, Харків, Україна.

Морозова Анастасія Геннадіївна – канд. техн. наук, доц. каф. теоретичної та прикладної інформатики, Харківський національний університет ім. В. Н. Каразіна, Харків, Україна.

Меняйлов Євген Сергійович – канд. техн. наук, доц., в.о. зав. каф. теоретичної та прикладної інформатики, Харківський національний університет ім. В. Н. Каразіна, Харків, Україна.

Момот Мирослав Олександрович – канд. техн. наук, доц., доц. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Kyrylo Rukkas - Doctor of Technical Sciences, Associate Professor, Professor at the Theoretical and Applied Informatics Department, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: rukkas@karazin.ua, ORCID: 0000-0002-7614-0793.

Anastasiia Morozova - Candidate of Technical Science, Associate Professor at the Theoretical and Applied Informatics Department, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: a.morozova@karazin.ua, ORCID:0000-0003-2143-7992.

Ievgen Meniailov – PhD in Mathematical Modelling and Optimization Methods, Associate Professor, Acting Head of the Theoretical and Applied Informatics Department, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: evgenii.menyailov@gmail.com, ORCID: 0000-0002-9440-8378.

Myroslav Momot – Candidate of Technical Science, Associate Professor, Associate Professor at the Computer Science and Information Technologies Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: m.momot@khai.edu, ORCID: 0000-0003-2580-5908.