


Article

Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks

Andrey Privalov ¹, Igor Kotenko ^{2,*}, Igor Saenko ², Natalya Evglevskaya ³ and Daniil Titov ¹

¹ Electrical Communication Department, Emperor Alexander I Saint-Petersburg State Transport University, 9 Moskovsky pr., St. Petersburg 190031, Russia; aprivalov@inbox.ru (A.P.); titovdd178@gmail.com (D.T.)

² Saint-Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS) 39, 14 Liniya, 199178 St. Petersburg, Russia; ibsaen@comsec.spb.ru

³ St. Petersburg Signal Academy, 3 Tikhoretsky Ave., 194064 St. Petersburg, Russia; n.evglevskaya@gmail.com

* Correspondence: ivkote@comsec.spb.ru

Abstract: Cyberattacks against the elements of technological data transmission networks represent a rather significant threat of disrupting the management of regional electric power complexes. Therefore, evaluating the functioning quality of data transmission networks in the context of cyberattacks is an important task that helps to make the right decisions on the telecommunication support of electric power systems. The known models and methods for solving this problem have limited application areas determined by the admissible packet distribution laws. The paper proposes a new method for evaluating the quality of the functioning of data transmission networks, based on modeling the process of functioning of data transmission networks in the form of a stochastic network. The proposed method removes restrictions on the form of the initial distributions and makes the assumptions about the exponential distribution of the expected time and packet servicing in modern technological data transmission networks unnecessary. The method gives the possibility to evaluate the quality of the network functioning in the context of cyberattacks for stationary Poisson transmission and self-similar traffic, represented by Pareto and Weibul flows models. The obtained evaluation results are in good agreement with the data represented in previously published papers.

Keywords: cyberattack; data transmission network; stochastic network; equivalent function; Laplace–Stieltjes transform; distribution function; functioning quality; delivery time of data packets; jitter; packet loss probability



Citation: Privalov, A.; Kotenko, I.; Saenko, I.; Evglevskaya, N.; Titov, D. Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks. *Energies* **2021**, *14*, 4755. <https://doi.org/10.3390/en14164755>

Academic Editor: Horia Andrei

Received: 30 June 2021

Accepted: 29 July 2021

Published: 5 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

According to the general global trend of the growth of information needs over the last 15–20 years, modernization of communication networks in the power industry is in progress; outdated networks are being replaced and digital telecommunication systems for processing and data transmission are being created.

The result of such modernization should be a unified technological communication system of the power industry, which is necessary for the stable operation of the whole power system and its components [1]. Large-scale implementation of packet telecommunication technologies in the power system largely ensures the cost-effective and uninterrupted functioning of all elements of electrical network, from control centers to substations and high-, medium- and low-voltage distribution devices (Figure 1).

A modern digital telecommunication network must meet the requirements of reliability, stability, security and efficiency in any of its segments.

The significant impact of the quality of the resources provided by the energy system on the development of most sectors of the national economy determines, on the one hand, high requirements for packet data transmission networks, and on the other hand, increased attention on them by intruders, whose targets are elements of the energy complex.

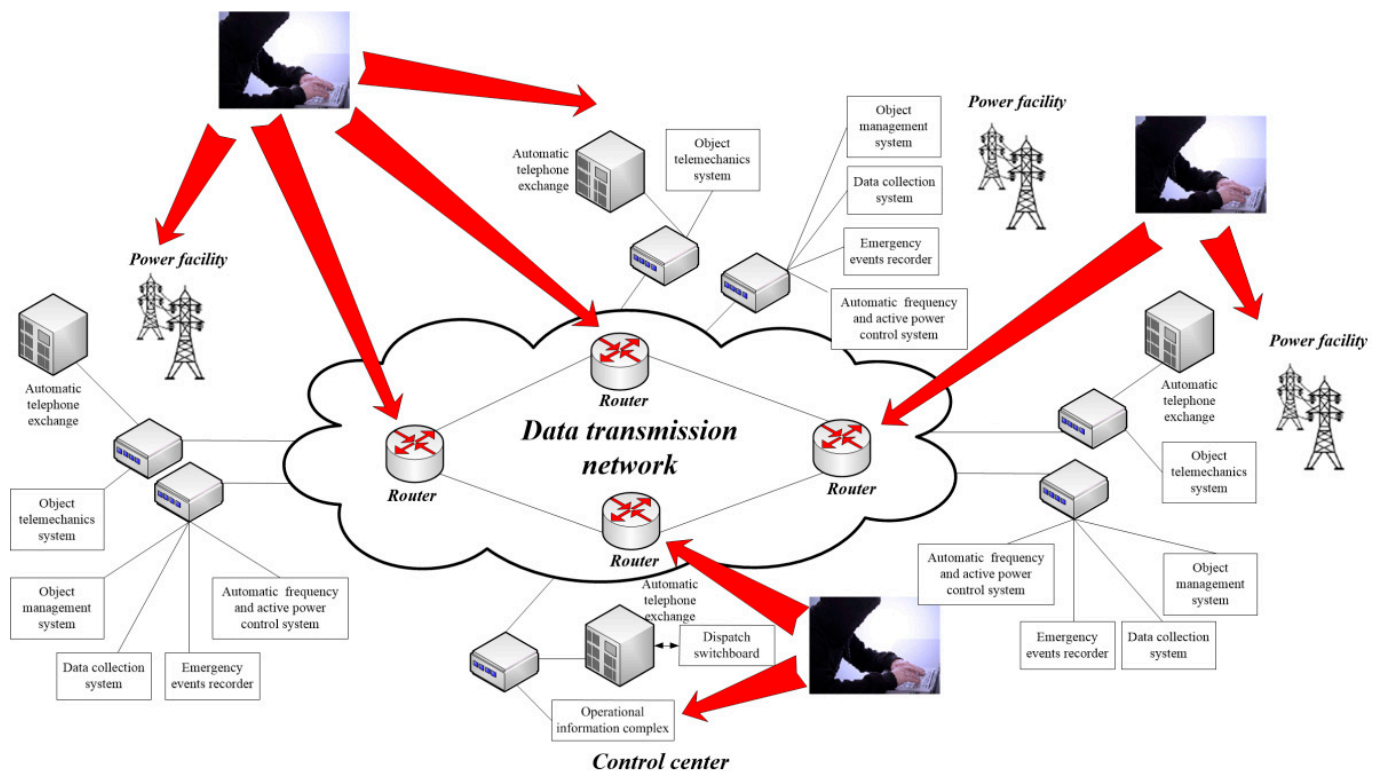


Figure 1. The location of the technological data transmission network in the branch electric power complex.

In fuel–power complex companies, the telecommunications network is usually divided into two segments—corporate and technological. The corporate segment is represented by a range of interconnected local area networks. The technological segment consists of the technological data transmission network (DTN).

In local area networks, there are workplaces for employees whose activities are not directly related to the management of industrial equipment. After penetration into the company’s infrastructure, malefactors are likely to get into this section of the network. Here, malefactors will be interested in computers that store confidential information. However, since the main goal of a cyberattack on the fuel and energy complex is the possibility of influencing production processes, the malefactor will not stop at the corporate segment. He/she will try to intrude into the technological segment, from which industrial systems are controlled, i.e., into the technological DTN. The malefactor will try to find a way to automatically control systems of technological processes, supervisory control and data acquisition (SCADA), industrial controllers, automatic blocking systems, relay protection terminals and other technological resources, depending on the goals of the malefactor. For example, when the malefactor carries out a cyberattack at an electrical substation, his/her intrusion in the behavior of the protective automation, in the case of an abnormal situation, can lead to power cuts for consumers. When the malefactor takes control of the main nodes of the network, he/she will be present secretly in the network until a decision is made to realize the active actions. However, it is possible that after examining reliable ways for access to important objects, the malefactor will leave the network to reduce the risk of his/her detection and return later.

Obviously, a technological DTN should be isolated from the corporate segment, but this does not always happen. Remote access to isolated segments can be carried out from dedicated computers of administrators who create special communication channels in order to simply implement their tasks.

In some companies, a technological DTN is completely separated from the corporate segment. This fact significantly complicates the implementation of cyberattacks, but does not mean that a malefactor’s access to the technological DTN is impossible. In this case,

malefactor can use other methods. The technique of replication through removable media, i.e., moving over the network using removable devices, was used in cyberattacks of a cybergroup called the “Equation Group”, which is one of the most powerful groups and has functioned since 2001. It was discovered by the Russian company Kaspersky Lab. The cybergroup was named the “Equation Group” because their members actively used encryption algorithms, advanced masking methods and other smart technologies.

The Fanny Trojan created a hidden section on a USB drive, where the commands were recorded as received from the control server. When an employee connected a USB flash drive to a computer of an isolated network, these commands were executed automatically. The Equation Group used a zero-day vulnerability in the .lnk file handler, so autorun shutdown on removable devices could not stop the Trojan spreading. The collected data were again written in the hidden section of the USB flash drive, and then, when the USB flash drive was connected to a computer with Internet access, the data were transmitted to the malefactors’ server [2].

By carrying out cyberattacks on automated systems and technological DTNs, malefactors disrupt the normal functioning of the power complex elements [3]. Therefore, the automation systems and technological DTNs that are being implemented in power complexes must provide operational management of energy resources, as well as meet the high cybersecurity requirements for both automation system elements and technological DTNs. Therefore, the task of evaluating the quality of the functioning of the technological DTN of the energy complex is relevant when a malefactor implements cyber actions.

This paper proposes and discusses one of the possible mechanisms to measure the impact of cyberattacks against the network elements of a technological DTN when assessing the quality of its functioning by the value of the probability of the successful delivery of data packets that provide control of the power complex elements.

By means of the mathematical tools of graphical evaluation and review technique (GERT) networks [4–6], the paper proposes a novel method, the essence of which is to represent the process of the functioning of the data transmission network, when malefactors realize a cyberattack, as a stochastic network, to specify the type of individual distributions, to determine an equivalent function, with the initial and central moments of distributions of the original random values calculated by means of numerical methods and specification of the final distribution function of the data packets’ delivery time.

The method proposed by the authors allows one to remove restrictions on the type of distributions which are used as original ones, and this method is free from the assumptions, indicated in [7,8], about the exponential distribution of the duration of packet waiting and service (transmission) in modern technological data transmission networks.

The novelty of the proposed method lies in defining the parameters of the quality of the service of the network in the context of cyberattacks in the absence of restrictions on the type of distribution functions of the transmission time, the duration of the successful realization of cyberattacks, the recovery time of the network elements and the type of network traffic.

The paper proposes the following new results:

- a mechanism taking into account the influence of cyberattacks on the quality parameters of a technological DTN is developed;
- a set of expressions for calculating the values of the distribution function and the times of the delivery of data packets in cyberattack conditions is obtained in an explicit form;
- the sensitivity of the results obtained on the type of traffic in the technological DTN is shown.

The rest of the paper is structured as follows. Section 2 reviews relevant papers on the research topic. Sections 3 and 4 describe the theoretical foundations of the proposed approach: Section 3—the problem statement, Section 4—the method to measure the impact of cyberattacks. Section 5 demonstrates the efficiency of the suggested method. Section 6

outlines the results of an experimental evaluation of the proposed approach. Section 7 contains the main conclusions on the work and directions for further research.

2. Related Work

To develop a mechanism for evaluating cyberattack actions and their impact on the functioning quality of data transmission networks, we will briefly review the existing approaches to evaluating the functioning quality of modern data transmission networks used to ensure the stable operation of automated control systems for technological processes.

The stated requirement for the use of a data transmission network allows one to distinguish, among a lot of quality indicators, which are standardized by the ITU-T, ETSI, 3GPP and IETF recommendations and existing locally produced directive documents, only those indicators that conform with the requirements imposed by the control system of technological processes for the information exchange process. Among such indicators, we can choose:

- data transmission path capacity, characterized by the average data transmission speed;
- the probability of data loss, estimated by the value of the probability of packet loss;
- data delay time, calculated as the average delivery time of a message (data packet) and jitter of the specified time.

In this case, the mechanism, which is under development, should take into account the randomness of flows transmitted in modern technological data transmission networks and their features, among which the main ones are significant nonstationarity and pulsations with long-term dependencies, explained by the existence of self-similarity (fractality) in the data flow [9–12].

In [10,13–17], an approach is proposed for the calculation of the packet loss probability, based on the usage of fundamental expressions, obtained for queuing systems M/M/1, taking into account the flow categorization and the claim operation discipline with the introduction of equalizing coefficients, considering the traffic variability [13], the Hurst index [10,14] and related parameters [15–17]. These works surely make a noticeable contribution to the development of the methods of teletraffic theory, but they do not take into account the impact of cyberattacks on packets losses.

The works [18–22] are focused on the calculation of the probabilistic and temporal characteristics of the data transmission network, such as the average data transmission speed, average queueing time and delay time jitter. In this case, the main attention in calculating the required values is given to taking into account the self-similarity of the transmitted data flow. In our opinion, the analysis of calculation methods has been carried out more completely in [22], where relations for determining the distribution functions of the data delay time, taking into account the categorization of the transmitted flows and their self-similarity. In this case, the distribution functions of the waiting time and the service time are approximated by exponential distributions. At the same time, the analysis of the Laplace–Stieltjes transformation of the service and waiting time distribution function given in [21,22] shows that this distribution is not exponential, therefore the delay time distribution is not exponential either; this distribution is defined as an integral convolution of the service and waiting time distributions. Besides that, the results given in these works do not take into account how results of the cyberattack implementation by a malefactor influence the value of the calculated parameters.

To evaluate the functioning quality of DTNs and to evaluate the protection mechanisms of telecommunication networks, in [7,8,23] it is proposed to use a complex of GERT models that allows one to estimate the average time and dispersion of the metadata file transmission time, organization and delivery time of control transfer commands to a software client of the telecommunication network. The main restriction of the solutions obtained in [7,8] is the limitation on the type of traffic transmitted in the network and the usage of individual exponential distributions characterizing the realization time of individual processes, namely, the transmission of an information packet and the formation and delivery of control transmission commands.

Thus, the main disadvantage of the approaches discussed above is the lack of mechanisms for evaluating the impact of cyberattacks on the quality of the technological DTN function. In addition, the outlined related works are limited to the considered packet distribution laws in the DTN. The proposed method removes these restrictions.

3. Problem Statement

Let us suppose that there is a data transmission network. In this data transmission network, data transmission routes are organized for information exchange in accordance with the required quality of user service (Figure 2).

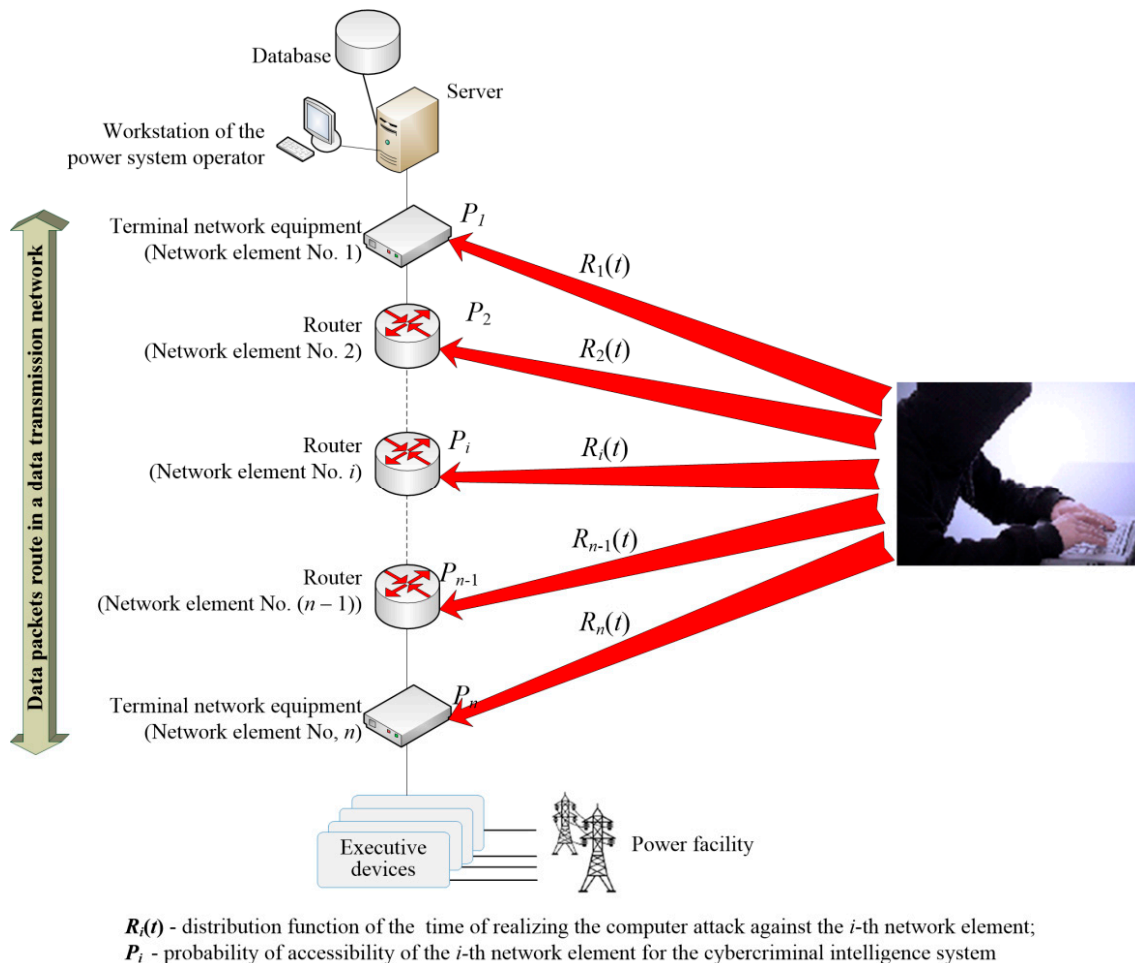


Figure 2. The route plan of the data packets' transmission in a network, functioning in the context of cyberattacks.

Let us suppose that the designated route for data delivery contains $(n - 1)$ sections and n nodes (including terminal network elements), each of which can be exposed to cyberattacks. In a general way, the data packet transmission time t_b is a random value that is characterized by the distribution function $B(t)$ and is specified by the volume V , the transmission speed S and the number of sections on this route n , i.e., $t_b = \frac{(n-1)V}{S}$.

Let us assume that a malefactor realizes a destructive information impact (cyberattack) on the data transmission network; in this case, the functioning of network elements is disrupted in a random time t_{ri} with the distribution function $R_i(t)$, where i is a number of the network element, $i = \overline{1, n}$.

The availability of network elements for the implementation of a cyberattack by a malefactor is characterized by the probability P_i that is determined using the known model of the cybercriminal intelligence system [8,24,25]. If the malefactor's actions are successful, then in a random time t_{di} with the distribution function $\Delta_i(t)$, $i = \overline{1, n}$, the network

administrator detects the impact and realizes measures to restore the functioning of the damaged network element because of the cyberattack, and the data packet received for transmission is transmitted again.

Data packets arrive at the input of the transmission route with intensity λ_{input} . The value of this intensity is determined in accordance with a specified network traffic model. In this case, a data packet received for transmission waits for operation during some time t_w with distribution function $W(t)$, which depends on the time of the successful transmission of the previously received data packet, the storage capacity K at the input of the network element and the characteristics of the incoming traffic.

Assumptions are as follows: operation is carried out according to the rule “first come, first served” and the coefficient of operational reliability of the network equipment is equal to one.

We need to determine the distribution function of the delivery time of data packets to the final user.

Let us present the process of data packet flow transmission, described in a task statement, in the form of a stochastic network (Figure 3).

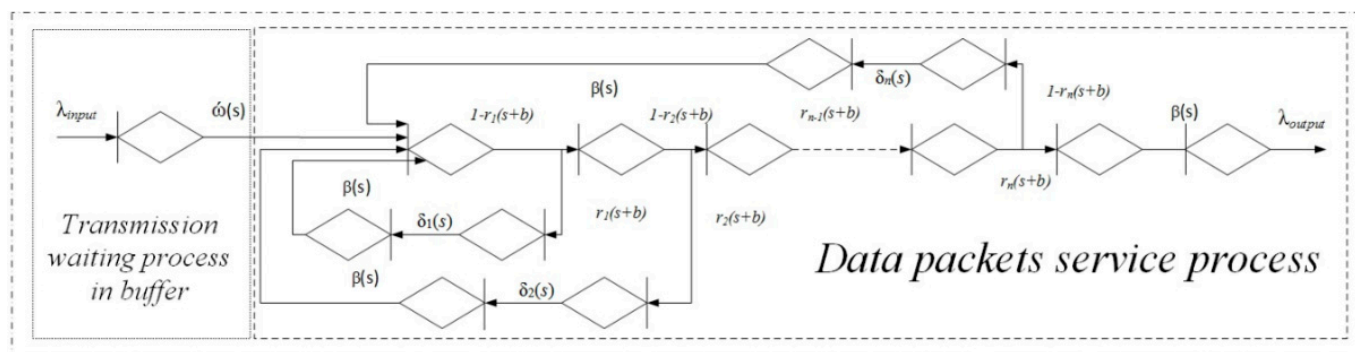


Figure 3. Stochastic network of data packet delivery process in the context of cyberattacks.

It is denoted in Figure 3 that:

$$\beta(s) = \int_0^\infty e^{-st} d[B(t)] \tag{1}$$

- Laplace–Stieltjes transformation of the distribution function of packet transmission time $B(t)$ without taking into account the malefactor’s information impact with a distribution parameter equal to $b = 1/\bar{t}_b$;

$$\delta_i(s) = \int_0^\infty e^{-st} d[\Delta_i(t)], i = \overline{1, n} \tag{2}$$

- Laplace–Stieltjes transformation of the distribution function of restoration time of the i -th network element functioning after a malefactor’s cyberattack with a distribution parameter equal to $d_i = 1/\bar{t}_{di}$;

$$r_i(s) = \int_0^\infty e^{-st} d[R_i(t)]; i = \overline{1, n} \tag{3}$$

- Laplace–Stieltjes transformation of the distribution function of the successful realization of the cyberattack against the i -th network element;

$$\omega(s) = \int_0^\infty e^{-st} d[W(t)] \tag{4}$$

- Laplace–Stieltjes transformation of the distribution function of service waiting time by packet.

It is observed in Figure 3 that the process of the data packet delivery contains a waiting subprocess, characterized by the transformation $\omega(s)$, and a service subprocess, characterized by the transformation $h(s)$ (Figure 4).



Figure 4. Enlarged stochastic network of the packet delivery process.

Therefore, we will solve the problem in two stages: at the first stage we will define the equivalent function of the part of the stochastic network which corresponds to the service process (data packet transmission) $h(s)$ and at the second stage— $\omega(s)$.

This sequence is due to the fact that the waiting time of the packet service depends not only on the characteristics of network traffic, but also on the time of the successful transmission of data packets along the advisory route.

4. Method for Evaluating the Impact of Cyberattacks

Let us consider the stages to solve the formulated problem.

4.1. The First Stage

Using the Mason equation for closed graphs [4–6], we shall define the equivalent function $h(s)$ of the stochastic network fragment (Figure 3) which corresponds to the service process:

$$h(s) = \frac{k_f \prod_{i=1}^n [1 - r_i (s + b)] (\bar{d} + \bar{c} + s) \beta(s)}{\left(1 - \sum_{i=1}^n r_i (s + b) \delta_i(s) \beta(s) \prod_{i=1}^{n-1} [1 - r_i (s + b)]\right) (\bar{d} + s)}, \tag{5}$$

where b is a mathematical expectation of the data packet transmission time;

$\bar{d} = \frac{1}{n} \sum_{i=1}^n \frac{P_i}{t_{di}}$ —mathematical expectation of the intensity of restoring the functioning of network elements after the successful realization of the cyberattack;

$\bar{c} = \frac{1}{n} \sum_{i=1}^n \frac{P_i}{t_{ri}}$ —mathematical expectation of the intensity of the information impact against network elements, each of which is accessible for the cybercriminal intelligence system, and realization of cyberattack with probability P_i [3,24];

$k_f = \frac{\bar{d}}{\bar{d} + \bar{c}}$ —coefficient that has the meaning of the probability of the successful operation of the network equipment when network traffic is absent until the time of the successful realization of the cyberattack, assuming that during the restoration of the function, the network element is not used for its intended purpose [24].

It is known [4,5,26] that knowledge of the equivalent function (5) allows one to determine the initial moments of the random delivery time by the means of numerical methods,

$$M_k = (-1)^k \frac{d^k}{ds^k} \left\{ \frac{h(s)}{h(0)} \right\}_{s=0}, \tag{6}$$

followed by using Pearson nomograms [27] to determine the desired distribution function.

However, many years of experience in the use of nomograms by the authors [27] for modeling complex organizational and technical systems shows that in the absolute majority of cases, the solution converges to a type III Pearson distribution, i.e., approximation of the real distribution function by an incomplete gamma function, which is consistent

with [28,29] and is confirmed by system studies [8,30]. In this case, the parameters of the shape and scale of the gamma distribution are determined as

$$\alpha = \frac{M_1^2}{M_2 - M_1^2}; \mu = \frac{M_1}{M_2 - M_1^2}, \tag{7}$$

and the distribution function of the service time (successful transmission in the context of cyberattacks) of the data packet is of the form:

$$H_\gamma(t) = \frac{\mu^\alpha}{\Gamma(\alpha)} \int_0^t x^{\alpha-1} \exp\{-\mu x\} dx, \tag{8}$$

this form corresponds to Laplace–Stieltjes image

$$h_\gamma(s) = \int_0^\infty \exp\{-st\} d[H_\gamma(t)] = \left(\frac{\mu}{\mu + s}\right)^\alpha \approx h(s). \tag{9}$$

It should be noted that the mathematical expectation and service time dispersion are equal:

$$T_h = M_1; D_h = M_2 - M_1^2. \tag{10}$$

In this particular case, when we use exponential distributions as initial distributions, the image (5) can be submitted in a fractional rational form $h(s) = f(s)\varphi(s)$, where $f(s)$ and $\varphi(s)$ are polynomials, respectively, of degrees m and n ($m < n$). This allows one to represent (5) as a number of residues [31]:

$$h(s) = \sum_{i=1}^n \frac{f(s_i)}{\frac{\partial \varphi(s)}{\partial s} \Big|_{s=s_i}} \times \frac{1}{s - s_i}, \tag{11}$$

and the service time distribution function is defined as

$$H(t) = \sum_{i=1}^n \frac{f(s_i)}{\frac{\partial \varphi(s)}{\partial s} \Big|_{s=s_i}} \times \frac{1 - \exp\{ts_i\}}{-s_i}. \tag{12}$$

Then, the average time of service (transmission) of a packet without taking into account the parameters of the incoming flow is equal to:

$$T_h = \int_0^\infty t d[H(t)] = \sum_{i=1}^n \frac{f(s_i)}{\frac{\partial \varphi(s)}{\partial s} \Big|_{s=s_i}} \times \frac{1}{(s_i)^2} \equiv M_1 \tag{13}$$

and dispersion:

$$D_h = \int_0^\infty (t - T_h)^2 d[H(t)] = \sum_{i=1}^n \frac{f(s_i)}{\frac{\partial \varphi(s)}{\partial s} \Big|_{s=s_i}} \times \frac{2}{(s_i)^3} - T_h^2 \equiv M_2 - M_1^2. \tag{14}$$

It should be noted that according to [4,5], the approximation error of function (12) by function $H_\gamma(t)$ does not exceed 3% and it is quite acceptable for performing the engineering calculations. Therefore, in the course of further discussions, we shall use expression (9), especially as it allows one to remove the restriction on the type of distribution of the initial random values.

As a conclusion of the first stage, let us determine the quadratic coefficient of variation of the service time (successful transmission of the data packet) in the context of cyberattacks:

$$C_b^2 = \frac{D_h}{T_h^2}. \tag{15}$$

4.2. The Second Stage

Let us determine the function $W(t)$ by means of the results [20–22], which make it possible to calculate the values of the average time and dispersion of the service waiting time for arbitrary distribution laws of arrival and service, but with the difference that the values included in them are determined by means of data obtained at the first stage.

Therefore, the average service waiting time for a packet flow is determined by the formula [20,21]:

$$T_w = \frac{T_h C_v \rho [1 + (K + 1)\rho + K\rho^{K+1}]}{(1 - \rho)(1 - \rho^{K+2})} \tag{16}$$

and dispersion [21,22]:

$$D_w = \frac{T_h^2 C_v^2 \rho [2(1 - \rho^K) + K\rho^K(1 - \rho)[\rho(K + 1) - K - 3]]}{(1 - \rho)(1 - \rho^{K+2})} - T_w^2, \tag{17}$$

where $\rho = \lambda T_h < 1$; $C_v^2 = \frac{C_w^2 + C_b^2}{2}$ —root mean square coefficient of distribution variation of the integrated time between packet arrival and service.

Depending on the type of network traffic, the value C_w^2 is equal to:

- Pareto distribution [27]:

$$C_{wp}^2 = \frac{1}{(2H - 1)(2H - 3)}; \tag{18}$$

- Weibull distribution [27]:

$$C_{wv}^2 = \frac{\Gamma\left(1 + \frac{2}{\alpha_v}\right)}{\Gamma\left(1 + \frac{2}{\alpha_v}\right)^2} - 1, \tag{19}$$

where $\alpha_v > 0$ —shape parameter of the Weibull distribution; $\Gamma(*)$ —gamma-function [27]; H —Hurst exponent; α —distribution shape parameter, which is numerically equal to:

- for Weibull distribution [14,16]:

$$\alpha_v = 2 - 2H; \tag{20}$$

- for Pareto distribution [16]:

$$\alpha_p = H^{-\frac{5}{4}}. \tag{21}$$

On the basis of the results [22] of the application of the diffusive approximation method [29,30], which in the context of a heavy load achieves the solution for the queueing systems with arbitrary distribution laws of the arrival and service of claims, based on the solution for an M/M/1/K type system and $K < \infty$, as well as the results [30], we assume that the waiting time for service is described by the gamma distribution [27] with parameters:

$$\theta = \frac{T_w}{D_w}; \eta = \frac{T_w^2}{D_w} \tag{22}$$

The utilized assumption is in good agreement with the data described in fundamental works [28,29,32].

In this case,

$$\omega(s) = \frac{\theta^\eta}{\Gamma(\eta)} \int_0^\infty t^{\eta-1} \exp\{-(s + \theta)t\} dt = \left(\frac{\theta}{\theta + s}\right)^\eta. \tag{23}$$

Then, the equivalent function of the stochastic network (Figure 4) is of the form:

$$Q(s) = \omega(s) * h(s) = \left(\frac{\mu}{\mu + s}\right)^\alpha \left(\frac{\theta}{\theta + s}\right)^\eta = \left(\frac{\beta_n}{\beta_n + s}\right)^{\alpha_n}, \tag{24}$$

where $\alpha_n = \frac{(T_h+T_w)^2}{D_w+D_h}$; $\beta_n = \frac{T_h+T_w}{D_w+D_h}$.

Hence, the distribution function of the delivery time of data packets in the context of cyberattacks can be defined as:

$$F(t) = \frac{(\beta_n)^{\alpha_n}}{\Gamma(\alpha_n)} \int_0^t x^{\alpha_n-1} \exp\{-t\beta_n\} dx. \tag{25}$$

Thus, the formulated task has been solved, and the solution obtained in general terms allows one to define:

1. Average delivery time of data packets:

$$T_f = T_h + T_w. \tag{26}$$

2. Jitter of packet delay time:

$$\sigma = \sqrt{D_h + D_w}. \tag{27}$$

3. Loss probability of packets [16,21]:

$$P_{Los} = \frac{1 - \rho}{1 - \rho^{\frac{K}{C_v} + 2}} \rho^{\frac{K}{C_v} + 1}. \tag{28}$$

The novelty of the obtained solution lies in the parameter definition for the quality of service of the network in the context of cyberattacks in the absence of restrictions on the type of distribution functions of the transmission time $B(t)$, the time of the successful realization of cyberattacks $R_i(t)$, the recovery time of the network element function $\Delta_i(t)$ and the type of network traffic.

5. Demonstration of the Efficiency of the Suggested Method

To demonstrate the effectiveness of the described method, consider the following example of assessing the quality of DTN functioning. The choice of this example is due to the fact that it is simple, clear and without loss of generality and allows one to understand the essence of the proposed method and the procedure for calculating the quality indicators of DTN functioning in cyberattack conditions.

Let us suppose that transmission of data packet flow with an average volume $V = 0.23$ Mbit, an average speed $S = 150$ Mbit/s and intensity of packet arrival $\lambda = 20$ packets/s is carried out along a route organized in the network. The indicated transmission route contains $N = 5$ network elements with storage capacity $K = 50$ (packets). Two network elements on the route are available with the probability $P_1 = P_2 = 0.5$ for a malefactor’s cybercriminal intelligence and, as a result of this, with the average time $t_{r1} = 300$ (s) and $t_{r2} = 400$ (s) with dispersion $D_{r1} = 200$ (s²) and $D_{r2} = 150$ (s²), their functioning is disrupted as a result of a cyberattack.

If the functioning of the network elements is not disrupted, then the packet that arrives for transmission will be successfully transmitted (serviced) in the average time $t_b = \frac{(N-1)V}{s} = 6.13 \times 10^{-3}$ (s) with dispersion $D_b = 1.2 \times 10^{-6}$ (s²).

If the cyberattack is successful, the network administrator detects and recovers the functioning of the network element in the average time $t_{d1} = t_{d2} = 5$ (s) with dispersion $D_{d1} = D_{d2} = 25$ (s²).

Let us suppose that the indicated random values are characterized by gamma distribution.

Network traffic is described by the Weibull model. Network traffic parameters are: $\lambda = 20$ packets/s, Hurst index $H = 0.71$. It is required to define the delivery probability of the data packet to the user in a time not exceeding $T_z = 5$ (s).

The equivalent function of the stochastic network when there are two types of action is as follows:

$$Q(s) = w(s)h(s), \tag{29}$$

where

$$w(s) = \left(\frac{\theta}{\theta + s}\right)^\eta; \quad h(s) = \frac{\left[1 - \left(\frac{r_1}{r_1 + b + s}\right)^{\alpha_{r1}}\right] \left[1 - \left(\frac{r_2}{r_2 + b + s}\right)^{\alpha_{r2}}\right] \left(\frac{h}{h + s}\right)^{\alpha_h} \frac{d(d+c+s)}{(d+s)(d+c)}}{\left[1 - \left(\frac{h}{h+s}\right)^{\alpha_h} \frac{d}{(d+s)} \left[\left(\frac{r_1}{r_1+b+s}\right)^{\alpha_{r1}} + \left(\frac{r_2}{r_2+b+s}\right)^{\alpha_{r2}} \left[1 - \left(\frac{r_1}{r_1+b+s}\right)^{\alpha_{r1}}\right]\right]\right]}. \tag{30}$$

Let us calculate the parameters of the scale and shape of the partial distributions:

$$r_{1(2)} = \frac{t_{r1(2)}}{D_{r1(2)}} = 1.5(2.65); \quad \alpha_{r1(2)} = \frac{t_{r1(2)}^2}{D_{r1(2)}} = 450(1.06 * 10^3); \tag{31}$$

$$h = \frac{t_b}{D_b} = 5.1 * 10^3; \quad \alpha_h = \frac{t_b^2}{D_b} = 31.4. \tag{32}$$

Then, by means of numerical methods, we shall receive the mathematical expectation and dispersion of the service (transmission) time:

$$M_1 = T_h = -\frac{d}{ds} \left(\frac{h(s)}{h(0)}\right)_{s=0} = 0.078 \text{ (s)}; \quad D_h = \frac{d^2}{ds^2} \left(\frac{h(s)}{h(0)}\right)_{s=0} - T_h^2 = 0.714 \tag{33}$$

and quadratic coefficient of the variation of the service time is equal to

$$C_b^2 = \frac{D_h}{T_h^2} = 117.3. \tag{34}$$

Further, by means of (16) and (17), and taking into account (19), we will determine the quadratic coefficient of variation of the data flow, mathematical expectation and dispersion of the waiting time at storage capacity $K = 50$:

$$C_{wv}^2 = 3.36; \quad T_w = 12.067 \text{ (s)}; \quad D_w = 145.6 \text{ (s}^2\text{)}. \tag{35}$$

Distribution parameters of the service waiting time are equal to:

$$\theta = \frac{T_w}{D_w} = 0.083; \quad \eta = \frac{T_w^2}{D_w} = 0.993. \tag{36}$$

Now we have the necessary data to calculate the parameters of the shape and scale of the delivery time distribution function in the context of cyberattacks:

$$\alpha_n = \frac{(T_h + T_w)^2}{D_h + D_w} = 1.1; \quad \beta_n = \frac{(T_h + T_w)}{D_h + D_w} = 0.083. \tag{37}$$

The probability of successful delivery, based on (8), is equal to:

$$P(t \leq T_z) = F(T_z = 5 \text{ s}) = 0.336, \tag{38}$$

meanwhile, the average data delivery time is equal to:

$$T_f = T_h + T_w = 12.145 \text{ (s)}. \quad (39)$$

Jitter of the delivery time is equal to:

$$\sigma = \sqrt{D_h + D_w} = 12.097 \text{ (s)}. \quad (40)$$

The probability of data loss is equal to:

$$P_{Los} = \frac{1 - \rho}{1 - \rho^{\frac{K}{C_b^2} + 2}} \rho^{\frac{K}{C_b^2} + 1} = 0.277. \quad (41)$$

The graph of the distribution function of the data delivery time in the context of cyberattacks is shown in Figure 5.

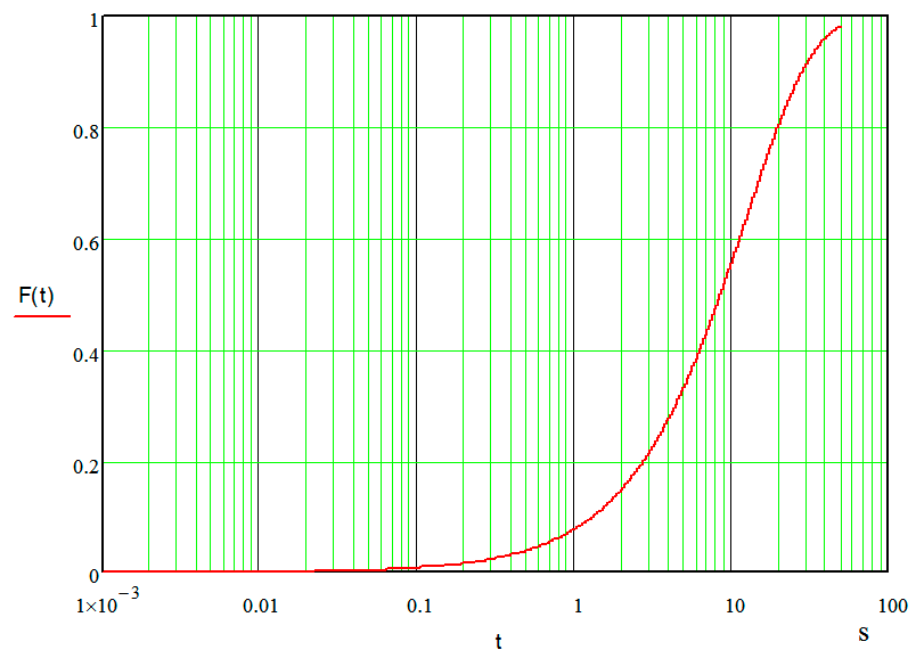


Figure 5. The graph of the distribution function of the data delivery time in the context of cyberattacks, when the initial data are specified in the calculation example.

6. Experimental Results

We will analyze the results of computational experiments using the above calculation example.

1. The probability of successful delivery of data packets cannot exceed some maximum value, which is determined on the condition that there is no malefactor information impact against the network, there is no queue for service and the network elements are absolutely reliable, i.e.,

$$P_{max}(t \leq T_z) = \lim_{\lambda \rightarrow 0} F(t = T_z) = \frac{h^{\alpha_h}}{\Gamma(\alpha_h)} \int_0^{T_z} t^{\alpha_h - 1} \exp\{-ht\} dt. \quad (42)$$

Meanwhile, the delivery time of the packet depends on only the number of sections on the route, the volume and speed of information transmission.

The form of the limit distribution function of the information delivery time is represented in Figure 6.

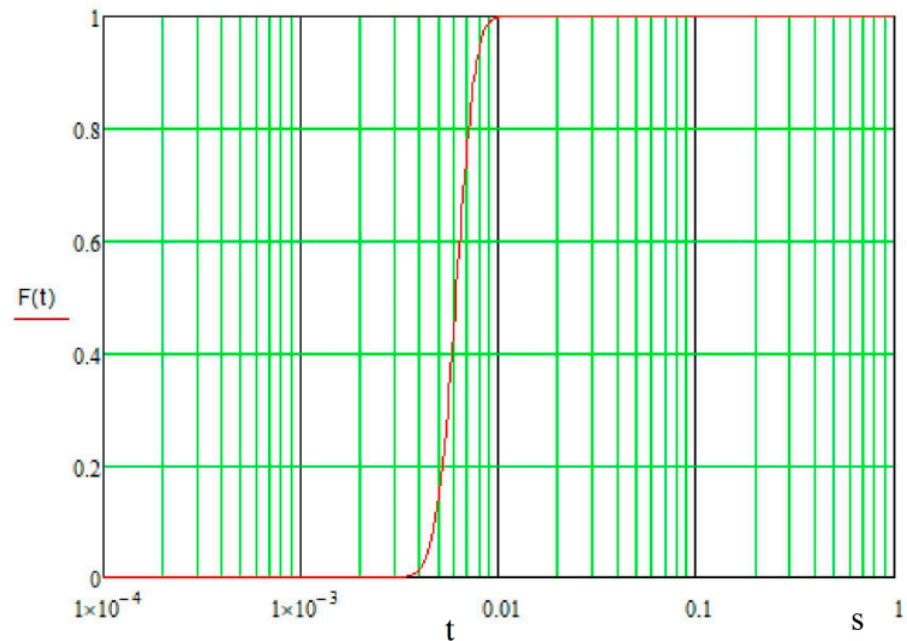


Figure 6. The graph of the distribution function of the information delivery time when $\lambda \rightarrow 0$ and there is no malefactor information impact.

2. If the intensity of information exchange increases, the influence of the type of network traffic model increases (Figure 7).

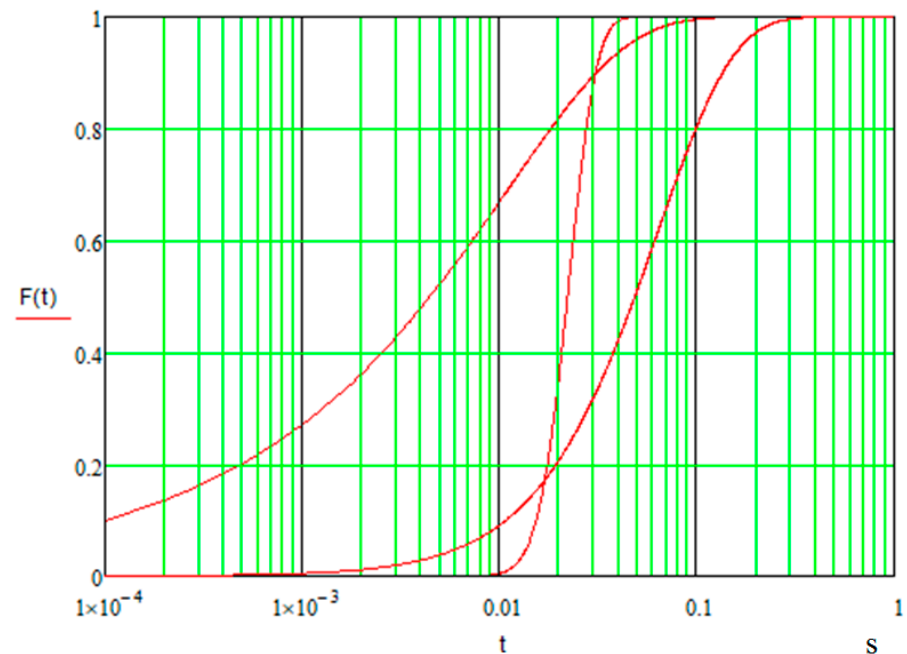


Figure 7. The graph of the distribution function of the information delivery time when $\lambda = 100$ packets/s and there is no malefactor information impact.

Meanwhile, according to the value of the average delivery time of data packets, the most favorable is the Poisson data flow; when the Weibull flow is serviced, the packet delivery time, depending on the value of the Hurst index H , can increase up to 5 ... 10 times in relation to the estimated time obtained for a Poisson flow. However, when the Poisson traffic is serviced, the variation in the packet delay time is almost twice as large

as when the Weibull flow is serviced. It should be noted that when the Weibull flow is serviced, we can observe an increase in the probability of packet loss, which is due to the limited storage capacity.

When values of the Hurst index are low ($H \leq 0.2$) (Figure 8), the differences in the values of the probabilities of successful packet delivery (especially at the level of requirements ($F(t) \geq P_z = P(t \leq T_z) = 0.95$) are negligible, if there are different models of input traffic.

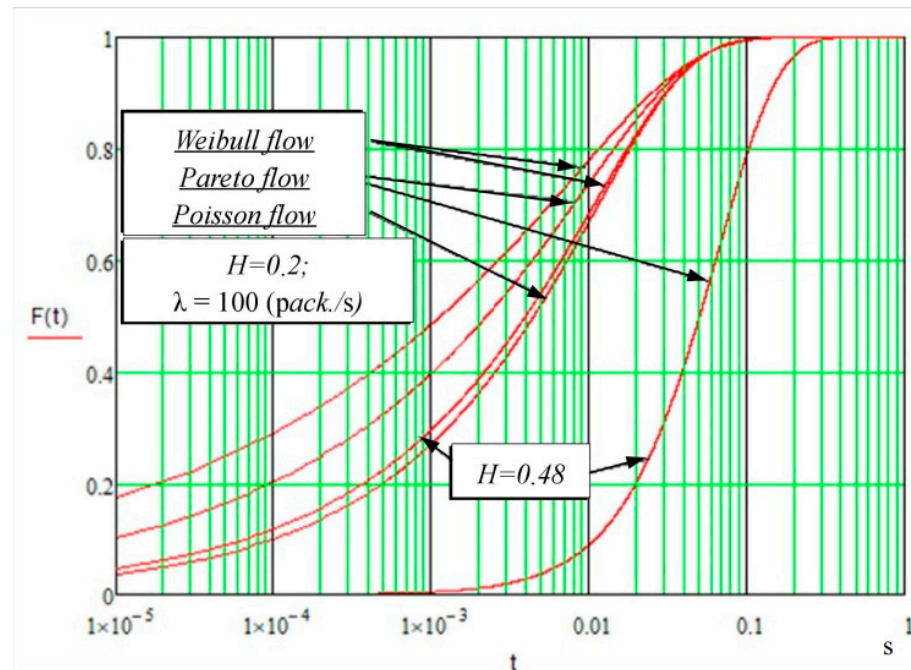


Figure 8. The graphs of the distribution functions of the delivery time of data packets, if there are different models of network traffic.

When the Hurst index increases ($H \geq 0.2$), the distribution function of the packet delivery time in the Weibull flow comes close to an exponential distribution, and when the Pareto flow is serviced, the distribution function goes down, which leads to a considerable increase in the average time of successful data delivery and an increase in the probability of packet loss. This is explained by the difference in the dependence of the variation coefficients of the Weibull and Pareto flows on the value of the Hurst index. It should be noted that, when we simulate the delivery process, the Hurst index value, close to $H \approx 0.5$, is the limiting value for the Pareto flow, because if $H \geq 0.5$, dispersion for this distribution is not determined [21] (Figure 9), therefore the simulated results of the delivery process obtained at these H values will be wrong.

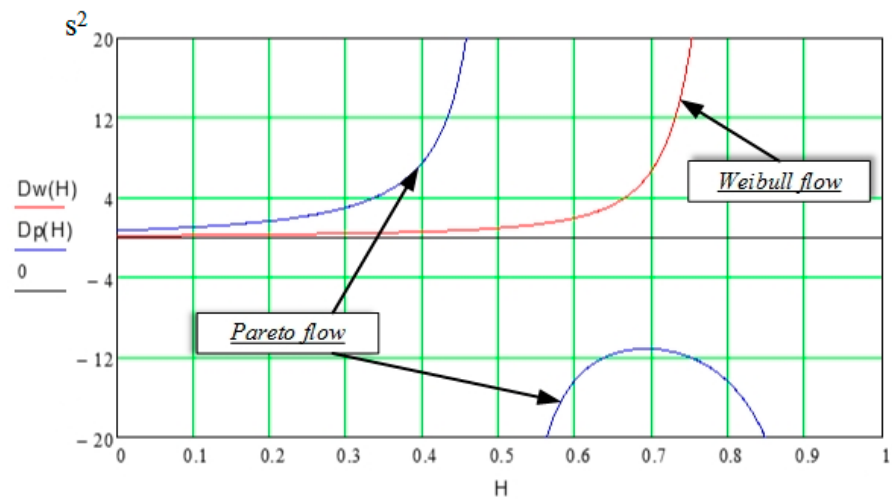


Figure 9. Dependence graph of dispersion of the Pareto and Weibull flows with the parameters of the distribution scale $k_w = k_p = 1$.

Analysis of the received results shows that they correspond completely with the data of works published previously by other authors [13,16,17,19–22,33] devoted to the development of quality evaluation methods of the functioning of telecommunication networks when self-similar and stationary Poisson traffic is transmitted. This confirms the adequacy of the developed model and the consistency of the received results.

3. In the case of the availability and implementation of an information impact by an attacker on network elements, the probability of the successful delivery of data packets in a given time significantly worsens (Figure 10).

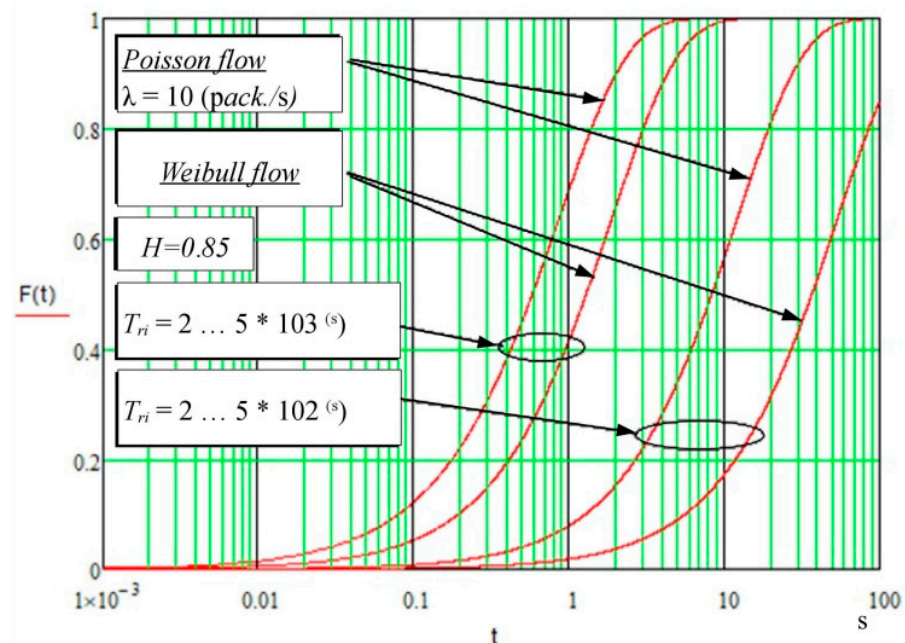


Figure 10. The graph of the distribution function of the information delivery time when $\lambda = 20$ packets/s in the context of a malefactor's impact.

Calculations show that in the context of cyberattacks, the time for the successful delivery of data packets increases by two or more times when the real bandwidth of the transmission route is reduced up to 10 times.

When the average time of the realization of cyberattacks is reduced tenfold, then the average packets delivery time increases by 2 ... 2.5 times, and in this case the packet

loss probability increases up to 0.4 and jitter of the delay time also increases up to tens of seconds. The impact of the dispersion of the time of the realization of cyberattacks on the quality of service indicators of the network is extremely nominal. For example, the probability change of successful delivery in a given time is less than 1%. There is still a tendency for the extension of influence of the type of transmitted traffic on the delivery time, which points at the inability to provide services to users in real time in the context of cyberattacks, as well as the expediency of limitation of the intensity of information exchange and the volumes of transmitted information.

The impact on the data delivery time of such a parameter as the probability of network elements being available to the cybercriminal intelligence should be noted, which allows the malefactor to choose in advance the most vulnerable network elements to realize cyberattacks in the future. Therefore, it is advisable to organize information exchange over the data transmission network in such a way that information transmission is carried out each time along routes which have not been used before and network elements are included in the work only when the received packet is transmitted with a prerequisite for the implementation of methods for increasing the reliability of network authentication. This will allow one to reduce the delivery time of data packets significantly, which is explained by the fact that, in this case, in order to complicate information exchange, a malefactor will have to have an effect on the network elements during the time interval of data packet transmission along this route. However, the development of such an algorithm of the network function may be a further direction for studies to neutralize cyberattacks and this transcends the scope of this paper.

4. The realization of cyberattacks against the network elements influences not only the functioning quality indicators of the network, but also the real bandwidth of data transmission routes (Figure 11), which is defined as $\lambda_p = \lim_{t \rightarrow \infty} \frac{dF(t)}{1-F(t)} \approx \frac{1}{T_r}$, where T_r is the mathematical expectation of the time of the successful delivery of data packets.

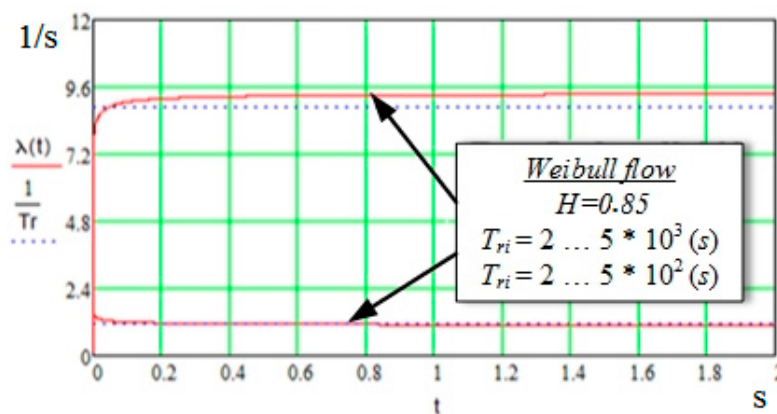


Figure 11. Dependence graph of flow intensity of successfully transmitted data packets when time values of the realization of cyberattacks are different.

The weak dependence of the flow intensity values of successfully delivered packets and their closeness to $(1/T_f)$ shows that when there is functioning in the context of malefactor information influences, the data flow at the output of the user’s end equipment can be considered Poisson. The results of calculations show that if there is successful realization of a cyberattack, the flow intensity of delivered packets is reduced sharply. This fact can be an additional sign for the network administrator and users that the network was exposed to a cyberattack and it is necessary to realize measures to protect against the information impact of a malefactor. It can allow one to reduce the recovery time of the network functioning after a cyberattack by a malefactor.

5. In the context of cyberattacks, the efficiency of detection and recovery of the operability of the data transmission route after an information impact essentially influences the time of successful data delivery (Figure 12).

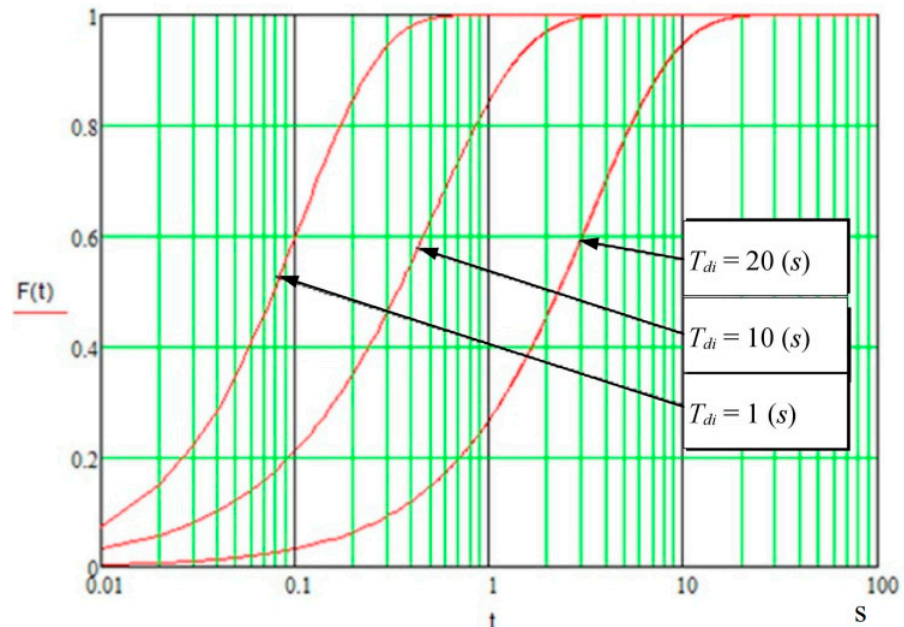


Figure 12. The graph of the distribution functions of successful data delivery in the context of cyberattacks when average time values T_{di} of rehabilitation of functioning of network elements are different.

For example, if the time T_{di} of detection and neutralization of the cyberattack against network elements and terminal equipment of users is reduced by up to one second, the average data delivery time will be reduced by more than 10 times.

This suggests the expediency and prospects of the early detection of cyberattacks, for example, using the methods described in [34].

Thus, experiments have shown that the proposed method allows analytical evaluation of the probabilistic behavior of the key parameters of DTN function (delivery time and real throughput of data transmission routes), depending on the following factors:

- the intensity of information exchange;
- the volume of transmitted information;
- the effectiveness of route restoration in the event of failures;
- the laws of packet distribution, which are subject to information flows in the DTN;
- capacity of packet storage systems at switching nodes;
- the duration of the cyberattacks.

Knowledge of the distribution laws that will obey the key parameters of the DTN operation allows one to make effective decisions on the management of the DTN in electric power systems. In this regard, the proposed method and its software implementation can be included in the DTN control system of electric power complexes as elements of mathematical and software support. With the help of such elements, it is possible to solve the problems of quickly predicting the behavior of the DTN under the influence of cyberattacks with various options for constructing the DTN.

7. Conclusions

Based on the general principles of the construction and operation of modern telecommunication networks and ensuring the quality of services provided to users when heterogeneous traffic is transmitted, the paper proposes a method for the investigation of

information transmission routes in a data transmission network for arbitrary distributions of the arrival and service of packets.

The method is based on the data delivery process view in the form of a stochastic network, definition of its equivalent function, calculation of the initial and central moments of waiting and service time, calculation of the parameters of the scale and shape of the incomplete gamma function and further definition of the distribution function of the time of the successful delivery of data packets.

The novelty of the proposed method consists in taking into account the parameters of the model of the realization of cyberattacks by a malefactor, which are set in the form of the distribution function of the attack realization time and the probability of network elements being available to the cybercriminal intelligence. For the initial distributions, it is proposed to use the gamma distribution as the most general, between distributions of the random time of the realization of private processes, which are implemented when communication is established and maintained in existing and prospective data exchange systems. The proposed method allows one to obtain estimates of the quality of the network functioning in the context of cyberattacks both during the transmission of stationary Poisson and self-similar traffic, which is represented in the method by the Pareto and Weibull flows models.

The presented method showed a good agreement of the obtained estimate results with the data given in previously published works, which allows one to analyze and develop directions for a quality increase in data transmission network functioning in the context of the destructive information impact of a malefactor.

It should be noted that in addition to the obvious advantages, the method proposed in the paper also has disadvantages that limit its use in practice. Therefore, for example, the method does not provide an analysis of the quality of DTN functioning when servicing a categorical data stream, which is typical for public telecommunication networks. In addition, the method requires a preliminary inspection of the DTN in relation to identifying cyber threats and modeling the cyber impact of an intruder on vulnerable network elements, as well as determining data transmission routes in the analyzed network in order to determine the initial data required for calculations. Therefore, future research and developments will be devoted to experimental implementation of the suggested method.

Author Contributions: A.P. and I.K. were responsible for conceptualization and methodology; I.S. analyzed the data; N.E. and D.T. conceived and designed the experiment; all authors wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the grant of RSF #21-71-20078 in SPC RAS.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Verhoef, P.C.; Broekhuizen, T.; Bart, Y.; Bhattacharya, A.; Dong, J.Q.; Fabian, N.; Haenlein, M. Digital transformation: A multidisciplinary reflection and research agenda. *J. Bus. Res.* **2019**, *122*, 889–901. [[CrossRef](#)]
2. Nguyen, T.N.; Liu, B.-H.; Nguyen, N.P.; Chou, J.-T. Cyber Security of Smart Grid: Attacks and Defenses. In Proceedings of the ICC 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
3. Qu, Z.; Dong, Y.; Qu, N.; Wang, L.; Li, Y.; Zhang, Y.; Mugemanyi, S. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation. *Math. Probl. Eng.* **2019**, *2019*, 15. [[CrossRef](#)]
4. Zhao, J.; Xue, Z.; Li, T.; Ping, J.; Peng, S. An energy and time prediction model for remanufacturing process using graphical evaluation and review technique (GERT) with multivariant uncertainties. *Environ. Sci. Pollut. Res.* **2021**. [[CrossRef](#)]
5. Tao, L.; Wu, D.; Liu, S.; Lambert, J.H. Schedule risk analysis for newproduct development: The GERT method extended by a characteristic function. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 464–473. [[CrossRef](#)]
6. Vlăduțu, A.; Comăneci, D.; Dobre, C. Internet traffic classification based on flows' statistical properties with machine learning. *Int. J. Netw. Manag.* **2017**, *27*, e1929. [[CrossRef](#)]
7. Vazquez, F.I.; Ferreira, D.S.; Formire, G.; Bahl, M.; Zsebi, T. TARC: Data Model for a Systematic Review of Network Traffic Analysis Research. *Appl. Sci.* **2020**, *10*, 4307.

8. Kotenko, I.; Saenko, I.; Laut, O. Modeling the Impact of Cyber Attacks. In *Cyber Resilience of Systems and Networks, Risk, Systems and Decisions*; Kott, A., Linkov, I., Eds.; Springer: Cham, Switzerland, 2019; pp. 154–196.
9. Gao, P.; Li, G.; Shi, Y.; Wang, Y. VPN traffic classification based on payload length sequence. In Proceedings of the IEEE International Conference on Networking and Network Applications (NaNA), Haikou City, China, 10–13 December 2020; pp. 241–247.
10. Freeman, R.L. *Fundamentals of Telecommunications*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2005.
11. Megduri, F.; Zsebi, T.; Vazquez, F.I. Analysis of lightweight feature vectors for attack detection in network traffic. *Appl. Sci.* **2018**, *8*, 2196. [[CrossRef](#)]
12. Kotenko, I.; Saenko, I.; Laut, O.; Kribel, A. An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. *Energies* **2020**, *13*, 5031. [[CrossRef](#)]
13. Dos Santos, E.; Schoop, D.; Simpson, A. Formal models for automotive systems and vehicular networks: Benefits and challenges. In Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC), Haikou City, China, 10–13 December 2020; pp. 1–8.
14. Lu, Y.; Li, J.; Guo, Q. Tactical Internet Communication traffic characteristics and modeling methods. In Proceedings of the IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1129–1133.
15. Zhang, L.; Li, Z.; Wang, H.; Li, P.; Chen, X. A new backup topology design method for IP fast recovery. In Proceedings of the IEEE 2nd International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016; pp. 1992–1997.
16. Maharrov, Z.; Abdullayev, V.; Mammadova, T. Modelling self-similar traffic of multiservice. *EUREKA: Phys. Eng.* **2019**, *1*, 46–54. [[CrossRef](#)]
17. Salazar, J. *Wireless Networks*, 1st ed.; Czech Technical University of Prague Faculty of Electrical Engineering: Prague, Czech Republic, 2017.
18. Kadhim, A.A. 5G and next generation networks. In Proceedings of the IEEE AI-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT), Baghdad, Iraq, 14–15 November 2018; p. 99.
19. Jawad, S.S.; Fyath, R.S. Performance Investigation of 5G-Mobile Fronthaul using Analog RoF Technology. In Proceedings of the IEEE AI-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT), Baghdad, Iraq, 14–15 November 2018; pp. 82–87.
20. Peng, G.-Q.; Xue, G.; Chen, Y.-C. Network Measurement and Performance Analysis at Server Side. *Future Internet* **2018**, *10*, 67. [[CrossRef](#)]
21. Hirchoren, G.A.; Porrez, N.; Sala, B.L.; Burachevski, I. Quality of Service in Self-Similar Traffic Networks. In Proceedings of the XVII Seminar on Information Processing and Control (RPIC), Mar del Plata, Argentina, 20–22 September 2017; pp. 1–5.
22. Chang, G.; Lee, C.C. A packet queueing engine for configurable network QoS. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 28 June–1 July 2011; pp. 842–849.
23. Bagretsov, S.A.; Laut, O.S.; Klimenko, A.I.; Balenko, E.G. Method for Providing Rationale of Basic Option of Information and Telecommunication Network under Hostile Action. In Proceedings of the International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 10–12 September 2019; pp. 1–7.
24. Norouzi, M.; Rafe, V. An approach to WF-nets generation using graph transformation system. In Proceedings of the IEEE 9th International Conference on Information and Knowledge Technology (IKT), Tehran, Iran, 18–19 October 2017; pp. 76–81.
25. Kotenko, I.; Saenko, I.; Laut, O. Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion. In Proceedings of the 10th International Workshop on Resilient Networks Design and Modeling (RNDM), Longyearbyen, Norway, 27–29 August 2018; pp. 1–8.
26. Wang, S.; Liu, S.; Fang, Z. Research on SoS-GERT network model for equipment system of systems contribution evaluation based on joint operation. *IEEE Syst. J.* **2020**, *14*, 4188–4196. [[CrossRef](#)]
27. Bijma, F.; Jonker, M.; van der Vaart, A. *An Introduction to Mathematical Statistics*; Amsterdam University Press: Amsterdam, The Netherlands, 2017.
28. Karavaev, I.S.; Selivantsev, V.I.; Shtern, Y.I.; Shtern, M.Y. The development of the data transmission method and the data transmission device for the industrial control systems of the energy carrier parameters. In Proceedings of the IEEE Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russia, 14–16 March 2018; pp. 1–4.
29. Moore, F.O. *Data Communication Protocols*; Northcentral University: San Diego, CA, USA, 2017.
30. Nelson, R.G.; Azaron, A.; Aref, S. The Use of a GERT Based Method to Model Concurrent Product Development Processes. *Eur. J. Oper. Res.* **2016**, *250*, 566–578. [[CrossRef](#)]
31. Ames, A.D.; Coogan, S.; Egerstedt, M.; Notomista, G.; Sreenath, K.; Tabuada, p. Control Barrier Functions: Theory and Applications. In Proceedings of the IEEE 18th European Control Conference (ECC), Napoli, Italy, 25–28 June 2019; pp. 3420–3431.
32. Salami, E.; Barrado, C.; Gallardo, A.; Pastor, E. General queueing model for optimal seamless delivery of payload processing in multi-core processors. *J. Supercomput.* **2018**, *74*, 87–104. [[CrossRef](#)]
33. Tyagi, N.; Gilad, Y.; Leung, D.; Zaharia, M.; Zeldovich, N. Stadium: A Distributed Metadata—Private Messaging System. In Proceedings of the 26th Symposium on Operating Systems Principles (SOSP), Shanghai, China, 28 October 2017; pp. 423–440.
34. Privalov, A.; Lukicheva, V.; Kotenko, I.; Saenko, I. Increasing the sensitivity of the method of early detection of cyber-attacks in telecommunication networks based on traffic analysis by extreme filtering. *Energies* **2020**, *13*, 2774. [[CrossRef](#)]