DEVELOPMENT OF A MATHEMATICAL MODEL OF THE FUNCTIONING OF ADAPTIVE ROUTING PROTOCOLS IN TELECOMMUNICATION NETWORKS WITH THE POSSIBILITY OF SELF-ORGANIZATION

Oleksii Nalapko[1]

[1]Central scientific-research Institute of Arming and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
aln.uax@gmail.com
ORCID: http://orcid.org/0000-0002-3515-2026

Nalapko, O. (2020). Development of a mathematical model of the functioning of adaptive routing protocols in telecommunication networks with the possibility of self-organization. ScienceRise, 4, 33–39. doi: 10.21303/2313-8416.2020.001388

ARTICLE INFO

Article history:
Received date 10.07.2020
Accepted date 05.08.2020
Published date 31.08.2020

Section:
Information Technology

DOI

10.21303/2313-8416.2020.001388

KEYWORDS

telecommunication network
network bandwidth
efficiency
routing
radio communication
mathematical model

ABSTRACT

The necessity of developing a mathematical model for the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize has been substantiated. The results of the study of the information transmission route choice in communication networks with the possibility of self-organization under the influence of deliberate interference and cyber-attacks are presented. New analytical dependencies have been obtained that allow calculating the influence of destabilizing factors on the efficiency of determining the route in the network.

Object of research: development of a mathematical model of the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize.

Investigated problem: taking into account additional destabilizing factors when choosing the information transmission route.

Main scientific results: when forming a route in a special-purpose network with the possibility of self-organization, the following are taken into account: battery charge, information transfer rate, the presence of cyber-attacks, the presence of deliberate interference, the reliability of the route and the time of packet delivery to the addressee. It has been established that the use of all parameters in the system allows to increase both the total operating time of a special-purpose network with the ability to self-organize as a whole, and an individual node. It is shown that the presence of a DoS attack in the network is identified by increasing the delay time for information transmission between network nodes.

Review of the practical use of research results: automated systems for various purposes.

Innovative technologies product: a technology for choosing the information transfer route, which can increase the efficiency of choosing the information transfer route, taking into account additional destabilizing factors.

Review of an innovative technological product: automated control systems, network controllers when choosing a route for information transmission.

1. Introduction

Existing and prospective special-purpose information transmission systems should serve a large number of stationary and mobile users, arbitrarily located within a certain territory. As a result, today there are promising systems that are able to organize wireless networks with the ability to self-organize. In wireless networks with the ability to self-organize, there is no need for centralized network management, each node is peer.

A network with the ability to self-organize provides two options for data transmission: direct communication between a node, transfers information and a node, receives it, or transit information transfer between them. In such systems, multicast access is provided in a common frequency channel, in which the nodes transmit and receive information independently of each other. The main mechanism for improving the efficiency of wireless networks with the ability to self-organize is routing protocols.

For a substantiated analysis of dynamic routing protocols in special-purpose wireless networks, it is necessary to solve the problem of assessing a telecommunication network operating under the conditions provided for by the corresponding model.

1. 1. The object of research

The object of research is a wireless network with the ability to self-organize, functioning under the influence of interference and cyber-attacks.

1. 2. Problem description

Research on modeling the processes of functioning of complex technical systems in the conditions of opposition of organizational and technical systems was carried out in works [1, 2]. The works [3, 4] are devoted to the problems of streaming models of buggy routing in telecommunication networks. The works [5, 6] are devoted to the development of a fault-tolerant routing model. The study of models with multicriteria choice is disclosed in [7].

The general problems of modeling telecommunication networks are highlighted in studies [8, 9].

In [10], the authors introduce a quantitative parameter of the stability of communication in a special wireless network under the condition of Ornstein-Uhlenbeck mobility.

Also, at present, a lot of work is devoted to improving routing models, to support QoS (Quality of Service) [11].

In [12], a model is proposed where, in routing modeled on the global satellite network, Spase X proposes the use of routes based on snapshots of network connectivity.

1. 3. Proposed solution the problem

However, the issues of modeling the process of functioning of the packet flow transmission system in the presence of information attacks and the impact of electronic suppression means have not been considered in the known literature.

The aim of research is to develop a mathematical model for the functioning of the dynamic routing protocol in special-purpose wireless networks with the ability to self-organize. The model being developed should take into account many parameters of both the physical and network layer of the OSI model, functioning in conditions of electronic suppression and in conditions of DoS attacks.

2. Materials and methods

For a scientific task, the author used the basic provisions of the theory of queuing, cyber security, noise immunity, electronic protection, multi-parameter optimization and routing.

3. Research results

To construct a radio communication model for mobile nodes, let's introduce the following designations for input parameters, restrictions and assumptions.

Parameters of a mobile radio network: the network is represented by a directed graph $G = (V, E)$, where $V = \{v_i\}$, $i = \overline{1, N}$ – a set of randomly located nodes, each of which has an identification number, and $E = \{e_l\}$, $l = \overline{1, L}$ – a set of radio channels between mobile nodes (symmetric, half-duplex). N – the total number of nodes in the mobile radio network.

Parameters of a mobile radio network node: each node is equipped with a battery, the capacity of which at each moment of time t can't exceed a certain maximum value $e_i^b(t) \le e_{i\max}^b$. The nodes of the mobile radio network have the ability to change the transmitter power depending on the situation $p_i(t) \le p_{i\max}$. Also, the receiver of each mobile node is characterized by a real sensitivity p_{rs}, which determines the minimum signal strength $p_{\text{ñ}}$ that can be received by the node.

Initial data for setting the problem. The network is represented as a set of mobile radio networks of various levels $l = \overline{0, 3}$ (l=0 – wireless sensor networks; l=1 – combat radio networks; l=2 – a network of mobile base stations; l=3 – a network of unmanned aerial vehicles), each of which can be represented in the form of a graph $G^l = (V^l, E^l)$ with many vertices $V^l = \{v_i\}$ and set of edges. $E^l = \{(i, j)\}$, $i, j = \overline{1, N}$, N – the number of nodes in the MR. Next, let's consider mobile nodes and the channels through which they are connected within the MR of the same level.

Parameters of node v_i: $e_{\varsigma_i}(t)$ – capacity of the node battery; $r_i(t)$=[0…$r_{\max}$] – data transmission rate $p_i(t) \le p_{\max}$ – transmission power of the i-th node; $g_i^{\hat{i}}(t) = \left[0...g_{i\max}^{\hat{i}}\right]$ – input load from flows of ξ-type at time t; (t)=[0…$\omega_{\max}$] – movement speed. The building of a route between the sender and the addressee is carried out using the DSR protocol, which provides the sending node

with information about the neighboring nodes v_k located at a distance of one or two relay intervals. Types of cyber-attacks – DoS.

Radio channel parameters $(i, j) \in E$: bandwidth $s_{ij}(t) \le s_{ij\max}$; t_d^{ξ} – delay time of the ξ-*th* traffic type; $\xi = \overline{1, 3}$ – traffic type (data, speech, video). Radio communication between network nodes is supported by one of the link layer protocols (random, with carrier sense, etc.). Types of interference – noise in the part of the band, noise barrage.

Assumptions: according to the organizational structure of the units in the tactical control level, a small MR zone, in which constant radio communication between the nodes should be ensured, there are many squad or platoon nodes, that is, consider that $N \le 10$. Within a zone (branch), the connection between mobile nodes occurs either directly or by building routes using a minimum number of relays (usually up to three). Taking into account the fact that each node has information about its neighboring nodes, as well as the decentralized principle of MR control and the dynamic nature of their functioning (frequent changes in MR topology caused by the mobility of all nodes), it can be concluded that the issue of radio communication should be considered separately between each a pair of nodes forming the *h*_th interval, and not along the entire transmission path m_{ab}.

For simplicity, let's denote the set of parameters that determine the state of the node and MR as $X = \{x_b(t)\}$, $b = \overline{1, B}$.

An intelligent control system operates as part of each mobile node (**Fig. 1**).

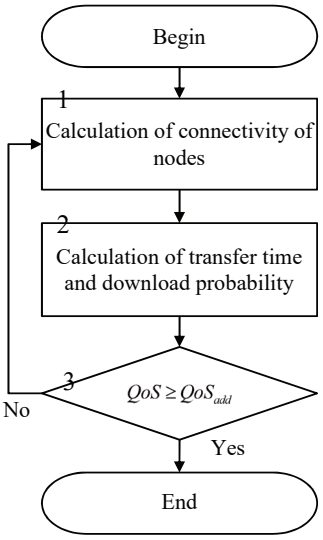

Fig. 1. Algorithm of the mathematical model of the functioning of adaptive routing protocols

Taking into account the fact that each node has information about neighboring nodes, as well as the decentralized principle of mobile wireless network management and the dynamic nature of their functioning (frequent changes in the topology of the mobile wireless network caused by the mobility of nodes), so we can conclude that the issue of radio communication It is advisable to consider the differences separately between each pair of nodes forming the *h*-th interval, and not along the entire transmission route m_{ab}.

The set of parameters that determine the state of a node and a mobile wireless network are denoted by $X = \{x_b(t)\}$, $b = \overline{1, B}$.

It is necessary: to develop a mathematical model for ensuring radio communication of the nodes of a mobile network $X(t) = \{x_b(t)\}$, $b = \overline{1, B}$, which, taking into account the current situation in a mobile wireless network (or its zone), will make it possible to make such management decisions at the physical $W_p(t)$ and $W_n(t)$ network levels of the OSI model that will meet the system objective function

$$W^*(t) = \arg \underset{W_p(t), W_N(t) \in \Omega}{opt} C(t)(X(t), W_p(t), W_n(t)), \ \forall \ Z_{ij} = 1, \ i, j \in N, i \ne j, \tag{1}$$

where $C(t)$ – the control goal at the moment of time,

$$C(t) = \{P(t);\ M(t)\}; \tag{2}$$

$$X(t) = \left\{ p_{ij}(t),\ p_{\text{ñ}}(t),\ p_{rf_i}, BER_{\xi_{ij}}(t), m_{ab},\ e_i^b(t),\ \xi(t), \Pi_{\xi ij}, \Upsilon_{ij}(t), P_{speed}(t) \right\}, \tag{3}$$

$X(t)$ – set of node states at a time; Z_{ij} – radio communication between nodes i and j.

This will minimize the energy consumption of mobile nodes and ensure the specified quality of service for the ξ-th type of traffic on the transmission route m_{ab} while meeting the resource constraints

$$\Omega = \{ p_{ij} \le p_{i\max}, p_{c_i}(t) \ge p_{rf_i},\ BER_{\xi_{ij}}(t) \le BER_{add\,\xi},\ e_{ij\ \min}^b < e_i^b \le e_{i\ \max}^b \}, \tag{4}$$

where $W_p(t)$ – set of control decisions of the nodal CS of the physical OSI model for choosing the optimal values of the transmission power $P(t) = \{p_{ij}(t)\}$, $i, j = \overline{1, N}$ in the radio channel ij; $W_n(t)$ – variety of control decisions at the network layer of the OSI model for choosing the optimal transmission routes $M(t) = \{m_{ab}(t)\}$, $a, b = \overline{1, N}$ between the sender v_a and destination nodes v_b or intermediate nodes v_i and v_j along the route m_{ab}; $e_{ij\ \min}^b$ – the minimum allowable battery capacity required to support the transmission of streaming traffic of the volume determined within the current connection (for bursty/random traffic, such as language or video in real time, is determined by the minimum allowable battery capacity $e_{ij\ \min}^b$ required for the operation of the node); $\Pi_{\xi ij}$ – priority of the ξ-st traffic type in the channel ij.

According to expressions (1)–(5), at the physical level of the OSI model, the condition for the successful transfer of information between each pair of nodes i – on the transmission route m_{ab} (or two nodes a and b) can be written as a system:

$$Z_{ij} = \begin{cases} 1, \text{ if } \hat{A}ER_{add\,\xi} - BER_{\xi_{ij}}(t) > 0; \\ 0, \text{ otherwise}, \end{cases} \tag{5}$$

where Z_{ij} – radio communication between nodes i and j $(i, j \in N, i \ne j)$; N – the total number of nodes of the mobile wireless network or its zone; $BER_{\xi_{ij}}(t)$ – a certain value of the error probability for the ξ-th traffic type at the moment of time t; $\hat{A}ER_{add\,\xi}$ – admissible value of the error probability for the ξ-th type of traffic.

As noted earlier, in the absence of a direct line of sight between the sender and the addressee, radio communication can be ensured by building transmission routes between them. Taking into account the fact that when transmitting information to a route that consists of h, $h = \overline{1, N-1}$ intervals (retransmission), the number of uncorrected errors will be added at each interval, we rewrite expression (5) in the following form:

$$Z_{ij} = \begin{cases} 1, \text{ if } \hat{A}ER_{add\,\xi} - \sum_{h=1}^{H} BER_{\xi}^h(t) > 0; \\ 0, \text{ otherwise}, \end{cases} \tag{6}$$

where $BER_{\xi}^h(t)$, $h = \overline{1, H}$ – certain value of the error probability for the ξ-th type of traffic at the time t between two nodes on the transmission route, which correspond to the h-th relay interval.

In the general case, physically, the interaction between two nodes in the process of transferring information can be described by the following system of equations:

$$\begin{cases} BER_{\xi ij}(t) = f\left(p_{ij}(t), BER_{\xi ij}(t-1)\right), \\ p_{ij}(t) = g\left(w_i(t), p_{ij}(t-1)\right), \end{cases} \tag{7}$$

where $p_{ij}(t)$, $p_{ij}(t-1) \in P(t)$ – power of the transmitter node at the current (t) and previous $(t-1)$ moments of time, respectively; $BER_{\xi ij}(t)$ and $BER_{\xi ij}(t-1)$ – the value of the error probability for the ξ-th traffic type at the moments of time (t) and $(t-1)$, respectively, determined by the receiver node; $w_i(t) \in W_p(t)$ – control decision of the node i on the choice of the required value of the transmitter power.

A model of the process of transmitting a stream of packets in conditions of cyberattacks, in which the time for transmitting packets from node *i* to node *j* for path *m* can be found using the following expression:

$$t_m = \sum_{n=1}^{N_m} t_{n,m}^{\text{tr.}} + \sum_{n=1}^{N_m} t_{n,m}^{\text{s.}}, \tag{8}$$

where N_m – the number of radio network nodes in the *m*-th path; $t_{n,m}^{\text{tr.}}$ – transmission time of packets through communication channels adjacent to the *n*-th node of the *m*-th path; $t_{n,m}^{\text{s.}}$ – service duration of the packet stream by the *n*-th node of the *m*-th path.

The time a node serves packets consists of the time the packet waits in the queue and the time the packet is processed by the node. If the packet processing time is fixed and usually small (from a few microseconds to several tens of microseconds), then the waiting time for a packet in the queue fluctuates within a very wide range and is, as a rule, a random value. If we accept as an assumption that the node is a single-channel queuing system with waiting, and the input stream is a Poisson stream, then the probability density of the packet servicing time by the n-th node will be described by the exponential law:

$$f_{\text{s}_n}(t) = \beta_{\text{s.}} \cdot e^{\beta_{\text{s.}} \cdot t}, \tag{9}$$

where β_s – intensity of the packet service by the node, taking into account the time of its processing and the waiting time of the packet in the queue; the parameter β_s is calculated as follows:

$$\beta_s = \mu \cdot (1-\rho), \text{ at } \rho = \frac{\lambda}{\mu}, \text{ so } \beta_{\text{s}} = \mu - \lambda, \tag{10}$$

where λ – intensity of the packet flow at the input of the node relays the packets; μ – intensity of the packet flow processing by the node by the packet relay.

To determine the distribution density of the probability of packet transmission time from node *i* to node *j* for the *m*-th path $f_m(t)$, it is necessary to convolve the distribution densities $f_{m,\text{s}_n}(t)$, at $n = [1; N_m]$ for all nodes of the *m*-th path:

$$f_m(t) = f_{m,\text{s}_1}(t) \cdot f_{m,\text{s}_2}(t) \ldots \cdot f_{m,\text{s}_n}(t), \tag{11}$$

where the convolution of two distribution densities, for example $f_{m,\text{s}_1}(t)$ and $f_{m,\text{s}_2}(t)$ is determined by the expression:

$$f_{m,\text{s}_{1,2}} = \int_{-\infty}^{+\infty} f_{m,\text{s}_1}(\tau) \cdot f_{m,\text{s}_2}(t-\tau)\text{d}t. \tag{12}$$

In the case when the number of nodes in the path is three or more, the problem of convolution of the distribution density $f_{m,\text{s}_n}(t)$ is a laborious task.

If to accept the assumption that the random servicing of packet streams by nodes retransmits the telecommunication network packets independent values, and the packet delay time on the path is determined by the sum of the packet stream servicing time by each node, retransmits, then the probability distribution of the packet stream transmission time from node *i* to node *j* can be describe the Gamma distribution. In this case, the distribution density $f_m(t)$ is determined by the expression:

$$f_m(t) = \frac{\beta_{\text{s}}^a}{\tilde{A}(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\beta_s \cdot t}, \tag{13}$$

where $\tilde{A}(\alpha)$ – the second-order Euler function.

4. Discussion of the results on the development of a mathematical model

A mathematical model of the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize is proposed.

The main advantages of the proposed model are:

– unambiguity of the obtained estimate of the channel state;

– wide scope of use (radio communication and routing systems);

– ability to adapt to the signaling environment in the channel;

– greater accuracy of channel state estimation;

– possibility of synthesizing the optimal structure of radio communications and network devices.

The advantages of this model are due to the fact that a greater number of destabilizing factors are taken into account than the known ones. The model takes into account in the complex intentional interference of an additive and multiplicative nature, destabilizing factors caused by the presence of cyber-attacks.

The disadvantages of the proposed mathematical model should be considered a large computational complexity compared to simpler mathematical models. This is due to the calculation of a larger number of channel state indicators.

The specified mathematical model is advisable to use in radio stations with programmable architecture, it functions under conditions of active electronic suppression, automated control systems and network devices

The specified complex mathematical model will allow:

– dentify the structure of the interference, its type and the law of setting;

– assess the state of the channel;

– use effective signal-code structures to ensure channel noise immunity;

– ensure efficient use of the radio frequency resource of programmable radio communications;

– increase the speed of evaluation of communication channels;

– develop measures aimed at increasing the noise immunity.

It is advisable to use the mathematical model proposed in the work in the development of software for modules (blocks) for evaluating promising radio communications, based on the interfaces of the open architecture of the SCA 2.2 version.

The directions for further research should be considered the development of a methodology for choosing a network topology, taking into account the influence of electronic suppression.

5. Conclusions

1. The development of a mathematical model of the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize.

The difference of the proposed model is as follows:

– allows to determine the factors influencing the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize at the physical and network levels of the OSI model;

– takes into account the effect of electronic suppression on the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize at the physical and network levels of the OSI model;

– takes into account the influence of cyber-attacks (DoS attacks in the network) on the functioning of adaptive routing protocols in telecommunication networks with the ability to self-organize at the physical and network levels of the OSI model.

2. Research results can be used in the development of automated control systems in special-purpose wireless networks with the ability to self-organize, operating in conditions of high dynamism of nodes, as well as automated control systems for robotic complexes for various purposes.

References

[1] Kozirackii, Iu. L., Budnikov, S. A., Ostrovskii, D. B. (2011). Model processa vozniknoveniia i protekaniia 1 konflikta informacionnykh sredstv raznykh vidov. Radiotekhnika, 8, 6–11.

[2] Kozirackii, Iu. L., Parinov, M. L., Petrenkov, S. V. (2011). Metodicheskie osnovi formirovaniia modeli konflikta. Telekommunikacii, 4, 2–7.

[3] Nalapko, O., Shyshatskyi, A. (2018). Analysis of technical characteristics of the network with possibility to self-organization. Advanced Information Systems, 2 (4), 78–86. doi: http://doi.org/10.20998/2522-9052.2018.4.14

[4] Shyshatskyi, A. V., Bashkyrov, O. M., Kostyna, O. M. (2015). Rozvytok intehrovanykh system zviazku ta peredachi danykh dlia potreb Zbroinykh Syl. Ozbroiennia ta viiskova tekhnika, 1 (5), 35–40.

[5] Sova, O. Ya. (2015). An intellectual model of the mobile nodes radio connectivity in the MANET. Systems of Arms and Military Equipment, 2 (42), 134–151.

[6] Lemeshko, A. V., Vavenko, T. V. (2012). Usovershenstvovanie potokovoi modeli mnogoputevoi marshrutizacii na osnove balansirovki zagruzki. Problemy telekommunikacii, 1 (6), 12–29.

[7] Sterin, V. L., Vavenko, T. V., Eferov, D. M. (2013). Marshrutizaciia s balansirovkoi nagruzki po dline ocheredi na uzlakh telekommunikacionnoi seti. Visnik NTU «KHPI». Seriia: Novi rishennia v suchasnikh tekhnologiiakh, 1 (977), 45–49.

[8] Lemeshko, A. V., Kozlova, E. V., Romaniuk, A. A. (2013). Matematycheskaia model otkazoustoichyvoi marshrutyzatsyy, predstavlennaia alhebraycheskym uravnenyiamy sostoianyia mpls-sety. Systemy obrobky informatsii, 2 (109), 217–220.

[9] Marino, P. P. (2013). Optimization of computer networks: modeling and algorithms: a hands-on approach. John Wiley & Sons, Ltd, 15–22.

[10] Mitsuo, G., Cheng, R., Lin, L. (2008). Network Models and Optimization Multiobjective Genetic Algorithm Approach. Springer-Verlag London Limited, 229–289. doi: http://doi.org/10.1007/978-1-84800-181-7

[11] Kuchuk, N., Mohammed, A. S., Shyshatskyi, A., Nalapko, O. (2019). The method of improving the efficiency of routes selection in networks of connection with the possibility of self-organization. International Journal of Advanced Trends in Computer Science and Engineering, 8 (1), 1–6.

[12] Salnyk, S. V., Salnyk, V. V., Sova, O. Y., Stempkovska, Y. O. (2016). A Model of intrusion in mobile radio networks class MANET. Scientific Works of Kharkiv National Air Force University, 1 (46), 79–84.