The mathematical model of monitoring information system with failure prediction

N R Storozhenko, A I Goleva, V I Potapov, E I Pastuhova, D A Tunkov, M L Ralovec and A R Fakhrutdinov
Omsk State Technical University, 11 Mira ave., Omsk, 644050, Russia
E-mail: frybkf07.93@mail.ru

Abstract. The article is based on the monitoring faults problem of information systems and contains the mathematical model description of the process for monitoring faulty parameters for network equipment, which takes into account the probability dependence of events on a time intervals, and offers a method of probabilistic forecasting of the state of network failure.

1. Introduction
The agile development of information systems in recent years has increased interest in the issues of reliability, security, efficient use of resources and rapid access to them. These problems are particularly acute in large computer systems of research centres, industrial enterprises and defence facilities. Such systems must respond to the requirements of fault-tolerance and availability for each registered user, because in total the performance of the organization depends on the operation of networks and information systems.

Thus, modern information systems and networks need constant control and monitoring, as the work of production shops, designers and technologists is impossible without a well-functioning communication system, instant data exchange, control systems, diagnostics and information security.

1.1. Research in the field of networks monitoring
The problem of ensuring the reliability, security and availability of network resources of any organization is now quite acute.

Due to the increasing complexity, scale and intensive development of the network, it becomes difficult to monitor and predict possible deviations in the parameters of the server and switching equipment. However, it is necessary to constantly carry out monitoring and diagnostic equipment, and in the case of detection of faults, report it to the administrator. These tasks can be attributed to a variety of the tasks of network management.

Monitoring of information systems it a functions of everlasting checking and verification of the technical condition of network objects in order to detect slowdowns, problems, failures and anomalies in their work and warn network administrators.

Monitoring systems provide automation the inspection of equipment and the collection of statistics on the network functioning, speed up the detection of problems and help minimize the time of their elimination.

Unlike system of detection and prevention of intrusion, monitoring not only involves security management, identifying and preventing potentially dangerous activities of unauthorized users, but also provides the operation of the subsystems of management network configuration, checking and
analysis of performance and reliability of network objects, error handling, and troubleshooting management.

Control problems and diagnostics of technical systems are considered by many authors [1-17 так нельзя делать, лучше тогда расписать, например в [1-2 такие то подходы, в 3-5 такие то и то].

According to the results of the literature review, the following can be noted now.

For the time being, one of the main and priority direction of activity in the field of information technology is the creation and application of systems for monitoring the state and behavior of network segments for the purpose of timely identify and prevent the influence of destructive factors.

So, reviewed works include either the typical methods of evaluating the basic parameters of reliability and performance of technical systems [1-3], or contain a enough consuming and hard mathematical methods for the description of specific systems and networks [4-9], or describe the need for the application systems of monitoring, control and diagnostics for data networks, as well as its advantages and principles of working [10-17 тоже разбег большой, так нельзя].

However, this works don't contain mathematical description of the systems of network monitoring and diagnostics, also don't take into account the functions performed by the monitoring system in the process of verification.

For this reason, this article is based on an attempt to eliminate these shortcomings by modeling the procedures for detecting anomalies and predicting the state of network failure. And that in turn allows to improve the adequacy of the model.

Before to start modeling the monitoring of an information system, need to consider in detail the processes associated with it.

2. Task definitions

Due to the implementation of the model for ease and evidence, it is advisable to present a network monitoring in the form as a complex process includes two main procedures — the procedure of collecting initial parameters and data on the operation of nodes in the network: statistics on a circulating in the network packets for various network protocols, the state of the ports of communication devices, etc. Then the procedure of analysis of the obtained at the first stage parameters is performed, and comparison of it with the specified reference values to make a decision on the normal operation or detection of the causes of slow or unreliable operation of the network elements.

In the structure of management a complex system — monitoring solves the following tasks:
1) checking of operability and analysis states of diagnostic object;
2) searching for defective items and causes of failure;
3) forecasting the technical state of the diagnostic object.

Network monitoring can be performed using a variety of software or hardware solutions. The choice of methods and objects of monitoring in the network depends on several factors — the configuration of the network, switching equipment and servers, existing network services, etc.

In this article, at modeling the monitoring process, not any specific solution but a generic and typical principle of functioning of modern monitoring systems was considered, for the possibility of universal application of designed model.

In general case, the monitoring objects include the following parameters:
- physical availability of equipment;
- state of equipment, services and network services;
- parameters of network operation: processor load levels, free disk space, performance, response time, memory, rapid increase in network traffic;
- logs and error reports (helps identify frequent or systematic failures).

To determine the degree of detection of various anomalies, faults and failures by a network monitoring system in this work, we propose the formulation and solution of the problem of mathematical modeling of the process of monitoring the parameters of the information system equipment.
3. Description of the task and mathematical model

The events in information systems and networks are random, therefore, probabilistic mathematical models of Queuing theory are the most suitable for their research and study. In this case, it is proposed to use the theory of Markov chains.

At the initial stage of modeling, it is necessary to determine the input data: as the states of the monitoring system it is proposed to consider the events associated with the detection of faults during the diagnosis and control of the equipment parameters tested by the monitoring system in the network.

Thus, we describe the possible states in the process of monitoring the parameters of network equipment:
- $S_0$ — no faults;
- $S_1$ — the problems of hardware;
- $S_2$ — the problems of RAM;
- $S_3$ — processor overload;
- $S_4$ — traffic overload;
- $S_5$ — the inaccessibility of the port;
- $S_6$ — physical unavailability of the device;
- $S_7$ — total network failure.

The described chain of events during network monitoring can be represented as a graph of states (figure 1).

![Figure 1. Graph of the detection of faulty settings in the monitoring process, where $S_i$ — is the state of the system, $\lambda_i$ — is the intensity of the $i$-th failure](image)

After determining the input parameters of the system, need to proceed to the mathematical description.

To build the model, we assume that the detection of any faults by described monitoring system is considered as a random process with a finite number of states. In this case, this model has the property of ordinairiness, because the events occur singly, not in groups of several at. Also described model doesn’t contain any aftereffects because for any two non-overlapping intervals of time, the number of events falling on one of them doesn’t depend on how many events fell on the other.
In this case, the probability of the $i$-th state is defined as the probability of finding the system in a state $S_i$, that is, the probability of detection by the monitoring system of the $i$-th faulty parameter in the network.

On the graph, each arrow corresponds to the intensity of the flow of events that takes the system from one state to another.

Monitoring, which involves constant operator control, is a system of orderly inquiry. The inquiry sequence is determined by the priority assigned by the administrator. The higher the priority of the parameter of network device, the higher the intensity of its inquiry. In this case, the intensity of the transitions is $\lambda_i$ — the intensity of the inquiry of the $i$-th parameter in the monitoring system.

Taking into account the above description of the monitoring system operation, it follows that monitoring system when performing a survey of network devices from the state $S_0$, in case of failure of any component, passes to the state of fault detection $S_i$ with intensity $\lambda_i$.

The graph is used to build a mathematical model of the monitoring process in the form of a system of equations (1):

\[
\begin{align*}
\frac{dp_0}{dt} &= -p_0(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6), \\
\frac{dp_1}{dt} &= p_0 \lambda_1 + p_1(\lambda_3 + \lambda_6 + \lambda_7), \\
\frac{dp_2}{dt} &= p_0 \lambda_2 + p_2(\lambda_2 + \lambda_5), \\
\frac{dp_3}{dt} &= p_0 \lambda_3 + p_3(\lambda_3 + \lambda_4 + \lambda_5), \\
\frac{dp_4}{dt} &= p_0 \lambda_4 - p_4(\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7), \\
\frac{dp_5}{dt} &= p_0 \lambda_5 + p_2 \lambda_5 + p_3 \lambda_5 + p_4 \lambda_5 - p_5 \lambda_6, \\
\frac{dp_6}{dt} &= p_0 \lambda_6 + p_1 \lambda_6 + p_2 \lambda_6 + p_3 \lambda_6 + p_4 \lambda_6 - p_5 \lambda_7, \\
\frac{dp_7}{dt} &= p_0 \lambda_7 + p_4 \lambda_7 + p_6 \lambda_7.
\end{align*}
\]

The solution of the system of differential equations (2) allows to track the dynamics of diagnosing faulty parameters in the process of network monitoring by tracking the probabilities at certain intervals of time observation.

If the probabilities of the state of the monitoring system in the limit steady-state mode are interesting, it is necessary to get a linear system of equations, equating the left parts of the differential equations to zero.

The scheme of the monitoring algorithm is shown in figure 2.
To modelling of the forecasting functions of the monitoring system, it is necessary to take into account the fact that the states in the next steps depend on the previous ones. Based on this, future states can be characterized by conditional probabilities (2):

\[ p(AB) = p(A) \cdot p(B | A), \]  

where \( p(AB) \) is the joint probability of events \( A \) and \( B \);
\( p(A) \) — probability of event \( A \);  
\( p(B | A) \) — probability of event \( B \) under the condition of occurrence events \( A \).

Then the probability of the state, taking into account the probabilities on the previous states, is determined by the formula:

\[ p(S_0S_1...S_n) = p(S_0) \cdot \prod_{j=1}^{n} p(S_j | S_0S_1...S_{j-1}), \]  

The process is \( n \)-connected, if the outcome of the test is mainly influenced by the results of \( n \) previous tests.

In our case, for the system with a graph (figure 1) \( S_0, S_1, ..., S_7, n=8 \).
If we consider that the results of previous tests have a great influence on the state of complete failure network in our case, then the equation is valid:

\[ p(S_1 \ldots S_n) = p(S_1) \cdot \prod_{j=2}^{n} p(S_j \mid S_1, S_2, \ldots, S_{j-1}), \] (4)

Thus, the obtained equation allows to implement statistical forecasting of the state of complete network failure in the monitoring process, using the data of previous failure states, it is makes it possible, in addition to modeling of the detection of faulty parameters (2), to mathematically describe the procedure for predicting of the monitoring system.

4. Conclusion
At present, the requirements for modern information systems as a medium of data transmission are constantly increasing for satisfactions of the increasing needs of modern organizations and enterprises and for ensuring the efficient and uninterrupted operation of various software and hardware. On this basis, control and diagnostics of information exchange means are of great importance.

For research and improvement of algorithms of monitoring, control and diagnostics of the equipment parameters of networks in this work the model describing process of network monitoring and fault detection is constructed on the basis of probabilistic methods.

In addition, the developed model allows to take into account the probabilistic prediction of the state of complete network failure with the help of probabilities of previous states.

Thus, the solution of the presented model will provide particular values of the probabilities of fault detection by the monitoring system, depending on the time of observation. The obtained values give a visual representation of the simulated processes of network monitoring.

Where appropriate, in the direction of further research, an algorithm (figure 2) and software implementation can be developed, to optimize the modeling process, and to implementation of the ability to control the behavior of the system in accordance with condition of changing the parameters.

5. References
[1] Ushakov I A 1985 Reliability of technical systems (Moscow: Radio and communication) p 608
[2] Ventzel E S 2018 Operations research: tasks, principles, methodology (Moscow: Justice) p 192
[3] Mozhaev A S 2003 Universal graphical-analytical method, algorithm and software module for the construction of monotonic and non-monotonic logical functions of system efficiency Proc. Int. Scientific. Schools (Saint-Petersburg: SUAI) pp 101-110
[4] Chervenchuk I V et al 2018 Performance characteristics describe the structure of descriptors Journal of Physics: Conference Series 1050 012017
[5] Potapov V I 2015 Model and numerical solving algorithm of counteraction problem for two restored after failure redundant engineering systems Journal of Automation and Information Sciences vol 47, No 8 pp 41–51
[6] Potapov V I et al 2016 Spectral analysis of retrospective data on power consumption 2016 Dynamics of Systems, Mechanisms and Machines (Dynamics) pp 1-4
[7] Potapov V I et al 2018 Numerically-analytical solution of problem gaming confrontation hardware-redundant dynamic system with the enemy operating in conditions of incomplete information about the behavior of participants in the game Journal of Physics: Conference Series 1050 012062
[8] Sandoval Y, Gallizo G and Curiel M 2012 Evaluation of monitoring tools for cloud computing environments Proc. Conf. on Informatica CLEI (Medellin) pp 1-10
[9] Ge J, Zhang B and Fang Y 2010 Research on the Resource Monitoring Model Under Cloud Computing Environment Web Information Systems and Mining Lecture Notes in Computer Science ed F L Wang, Z Gong, X Luo and J Lei (Springer Berlin Heidelberg) pp 111–8
[10] Wolters D, Gerth C and Engels G Visual 2017 Requirements Modeling for Cross-Device Systems Computer Science and Information Systems 14 pp 517–36
[11] Kufel L 2013 Security Event Monitoring in a Distributed Systems Environment *IEEE Security and Privacy* **11** (Washington: IEEE Computer Society) pp 36-43

[12] Fukatsu T and Hirafuji M 2005 Field monitoring using sensor-nodes with a web server *Journal of Robotics and Mechatronics* **17** pp 164–72

[13] Kufel L 2016 Tools for Distributed Systems Monitoring *Foundations of Computing and Decision Sciences* **41** (Poznan: University of Technology) pp 237–60

[14] Achilov R 2013 *Building secure enterprise networks* (Moscow: Science and technology) p 250

[15] Wilson E 2002 *Network Monitoring and Analysis. A Protocol Approach to Troubleshooting* (Moscow: Lori) p 364

[16] Averchenkov V I 2011 *Monitoring and system analysis of information on the Internet* M.: (Moscow: Flinta) p 160

[17] Lee S, Levanti K and Kim H S 2014 Network monitoring: Present and future *Computer Networks* **65** pp 84–98.