UDC 004.056
DOI: 10.15587/1729-4061.2016.73315

A MODEL DEVELOPED FOR TEACHING AN ADAPTIVE SYSTEM OF RECOGNISING CYBERATTACKS AMONG NON-UNIFORM QUERIES IN INFORMATION SYSTEMS

V. Lakhno
Doctor of Technical Science, Associate Professor
Department of Managing Information Security*
E-mail: lva964@gmail.com
H. Mohylnyi
Candidate of Technical Science, Associate Professor**
E-mail: g.mogilniy@gmail.com
V. Donchenko
Assistant**
E-mail: donchenko79@mail.ru
O. Smahina
Candidate of Pedagogic Sciences, Senior Lecturer**
E-mail: smagina1804@gmail.com
M. Pyroh
Lecturer
Department of Information Systems and
Mathematical Sciences*
E-mail: mykola.pyroh@bigmir.net
*European University
Academician Vernadskiy blvd., 16B, Kyiv, Ukraine, 03115
**Department of Information Technologies and Systems
Luhansk Taras Shevchenko National University
Gogol Square, 1, Starobilsk, Luhansk Region, Ukraine, 92703

Запропоновано математичну модель для модуля системи інтелектуального розпізнавання кібератак для неоднорідних потоків запитів та мережних класів кібератак. Модель враховує неоднорідні вхідні потоки запитів та можливість зміни нападниками інтенсивності запитів у інформаційних системах, що дозволяє здійснювати вибір способів протидії та нейтралізації наслідків від їхнього впливу, аналізувати більш складні види кібератак. За допомогою імітаційних моделей, створених у MatLAB та Simulink, досліджено динаміку зміни станів підсистеми блокування запитів у процесі розпізнавання кібератак у критично важливих комп'ютерних системах

Ключові слова: розпізнавання кібератак, інтелектуальні системи, шаблон кібератаки, неоднорідні потоки запитів

Предложена математическая модель для модуля системы интеллектуального распознавания кибератак для неоднородных потоков запросов и сетевых классов кибератак. Модель учитывает неоднородные входные потоки запросов и возможность изменения нападающими интенсивности запросов в информационных системах, позволяет осуществлять выбор способов противодействия и нейтрализации последствий их реализации, анализировать более сложные виды кибератак. С помощью имитационных моделей, созданных в MatLAB и Simulink, исследована динамика изменения состояний подсистемы блокировки запросов в процессе распознавания кибератак в критически важных компьютерных системах

Ключевые слова: распознавания кибератак, интеллектуальные системы, шаблон кибератаки, неоднородные потоки запросов

1. Introduction

Active expansion of information and communication systems (ICS) and mission-critical information systems (MCIS) in many countries around the world is accompanied by the emergence of new threats to cybersecurity (CS), as evidenced by the growing number of incidents related to information protection and identified vulnerabilities in MCIS.

Global development of corporate information systems (CIS) and MCIS, particularly in segments such as e-business (EB) in production industries, transport and communications requires constant tracking of cyber threats and vulnerabilities of technical components, software (SW), and database management systems. One of the priorities of cyberdefence, which contributes to the timely detection of cyberattacks and prevents their implications for CIS and MCIS, is to develop systems of intellectual recognition of cyberattacks (SIRCA). For such systems, it is always important to maximize the applicability of the models and algorithms for detecting cyberattacks that allow taking into account not only the presence and length of query queues in CIS or MCIS but also the possibility of using additional information about the structure of the input streams or any change made by attackers to the queries intensity, attack speed, or impulse duration. Consequently, the significance of research on developing SIRCA adaptability to educational conditions is doubtless, for it helps detect the whole repository of patterns of cyberattacks and the systems' efficiency.

2. Literature review and problem statement

The issue of improving the models of recognising complex cyberattacks by cyberdefence systems in CIS and MCIS has been the subject matter of many studies. In [1, 2], models are suggested for cyberattacks detection systems (CADS) that take into account the presence and length of query queues in CIS [3], but the authors do not consider the possibility of changing the inflow rate of queries to the server.

There are studies on models and algorithms for detection of cyberattacks that take into account queries in modules of “client-bank” systems, electronic invoices and communication systems [4, 5], the flow rate of requirements [6, 7], the interval between the requirements [8, 9], and the types of queries [10–12]. However, these studies do not consider the use of information systems of a variable structure, including the ones equipped with multiple servers and cyberdefence components, that are able to deal with a complex behaviour of query queues in terms of their heterogeneity (conflict). Thus, most studies that have been devoted to the issue of intellectual recognition of cyberattacks directed against CIS or MCIS concern only the basic features of cyberattacks. These publications do not take into account the changing modes of CIS or MCIS in case of a query loss due to blocking heterogeneous flows by relevant protection systems as a result of complex cyber interventions such as targeted attacks or when queries are lost due to the queue overflow in CIS and MCIS servers.

A large number of publications are devoted to the problems of designing systems of recognising cyberattacks (SRCA). Models of detecting cyberattacks that are based on finite automata (FA) are described in detail in [13, 14]. Methods of computational intelligence in SRCA are explored in [15–17]. Such systems are still under construction. In [18, 19], a Bayesian network model is suggested for SRCA. However, analysis of these studies reveals that in most cases such SRCA are based on decisions being made with the help of a statistical analysis of the presence of anomalies, threats and cyberattacks, without taking into account the possibility of implementing complex targeted cyberattacks. A widespread use of such SRCA is prevented by a significant complexity of the operational set-up of the repository of object recognition templates.

Many studies are devoted to the models and methods of detection based on the use of Markov chains [20–23]. The typical disadvantage of most SRCA that are proposed in these studies is lack of an opportunity to quickly replenish the repository of cyberattacks' patterns, as they almost always use only one methodology of recognition.

In the above studies, which are of interest in solving the problems of identifying cyberattacks, the models used are based only on information about query inflows and saturation streams [6, 8, 15, 16, 20]. Recent cyberattacks have become extremely complex. Narrowly focused, systematic and shared attacks, which are known as persistent sophisticated threats, are able to hide from anti-viruses and are not detected by firewalls and intrusion detection systems [9, 17, 22]. These targeted threats either have no signatures or are well disguised [4, 23].

Thus, further research should be aimed at developing methodological and theoretical bases for creating systems of intellectual recognition of cyberattacks, which would involve using additional information about the structure of the incoming flow, a possible change produced by attackers on the query intensity, the speed and duration of the impulse, and other parameters of cyberattacks.

3. The aim and tasks of the research

The aim of the undertaken research is to develop a model for training in the created adaptive system of intelligent recognition of cyberattacks to help take into account and store in the repository the patterns of sophisticated cyberattacks that have variable intensity of the incoming flow of queries in CIS or MCIS.

To achieve the purpose of the study, it is necessary to do the following tasks:

– to develop a model of intelligent recognition of complex targeted cyberattacks with variable parameters of query streams in CIS or MCIS;

– to carry out simulation tests on cyberattacks for heterogeneous query flows in information systems.

4. A model of an intelligent recognition module for cyberattacks of heterogeneous flows of queries in information systems

The mathematical description of the module of SIRCA for heterogeneous flows of queries is presented as follows:

$$\Delta = \left\langle IS \times T \times SS \times \Omega S \times KB, MX^{|2|}, MB^{|2|}, o_1, o_2 \right\rangle, \qquad (1)$$

where IS is a set of input signals that determine the state of cybersecurity in CIS or MCIS; T is a set of time points for the data on the state of information security (IS) of the object of protection; SS is a signature space for recognising a certain class of cyberattacks; ΩS is the space of the functional states of IS; KB is a knowledge base to identify cyberattacks; $MX^{|2|}$ is an instructional matrix (standard) that is stored in the repository of SIRCA; $MB^{|2|}$ is an instructional binary matrix; o_1 and o_2 are operators that form the instructional input and the binary matrices of SIRCA, respectively.

The SIRCA structure is shown in Fig. 1. The operator $O\Theta: MB^{|2|} \to MR^{|2|}$ is used to divide the space of cyberattack features into two classes of recognition. The parameter of the features (PF) is used to test the statistical hypothesis that the object of recognition belongs to a simulated class of cyberattacks. After evaluating the statistical hypotheses by using an oy operator, a plurality AR^{Q} is formed to contribute to the accuracy of recognising a cyberattack in SIRCA. It is assumed that q is the number of the statistical hypotheses, and $g=q^2$ is the quantity of SIRCA characteristics. The operator $o\mu$ generates an exploit kit (EK) plurality, which allows performing the procedure of evaluating the effectiveness of attack recognition within the class. The operator $o\beta$ is used to optimize the system of control deviations from the patterns of cyberattacks. The set SW is consistently closed by the operator $o\alpha_1: EK \to SW$ and the operator $o\alpha_2: SW \to MX,$ which allow changing the implementation of various features of cyberattacks of different classes in the process of teaching SIRCA.

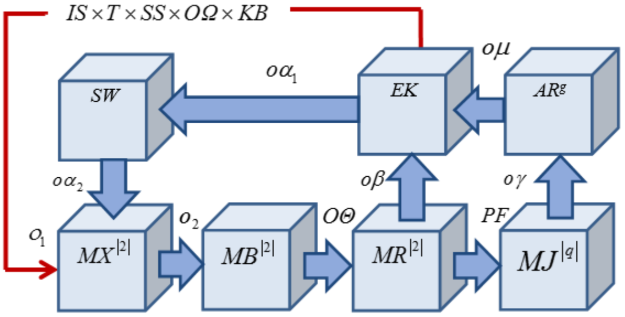


Fig. 1. A schematic diagram of SIRCA

A model is suggested for the knowledge base for identifying cyberattacks in SIRCA (or the repository) when the attackers are able to create heterogeneous queries with variable parameters during the attack.

The query streams are considered to be heterogeneous under the following conditions:

(1) there is no possibility to summarize the incoming flows of queries and to reduce the problem of recognition in SIRCA when it concerns suspicious queries about a one-dimensional case;

(2) applications from heterogeneous streams are processed in intervals that do not overlap;

(3) the system contains the so-called "intervals of inaccessibility" during which the streams are unattended, for example in the case of analysing queries by an intrusion detection system in MCIS.

The recognition system a priori contains the most intensive input streams of queries (streams that are primarily important in terms of the servicing speed) and streams of low intensity. The functional diagram of such cyberattacks is shown in Fig. 2.

Let us assume that the incoming flows of queries k_1, k_2, and k_3 are formed in some random environment (RE). The state of the RE may determine the probabilistic structure of the query flows. The variants can be as follows:

(1) if the RE is in a state of $c^{(0)}$, the incoming demand streams are regular query streams, which are the typical mode of CIS or MCIS;

(2) if the RE acquires the state of $c^{(1)}$, the incoming streams are streams of packets (a query flow is a sequence of "packets" [21, 23, 24]).

It is assumed that: k_1 is a priority stream of queries that come with low intensity, k_2 is a stream of queries of a normal priority and low intensity, and k_3 is a priority stream of queries coming with the highest intensity.

The informational flow k_1 means that the dynamics of the system reflect the availability of applications in the storage NO_1 and the incoming queries down this stream. Priority of an appropriate flow is the prerequisite for operational maintenance of the queries that have come in the CIS or MCIS. For example, for the flow k_3, the priority means that a gap or absence of queries for the stream k_1 facilitates continuity in servicing the queries of the stream k_3.

According to the topology of CIS or MCIS and the assumptions about the state of the RE, the work of the maintenance equipment (ME) is organized, for example, for servers of MCIS and elements of SIRCA. According to the graph, let us mark the states of the system as $S^{(r)}, r=\overline{1,7}$. The states of the system form a plurality $S=\left\{S^{(r)}: r=\overline{1,7}\right\}$. The system is in a state of $S^{(r)}$ for the time $\tau_r, r=\overline{1,7}$. The ME performs the task of analysing and meeting the requirements, and it also controls the input streams and forms queues in the NO_i. Selection of queries from the queues is made according to their priority and by using the strategies of service designated as α_{01}, α_{02}, and α_{03}. The state $S^{(2j-1)}$ for j=1, 2, and 3 entails that the ME meets the service requirements of the stream k_j. In the state $S^{(2j)}$ for j=1, 2, and 3, the queries of all the incoming streams are left unattended. In the state $S^{(7)}$, the servicing is performed for the stream k_3. According to the graph, with each r=1, 2, 3, or 4, the state $S^{(r)}$ becomes the state $S^{(r+1)}$.

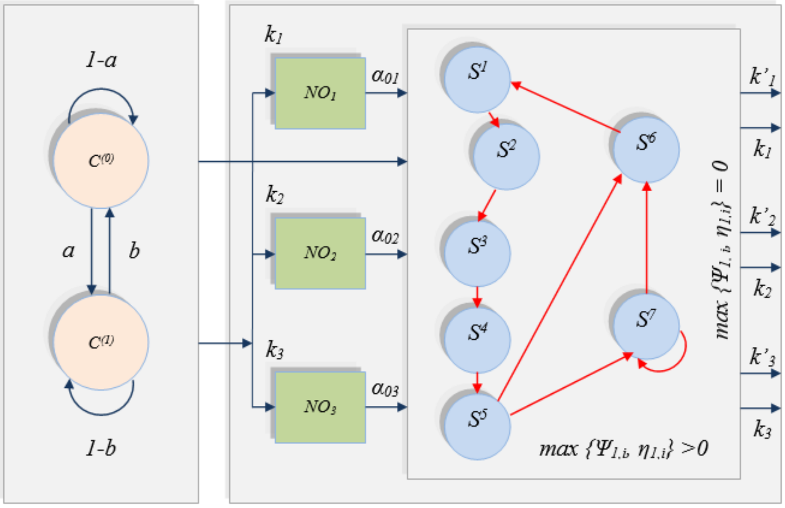


Fig. 2. A functional diagram of cyberattacks with mixed flows of queries: S^1 is the entry into a CIS or MCIS, S^2 is the scan of the available resources (AR) in a CIS or MCIS, S^3 is the waiting for the response about the presence of AR, S^4 is the connection to the AR, S^5 is the data transmission in the CIS or MCIS, S^6 is the data transmission to the available resources (automated workstations (AWSs) or personal computers (PCs), and S^7 is the loading of the query dispatch to the servers of the CIS or MCIS

Let us consider a situation where hackers that attack a system can create a queue. Accordingly, the output streams in the system at the maximum load and with the ME functioning continuously are transformed into saturation flows marked as k'_1, k'_2, and k'_3, unlike the real query flows – k_1, k_2, and k_3 – in the system.

We considered such options of the intelligent recognition of cyberattack threats:

(1) when packets are sent at a zero rate within a time scale of queries that pass to the addressee and back;

(2) when during a cyberattack the attacker can vary the impulse duration;

(3) when there are minimal random values within a time scale of queries that pass to the addressee and back.

All random objects – which are analysed further, were used to construct a cyberattack model, and are related to the process of servicing queries – are addressed in the probability space $(\Omega, A, P(*))$ of elementary random events $\omega \in \Omega$ with a probability of the query penetration into the system – P(A). The incoming flows of queries are described by using a nonlocal way. Any query stream k_j in the system is described as a random sequence of the vector $\{(\tau_i, v_i, \eta_{j,i});$ $i \geq 0\}$, where $\eta_{j,i}$ is the number of applications that are patterned like v_i, which are respectively received during the time interval $[\tau_i, \tau_{i+1})$ within this flow. In SIRCA, the application sample is determined by the marker v_i in the form of a binary matrix of signs [25, 26] stored in the repository as well as by the state of the RE. To simplify the model, the behaviour of the random environment is described by a homogeneous Markov sequence $\{v_i; i \geq 0\}$ of two states: of $c^{(0)}$ as a flow of queries with low intensity and of $c^{(1)}$ as a high flow of applications with the probability of a transition a, b $0 \leq a < b << 1$. In accordance with the accepted restrictions, changes in the intensity of the flow are not frequent; therefore, the normal operation of MCIS with a low-intensity stream of applications is more typical than with a stream of a large number of queries. Thus, according to the research findings, within the time τ_r, with the ME in the state $S^{(r)}$, the intensity of queries will remain unchanged. The random elements $v_i; i \geq 0$ are correlated as $v_{i+1} = \varphi_i(v_i, \omega_i)$, where φ_i is a description of the space $\{c^{(0)}, c^{(1)}\} \cdot \{0,1\}$ within $\{c^{(0)}, c^{(1)}\}$, and $\{\omega_i; i \geq 0\}$ is a consistent set of independent random variables of a known distribution. For the model, the distribution is assumed as uniform in the interval $(0,1)$.

The maintenance equipment at any time of $\tau > 0$ is in a state of $S(\tau) \in S$. The control of the incoming flows of queries and the transition between the states of the ME, according to the graph and taking into account the previous comments, are described as follows:

$$S_{i+1} = u(S_i, \psi_{1,i}, \eta_{1,i}) = \begin{cases} S^{(1)} \quad \text{at } S_i = S^{(6)}; \\ S^{(r+1)} \text{ at } S_i = S^{(r)} \; r = \overline{1,4}; \\ S^{(6)} \quad \text{at } S_i \in \{S^{(5)}, S^{(7)}\} \,\&\, \max\{\psi_{1,i}, \eta_{1,i}\} > 0; \\ S^{(7)} \quad \text{at } S_i \in \{S^{(5)}, S^{(7)}\} \,\&\, \max\{\psi_{1,i}, \eta_{1,i}\} = 0; \end{cases} \quad (2)$$

where $\psi_{j,i} = f(w)$ is the length of the queue in NO_j down the stream k_j for i=0, 1, ..., and k.

Given the decision rules $DR(p_{axi})$ [25], which determine the system states in case of threats to information security, we have received recursive dependencies for intelligent recognition of sophisticated cyberattacks, where the attacker creates a situation in which $S_i \in \{S^{(5)}, S^{(7)}\}$ can be served only for the query flow k_3; then at r=6 for

$$y = 0,1,; x_{j,k} = \{0,1,\ldots k\},$$

we find that

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, 0, w_3, DR(p_{axi})\right) = 0$$

at all $w_3 \geq 0$ and $i \geq 0$. With $w_1 \geq 1$, the dependence is the following:

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, w_1, 0, DR(p_{axi})\right) = \\ = \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{x=0}^{w_1} \sum_{y=0}^{l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}\left(w_1 - x, T_5\right) \cdot \sum_{n_3=0}^{l_{3,h}-y} \varphi_{3,h}\left(n_3, T_5\right) + \\ + \sum_{x=0}^{w_1} \sum_{y=0}^{l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}\left(w_1 - x, T_7\right) \cdot \sum_{n_3=0}^{l'_{3,h}-y} \varphi_{3,h}\left(n_3, T_7\right) \end{array} \right], \quad (3)$$

where p_{axi} stands for signs of unlawful activities (a cyberattack) in the segment of the network; $l_{1,s}, l_{3,s}, l'_{3,s}$ are the whole values of $\mu_{1,s}T_1$, $\mu_{3,s}T_5, \mu_{3,s}T_7$, and $\mu_{j,s}$ is the service intensity down the stream k_j if the system is in a state of $c^{(s)}$ or $c^{(h)}$, whereas at $w_3 \geq 1$:

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, w_1, w_3, DR(p_{axi})\right) = \\ = \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{x=0}^{w_1} \sum_{y=0}^{w_3 + l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}\left(w_1 - x, T_5\right) \times \\ \times \varphi_{1,h}\left(w_3 + l_{3,h} - y, T_5\right) + \\ + \sum_{x=0}^{w_1} \sum_{y=0}^{w_3 + l'_3} Q_i\left(S^{(7)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}\left(w_1 - x, T_7\right) \times \\ \times \varphi_{1,h}\left(w_3 + l'_{3,h} - y, T_7\right) \end{array} \right]. \quad (4)$$

For the probability of

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, w_1, w_3, DRv(p_{axi})\right),$$

we get

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, w_1, w_3, DR(p_{axi})\right) = 0$$

at any $w_1 \geq 0$, $i \geq 0$, $s \in \{1,0\}$:

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, 0, 0, DR(p_{axi})\right) = \\ = \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{y=0}^{l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}\left(0, T_5\right) \cdot \sum_{n_3=0}^{l_{3,h}-y} \varphi_{3,h}\left(n_3, T_5\right) + \\ + \sum_{y=0}^{l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}\left(0, T_7\right) \cdot \sum_{n_3=0}^{l'_{3,h}-y} \varphi_{3,h}\left(n_3, T_7\right) \end{array} \right], \quad (5)$$

and at any $w_3 \geq 0$, $s \in \{1,0\}$:

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, 0, w_3, \quad DR(p_{axi})\right) = \\ = \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{y=0}^{w_3 + l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}\left(0, T_5\right) \cdot \varphi_{3,h}\left(w_3 + l_{3,h} - y, T_5\right) + \\ + \sum_{y=0}^{w_3 + l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}\left(0, T_7\right) \cdot \varphi_{3,h}\left(w_3 + l'_{3,h} - y, T_7\right) \end{array} \right]. \quad (6)$$

Given the recurrent expressions (2) through (6) and using the instruments of simulating the environment MATLAB 7 and Simulink, we have developed a simulation model to analyse the impact of cyberattacks on the functionality of a segment of CIS or MCIS if the attacker uses heterogeneous flows of queries in the system.

5. A simulation model of cyberattacks in heterogeneous flows of queries in information systems

The simulation model (for a segment of MCIS) consists of one data line and three stations (automated workstations, AWSs) that send regular claims for data transfer down the line (Fig. 3, *a*). The query settings are formed according to the data in Fig. 3, *b*: AWS1 reflects the low-intensity priority stream k_1, AWS2 means the low-intensity flow k_2, and AWS3 stands for the priority stream of the greatest intensity k_3. We also assume that the time is discrete and it varies from 0 to some value T. The AWSs are independent of one another, and at any moment there is a certain probability of any station to send a data request or to empty the line. In the unit of traffic analysis, using the unit of threats recognition [25] and the predetermined crucial rules of $DR(p_{axi})$, it is possible to obstruct any related attacks and unauthorized network activities. The yellow colour in the diagram shows the components that are used to visualise the traffic or separate heterogeneous flows of queries to the server of a CIS. The green colour represents the components that allow changing the parameters of inhomogeneous flows of queries – the presence and length of the query queues in a CIS or MCIS, the structure of the input streams k_1, k_2, and k_3, the attacking intensity change in the queries, the attack speed, and the impulse duration.

To implement the process of intellectual recognition of individual classes of threats, cyberattacks and anomalies in the simulation model via the expansion pack Fuzzy Logic Toolbox, there were drawn up the rules for the system of recognition shown in Fig. 4.

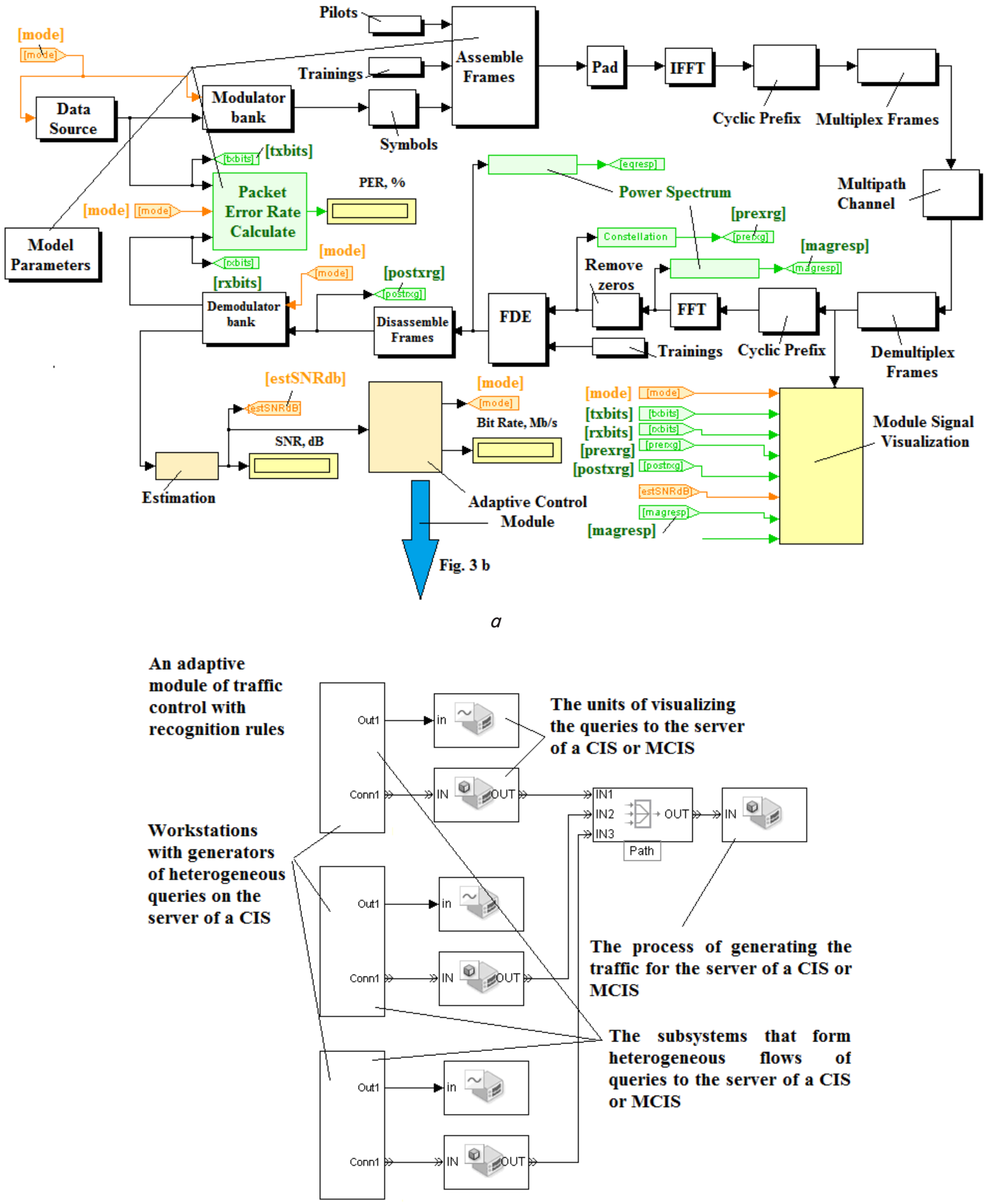
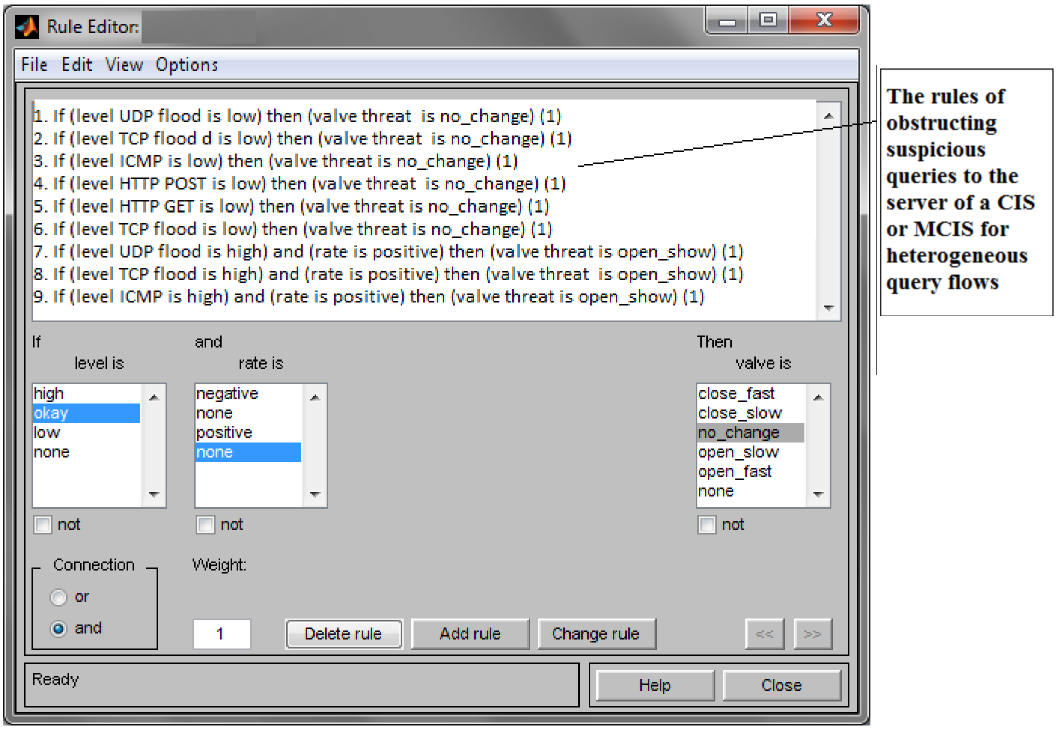


Fig. 3. A scheme of the cyberattack simulation modelling for heterogeneous flows of queries in a segment of a CIS or MCIS: a is a segment of a CIS or MCIS (we used library components of MATLAB); b is a unit for simulating a cyberattack for heterogeneous flows of queries

Fig. 5 below shows a subsystem of obstructing queries from AWSs as part of a CIS or MCIS in detecting an abnormal queue of queries coming from a terminal.

To study the possibility of detecting cyberattacks with mixed flows of queries, a simulation experiment was conducted in a segment of the computer network of a CIS. The network was working normally, and then it was subjected to an attack. To visualize the signals, we had designed a special unit – "Signal Visualization" (Fig. 6), which allowed analysing the basic parameters of the segment of the MCIS at the level of transmitted data packets, including a change in the number of queries **R** during the time interval **t**.



1. If (level UDP flood is low) then (valve threat is no_change) (1)
2. If (level TCP flood d is low) then (valve threat is no_change) (1)
3. If (level ICMP is low) then (valve threat is no_change) (1)
4. If (level HTTP POST is low) then (valve threat is no_change) (1)
5. If (level HTTP GET is low) then (valve threat is no_change) (1)
6. If (level TCP flood is low) then (valve threat is no_change) (1)
7. If (level UDP flood is high) and (rate is positive) then (valve threat is open_show) (1)
8. If (level TCP flood is high) and (rate is positive) then (valve threat is open_show) (1)
9. If (level ICMP is high) and (rate is positive) then (valve threat is open_show) (1)

level is: high, okay (selected), low, none — □ not

rate is: negative, none, positive, none (selected) — □ not

valve is: close_fast, close_slow, no_change (selected), open_slow, open_fast, none — □ not

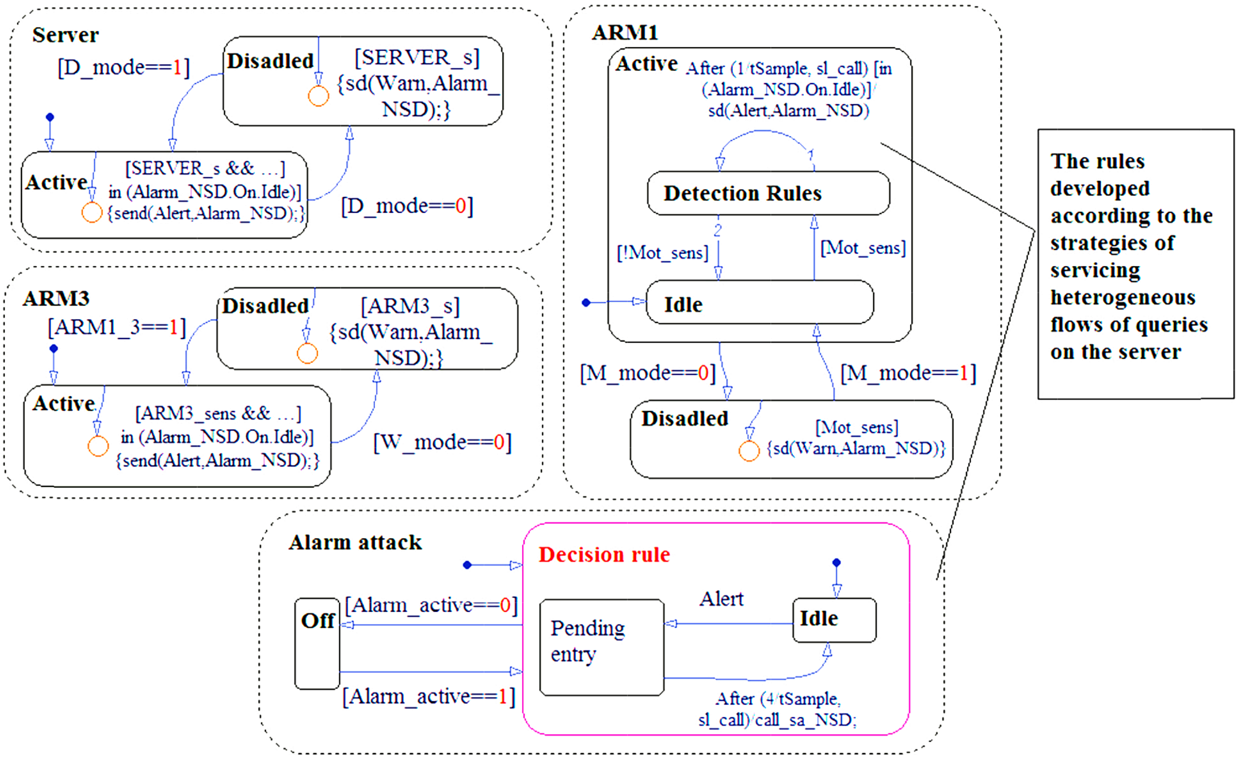
Connection: ○ or ● and

Weight: 1

Ready

The rules of obstructing suspicious queries to the server of a CIS or MCIS for heterogeneous query flows

Fig. 4. A system of rules to detect cyberattacks



The rules developed according to the strategies of servicing heterogeneous flows of queries on the server

Fig. 5. The subsystem of obstructing queries in the system of intellectual recognition of cyberattacks in MCIS

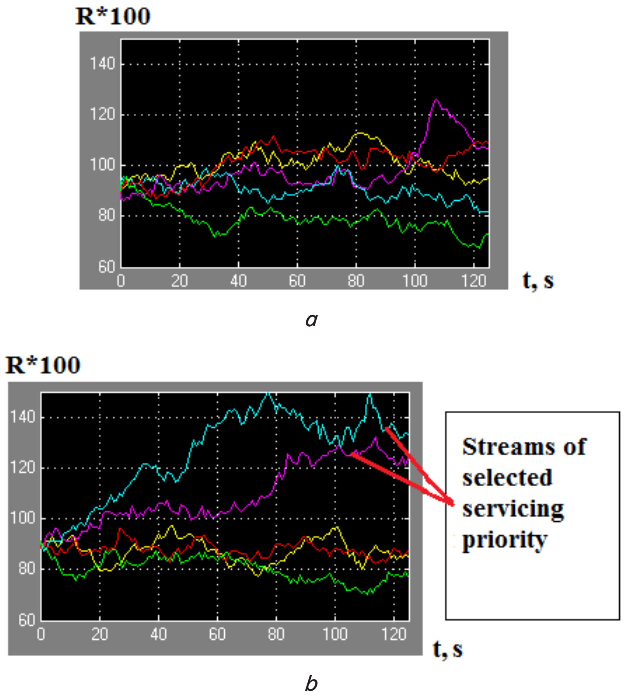


Fig. 6. Visualization of the flows of queries in the MCIS: *a* is the normal mode of the MCIS segment; *b* is the simulation of a cyberattack with mixed flows of queries

The simulation modelling was used to study the modes of CIS or MCIS for cases of blocking queries whenever they deviate from the "normal" mode. The relevant results of the simulation modelling are presented in the next section.

6. The results of a simulation modelling of cyberattacks for heterogeneous flows of queries in information systems

The simulation model (SM) was used to check the validity of the results of implementing cyberattacks, such as "denial of service" and "buffer overflow", in the ICS of a CIS. The source data were the results of measuring the parameters of the received incoming streams in the SM. The simulation and the analytical calculation [3, 4, 21–23, 25, 26] of the bandwidth used in the CIS or MCIS were conducted for different sets of heterogeneous implementations of the streams k_1 and k_3. Table 1 shows the data obtained during the simulation experiment – the time of the delay and the probability of the query loss, as well as the comparative parameters of the expected features. Accordingly, $T_{cf.\ pr.}$ and $P_{pr.}$ are the comparative tentative and probable parameters of the delay and loss in processing the queries, $T_{cf.\ cl.}$ and $P_{cl.}$ are the network parameters that were calculated by the classic method, whereas $T_{cf.\ sug.}$ and $P_{sug.}$ are the network parameters that were calculated by the suggested models. The analysis and comparison of the results have produced a conclusion about the adequacy of calculating the characteristics of SIRCA elements in the network segment of a CIS or MCIS.

Table 2 shows the results of a simulation modelling in terms of a cyberattack "denial of service" to the server and the workstation within the CIS model.

The average error of the calculated probability of the query loss V_q as a result of such cyberattacks does not exceed the standard deviation in the frequency of losses F_q in the series of the experiments.

Table 1

The value of the probable time characteristics at a cyberattack "denial of service"

Number of the implementation	$T_{cf.\ pr.}$, ms	$T_{cf.\ cl.}$, ms	$T_{cf.\ sug.}$, ms	$P_{pr.}$	$P_{cl.}$	$P_{sug.}$
1	10	11.7	10.2	$5x10^{-8}$	$6.28x10^{-8}$	$4.93x10^{-8}$
2	20	24.7	20.3	$7x10^{-8}$	$7.79x10^{-8}$	$7.12x10^{-8}$
3	50	61.0	49.5	$3x10^{-6}$	$3.6x10^{-6}$	$3.15x10^{-6}$
4	100	97.3	98.4	$1.5x10^{-6}$	$2.36x10^{-6}$	$3.07x10^{-6}$
5	150	107.3	101.4	$1.7x10^{-6}$	$256x10^{-6}$	$2.98x10^{-6}$
6	200	111.3	119.4	$1.8x10^{-6}$	$2.7x10^{-6}$	$2.81x10^{-6}$
7	250	125.3	128.4	$1.95x10^{-6}$	$2.8x10^{-6}$	$2.47x10^{-6}$
8	300	147.3	148.4	$2x10^{-6}$	$2.9x10^{-6}$	$2.03x10^{-6}$
9	350	180.3	155.4	$9.1x10^{-5}$	$9.05x10^{-5}$	$9.29x10^{-5}$
10	400	247.3	190.4	$9.7x10^{-5}$	$9.9x10^{-5}$	$9.87x10^{-5}$

Table 2

The results of the simulation modelling of a CIS segment under a cyberattack "denial of service"

The number of the modelled sessions	N	10
The average value of the query loss frequency	V_{zap}	8.6E-2
The standard deviation in the loss frequency	F_{zap}	1.01E-3
The calculated probability of the query loss	P_{zap}	8.41E-2
The average error	ΔP_{zap}	3.9E-4

Fig. 7, 8 show the main results of modelling heterogeneous query flows k_1, k_2, and k_3 in an MCIS. Therefore, in the case of creating heterogeneous priority flows of queries in an MCIS, the data processing time increases 1.5–3.5 times.

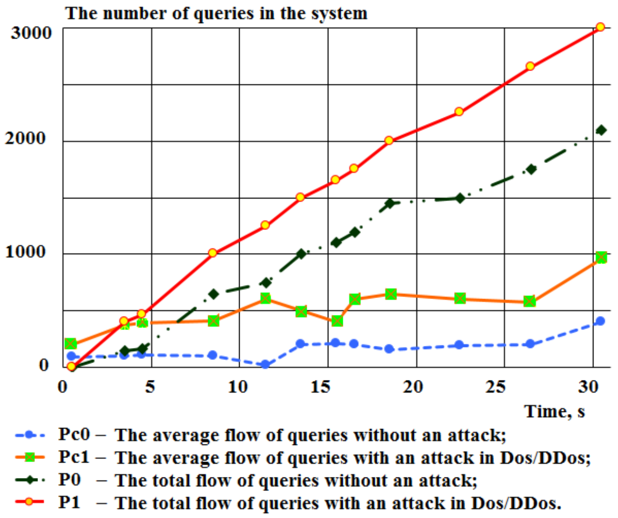


Fig. 7. The distribution of the total (P0 and P1) and average (Pc0 and Pc1) flows of queries during normal operation of a segment of a CIS or MCIS

The analysis of the obtained results shows that the likelihood of penetrating into the system can be significantly increased if the attacker uses the tactics of assigning a high-priority status to a low-intensity flow and if the cyber-intrusion is sufficiently prolonged. In this case, the attacker does not necessarily change the parameters of the flow k_3, which has the highest intensity and the top priority in the system (Fig. 8).

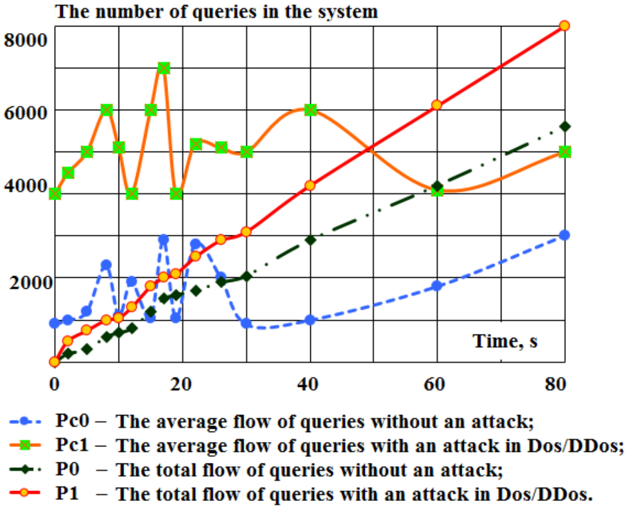


Fig. 8. The distribution of the total (P0 and P1) and average (Pc0 and Pc1) flows of queries when attackers create heterogeneous queries

Fig. 9 shows a graph of the dependence of the theoretical estimation of the query loss probability in a CIS or MCIS on the number of steps in the suggested iterative procedure of (2) through (6). The present graph suggests a conclusion about the required number of iterations for a given accuracy of the simulation model.

During the study, we found that the likelihood of solving the problem of recognising sophisticated cyberattacks in heterogeneous flows of queries as well as network types of cyberattacks constituted 85–98 %, depending on the type of the attack.

The analysis of the results of the simulation experiment allows making a conclusion that the suggested model of recognising sophisticated cyberattacks in non-uniform flows of queries is more accurate, by 5–7 %, than the other existing models.

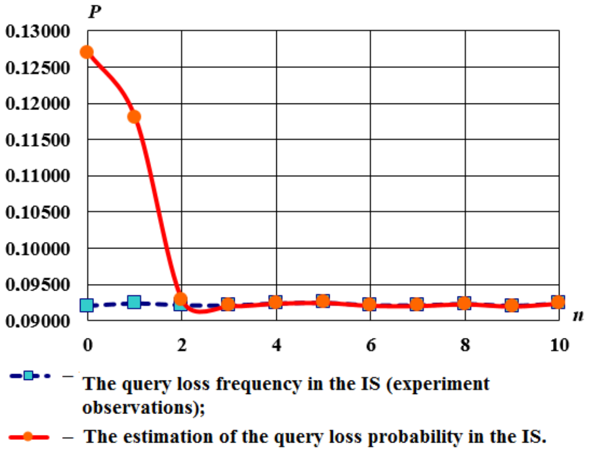


Fig. 9. The dependence of the theoretical estimation of the probability (P) of losing a query (application) on the number of steps (n) in the iterative procedures

Thus, a successful cyberattack at the information resources of a CIS or MCIS, especially of the “denial of service” type, does not necessarily create a large number of queries to the server or reduce the traffic bandwidth. There is a fairly high probability of success in exploiting the system vulnerability by creating a low-intensity priority flow and changing its parameters such as the package speed (low-speed attacks) or the impulse duration, etc.

According to preliminary estimates, the developed simulation models make it possible to reduce by 25–30 % the time for setting up SIRCA projects for a CIS or MCIS.

7. Discussion of the model testing results and prospects for further research

The described models of implementing cyberattacks with mixed flows of queries in CIS or MCIS are not only of independent practical interest, but they are an example of a possible formalisation of describing other complex scenarios of cyberattacks.

It has been determined that Markov models of processes are widely used in the analysis and synthesis of CIS and MCIS, and their properties set certain limitations to the real signals used, but this is quite sufficient to develop meaningful methods of analysis and synthesis of complex cyberdefence systems. As each state of the system can be characterised by a set of values of quantised digital signals that are typical of S_i, the quantity of gradations – the quantisation levels – in the signs of cyberattacks in the SIRCA system acts as a universal set whose capacity is equal to the maximum quantisation level, characteristic of a particular model.

The downside of the model is cumbersome calculations, which complicates the practical use of the system of Markov chains in modelling the considered processes. However, the exponential approximation simplifies the estimation of the cyberattack probability.

The presented approach allows making quantitative estimation of the probability of network threats and attacks in the computer networks of CIS or MCIS with regard to the time factor and, thereby, increases the validity of measures to protect information.

Scientific and practical research in the form of hardware and software applications and educational materials during the years of 2014 and 2015 were introduced at the state enterprise “Design and engineering office for automating control systems at the Ukrainian railways” of the Ministry of Infrastructure of Ukraine, as well as in the information security service of the computing centre of the Near-Dnipro Railways and the State University of Telecommunications as part of the research project “Safety-05P”.

The results that were previously presented in [25, 26] and the results of the tests of the individual modules of SIRCA have facilitated the development of a decision-making support system and an expert system, and the repository of the cyberattacks’ patterns has been expanded.

8. Conclusion

1. The study was focused on developing a model of intelligent recognition of sophisticated cyberattacks, which, unlike the existing ones, takes into account the change in the intensity of the incoming flows of queries in information

systems. It helps assess the quality of a CIS functioning with regard to a possibility that attackers will change the parameters of the cyberattack.

2. The tests and the justification of the suggested model were carried out by using simulation modelling in the environment of MATLAB and Simulink. It has been found that the suggested model of recognising sophisticated cyberattacks is by 5–7 % more accurate than the other existing models if attackers use non-uniform flows of queries. The developed simulation models enable a 25–30 % decrease in the setup time for projects of cyberdefence systems, including SIRCA for CIS or MCIS.

References

1. Yu, S. Can We Beat DDoS Attacks in Clouds? [Text] / S. Yu, Y. Tian, S. Guo, D. O. Wu // IEEE Transactions on Parallel and Distributed Systems. – 2014. – Vol. 25, Issue 9. – P. 2245–2254. doi: 10.1109/tpds.2013.181
2. Peng, T. Survey of Network-Based Defense Mechanisms Countering the dos and ddos Problems [Text] / T. Peng, C. Leckie, K. Ramamohanarao // ACM Computing Surveys. – 2007. – Vol. 39, Issue 1. – P. 1–3. doi: 10.1145/1216370.1216373
3. Bogdanoski, M. Analysis of the SYN Flood DoS Attack [Text] / M. Bogdanoski, T. Shuminoski, A. Risteski // International Journal of Computer Network and Information Security. – 2013. – Vol. 5, Issue 8. – P. 11–15. doi: 10.5815/ijcnis.2013.08.01
4. Logota, E. Analysis of the Impact of Denial of Service Attacks on Centralized Control in Smart Cities [Text] / E. Logota, G. Mantas, J. Rodriguez, H. Marques. – Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2015. – P. 91–96. doi: 10.1007/978-3-319-18802-7_13
5. Zargar, S. T. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks [Text] / S. T. Zargar, J. Joshi, D. Tipper // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, Issue 4. – P. 2046–2069. doi: 10.1109/surv.2013.031413.00127
6. Ciancamerla, E. Modeling cyber attacks on a critical infrastructure scenario [Text] / E. Ciancamerla, M. Minichino, S. Palmieri // Information, Intelligence, Systems and Applications (IISA), Fourth International Conference, 2013. – P. 1–6. doi: 10.1109/iisa.2013.6623699
7. Rinaldi, S. M. Identify, understanding, and analyzing critical infrastructure interdependencies [Text] / S. M. Rinaldi, J.P. Peerenboom, T. K. Kelly // IEEE Control Systems Magazine. – 2001. – Vol. 21, Issue 6. – P. 11–25. doi: 10.1109/37.969131
8. Ahmed, I. Scada systems: Challenges for forensic investigators [Text] / I. Ahmed, S. Obermeier, M. Naedele, G. G. Richard III // Computer. – 2012. –Vol. 45, Issue 12. – P. 44–51. doi: 10.1109/mc.2012.325
9. Liu, R. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid [Text] / R. Liu, C. Vellaithurai, S.S. Biswas, T. T. Gamage, A. K. Srivastava // IEEE Transactions on Smart Grid. – 2015. – Vol. 6, Issue 5. – P. 2444–2453. doi: 10.1109/tsg.2015.2432013
10. Chen, Q. A Model-Based Validated Autonomic Approach to Self-Protect Computing Systems [Text] / Q. Chen, S. Abdelwahed, A. Erradi // IEEE Internet of Things Journal. – 2014. – Vol. 1, Issue 5. – P. 446–460. doi: 10.1109/jiot.2014.2349899
11. Wasicek, A. Aspect-oriented modeling of attacks in automotive Cyber-Physical Systems [Text] / A. Wasicek, P. Derler, E. Lee // Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference - DAC '14, 2014. – P. 1–6. doi: 10.1145/2593069.2593095
12. Ericsson, G. N. Cyber security and power system communication-essential parts of a smart grid infrastructure [Text] / G. N. Ericsson // IEEE Transactions on Power Delivery. – 2010. – Vol. 25, Issue 3. – P. 1501–1507. doi: 10.1109/tpwrd.2010.2046654
13. Ilgun, K. State transition analysis: a rule-based intrusion detection approach [Text] / K. Ilgun, R. A. Kemmerer, P. A. Porras // IEEE Transactions on Software Engineering. – 1995. –Vol. 21, Issue 3. – P. 181–199. doi: 10.1109/32.372146
14. Khan, L. A new intrusion detection system using support vector machines and hierarchical clustering [Text] / L. Khan, M. Awad, B. Thuraisingham // The VLDB Journal. – 2007. – Vol. 16, Issue 4. – P. 507–521. doi: 10.1007/s00778-006-0002-5
15. Al-Jarrah, O. Network Intrusion Detection System using attack behavior classification [Text] / O. Al-Jarrah, A. Arafat // 2014 5th International Conference on Information and Communication Systems (ICICS), 2014. – P. 1–6. doi: 10.1109/iacs.2014.6841978
16. elim, S. Intrusion Detection using Multi-Stage Neural Network [Text] / S. Selim, M. Hashem, T. M. Nazmy // International Journal of Computer Science and Information Security (IJCSIS). – 2010. – Vol. 8, Issue 4. – P. 14–20.
17. Pawar, S. N. Intrusion detection in computer network using genetic algorithm approach: a survey [Text] / S. N. Pawar // International Journal of Advances in Engineering Technology. – 2013. – Vol. 6, Issue 2. – P. 730–736.
18. Heckerman, D. A tutorial on learning with bayesian networks. Innovations in Bayesian Networks [Text] / D. Heckerman // Theory and Applications. – 2008. –Vol. 156. – P. 33–82. doi: 10.1007/978-3-540-85066-3_3
19. Nguyen, K. C. A decentralized Bayesian attack detection algorithm for network security [Text] / K. C. Nguyen, T. Alpcan, T. Basar // IFIP – The International Federation for Information Processing, 2008. –P. 413–428. doi: 10.1007/978-0-387-09699-5_27
20. Vrakopoulou, M. Chapter Cyber Physical Systems Approach to Smart Electric Power Grid [Text] / M. Vrakopoulou, P. Mohajerin Esfahani, K. Margellos, J. Lygeros, G. Andersson. – Power Systems, 2015. – P. 303–328. doi: 10.1007/978-3-662-45928-7_11
21. Lecchini-Visintini, A. Stochastic optimization on continuous domains with finite-time guarantees by markov chain monte carlo methods [Text] / A. Lecchini-Visintini, J. Lygeros, J. Maciejowski // IEEE Transactions on Automatic Control. – 2010. – Vol. 55, Issue 12. – P. 2858–2863. doi: 10.1109/tac.2010.2078170
22. Befekadu, G. K. Risk-Sensitive Control Under Markov Modulated Denial-of-Service (DoS) Attack Strategies [Text] / G. K. Befekadu, V. Gupta, Panos J. Antsaklis // IEEE Transactions on Automatic Control. – 2015. – Vol. 60, Issue 12. – P. 3299–3304. doi: 10.1109/tac.2015.2416926

23. Subil, A. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains [Text] / A. Subil, N. Suku Nair // Journal of Communications. – 2014. – Vol. 9, Issue 12. – P. 899–907. doi: 10.12720/jcm.9.12.899-907
24. Esmalifalak, M. Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study [Text] / M. Esmalifalak, G. Shi, Z. Han, L. Song // IEEE Transactions on Smart Grid. – 2013. – Vol. 4, Issue 1. – P. 160–169. doi: 10.1109/tsg.2012.2224391
25. Lakhno, V. Improving the transport cyber security under destructive impacts on information and communication systems [Text] / V. Lakhno, A. Hrabariev // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 1, Issue 3(79). – P. 4–11. doi: 10.15587/1729-4061.2016.60711
26. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering [Text] / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, Issue 9 (80). – P. 18–25. doi: 10.15587/1729-4061.2016.66015

UDC 621.391
DOI: 10.15587/1729-4061.2016.75716

THE ANALYSIS OF METHODS FOR DETERMINING DIRECTION OF ARRIVAL OF SIGNALS IN PROBLEMS OF SPACE-TIME ACCESS

Naors Y. Anad Alsaleem
PhD
Department of Computer Engineering
Al-Safwa University College
Oletsa-almamalje, Karbala, Iraq, 56001
E-mail: nawrasyounis@yahoo.com

M. Moskalets
PhD, Associate Professor*
E-mail: mykola.moskalets@nure.ua

S. Teplitskaya
PhD, Associate Professor*
E-mail: svitlana.teplytska@nure.ua

*Department of Telecommunication Systems
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Проводиться аналіз методів визначення напрямку приходу сигналів в задачах просторово-часового доступу на основі методів радіопеленгації в системах мобільного зв'язку. Показана процедура оцінки вектора розподілу поля, значення якого може бути обчислено спільно з оцінкою вектора вагових коефіцієнтів адаптивної антенної решітки. Отримано результати імітаційного моделювання методів зверхрозподілу сигналів, що підтверджує їх статистичну спроможність

***Ключові слова:** просторово-часовий доступ, діаграма спрямованості, пеленг, зверхрозподіл сигналів, вектор вагових коефіцієнтів*

Проводится анализ методов определения направления прихода сигналов в задачах пространственно-временного доступа на основе методов радиопеленгации в системах мобильной связи. Показана процедура оценки вектора распределения поля, значение которого может быть вычислено совместно с оценкой вектора весовых коэффициентов адаптивной антенной решетки. Получены результаты имитационного моделирования методов сверхразрешения, подтверждающие их статистическую состоятельность

***Ключевые слова:** пространственно-временной доступ, диаграмма направленности, пеленг, сверхразрешение, вектор весовых коэффициентов*

1. Introduction

As international literary sources [1, 2] claim, by the year 2020 and in future, 5G mobile communication systems will be able to provide mobile users with unlimited high-speed access to information at any place and any time. To achieve the set goal, a considerably large variety of applications and devices is needed and networks of mobile communication and broadband wireless access currently have them. Due to this fact, there emerged a necessity to implement long-term technological methods in 5G systems aimed at solving problems of mobile user access and issues of effective link resources utilization. The key long-term technological solutions implemented in the mobile communication systems of the 5th generation are [1, 2]:

– application of evolutional massive (multi-dimensional) multi-antenna MIMO technologies;

– ability to effectively use the modes of dynamic 3D-beamforming. This will allow considerable increasing the signal power for remote users in high frequency bands and improving coverage in ultradense micro- and picocells;

– application of micro-, pico- and femtocells in areas of ultradense user location, which decrease the load on macrocells, with the division of transmission of user traffic and control signals between macro- and microcells in different frequency ranges;

– implementation of the full duplex in common bandwidth (transmission and reception are on the same frequencies);