Chemical Technology, Control and Management

Volume 2019
Issue 4 SPECIAL ISSUE 4-5

10-26-2019

Mathematical Model Of The Implemented Impairer Of The Information Impact Process On The Operative-Technological Communication Network Based On Ip-Technologies

Abdulxak Abdulxairovich Khalikov
*Tashkent Institute of Railway Engineers, Address: 1 Adilxodjaeva st., 100167, Tashkent city, Republic of Uzbekistan*, xalikov_abdulxak@mail.ru

Olimdjan Khikmatovich Urakov
*Tashkent Institute of Railway Engineers, Address: 1 Adilxodjaeva st., 100167, Tashkent city, Republic of Uzbekistan*, sherzod_piter@mail.ru

Follow this and additional works at: [https://uzjournals.edu.uz/ijctcm](https://uzjournals.edu.uz/ijctcm)

Part of the Engineering Commons

**Recommended Citation**

Available at: [https://uzjournals.edu.uz/ijctcm/vol2019/iss4/7](https://uzjournals.edu.uz/ijctcm/vol2019/iss4/7)

This Article is brought to you for free and open access by 2030 Uzbekistan Research Online. It has been accepted for inclusion in Chemical Technology, Control and Management by an authorized editor of 2030 Uzbekistan Research Online. For more information, please contact sh.erkinov@edu.uz.
Mathematical Model Of The Implemented Impairer Of The Information Impact Process On The Operative-Technological Communication Network Based On IP-Technologies

Cover Page Footnote

Erratum
??????

This article is available in Chemical Technology, Control and Management: https://uzjournals.edu.uz/ijctcm/vol2019/iss4/7
MATHEMATICAL MODEL OF THE IMPLEMENTED IMPAIRER OF THE INFORMATION IMPACT PROCESS ON THE OPERATIVE-TECHNOLOGICAL COMMUNICATION NETWORK BASED ON IP-TECHNOLOGIES

Abdulxak Abdulxairovich Khalikov¹, Olimdjan Khikmatovich Urakov²

¹Tashkent Institute of Railway Engineers
Address: 1 Adilxodjaeva st., 100167, Tashkent city, Republic of Uzbekistan
E-mail: xalikov_abdulxak@mail.ru;
²Tashkent Institute of Railway Engineers
Address: 1 Adilxodjaeva st., 100167, Tashkent city, Republic of Uzbekistan
E-mail: sherzod_piter@mail.ru.

Annotation: The article discusses the mathematical model of the implemented intruder of the process of information impact on the operational-technological communication network based on IP technologies, representing the process of functioning of the IP telephone network in the form of a stochastic network, using the Mason equation for closed graphs, an equivalent function of the stochastic network, the network functioning process operational-technological communication-IP in the conditions of the nth type of cyber attack of the intruder. To demonstrate the method for determining the distribution function of time for bringing data packets in the operational-technological communication-IP network, a particular problem is considered. Using the Mason equation for closed graphs, the equivalent function of the stochastic network is compiled, it is established that the developed model provides results that do not contradict the logic, is sensitive to changes in input parameters and is operable, is in good agreement with the data obtained using known models, and allows you to determine the average time spent on implementation of the selected type of computer attack.

Keywords: operational-technological communication, Mason equations for closed graphs, cyberattack, disruptions, stochastic network, mathematical expectations, data packet transmission time.

Annotation: Маколада IP технологиялар асосида тезкор-технологик алоқа тармоғида амалга оширилган ахборотга тасšíр ўтказиш жараёнини математик модели, стохастик тармоқ шаклида IP телефон тармоғининг ишлаш жараёнини акс этирмиси, ёпиқ графиклар учун Мейсон тенгламасидан фойдаланган холда, стохастик тармоқни эквивалент функцияси, тармоқни ишлаш тасвирланган, тажқкурснориси кибер хужумни нинг п-туриси шароитида тезкор-технологик алоқа-IP тармоғида маълумотлар пакетлари олиб келиш вақтини таъсирлайди функциясини аниқлаш учун маълумотларни аниқлаш вақтини таъсирлайди функциясини аниқлаш учун маълумотларнинг усуллари аниқланган. Ёпиқ графиклар учун Мейсон тенгламасидан фойдаланиб, стохастик тармоқни эквивалент функцияси тузилган, аннотация модел мантиққа эки бўлган натижалари берган, кириш параметрларининг ўзароқ артиқланишеб, саннинг ва ишлатиш вақт тасвирлайди амалга оширилган маълумотларни мос келиш ва карорлайди ўртача вақтини аниқлашга имкон беради.

Таянч сўзлар: тезкор-технологик алоқа, ёпиқ графиклар учун Мейсон тенгламаси, киберхужумлар, узилишлар, стохастик тармоқ, математик тахминлар, маълумот узатиш вақти.

Annotation: Рассматривается математическая модель реализуемого нарушителя процесса информационного воздействия на сеть оперативно-технологической связи на базе IP-технологий, представляя процесс функционирования телефонной IP-сети в виде стохастической сети, с использованием уравнения Мейсона для замкнутых графов составлен эквивалентная функция стохастической сети, процесса функционирования сети оперативно-технологической связи-IP в условиях n-го вида кибератаки нарушителя. Для демонстрации метода определения функции распределения времени доведения пакетов данных в оперативно-технологической связи-IP сети рассмотрена частная задача. Используя уравнение Мейсона для замкнутых графов, составленная эквивалентная функция стохастической сети, установлена, что разработанная модель обеспечивает получение не противоречащих логике результатов, чувствительна к изменениям входных
Introduction

For the Republic of Uzbekistan, railway transport is of great strategic importance. It links together the economic system of the Republic, ensuring the stability of industrial enterprises, timely delivery of the most important goods to the most remote corners of the country. Joint Stock Company “Uzbekistan Temir Yollari” (UTY JSC), currently carries out about 40% of cargo and more 70% of the country's passenger traffic [1].

The quality of the railway transportation process is determined by the speed, reliability and safety of the delivery of goods and passengers to their destination. These indicators depend on the successful functioning and interaction of departments and farms [2, 3]. The significant role of this interaction in telecommunication networks of railway transport. The telecommunication network of railway transport is designed to provide communications for enterprises and structural divisions of railway transport, in accordance with the rules for the technical operation of railways of the Republic of Uzbekistan [10-21]. In accordance with the needs of the railway transport management system, the networks provided to subscribers are necessary volumes and quality of communication are determined taking into account the development of communication technology and the possibility of expanding the list of services.

Research Methods and Results

The potential impacting factors on the OTC network are analyzed, since the results of the analysis show that the main ones can be considered when transmitting information in OTC networks based on IP technologies as: interception of address data; “Denial of service”); “Telephone spam”; “Substitution of numbers” and "theft of services." To ensure the required level of quality of OTC telecommunication services in certain areas, it is necessary to solve the following tasks:

- modeling of the process of functioning of the OTN network based on IP technologies in the context of information impacts. Imagine the process of functioning of an IP telephone network as described in the statement of the problem in the form of a stochastic network [6] (Fig. 1). In the stochastic network, it is indicated: and - the Laplace – Stieltjes transforms of the corresponding distribution functions, which mean the FR value of the packet transmission time without taking into account the cyber attack (CA) of the intruder, that is, under “ideal conditions” and the FR of

\[
\beta(s) = \int_0^n e^{-s} d[B(t)]
\]

Fig. 1. Stochastic process network.
Using the Mason equation for closed graphs [5], we compose the equivalent function of the stochastic network:

\[ h_n(s) = \frac{k\beta(s)(\bar{d} + \bar{c} + s) \cdot \prod_{i=1}^{n}(1-P) \cdot 1 - \beta(s) \sum_{i=1}^{n} P_i \delta_i(s) \prod_{j=1}^{i-1}(1-P_j) \cdot (\bar{d} + s)}{U(s)} = V(s) \]

where

\[ \bar{d} = \sum_{i=1}^{n} l_{i1} P_i, \quad \bar{c} = \sum_{i=1}^{n} r_{i1} P_i \] – mathematical expectations of recovery intensities and implementation by the intruder of the spacecraft, respectively;

\[ k = \frac{d}{d + c} \] – the likelihood of network elements recovering during a packet retransmission and another spacecraft implementation. To obtain the mathematical expectation and the distribution time distribution function, it is necessary to calculate the value of the derivatives of the polynomials of the numerator and denominator (3) at the point \( s = 0 \):

\[ V'(s) = k \prod_{i=1}^{n}(1-P) \left[ \beta'(s)(\bar{d} + \bar{c} + s) + \beta(s)(\bar{d} + \bar{c}) \right] \]

\[ V'(0) = k(\bar{d} + \bar{c})(1 - \beta) \cdot \prod_{i=1}^{n}(1-P) \] ;

\[ U'(s) = d \left[ 1 - \beta(s) \sum_{i=1}^{n} P_i \delta_i(s) \prod_{j=1}^{i-1}(1-P_j) \right] + \]

\[ + (\bar{d} + s) \left[ -\beta'(s) \sum_{i=1}^{n} P_i \delta_i(s) \prod_{j=1}^{i-1}(1-P_j) - \beta(s) \sum_{i=1}^{n} P_i' \delta_i(s) \prod_{j=1}^{i-1}(1-P_j) \right] \]

\[ U'(0) = d \left[ 1 - (1 - \beta) \sum_{i=1}^{n} P_i \prod_{j=1}^{i-1}(1-P_j) + \sum_{i=1}^{n} P_i' \prod_{j=1}^{i-1}(1-P_j) \right] \]

The mathematical expectation of the packet transmission time in the spacecraft conditions is defined as

\[ \bar{T}_h = \frac{-d}{ds} \left. \frac{h_n(s)}{h_n(0)} \right|_{s=0} \] .

Replacing

\[ \bar{P} = \prod_{i=1}^{n}(1-P_i); \quad \bar{E} = 1 - \sum_{i=1}^{n} P_i \prod_{j=1}^{i-1}(1-P_j) \] ,

we obtain from equation (6) in the form:

\[ \bar{T}_h = \frac{\bar{P}}{(1-\bar{E})^2} \left[ \sum_{i=1}^{n} P_i \delta_i \cdot \prod_{j=1}^{i-1}(1-P_j) + \bar{\beta} \right] .\]
Accordingly, the variance is determined by the formula [9, 10]

\[
D[t_n] = h_i - h_i^2 = \frac{d^2}{ds^2} \left[ \frac{h_n(s)}{h_n(0)} \right]_{s=0} - \frac{d}{ds} \left[ \frac{h_n(s)}{h_n(0)} \right]_{s=0}^2.
\]

(8)

It is necessary to carry out the reverse process to obtain the function of distribution of packet transmission time, which allows to calculate the original from its image [4, 6]. To demonstrate the described method for determining the distribution function of time for bringing data packets in the OTC-IP network, we consider the following particular problem.

**Statement of a particular problem:** we assume that the intruder’s goal is to block the equipment of the corresponding nodes of the OTC-IP network, to which the intruder performs spacecraft and disrupts their operability with probability and, accordingly. If the operation of the nodes is not broken, then the packet received at the input of the communication channel will be transmitted in a time determined by the technical transmission rate and the amount of data transmitted, i.e. \( t_{\text{per}} = \frac{V}{R} \).

When transmitting packets of arbitrary volume, it is a random variable distributed according to the law \( B(t) \). In the event of a malfunction, the network is restored in a random time \( t_{\text{es}} \), \( i = 1, \ldots, n \) with FR recovery time \( \Delta_i(t) \), and the received data packet is retransmit.

The incoming stream of data packets is rare, and Cyberattack spacecraft are possible both during packet transmission and in pauses between them. The number of places to wait for the transfer is considered unlimited. It is required to determine the mathematical expectation \( h(T) \) and the time distribution function of the successful \( F(t) \) transmission of data packets in the spacecraft conditions implemented by the intruder.

Decision: Imagine the process of functioning of the Operational and technological communication -IP network when an intruder realizes two types of spacecraft in the form of a stochastic network (Fig. 2). Let’s pretend that \( \delta_i(t) = 1 - e^{\delta_i} \);

\[
\begin{align*}
\beta(s) & \quad \delta_2(s) \\
\lambda_{\text{es}} & \quad 1 - P_1 & \quad P_2 \\
\beta(s) & \quad \delta_1(s) & \quad P_1 & \quad \beta(s) \\
\end{align*}
\]

Fig. 2. *The stochastic network of the Operational and technological communication-IP network functioning process upon sale by an intruder of two types of spacecraft Cyberattack.*

Using the Mason equation for closed graphs, we compose the equivalent function of the stochastic network:

\[
h(s) = \frac{(1 - P_1)(1 - P_2)\beta(s)k\left(\hat{d} + s + c\right)}{[1 - P_2\delta_2(s)\beta(s) - P_2\delta_2(s)\beta(s)(1 - P_2)](\hat{d} + s)},
\]

(9)
where \( h_b = \frac{b(P_1-1)(P_2-1)(\bar{c}+\bar{d})}{d(P_1+P_2-P_1P_2-b)} \); \( \bar{d} = d_1P_1 + d_2P_2 \); \( \bar{c} = \frac{P_1}{t_{p1}} + \frac{P_2}{t_{p2}} \); \( k = \frac{d}{\bar{d} + c} ; d_1 = \frac{1}{t_{c1}} ; d_2 = \frac{1}{t_{c2}} ; b = \frac{1}{t_n} \).

We represent the denominator of the equivalent function in canonical form, that is, this allows us to move on to the Heaviside expansion for the case of simple poles \([6, 8]\):

\[
h(s) = \sum_{i=1}^{4} \left( \frac{(d + c + s)(d_i + s)(d_i + s)(1 - P_i)(1 - P_i)}{4(s_i)^3 + 3(s_i)^2 \cdot A + 2s_i \cdot B + C} \right),
\]

where: \( A = b + \bar{d} + d_1 + d_2 \); \( B = b\bar{d} - P_dP_2 - P_1d_2 - P_2d_1 + bd_1 + bd_2 - d_1^2 + d_2^2 + d_1d_2 + d_1d_2 + P_1P_2d_2 \);

\( C = b\bar{d}d_1 - P_2\bar{d}d_2 - P_1d_1d_2 - P_2d_1d_2 - P_1\bar{d}d_2 + b\bar{d}d_2 + bd_2d_2 + d_1d_2 + P_1P_2d_2 + P_1P_2d_2 \).

Average time \( \bar{T}_h \) successful packet transmission equals:

\[
\bar{T}_h = \frac{k(P_1-1)(P_2-1)\left(\bar{d}^2d_2d_2 - P_2^2\bar{d}^2d_2^2 + b\bar{d}d_1d_2 + \bar{c}d_1d_2 + P_1\bar{d}^2d_2 + P_2\bar{d}^2d_1 - b\bar{d}^2d_2d_2\left(P_2 - P_1 - 1\right)^2 + P_2^2b\bar{d}d_2 + P_2b\bar{d}d_1d_2 - P_1b\bar{d}d_1d_2 - P_2b\bar{d}d_2 + P_2b\bar{d}d_2 \right)}{h(0)}.
\]

The probability density function of the transmission time probability

\[
h(t) = \sum_{i=0}^{3} \left[ \frac{(d + s_i + \bar{c})(d_i + s_i)(d_i + s_i)(1 - P_i)b_k}{4(s_i)^3 + 3(s_i)^2 \cdot A + 2s_i \cdot B + C} \right],
\]

and the integral function of the probability distribution density of the transmission time

\[
H(t) = \sum_{i=0}^{3} \left[ \frac{(d + s_i + \bar{c})(d_i + s_i)(d_i + s_i)(1 - P_i)b_k}{4(s_i)^3 + 3(s_i)^2 \cdot A + 2s_i \cdot B + C} \right](1 - e^{s_i t}).
\]

According to formulas (11–13), calculations were performed, the results of which are presented as a family of distribution functions in Fig. 3.

During the calculations, it was assumed that:

- average data packet transmission time with volume \( V = 10 \text{ mbit} \) between the corresponding nodes is equal to 1s;
- the average recovery time of the operational and technological communication-IP network after successful implementation by the intruder cyberattacks of the spacecraft varies within \( t_b1 = 3 \ldots 5 \text{ S} \) and \( t_b2 = 2,5 \ldots 4 \text{ S} \) respectively;
- average implementation time by the intruder cyberattacks equally \( t_{pb1} = 50 \text{ S} \) and \( t_{pb2} = 100 \text{ S} \);
- average implementation time by the intruder cyberattacks equally \( t_{pb1} = 50 \text{ S} \) and \( t_{pb2} = 100 \text{ S} \);
- the probability of successful implementation by the intruder cyberattacks of the spacecraft takes values in the range of 0.08–0.8.

In terms of implementation cyberattacks the role of the effectiveness of the mechanism for organizing information security networks operational and technological communication based on IP-technologies, characterizing the working time in the model after cyberattacks.

So, for example, if the offender is likely to succeed cyberattacks \( P_i = 0.5 \) a slight increase in the recovery time leads to a sharp increase in the average transmission time of packets \([7, 8]\):

- the time of successful transmission of information in the network depends on the ability of the intruder to render cyberattacks the spacecraft to the network elements.
So, for example, if the intruder is able to successfully implement the impact with a probability no worse $P_i = 0.7$, we should expect an increase in the average time for bringing information on the network by more than five times;

- the law of distribution of time of successful transmission of a packet in the general case is hyperexponential and, as shown in [7–9], can be approximated with sufficient accuracy by an incomplete Gamma function. Calculations show that the resulting distribution has significant right-hand asymmetry (asymmetry coefficient $K_1 = 1.9$) is insignificantly peaked (excess coefficient $E_4 = 5.7$), and the stream of successfully transmitted packets is heterogeneous (coefficient of variation $K_2 = 1.3$) [5].

Expect packet flow parameter of successfully transmitted packets $\lambda(t) = \frac{f(t)}{1 - F(t)}$

is unstable in time and when:

$$\lim_{t \to \infty} \lambda(t) = \lim_{t \to \infty} \frac{\sum_{k=1}^{n} V(s_k) e^{s_k t}}{1 - (\sum_{k=1}^{n} U'(s_k) S_k^{-1} (1 - e^{s_k t}))} \leq \frac{1}{T_h};$$

(14)

that is, the intensity of successful packet transmission does not exceed the intensity defined as the reciprocal of the average time of successful packet transmission $\frac{1}{T_h}$.

**Conclusion**

Thus, the stream of successfully transmitted packets is not the simplest, in connection with which the task of assessing the time of information transfer in the networks of operational-technological communication with IP-telephony is relevant for the case when the incoming stream is not rare, but corresponds to the actual interaction of the corresponding pairs in the network, the developed model ensures the receipt of results that do not contradict the logic, is sensitive to changes.
in input parameters and is operable; they are in good agreement with the data obtained using known models and allows you to determine the average time spent on the implementation of the selected type of computer attack.

References: