mathematics

MDPI

Article

Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems

Fazliddin Makhmudov [1], Andrey Privalov [2], Alexander Privalov [3], Elena Kazakevich [2], Gamzatdin Bekbaev [4], Alexey Boldinov [2], Kyung Hoon Kim [5] and Young Im-Cho [1,*]

[1] Department of Computer Engineering, Gachon University, Seongnam 1342, Republic of Korea; fazliddin12@gachon.ac.kr
[2] Department of Electrical Communication, St. Petersburg State Transport University, Moskovskiy Prospekt, 9, 190031 St. Petersburg, Russia; aprivalov@inbox.ru (A.P.); kazakevich@prups.ru (E.K.); 23boldinov98@gmail.com (A.B.)
[3] Department of Applied Mathematics, Moscow Automobile and Road State Technical University, Leningradsky Ave, 64, 125319 Moscow, Russia; a_privalov@bk.ru
[4] Department of Finance and Business Analytics, Tashkent State University of Economics, Tashkent 100066, Uzbekistan; g.bekbaev@tsue.uz
[5] KT Corporation, Seongnam 13606, Republic of Korea; kkhdatahub@gmail.com
* Correspondence: yicho@gachon.ac.kr

Abstract: This article introduces a refined mathematical model to evaluate the quality of mobile radio channels within cyber-physical systems, employing the topological transformation of stochastic networks. The operation of the radio channel is conceptualized as a stochastic network, enabling the derivation of critical metrics such as an equivalent function, mathematical expectation, variance, and the time distribution function of the implemented processes. The model uses the Gamma distribution for the initial distribution functions of random variables, enhancing its analytical precision. A significant advancement of this study is the development of a comprehensive model that describes the data transmission process through phases of connection establishment, information transmission, and connection maintenance. The innovative aspect of this research lies in applying an equivalent function to a stochastic network that includes a logical "AND" node with gamma-distributed incoming branches. The stochastic network presented in the article, which includes a logical "AND" node, helps to elucidate the mechanism for obtaining an equivalent function for such networks, allowing the application area of the GERT method to be expanded. This methodological enhancement extends the previously limited scope of topological transformation methods, which only applied to exponential distribution models for the timing of branch inputs. By integrating a Gamma distribution, the model simplifies the equivalent function and reduces the computational complexity required to assess the radio channel's quality, ensuring the accuracy needed for engineering calculations. Moreover, the proposed method requires 25–40% fewer series members than the traditional Taylor series decomposition, while maintaining comparable computational complexity for the typical series members. Furthermore, the maximum absolute error in the calculations is capped at 9×10^{-3}, which is well within acceptable limits for engineering purposes. Primarily designed for radio channels in cyber-physical systems, the model's applicability extends to wireless communications, providing a valuable tool for evaluating channel efficiency and security in the face of increasing cyber threats.

Keywords: radio channel; cyberattack; cyber-physical systems; Gamma distribution; stochastic network

MSC: 90B15

check for updates

Citation: Makhmudov, F.; Privalov, A.; Privalov, A.; Kazakevich, E.; Bekbaev, G.; Boldinov, A.; Kim, K.H.; Im-Cho, Y. Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems. *Mathematics* **2024**, *12*, 1452. https://doi.org/10.3390/math12101452

Academic Editors: Cheng-Chi Lee, Dinh-Thuan Do and Daniel-Ioan Curiac

Received: 18 March 2024
Revised: 28 April 2024
Accepted: 6 May 2024
Published: 8 May 2024

1. Introduction

The control system for the digital communication network in railway transport is designed to ensure the optimal functioning of all network segments, effectively utilizing and developing communication resources to meet the diverse needs of railway transport for communication services. This includes maintaining the reliability and resilience of the railway communication network amid various external destabilizing factors. Additionally, it should fulfill the requirements and expectations of communication service users, facilitate network structure reconfiguration, address failure consequences, monitor the quality of service for subscribers and data transmission, and safeguard transmitted information against unauthorized access.

Existing radio networks face increasingly higher demands for the speed and timing of transmitted data each year, driven by the development of systems that manage train movements. In turn, radio channels are used to ensure data transmission between mobile objects and the radio network. Therefore, the process of data transmission over the radio channel must be built in accordance with the requirements necessary for cyber-physical systems (CPSs). The main task of CPSs is the ability to integrate physical objects and processes occurring in the infotelecommunication environment. The consistent development of rolling stock and railway infrastructure in the context of increased transport intensity has led to the emergence of CPSs that provide train traffic control. A cyber-physical system represents a sophisticated nexus of interwoven physical entities and computational elements, orchestrated within an engineering framework [1–3].

1.1. Relevance

A CPS features a multifaceted architecture where each layer is interdependent and interacts dynamically with the others. Specifically, Figure 1 depicts the architecture of a CPS, which comprises physical, network, and cybernetic layers. The cyber layer is responsible for creating a database of events. It processes incoming data from physical objects and formulates control commands. These commands are then relayed to the controlled objects via the mobile communication radio channel situated within the network layer. This structure ensures efficient data flow and command execution across the system.

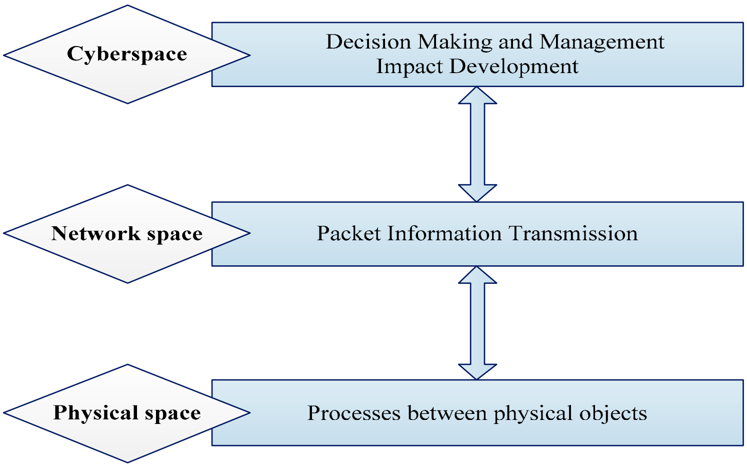
Cyberspace
Decision Making and Management
Impact Development
Network space
Packet Information Transmission
Physical space
Processes between physical objects

Figure 1. Cyber-physical system architecture.

CPSs play a crucial role in organizing and ensuring the safety of the transportation process for Russian Railways (RRs), which are recognized as a critical component of Russia's Critical Information Infrastructure (CII) [4]. The significant impact of RRs on various sectors of the Russian economy imposes high standards on the mobile radio communication networks that support these operations. Furthermore, the essential nature of these systems attracts increased attention from malicious entities aiming to disrupt the operational integrity of RRs' CPSs [4].

Consequently, the control systems and wireless data communication networks employed in RRs' CPSs must not only facilitate efficient transportation management but also meet stringent security standards to protect against both physical and cyber threats [5]. This dual requirement underscores the critical need to rigorously assess the performance and security of technological data transmission networks within mobile radio communications, particularly under potential cyberattack scenarios.

The importance of enhancing the performance quality of mobile radio communication networks for data transmission is a major focus for experts in the field. This focus drives substantial interest in the design and development of robust mobile radio communication networks tailored to meet the specific needs of various applications, ensuring both operational efficiency and security.

1.2. Previous Surveys

For instance, reference [6] introduces a mathematical model for the MIMO radio channel. This model is developed considering the real signal-noise environment, including the impact of both artificial and natural interferences. While this model primarily aims to evaluate the theoretical bandwidth of the radio channel, it does not incorporate time parameters. Consequently, this omission prevents an assessment of the time required to communicate information to consumers.

In [7], the application of Markov models to evaluate the availability of the radio channel is discussed. The operational states of the radio channel are modeled, including an operable state, a state indicating the potential for information transmission blocking, and a state of complete blocking. The evaluation focused on the occurrence of threats and calculated the operational uptime of the radio channel. However, this study overlooked the processes of establishing and maintaining connections, which limits the analysis of how effectively an intruder’s actions to block logical channels impact the success of information exchange.

In another study, the authors in [8] analyzed the efficiency of radio channel utilization based on an indicator that reflects the proportion of the channel’s capacity available for data transmission. Despite this analysis, the study did not incorporate a mechanism to assess how this usage indicator influences the timing of information transmission over the radio channel. Further, in references [9,10], the authors examine a signal transmission algorithm that accounts for the characteristics of the transmitted traffic. By analyzing the volume and duration of the data transmitted, they provide an estimate of the proportion of total data volume successfully transmitted. However, this methodology does not allow for the assessment of data transmission time or the evaluation of transmission timing throughout the complete data delivery cycle, as it does not consider the operations within the logical communication channels.

The method discussed in [11] is notable, as it involves using a logical channel for establishing connections through a technique that employs sudden frequency changes for automatic link establishment. The authors investigated the probability of establishing a communication channel and the associated bandwidth value. However, their assessment lacked an examination of the time characteristics essential for determining the duration required to establish a connection or to perform frequency reconfiguration, if necessary. This methodology is also reviewed in [12], where the focus is solely on the bit error rate, neglecting the critical aspect of connection establishment time.

Various methodologies are utilized to evaluate radio communication channels, as detailed in scholarly articles [13–16]. Researchers focus on the signal propagation environment and employ models such as line-of-sight propagation and the Okumura-Hata model, which is particularly suited to densely populated urban settings. Their analyses determine how signal attenuation varies with transmission distance, computing metrics like the signal-to-noise ratio, noise coefficient, and reference signal power. Nonetheless, these approaches fail to capture the time dynamics of signal delivery that are influenced by the propagation environment.

In studies [17–20], the mathematical modeling of traffic and the assessment of data transmission quality are explored. Through scenario-based analysis, these studies compare channel gain deviation indicators under various conditions to select optimal antenna systems. However, the available operational data do not facilitate the calculation of channel occupancy times or the probability of successful connection completions.

Other research efforts, specifically [21,22], focus on analyzing radio signaling standards that facilitate data exchanges between trains and radio block centers. Notably, these studies delve into the European Rail Traffic Management System (ERTMS), developed to standardize train traffic management and enhance safety [23–25]. During their investigations, researchers explored how to improve data collection methods from trains via the radio channel to expedite data retrieval. They also examined the impact of train speed on the accuracy and timeliness of acquiring data about train characteristics.

The motivation for developing this refined model stems from several key challenges observed in existing models, one such being that while these studies emphasize temporal parameters, they do not provide a means to assess the likelihood of successful process realization.

Limitations in Distribution Assumptions: Prior models were restricted to exponential distributions, which limited their accuracy and applicability to real-world scenarios, where data transmission times often follow more complex distributions.

Need for Enhanced Precision: Accurate assessment of radio channel quality is crucial for ensuring reliable communication in CPS, especially in critical infrastructures like railway transport systems. Improving precision in mathematical modeling directly translates to better decision-making and operational efficiency.

Addressing Cybersecurity Threats: With the increasing prevalence of cyber threats, there is an urgent need for models that can predict and mitigate potential vulnerabilities in CPS. The enhanced model aims to provide a robust framework for assessing and improving the security and resilience of mobile radio networks.

The article proposes a model of the data transmission process via a radio channel that is free from the aforementioned shortcomings. Additionally, the absence of a mechanism for obtaining an equivalent function for a stochastic network containing a logical "AND" node and incoming branches with gamma distribution significantly narrows the application scope of the GERT method for modeling complex technical organizational systems, including CFS. The stochastic network presented in the article, which includes a logical "AND" node, helps to elucidate the mechanism for obtaining an equivalent function and expands the application area of the GERT method.

This paper makes several significant contributions to the field of CPSs and mobile radio communications:

- By integrating the Gamma distribution and a logical "AND" node, the model offers a more flexible and comprehensive approach to understanding and predicting the behavior of radio communication networks.
- The application of the Gamma distribution allows for a more accurate description of time-related processes in data transmission, thereby enhancing the model's utility in engineering calculations.
- The model is designed to be practically applicable, particularly in railway CPSs, where it can help optimize network performance and resilience against disruptions, including cyberattacks.
- The new approach reduces the computational burden by requiring fewer series members than traditional methods while maintaining high accuracy, as evidenced by a maximum absolute error within acceptable engineering limits.

These methodological advancements significantly extend the GERT method's scope beyond its previous limitations, paving new avenues for research and practical applications in complex technical organizational systems. This model removes traditional restrictions on the types of probability distributions that can be used for the random time durations associated with each process, thereby offering an innovative tool for ensuring efficient and secure data transmission across mobile radio networks.

2. Mathematical Model and Methodology

2.1. Descriptive Model

The data transmission process via a radio channel involves multiple phases. Initially, the controlled entity initiates the process by sending a connection request to the controlling entity. Should this request go unacknowledged, the controlled entity issues a retransmission request [26]. Upon successful acknowledgment, the controlled entity confirms the establishment of the connection. Following this confirmation, the system identifies an available physical channel for data transmission and establishes the connection using Call Proceeding control (CPC). Once the connection is securely established, the controlled entity proceeds to transmit control data to the controlling entity, which includes essential control commands. Concurrently, to ensure continuous and stable communication, the process of maintaining the connection is actively managed as depicted in Figure 2. This structured approach ensures that each step in the transmission process is clearly defined and effectively managed for optimal data communication.

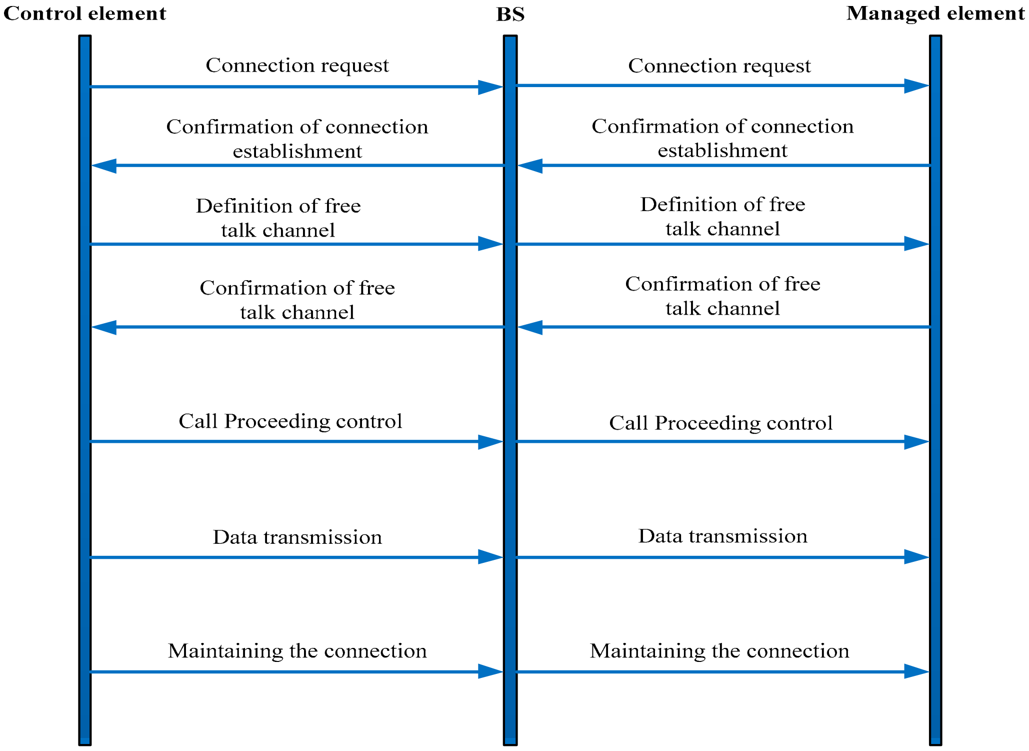
Control element
BS
Managed element
Connection request
Connection request
Confirmation of connection establishment
Confirmation of connection establishment
Definition of free talk channel
Definition of free talk channel
Confirmation of free talk channel
Confirmation of free talk channel
Call Proceeding control
Call Proceeding control
Data transmission
Data transmission
Maintaining the connection
Maintaining the connection

Figure 2. Data transmission diagram.

2.2. Problem Statement

Consider a radio channel that facilitates the control of a CPS. This channel includes both physical and logical components responsible for data transmission, connection establishment, and the ongoing maintenance of connections. This radio channel operates in conditions of persistent random interference and cyberattack is executed by the attacker successfully with a probability of P_{ca}, aiming to disrupt the control of the CPS. The determination of the probability of a successful cyberattack by an intruder is carried out using the models presented in [27]. When there is a need for data transmission, the process of establishing a connection is initiated through logical channels. Suppose the process of establishing a connection successfully happens within a random time frame t_h, characterized by a distribution function $H(t)$. Once the connection is set up, the data transmission over a physical channel takes place within a random time period t_a, governed by a distribution function $H(t)$. In this case, the data transmission process is accompanied by the transmission of commands over the logical channel to maintain an established connection during a random time t_b with a distribution function $B(t)$. If the impact on the data transmitted over the physical channel is not successful, and the probability of this event is $1 - P_{ca}$, then the data to be transmitted will be successfully delivered to the CPS recipient in a random time t_{b1} with a distribution function $B_1(t)$, determined by the transmission rate R and the volume of the transmitted data V. Otherwise, with a probability P_{ca}, the cyber activity is neutralized during a random time t_{d1} with the distribution function $D_1(t)$, and the data will be transmitted again. A command to maintain an established connection having a random duration t_c with a distribution function $C(t)$ is transmitted during a random time interval t_b with a distribution function $B(t)$ with probability $P(t_c > t_b)$. With the opposite probability $P(t_c \leq t_b)$, the command to maintain the connection will be retransmitted. It is necessary to calculate both the average time and the time distribution function for successful data transmission over a radio channel.

2.3. Solution

Let us represent the information transmission process described in the problem statement as an aggregated stochastic network [28], as depicted in Figure 3. The data transmission process includes private processes: the process of establishing $h(s)$, the process of maintaining the established connection $b(s)$, and the process of data transmission $a(s)$.

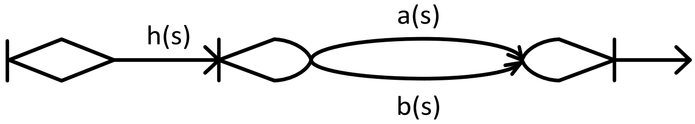

Figure 3. An aggregated stochastic network of the data transmission process over a mobile radio communication channel of a standard.

The Process of Establishing a Connection (h(s)): This initial phase involves setting up the necessary communication links between devices or network nodes. It is critical for determining the feasibility and parameters of the subsequent data transmission, ensuring that the connection is secure and reliable.

The Process of Maintaining the Established Connection (b(s)): Once a connection is established, maintaining it becomes essential, especially in dynamic environments where network conditions can change rapidly. This process ensures that the connection remains robust, handling any potential disruptions or variations in network quality to provide a steady communication channel.

The Process of Data Transmission (a(s)): This is the actual transfer of data across the established and maintained connection. It involves the encoding, sending, and decoding of the transmitted data, ensuring that the information is delivered accurately and efficiently from the source to the destination.

Each of these subprocesses plays a crucial role in the seamless execution of data transmission, working together to ensure that data not only reach their destination but do so in a manner that is timely, secure, and consistent with the quality requirements of the network.

To address the problem at hand, it is essential to initially determine the equivalent functions for each individual process.

1. Determination of the distribution function of the connection establishment process. The process of establishing a connection through a logical channel was investigated in [29], and the equivalent function for this process is detailed in Equation (1).

$$h(s) = \frac{P_1 b(s) r(s)[P_2 + (1 - P_2)u(s)P_3 r(s)]}{1 - (1 - P_1)b(s) - (1 - P_2)u(s)(1 - P_3)P_1 b(s) r(s)} \tag{1}$$

where P_1—the probability of successfully receiving the KVS frame; P_2—the probability of successfully receiving UPS, KPS, and DISTANCE; P_3—the probability of successfully receiving UPS, KPS, and DISTANCE base station (BS) signals after power regulation;

$b(s),\ r(s),\ u(s)$—the Laplace–Stieltjes transforms of the probability distribution functions of KVS reception time, successful reception times for UPS, KPS, and DISTANCE, and the power regulation time for random variables (2):

$$\begin{aligned} b(s) &= \int\limits_0^\infty e^{-st} d[B(t)] \\ r(s) &= \int\limits_0^\infty e^{-st} d[R(t)] \\ u(s) &= \int\limits_0^\infty e^{-st} d[U(t)] \end{aligned} \tag{2}$$

Building upon the method described in [29], we will determine the distribution function for the time required to establish a connection using the two-moment approximation method, as detailed in [30]. This involves calculating the first two moments of the random time interval required for connection establishment. Furthermore, we will identify the shape and scale parameters of the Gamma distribution, as outlined in Equation (3):

$$\begin{gathered} M_{1h} = (-1)^1 \frac{d}{ds}\left(\frac{h(s)}{h(0)}\right)_{s=0}; \\ M_{2h} = (-1)^2 \frac{d^2}{ds^2}\left(\frac{h(s)}{h(0)}\right)_{s=0}; \\ D_h = M_{2h} - M_{1h}^2 \end{gathered} \tag{3}$$

where
$v = \frac{M_{1h}}{D_h}$—scale parameter;
$\varsigma = \frac{M_{1h}^2}{D_h}$—shape parameter.

Consequently, the distribution function for the connection establishment time is represented as follows in Equation (4):

$$H(t) = \frac{v^{\varsigma}}{\Gamma(\varsigma)} \int_0^e t^{\varsigma-1} e^{-vt} dt \tag{4}$$

which has an image $h(s) = \left(\frac{v}{v+s}\right)^{\varsigma}$.

2. Determination of the probability distribution function of the data transmission process.

Let us represent the data transmission process as a stochastic network (Figure 4).

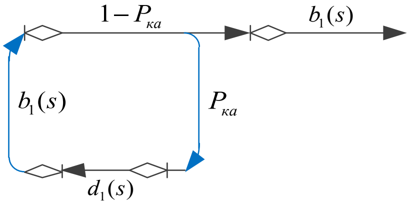

Figure 4. Stochastic network of the data transmission process over the physical channel.

Figure 4 indicates P_{ca}—the probability of a computer attack occurring and $b_1(s)$, $d_1(s)$—the Laplace–Stieltjes transforms of the distribution functions for the packet transmission time of a specified volume and the recovery time following a cyber attack, which are defined for the respective random variables in Equation (5):

$$\begin{aligned} b_1(s) &= \int\limits_0^\infty e^{-st} d[B_1(t)] \\ d_1(s) &= \int\limits_0^\infty e^{-st} d[D_1(t)] \end{aligned} \tag{5}$$

The functional representation corresponding to the network shown in Figure 4 is articulated as Equation (6):

$$a(s) = \frac{(1 - P_{ka})b_1(s)}{1 - P_{ka}b_1(s)d_1(s)} \tag{6}$$

The probability distribution function for data transmission time is similarly determined and is represented by a Gamma function, as shown in Equation (7):

$$\begin{aligned} M_{1a} &= (-1)^1 \tfrac{d}{ds}\left(\tfrac{a(s)}{a(0)}\right)_{s=0}; \\ M_{2a} &= (-1)^2 \tfrac{d^2}{ds^2}\left(\tfrac{a(s)}{a(0)}\right)_{s=0}; \\ D_a &= M_{2a} - M_{1a}^2 \end{aligned} \tag{7}$$

where

$\sigma = \frac{M_{1a}}{D_a}$—scale parameter;

$\rho = \frac{M_{1a}^2}{D_a}$—shape parameter.

Then, the connection establishment time distribution function is (8):

$$A(t) = \frac{\sigma^\rho}{\Gamma(\rho)} \int_0^t t^{\rho-1} e^{-\sigma t} dt \tag{8}$$

3. Define the distribution function of the connection maintenance process.

The procedure for maintaining the connection is illustrated by the network presented in Figure 5.

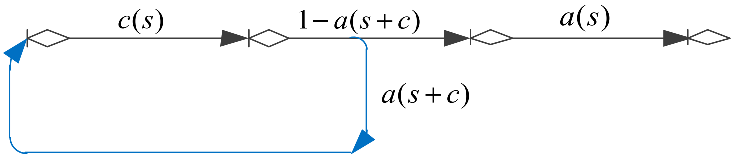

Figure 5. Stochastic network of the connection maintenance process over the logical channel.

Figure 5 indicates:

$c(s)$—the Laplace–Stieltjes transform is applied to the probability distribution function representing the duration of the connection maintenance command;

$a(s+c)$—the Laplace–Stieltjes transform is utilized for the probability distribution function corresponding to the time required for re-establishing a connection during data transmission;

$a(s)$—the transformation of the probability distribution function of the data transmission duration using the Laplace–Stieltjes method is denoted as Equation (9):

$$\begin{aligned} c(s) &= \int\limits_0^\infty e^{-st} d[C(t)] \\ a(s) &= \int\limits_0^\infty e^{-st} d[A(t)] \end{aligned} \tag{9}$$

Equivalent function of stochastic network (Figure 5) has the form (10):

$$b(s) = \frac{c(s)(1 - a(s+c))a(s)}{1 - c(s)a(s+c)} \tag{10}$$

The connection maintenance time distribution function is similarly defined and represented as Gamma function (11):

$$B(t) = \frac{\theta^\varsigma}{\Gamma(\varsigma)} \int_0^t t^{\varsigma-1} e^{-\theta t} dt \tag{11}$$

$M_{1b} = (-1)^1 \frac{d}{ds}\left(\frac{b(s)}{b(0)}\right)_{s=0}$; $M_{2b} = (-1)^2 \frac{d^2}{ds^2}\left(\frac{b(s)}{b(0)}\right)_{s=0}$; $D_b = M_{2b} - M_{1b}^2$.
$\theta = \frac{M_{1b}}{D_b}$—scale parameter;
$\zeta = \frac{M_{1b}^2}{D_b}$—shape parameter.

The outcomes from steps 1–3 enable us to ascertain the equivalent function of the stochastic network, as shown in Figure 3.

$$Q(s) = h(s)L\{A(t)B(t)\} \tag{12}$$

where $L\{A(t)B(t)\}$—the Laplace transform operator of the product of two probability distribution function [31].

To calculate the Laplace transform of the right multiplier in Equation (12) using Equations (8) and (11), we propose the following method:

Let the distribution function (13) be given:

$$F(x) = \frac{\sigma^\rho \theta^\varsigma}{\Gamma(\rho)\Gamma(\varsigma)} \int_0^x t^{\rho-1} e^{-\sigma t} dt \cdot \int_0^x t^{\varsigma-1} e^{-\theta t} dt \tag{13}$$

with density function (14):

$$f(x) = \frac{\sigma^\rho \theta^\varsigma}{\Gamma(\rho)\Gamma(\varsigma)} (g(x)G_1(x) + g_1(x)G(x)) \tag{14}$$

where $g(x) = g(t) = t^{\rho-1}e^{-\sigma t}$ and $g_1(x) = g_1(t) = t^{\varsigma-1}e^{-\theta t}$, G—their antiderivatives: $G(x) = \int_0^x t^{\rho-1}e^{-\sigma t}dt$ and $G_1(x) = \int_0^x t^{\zeta-1}e^{-\theta t}dt$.

Let us determine the Laplace transforms of the derivatives and their antiderivatives (15)–(18):

$$L(g, s) = \int_0^x t^{\rho-1}e^{-\sigma t}e^{-st}dt = \frac{1}{(s+\sigma)^\rho}\int_0^\infty u^{\rho-1}e^{-u}du = \frac{\Gamma(\rho)}{(s+\sigma)^\rho} \tag{15}$$

$$L(g_1, s) = \int_0^x t^{\varsigma-1}e^{-\theta t}e^{-st}dt = \frac{1}{(s+\theta)^\varsigma}\int_0^\infty u^{\varsigma-1}e^{-u}du = \frac{\Gamma(\varsigma)}{(s+\theta)^\varsigma} \tag{16}$$

$$L(G, s) = \frac{1}{s}L(g, s) = \frac{\Gamma(\rho)}{s(s+\sigma)^\rho} = \frac{\Gamma(\rho)}{(s+\sigma)^{\rho+1}}\sum_{k=0}^\infty \left(\frac{\sigma}{s+\sigma}\right)^k = \Gamma(\rho)\sum_{k=0}^\infty \frac{\sigma^k}{(s+\sigma)^{\rho+k+1}} \tag{17}$$

$$L(G_1, s) = \frac{1}{s}L(g_1, s) = \frac{\Gamma(\varsigma)}{s(s+\theta)^\varsigma} = \frac{\Gamma(\varsigma)}{(s+\theta)^{\varsigma+1}}\sum_{k=0}^\infty \left(\frac{\theta}{s+\theta}\right)^k = \Gamma(\varsigma)\sum_{k=0}^\infty \frac{\theta^k}{(s+\theta)^{\varsigma+k+1}} \tag{18}$$

Substituting (15)–(18) in (14), we obtain an image of the density function (19):

$$HA(s, N) = [HA_1(s, N) + HA_2(s, N)]\frac{\sigma^\rho\theta^\varsigma}{\Gamma(\rho)\Gamma(\varsigma)} \tag{19}$$

where

$HA_1(s,\ N) = \Gamma(\rho+\zeta)\sum_{k=0}^{N}\left[\frac{\sigma^k(\sigma+\theta)^{\rho+\zeta+k}}{(s+\sigma+\theta)^{\rho+\zeta+k}(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,\ k)}{f(\rho+k,\ k+1)}\right]$

$HA_2(s,\ N) = \Gamma(\rho+\zeta)\sum_{k=0}^{N}\left[\frac{\theta^k(\sigma+\theta)^{\rho+\zeta+k}}{(s+\sigma+\theta)^{\rho+\zeta+k}(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,\ k)}{f(\zeta+k,\ k+1)}\right]$

$f(x,\ k) = \left|\begin{array}{ll} \prod_{j=0}^{k-1}(x-j), & at \quad k > 0 \\ 1, & at \quad k = 0 \end{array}\right.$ —descending factorial.

By taking each term back to the original domain, integrating the obtained result with a variable upper limit, we will obtain the desired distribution function (20):

$$HF(t,N) = [HF_1(t,N) + HF_2(t,N)]\frac{\sigma^{\rho}\theta^{\varsigma}}{\Gamma(\rho)\Gamma(\varsigma)} \tag{20}$$

where

$HF_1(t,\ N) = \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\sigma^k\gamma[(\sigma+\theta)t,\ \rho+\zeta+k]}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,\ k)}{f(\rho+k,\ k+1)}\right];$

$HF_2(t,\ N) = \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\theta^k\gamma[(\sigma+\theta)t,\ \rho+\zeta+k]}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,\ k)}{f(\zeta+k,\ k+1)}\right].$

$\gamma[(\sigma+\theta)t,\ \rho+\varsigma+k]$—Gamma distribution with parameters $(\sigma+\theta)t$ and $(\rho+\varsigma+k)$. Substituting (19) into (12), we obtain (21):

$$\begin{aligned} QA(s,N) &= \left(\tfrac{\nu}{\nu+s}\right)^{\zeta}[HA_1(s,N)+HA_2(s,N)]\tfrac{\sigma^{\rho}\theta^{\zeta}}{\Gamma(\rho)\Gamma(\zeta)} \\ &= \tfrac{\sigma^{\rho}\theta^{\zeta}}{\Gamma(\rho)\Gamma(\zeta)}\left\{\begin{array}{l} \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\sigma^k(\lambda_k)^{\alpha_k}}{(s+\lambda_k)^{\alpha_k}(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\rho+k,k+1)}\right]+ \\ \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\theta^k(\lambda_k)^{\alpha_k}}{(s+\lambda_k)^{\alpha_k}(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\zeta+k,k+1)}\right] \end{array}\right\} \end{aligned} \tag{21}$$

where

$\lambda_k = \frac{T_k}{D_k};\ \alpha_k = \frac{(T_k)^2}{D_k}$—$k$-th scale and form parameters.

$T_k = \frac{\rho+\varsigma+k}{\sigma+\theta} + M_{1h};\ D_k = \frac{(\rho+\zeta+k)+(\rho+\zeta+k+1)}{(\sigma+\theta)^2} + D_h.$

By reverting to the original space in a consistent manner and integrating the result from Equation (21) up to a variable upper limit, we obtain the function that characterizes the distribution of successful data transmission duration over the CPS radio channel, as described in Equation (22):

$$QF(t,N) = L^{-1}\{QA(s,N)\} = \frac{\sigma^{\rho}\theta^{\zeta}}{\Gamma(\rho)\Gamma(\zeta)}\left\{\begin{array}{l} \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\sigma^k\gamma[\lambda_k t,\alpha_k]}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\rho+k,k+1)}\right]+ \\ \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\theta^k\gamma[\lambda_k t,\lambda_k]}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\zeta+k,k+1)}\right] \end{array}\right\} \tag{22}$$

where $L^{-1}\{QA(s,N)\}$—the inverse Laplace transform operator of the function $QA(s, N)$, defined by the formula (21).

In turn, the average time of successful data transmission over the radio channel (23):

$$T(N) = -\frac{d}{ds}\left[\frac{QA(s,N)}{QA(0,N)}\right]_{s=0} = \frac{\sigma^{\rho}\theta^{\zeta}}{\Gamma(\rho)\Gamma(\zeta)}\left\{\begin{array}{l} \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\sigma^k T_k}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\rho+k,k+1)}\right]+ \\ \Gamma(\rho+\zeta)\sum\limits_{k=0}^{N}\left[\frac{\theta^k T_k}{(\sigma+\theta)^{\rho+\zeta+k}}\frac{f(\rho+\zeta+k-1,k)}{f(\zeta+k,k+1)}\right] \end{array}\right\} \tag{23}$$

Therefore, the problem at hand has been successfully resolved, providing a comprehensive solution to the challenges encountered.

3. Results and Discussion

3.1. Calculation Example

Using the relationships identified, calculations were performed with the initial data provided in Table 1.

The data shown in Figure 6, presented graphically, indicate that, based on the specified initial conditions, the radio channel ensures that information is delivered to the controlled entity of the CPS with a probability of at least 0.95 within a maximum of 3.3 s. This performance meets the standards set for data transmission channels in general-purpose CPSs.

Table 1. Initial data.

Reception time for KVS frames	$t_B = 0.35$ (s)
Reception time for UPS, KPS and DISTANCE	$t_r = 0.34$ (s)
UI adjustment time	$t_i = 0.56$ (s)
Probability values	$P_1 = P_2 = P_3 = 0.999$
Packet transmission time	$t_{b1} = 0.95$ (s)
Cyberattack neutralization time	$t_{d1} = 1$ (s)
Probability of a cyberattack by the attacker	$P_{ca} = 0.01$
Connection maintenance time	$t_c = 0.1$ (s)

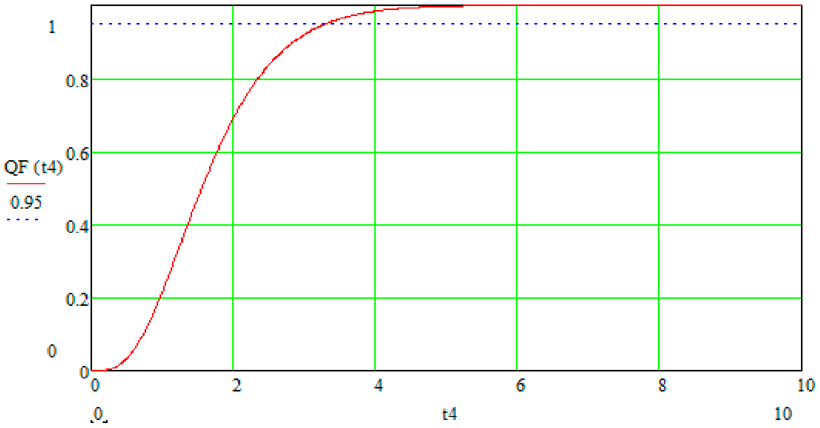

Figure 6. The probability distribution function for the time taken for successful data transmission over the CPS radio network.

3.2. Analysis of the Results Obtained

1. The likelihood of successful data delivery is capped at a specific maximum value, which is determined under the condition of no informational interference with the network from attackers and perfectly reliable components $P_{max}(t \leq T_Z) = lim_{\substack{P_{ca} \to 0 \\ P_i \to 1}} QF(t = T_Z, N)$.

Figure 7 displays the shape of the boundary distribution function for the time taken to deliver information.

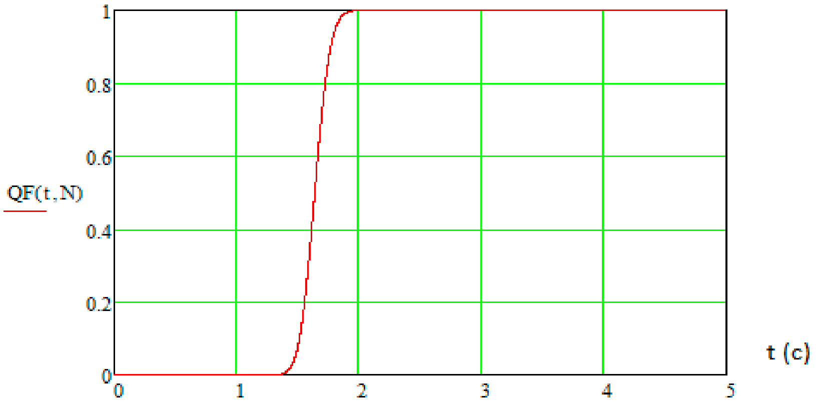

Figure 7. The probability distribution function for the time of successful data transmission, assuming completely reliable components of the radio channel and the absence of informational interference.

In this scenario, the packet delivery time is primarily determined by the data volume, transmission rate, and the established procedure for setting up the connection. However, when an attacker introduces and executes informational interference on the physical data transmission channel, the probability of successfully delivering data packets within a specified timeframe significantly decreases (Figure 7). This decline in delivery success is not related to the amount of data, its transmission speed, or the method of connection establishment but is directly influenced by the interference on the physical channel.

2. Calculations show that under conditions of cyberattacks by an attacker, the data packet delivery time can increase fourfold or more, accompanied by a decrease in the actual throughput of the transmission route.

For example, an increase in the probability of cyberattacks by the attacker from $P_{ca} = 0.009$ to $P_{ca} = 0.5$, results in an increase in the average data delivery time from $T_r = 2(\mathrm{s})$ to $T_r = 6.54(\mathrm{s})$ (Figure 8).

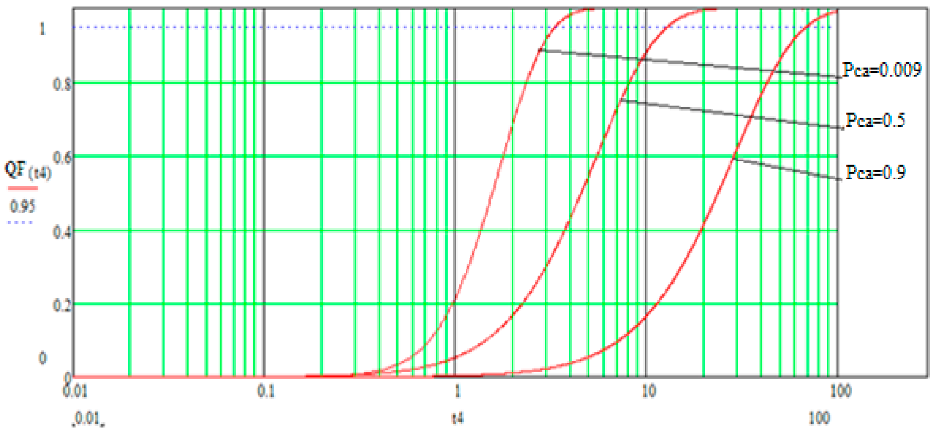

Figure 8. The probability distribution function for the duration of successful data transmission under different probabilities of a cyber attack by an adversary.

3. The implementation of a cyberattack by the attacker on the physical data transmission channel not only affects the time of successful data transmission but also impacts the actual throughput of the radio channel, which is determined as follows $\lambda_1(t,N) = \frac{\frac{d}{dt}QF(t,N)}{1-QF(t,N)}$. The minimal impact on the intensity values of successfully delivered packets suggests that under the influence of an attacker's informational disruptions, the data stream at the output of the radio channel can be characterized by a Poisson distribution, as illustrated in Figure 9.

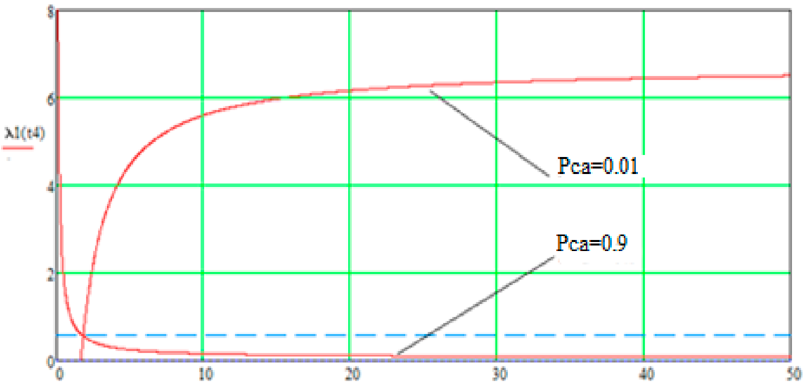

Figure 9. Graph depicting the relationship between the intensity of successfully transmitted data packets at various values of the probability of a computer attack by the attacker.

The results of the calculations indicate that the intensity of the delivered packet flow decreases sharply with the successful execution of a cyberattack. This significant drop can serve as an additional indicator that a cyberattack is underway, highlighting the need to implement measures to protect against informational interference.

4. When impacted by a cyberattack, the speed of detecting and restoring the functionality of the data transmission channel after informational disruptions is critical in determining

the time required for successful data delivery. Figure 10 displays a graph of the probability distribution function for the time of successful data delivery under cyberattack conditions, which varies with different average durations T_{neutr} for neutralizing the informational interference caused by the attacker.

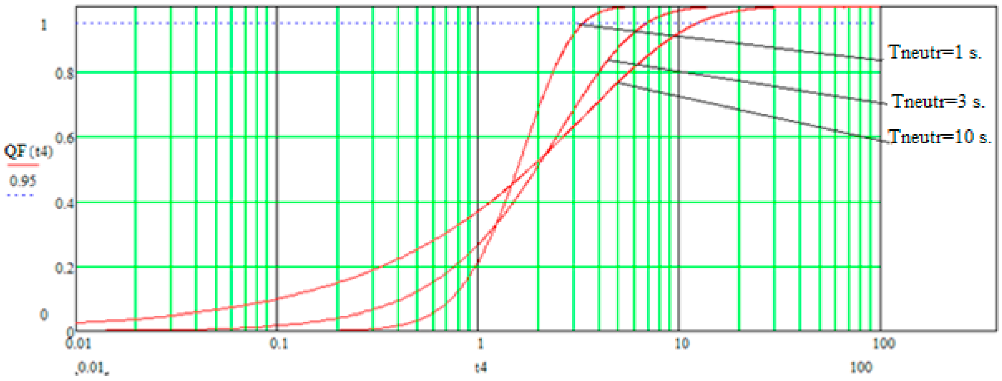

Figure 10. The probability distribution function for the time of successful data delivery in the context of cyberattacks by an attacker, varying according to different timeframes for their detection and neutralization.

For example, reducing the detection and neutralization time of cyberattacks (T_{neutr}) on the physical data transmission channel to one second leads to a more than threefold reduction in the average data delivery time. This significant decrease highlights the effectiveness and underscores the necessity of developing advanced methods for the early detection of cyberattacks.

5. The article proposes a method for determining the equivalent function of a segment of a stochastic network that includes a logical "AND" node. This method involves expanding the Laplace-transformed partial derivatives of density functions, as described in Equation (14), into a series (Equation (19)) and subsequently determining the distribution function (Equation (20)). The results of the calculations demonstrate that the values obtained using Equation (20) are in complete agreement with the original distribution function (Equation (13)), as shown in Figure 11.

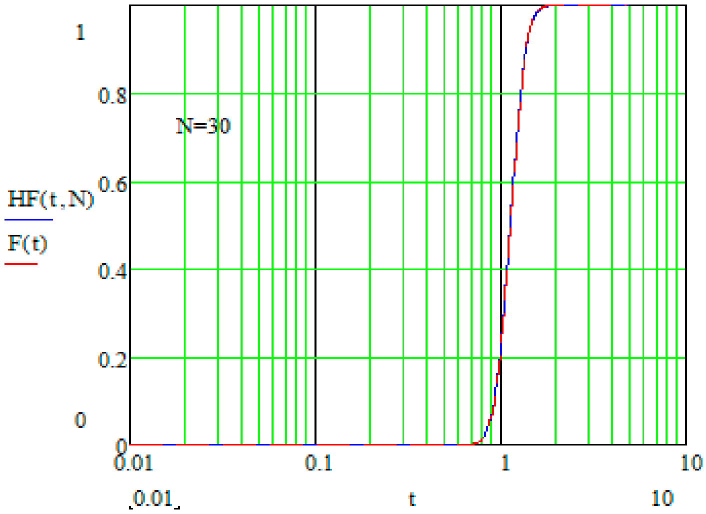

Figure 11. Distribution functions of the time of realization of the logical "AND" node obtained using Formulas (13) and (20).

The calculations indicate that as the number of terms in the series increases, the error decreases rapidly, becoming negligible when the number of series members exceeds 30, as shown in Figure 11. Figure 12 presents the relationship between the number of series terms N used and the absolute error in the calculations of function (13) using Equation (20).

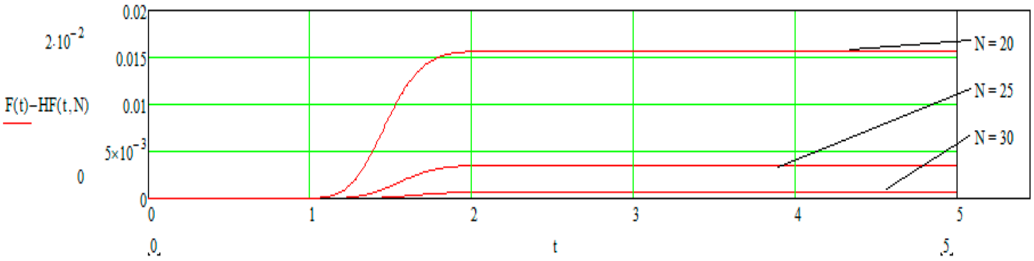

Figure 12. Graphs illustrating the dependence of the absolute error in determining the distribution function $F(t)$ using the series $HF(t,N)$.

It should be noted that the authors have successfully derived an equivalent function for a segment of a stochastic network containing a logical "AND" node for the first time. This derivation assumes that the random times of realization for the branches leading into the "AND" node are independent random variables with a gamma distribution. This breakthrough enables the straightforward derivation of an equivalent function for a stochastic network that includes a logical "OR" node as well. Given that the expression for the equivalent function (Equation (21)) is quite complex, it is recommended to simplify it by approximating with the Laplace-transformed incomplete gamma function.

$$Q_i(s) \approx \left(\frac{\mu}{\mu+s}\right)^{\beta}$$

with parameters $\mu = \frac{M_{1\gamma}}{D_\gamma}$ and $\beta = \frac{M_{1\gamma}^2}{D_\gamma}$, where $M_{1\gamma} = (-1)^1 \frac{d}{ds}\left[\frac{QA(s,N)}{QA(0,N)}\right]_{s=0}$; $M_{2\gamma} = (-1)^2 \frac{d^2}{ds^2}\left[\frac{QA(s,N)}{QA(0,N)}\right]_{s=0}$; and $D_\gamma = M_{2\gamma} - M_{1\gamma}^2$.

Consequently, the distribution function for the realization time of a segment of the stochastic network that includes the logical "AND" node is represented as follows (Equation (24)):

$$F_\gamma(t) = \frac{\mu^\beta}{\Gamma(\beta)} \int_0^t t^{\beta-1} e^{-\mu t} dt \tag{24}$$

The results of the assessment of the absolute error of such an approximation are presented in Figure 13. The analysis conducted by the authors shows that the maximum absolute error of calculations in this case will not exceed 9 × 10^{-3}, which is entirely satisfactory for engineering calculations.

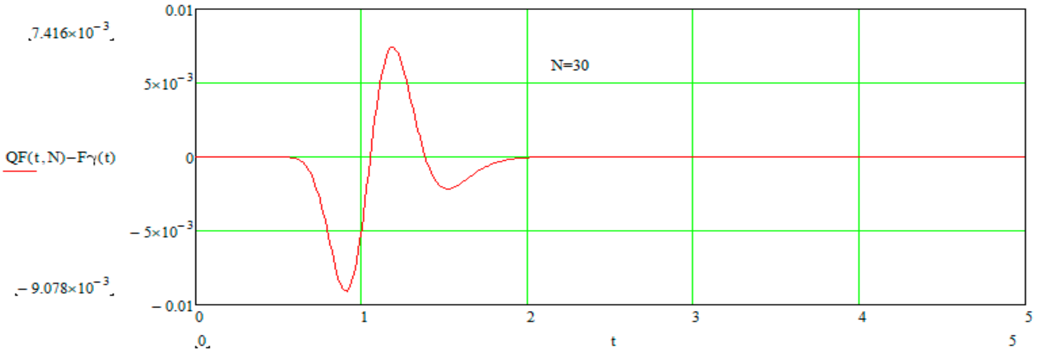

Figure 13. Dependency of the absolute error in the approximation of the distribution function $F_\gamma(t)$ with a Gamma distribution.

6. To compare the resulting solution (20)–(23) with other methods, we use it to calculate the integral of the form (25):

$$G(t) = \int_0^t x^{w-1} e^{-mx} dx \tag{25}$$

When applying the proposed approach, we will obtain (26):

$$P(t, N) = e^{-mt} t^w \sum_{k=0}^{N} \left(\frac{(mt)^k}{f(w+k, k+1)^2} \right) \tag{26}$$

where $f(x,\ k) = \left| \begin{array}{ll} \prod_{j=0}^{k-1} (x-j), & at \quad k > 0 \\ 1, & at \quad k = 0 \end{array} \right.$ —descending factorial, and using, for example (27), the well-known Taylor series decomposition [32]:

$$P_1(t, N) = t^w \sum_{k=0}^{N} \frac{(-mt)^k}{k!(w+k)} \tag{27}$$

Function graphs $G(t)$, $P(t, N)$, and $P_1(t, N)$ with different numbers of N series members are shown in Figure 14.

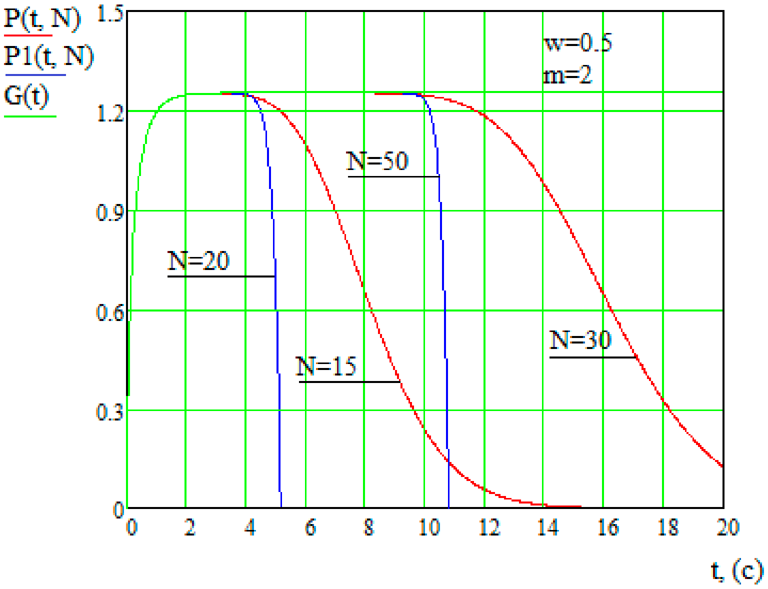

Figure 14. Result of comparison, proposed solution and Taylor series decomposition solution.

The calculations show that at a given value of t, the proposed approach will require 25–40% less series members than when using Taylor series decomposition, with comparable computational complexity of common series members.

4. Conclusions

This article introduces a mathematical model for the functioning of a radio channel within a cyber-physical system. This model comprehensively details the processes involved in establishing a connection, transmitting information, and maintaining the established connection. A unique aspect of this model is its consideration of both the energy parameters and the resilience of the radio channel to cyberattacks. During the model's development, an equivalent function for a segment of a stochastic network containing an "AND" logical node was established. It has been demonstrated that the time distribution function for the implementation of the "AND" node can be effectively approximated by the Gamma distribution. This approximation not only simplifies the equivalent function but also marginally reduces the computational complexity required to assess the radio channel's operational quality, without significantly affecting the accuracy of the results. Moreover, the proposed method requires 25–40% fewer series members than the traditional Taylor series decomposition, while maintaining comparable computational complexity for the typical series members. Furthermore, the maximum absolute error in the calculations is capped at 9×10^{-3}, which is well within acceptable limits for engineering purposes. Additionally, our analysis underscores the necessity of developing effective early detection methods for cyber impacts, crucial for preventing disruptions in data transmission over the radio channel.

Author Contributions: Conceptualization, F.M., A.P. (Alexander Privalov) and G.B.; methodology, F.M., A.P. (Andrey Privalov) and G.B.; validation, Y.I.-C. and A.P. (Andrey Privalov); formal analysis, E.K., G.B., K.H.K. and A.B.; investigation, G.B.; resources, K.H.K. and A.P. (Andrey Privalov); data curation, E.K. and A.B.; writing—original draft preparation, F.M. and G.B.; writing—review and editing, F.M. and G.B.; visualization, G.B. and E.K.; supervision, A.P. (Andrey Privalov) and Y.I.-C.; project administration, A.P. (Alexander Privalov); funding acquisition, Y.I.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This study was funded by the Korea Agency for Technology and Standards in 2022. The project numbers are 1415181629 (20022340, Development of International Standard Technologies based on AI Model Lightweighting Technologies) and 1415180835 (20020734, Development of International Standard Technologies based on AI Learning and Inference Technologies).

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to Russian Railway regulations.

Acknowledgments: The authors would like to express their sincere gratitude and appreciation to the supervisors, Privalov Andrey and Young Im-Cho (Gachon University), for their support, comments, remarks, and engagement over the period in which this manuscript was written. Moreover, the authors would like to thank the editor and anonymous referees for the constructive comments in improving the contents and presentation of this paper.

Conflicts of Interest: Author Kyung Hoon Kim was employed by the KT Corporation. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The KT Corporation 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.

Abbreviations

Variable	**Definition**
P_{ca}	Probability of a cyberattack being carried out by a perpetrator
$1 - P_{ca}$	Probability of no cyberattack being carried out by a perpetrator
t_h	Random time of the connection establishment process
t_b	Random time of the connection maintenance process
t_a	Random time of the command transmission process
t_{b1}	Random time of successful data transmission in the absence of a cyberattack
t_{d1}	Random time of cyberattack neutralization
t_c	Random duration of the command to maintain an established connection
$B(t)$	Distribution function of the connection maintenance process
$A(t)$	Distribution function of the command transmission process
$B_1(t)$	Distribution function of data transmission in the absence of a cyberattack
$H(t)$	Distribution function of the connection establishment process
$D_1(t)$	Distribution function of the cyberattack neutralization process
$C(t)$	Distribution function of the process of maintaining an established connection command
R	Data transmission rate
V	Volume of data transmitted

$h(s)$	Laplace–Stieltjes transform of the probability distribution function of connection establishment time
$b(s)$	Laplace–Stieltjes transform of the probability distribution function of connection maintenance time
$a(s)$	Laplace–Stieltjes transform of the probability distribution function of command transmission time
$Q(s)$	Final equivalent function
$F(x)$	Distribution function of data transmission and connection maintenance processes
$f(x)$	Density function of data transmission and connection maintenance processes
$HA(s,N)$	Graph of the density function of data transmission and connection maintenance processes
$HF(t,N)$	Distribution function of data transmission and connection maintenance processes obtained through series expansion
$QA(s,N)$	Equivalent function of a stochastic network considering series expansion
$QF(t,N)$	Distribution function of the duration of successful data transmission via radio channel
$T(N)$	Average time of successful data transmission via radio channel
N	Number of series terms
T_r	Average time of data delivery
$\lambda_1(t,N)$	Actual channel throughput
T_{neutr}	Average time of the cyberattack neutralization process

References

1. *GOST R 1.16-2011*; Standardization in Russian Federation: Preliminary National Standards. Instructions for Development, Taking Over, Application and Cancellation; Section 5 and 6. The Federal Agency on Technical Regulating and Metrology (GOST R): Moscow, Russia, 2011.
2. Zegzhda, P.D.; Poltavtseva, M.A.; Lavrova, D.S. Systematization of cyber-physical systems and their security assessment. *Probl. Inf. Secur. Comput. Syst.* **2017**, *2*, 127–138. [CrossRef]
3. Zegzhda, D.P. (Ed.) *Theoretical Foundations of Cyber Resilience and Practice of Prognostic Protection Against Cyberattacks: Monograph*; Polytech-Press: St. Petersburg, Russia, 2022; 489p.
4. On the Security of Critical Information Infrastructure of the Russian Federation. Federal Law of 26 July 2017 (No 187-FZ). Available online: https://www.prlib.ru/en/node/692141 (accessed on 12 November 2023).
5. Boldinov, A.M. Threats to telecommunications networks in cyberphysical systems. In *SPbNTORES: Works of the Annual NTK, Proceedings of the 77th Scientific and Technical Conference of the St. Petersburg, NTO RES Named after A.S. Popova Dedicated to Radio Day, St. Petersburg, Russia, 25–29 April 2022*; Boldinov, A.M., Privalov, A.A., Eds.; Saint Petersburg Electrotechnical University: St. Petersburg, Russia, 2022; No 1/77; pp. 182–184.
6. Bydanov, E.V.; Barinov, D.M. Mathematical models of the MIMO radio channel. *Mod. Sci. Res. Innov.* **2020**, *111*, 3–10. Available online: https://web.snauka.ru/issues/2020/07/92926 (accessed on 12 November 2023).
7. Babkin, A.N.; Akchurina, L.V. The use of Markov models to assess the availability of information in the radio channel. *Bull. Voronezh Inst. Fed. Penitentiary Serv. Russ.* **2020**, *4*, 9–15.
8. Polshchikov, K.A.; Lazarev, S.A.; Kiseleva, E.D.; Kiselev, V.E. Mathematical models for assessing the use of radio channels when transmitting real-time streams in a wireless self-organizing network. *Info Commun. Technol.* **2019**, *17*, 336–341. Available online: https://www.elibrary.ru/item.asp?id=41569018 (accessed on 12 November 2023).
9. Tolstova, A.V.; Zaluzhnyi, O.V.; Hol, V.D. Algorithm for Forming Structure and Stages of Message Transfer in Unidirectional Radio Systems. *Radioelectron. Commun. Syst.* **2020**, *63*, 265–272. [CrossRef]
10. Rajba, S.; Rajba, T.; Raif, P. Simulation study of the random access control in the wireless sensor network. *Ukr. Sci. J. Inf. Secur.* **2013**, *19*, 7–13. [CrossRef]
11. Khodaverdizadeh, M.; Haghbin, A.; Razzazi, F. Improving the Performance of HF Radio Networks in the Presence of Interference through Automatic Link Establishment with Frequency Hopping Technique. *Wireless Pers. Commun.* **2022**, *127*, 2647–2666. [CrossRef]
12. Bilal, A.; Sun, G. Automatic Link Establishment for HF Radios. *ICSESS Wirel. Pers. Commun. Int. J.* **2017**, *127*, 640–643.
13. Ayad, M.; Alkanhel, R.; Saoudi, K.; Benziane, M.; Medjedoub, S.; Ghoneim, S.S. Evaluation of Radio Communication Links of 4G Systems. *Sensors* **2022**, *22*, 3923. [CrossRef]
14. Vithanawasam, C.K.; Then, Y.L.; Su, H.T. Calculation of Data Rates for Varying Scenarios Using Free Space Path Loss and Okumura-Hata Model in the TVWS Frequency Band. In Proceedings of the IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), Kuching, Malaysia, 1–3 December 2020.
15. Li, H.; He, X.; He, W. Review of wireless personal communications radio propagation models in high altitude mountainous areas at 2.6 GHz. *Wirel. Pers. Commun.* **2018**, *101*, 735–753. [CrossRef]
16. Myagmardulam, B.; Tadachika, N.; Takahashi, K.; Miura, R.; Ono, F.; Kagawa, T.; Shan, L.; Kojima, F. Path Loss Prediction Model Development in a Mountainous Forest Environment. *IEEE Open J. Commun. Soc.* **2021**, *2*, 2494–2501. [CrossRef]

17. Willhammar, S.; Flordelis, J.; Van Der Perre, L.; Tufvesson, F. Channel Hardening in Massive MIMO: Model Parameters and Experimental Assessment. *IEEE Open J. Commun. Soc.* **2020**, *1*, 501–512. [CrossRef]
18. Ghiaasi, G.; Abraham, J.; Eide, E.; Ekman, T. Effective channel hardening in an indoor multiband scenario. *Int. J. Wireless Inf. Newt.* **2019**, *26*, 259–271. [CrossRef]
19. Gao, X.; Edfors, O.; Rusek, F.; Tufvesson, F. Massive MIMO performance evaluation based on measured propagation data. *IEEE Trans. Wireless Commun.* **2015**, *14*, 3899–3911. [CrossRef]
20. Sanguinetti, L.; Bjornson, E.; Hoydis, J. Toward massive MIMO 2.0: Understanding spatial correlation interference suppression and pilot contamination. *IEEE Trans. Commun.* **2020**, *68*, 232–257. [CrossRef]
21. Rosberg, T.; Thorslund, B. Radio communication-based method for analysis of train driving in an ERTMS signaling environment. *Eur. Transp. Res. Rev.* **2022**, *14*, 18. [CrossRef]
22. Rosberg, T.; Cavalcanti, T.; Thorslund, B.; Prytz, E.; Moertl, P. Driveability Analysis of the European Rail Transport Management 4 System (ERTMS): A systematic literature review. *J. Rail Transp. Plan. Manag.* **2021**, *18*, 100240. [CrossRef]
23. Ranjbar, V. Migration to ERTMS for dense traffic lines: Investigation methodologies and application to the Stockholm City case study. *Tecnoscienza Ital. J. Sci. Technol. Stud.* **2021**, *76*, 937–977.
24. Furness, N.; Van Houten, H.; Arenas, L.; Bartholomeus, M. ERTMS Level 3: The Game-Changer. *IRSE News* **2017**, *232*, 2–9.
25. Mansson, J.; Wallenbro, K. Reliability Study of ERTMS in Sweden. An analysis of Swedish Signaling Systems. Bachelor's Thesis, Lund University (LTH), Helsingborg, Sweden, 2020.
26. Shelukhin, O.I.; Filinova, A.S.; Vasina, A.V. Detection of abnormal intrusions into computer networks by statistical methods. *Informatics* **2015**, *9*, 42–49.
27. Kotenko, I.; Saenko, I.; Privalov, A.; Lauta, O. Ensuring SDN resilience under the influence of cyber-attacks: Combining methods of topological transformation of stochastic networks, Markov processes, and neural networks. *Big Data Cogn. Comput.* **2023**, *7*, 66. [CrossRef]
28. Privalov, A.A. *The Method of Topological Transformation of Stochastic Networks and Its Use for Analyzing Navy Communication Networks*; Military Academy of Communications (VMA): St. Petersburg, Russia, 2000; 166p.
29. Boldinov, A.M.; Privalov, A.A. Mathematical model of the control channel of the GSM-R radio communication standard. In *Izvestia of St. Petersburg University of Transports*; St. Petersburg State Transport University (PGUPS): St. Petersburg, Russia, 2022; Volume 19, pp. 743–751.
30. Wentzel, E.S. *Probability Theory: Studies. For University*, 5th ed.; Mir Publishers: Moscow, Russia, 1998; 576p.
31. Zorich, V.A. *Mathematical Analysis II*; Springer: Berlin/Heidelberg, Germany, 1984; 640p.
32. Konev, V.V. *Preparatory Course of Mathematics*; Tomsk Polytechnic University: Tomsk, Russia, 2009; 123p.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.