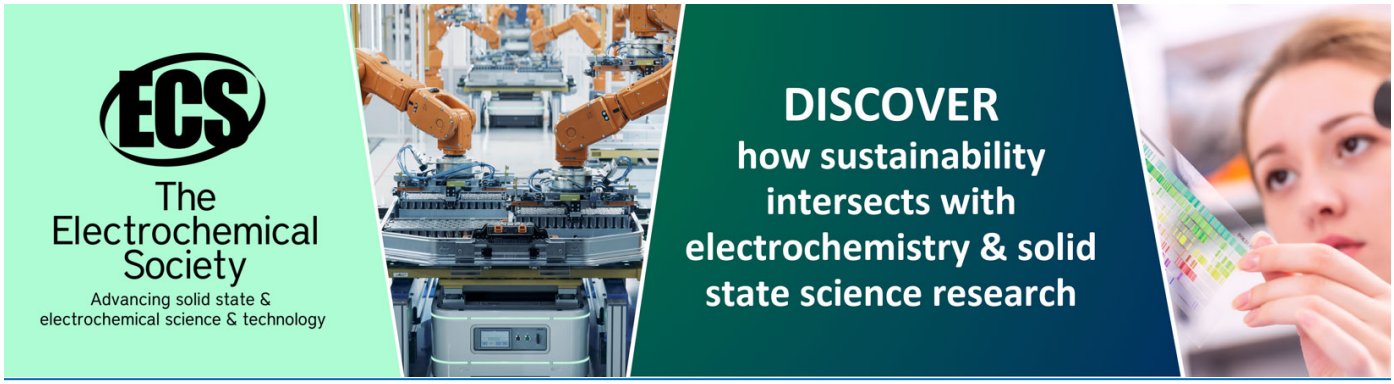
Detection of network attacks based on adaptive resonance theory



IOP Conf. Series: Journal of Physics: Conf. Series **1015** (2018) 042007 doi:10.1088/1742-6596/1015/4/042007

Detection of network attacks based on adaptive resonance theory

D G Bukhanov, V M Polyakov

Belgorod State Technological University named after V.G. Shukhov, 46 Kostukova Str., Belgorod, 308012, Russia

E-mail: db.old.stray@gmail.com

Abstract. The paper considers an approach to intrusion detection systems using a neural network of adaptive resonant theory. It suggests the structure of an intrusion detection system consisting of two types of program modules. The first module manages connections of user applications by preventing the undesirable ones. The second analyzes the incoming network traffic parameters to check potential network attacks. After attack detection, it notifies the required stations using a secure transmission channel. The paper describes the experiment on the detection and recognition of network attacks using the test selection. It also compares the obtained results with similar experiments carried out by other authors. It gives findings and conclusions on the sufficiency of the proposed approach. The obtained information confirms the sufficiency of applying the neural networks of adaptive resonant theory to analyze network traffic within the intrusion detection system.

1. Introduction

Modern information systems are often exposed to various attacks. According to the 2015 report on cyber attacks of the Positive Technologies [1], in most cases (56%) cyber-criminals used web applications vulnerability while only 20% of cases used zero day vulnerabilities. This fact demonstrates that the victims had an opportunity to efficiently protect their systems, but they did not make the best use of it. Lack or bad choice of security software against attacks also played a vital role.

One of the most efficient security tools are intrusion detection systems (IDS) [2]. IDS is used to detect unauthorized access to computer networks or operations with its resources by unauthorized users. IDS can be centralized or decentralized, and can be based on network computers or a certain machine analyzing the network traffic. Regardless of its type, the kernel of any IDS is the traffic analysis system. Recent trends in network traffic analysis are closely linked to intelligent techniques that can be applied to solve this task.

In paper [3], the authors suggest approaches based on fuzzy logic, but their use implies additional actions, such as extended clustering, rule base, and generally requires an expert in this particular subject domain.

At present, artificial neural networks represent the most actively developing section of intelligent data analysis techniques [4]. Their application in the field is considered the most promising.

The paper [5] proposes two-stage processing of incoming information. The first stage deals with the reduction of a vector length of incoming data through nonlinear recirculating neural network, while the second stage covers the attack detection using multilayer perceptron, which processes the

confined space of incoming images in order to detect the type of attack. This approach requires preliminary analysis of network parameters for further development of a nonlinear recirculating neural network.

The authors of paper [6] focus on search and extraction of informative features, their compression using the principal component analysis and recirculating the neural network and further application of two-layer perceptron and the Kohonen network based on selected features of data vectors. However, this approach significantly increases time complexity when adapting the network to detect new types of network attacks.

The paper suggests an IDS structure and application of the artificial neural network based on adaptive resonant theory (ART) to provide for the solution of traffic analysis.

2. Description of general network attack detection systems

The proposed intrusion detection system includes two types of modules:

- data acquisition and connection management modules;
- network analysis modules.

Figure 1 shows the general scheme of the network analysis module within the detection system in local area networks (LAN).

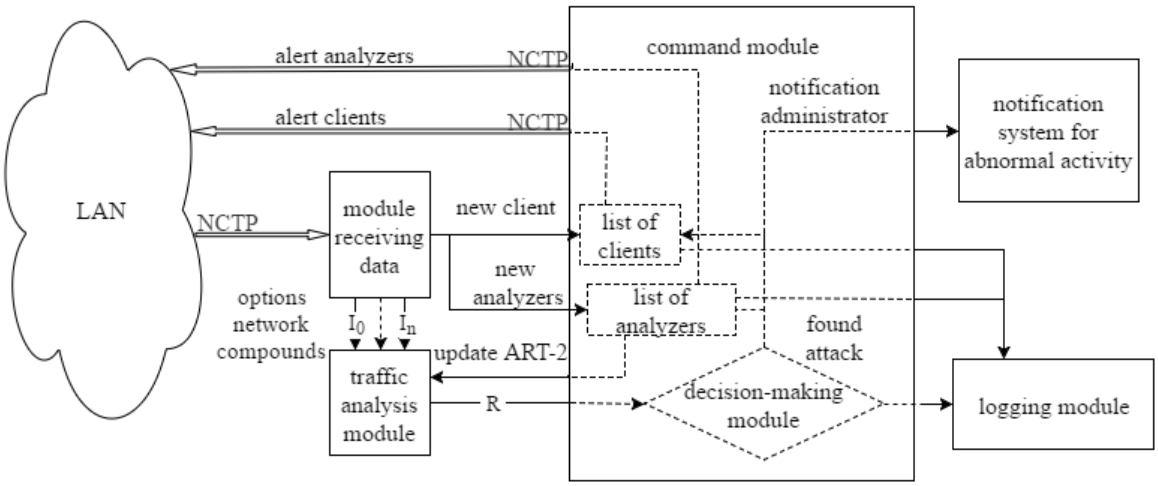


Figure 1. General scheme of network analysis module

As Figure 1 shows, the network analysis module consists of the following parts: a data receiving module, a traffic analysis module, a command module, a notification system for abnormal activity, a logging module.

The data receiving module is intended to receive information collected by client modules of data acquisition and connection management. The received data represent a vector of 41 parameters of the network connection supported by the client module. The received data are transmitted to the traffic analysis module.

The traffic analysis module includes a neural network based on adaptive resonant theory. The ART-2 network allowing to work with the input vectors consisting of real numbers was chosen for this system. The network determines memberships to a network connection cluster, which are typical for normal or abnormal network status. The abnormal network status is understood as the condition under which illegal acts are performed, i.e. one of the network attacks considered in KDD'99 selection is made [7].

The result of the analysis module is transmitted to the command module. The command module consists of the following parts: a decision-making module, attack notification of client modules of data acquisition and connection management, attack notification of other analytical modules.

In case the network attack is detected, the command module notifies all client modules of data acquisition and connection management on the attack, and sends a command to reject network connection with a source of attack for the time specified in the system settings. Besides, the analytical module, which detected the attack of the network or its regulating network segment, delegates the notification task of data acquisition and connection management modules, not belonging to its client list, to other analytical modules by notifying on the attack.

The decision on the response to the detected attack is made in a semi-automatic mode: if the attack belongs to the list of permanently blocked attacks specified in system settings, then the attack is blocked without the operator; if the attack does not belong to the above-stated list, then the decision on blocking the source of the attack is made by a network administrator or an expert dealing with information security of an enterprise network.

The system of abnormal activity notification is aimed to notify the network administrator on the attack.

The logging module is intended to record all connections processed by this analysis module.

All system nodes are connected through the secure channel formed according to NCTP protocol [8].

Figure 2 shows the general diagram of the data acquisition and connection management module.

As shown in Figure 2, the data acquisition and connection management module consists of the following parts: a network traffic aggregation module, a data transfer module to the analyzer, a connection management module, and an interpreter command analyzer.

The module of network traffic aggregation is used as a capture of network packets and analysis for membership of a particular connection. After these actions are performed, the analyzed parameters of the appropriate connection are updated.

The data transfer module to the analyzer is used to transmit input and output network connection parameters provided by the aggregation module for further analysis. Parameters are sent once over the period at intervals specified in the settings.

If the data passing through a network serve the analysis module command, then it is transmitted to the interpreter command analyzer, i.e. to the connection management module. The interpreter command analyzer is used for the following:

- to reject certain network connections for some period;
- to perform actions in case of attack specified in the settings;
- to perform actions specified in the settings for a particular attack upon its detection.

The connection management module operates network connections of the workstation, into which the module of data acquisition and connection management, is inbedded.

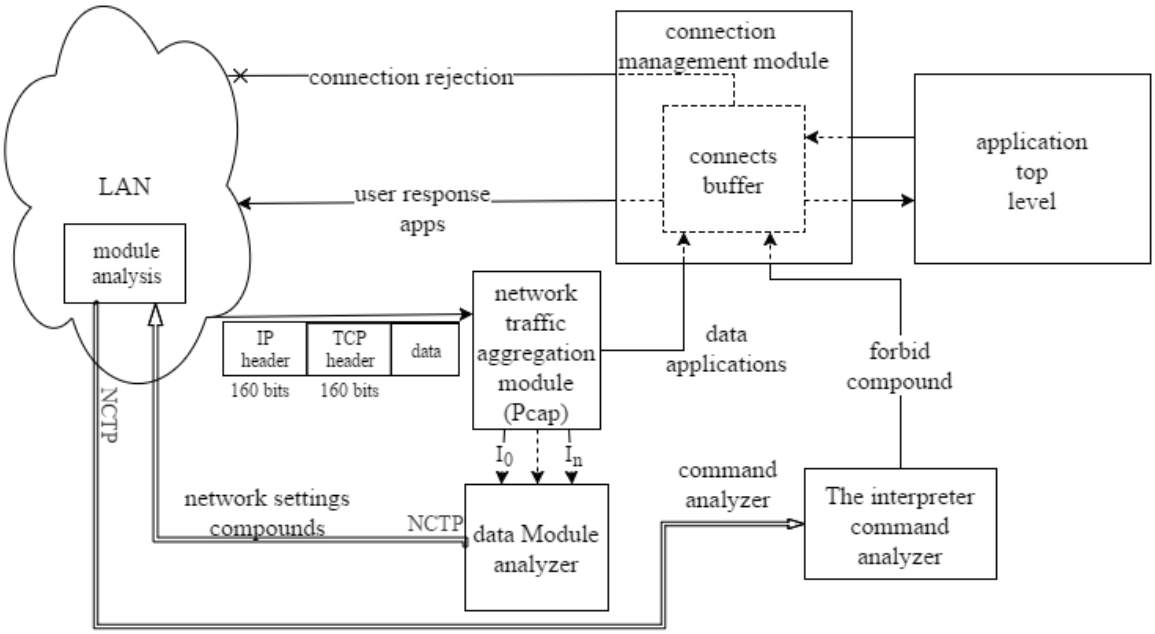


Figure 2. General scheme of data acquisition and connection management module

The connection management module consists of the following:

– buffer of current connections;

– logic allowing one to reject network connections, which were marked as a network attack by the analytical module.

3. Description of traffic recording system

The PCap library (Packet Capture) is used to collect the network traffic [9]. This library is based on BPF technology [10]. It consists of the following main parts: network trap, BPF filter, saving buffer, time delay buffer. Psap library allows considerably reducing time to receive the traffic. Paper [11] provides an example of using the PCap driver and its modification WinPCap to collect parameters of a network traffic.

It is suggested to highlight 41 traffic parameters according to the description made at the International Knowledge Discovery and Data Mining Tools Competition [7] for further analysis. Key parameters are as follows: connection duration in seconds; transfer layer protocol (tcp, udp, etc.); application layer protocol (http, telnet, etc.); quantity of received data bytes; quantity of transmitted data bytes; connection status (successful or failed); accuracy of packet fragmentation; number of failing authorization attempts; whether the user that sent a request is authenticated; whether packets include commands for remote code execution, etc. This approach can be considered redundant. There are other approaches that reduce the quantity of analyzed parameters without the loss of accuracy [5], however this considerably complicates the overall architecture of the analysis module and, potentially reduces its efficiency.

4. ART-2-based approach to network traffic analysis

In 1976, S. Grossberg made general assumptions on the adaptive resonant theory (ART), which were later described in detail in his fundamental study [12]. The main idea is that the image recognition is the result of partial or full compliance of weight states of one of the trained recognition neurons with the input normalization vector, i.e. access of sensor and recognition network layers into a resonance. Such resonance is assessed by control neurons. If it is sufficient, i.e. exceeds a pre-determined

threshold, then it is believed that the compliance between the data entry vector and an image from a network memory is established. Otherwise, the control layer freezes the resonant neuron of the recognition layer and the recognition procedure is repeated. If at the end, all neurons of the recognition layer are frozen, then the new neuron is added to this layer and its weights are trained to ensure maximum compliance to the input data vector, i.e. there is additional training of a network. Thus, the system proposes to acquire new knowledge without disturbing the existing one.

Figure 3 shows the diagram of the ART-2 neural network. At the input, this network accepts vectors of real numbers.

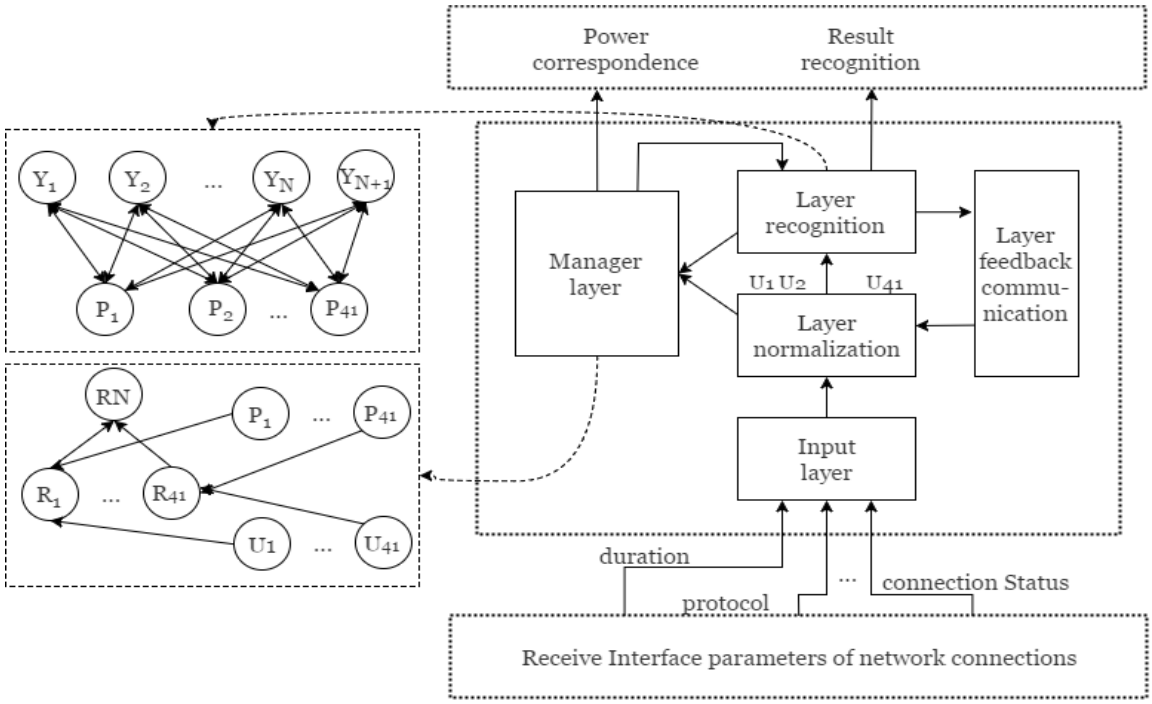


Figure 3. Network Diagram ART-2 to detect network attacks

Each input vector contains 41 network parameters allocated from the traffic. Then, input data normalization takes place in the normalization block. The received vector is combined with feedback information of the recognition layer. After normalization, data get into the group of neurons of the P recognition layer. Then, values of neurons of the Y layer are calculated on the basis of the corresponding link weights from P to Y:

$$Y_j = P_i \times z_{ij};$$

where z_{ij} – link weight from P_i to Y_j; $j = (1..N)$; $i = (1..41)$; N – amount of neurons in the Y layer.

The maximum values are defined for neurons of the Y layer. Then neurons of the P layer are corrected using link weights from the chosen maximum neuron of the Y layer:

$$m = \max(Y);$$

$$P_i = U_i + d \times z_{mi};$$

where $\max()$ – function returning the index of the maximum neuron from the Y layer; $i = (1..41)$; U_i – output neuron of the normalization layer, d – constant equals 0.9.

The received result is estimated via calculation of the group of neurons R of the control layer based on values of output vectors of normalization and recognition layers:

$$R_i = U_i + c \times P_i;$$

where $i = (1..41); c = 0{,}1$.

Then, norm RN of vector R is calculated and its compliance to the threshold value of network accuracy is defined. If RN does not satisfy the threshold value, then the chosen neuron of the Y layer is frozen, and the recognition repeats once again without it unless all neurons are frozen or unless a neuron, which result of recognition would satisfy the threshold value, is found:

$$RN = \| R \|,$$

$$vagilance / (eps + RN) < 1;$$

where $vagilance$ – threshold value, eps – small number to prevent division by zero.

If as a result of repeated recognition, all neurons of the Y recognition layer are frozen, then the new neuron is added to neurons of the Y layer and its link weights with neurons of the P layer are trained.

To solve the task of traffic analysis and detect network attacks, the ART-2 networks have the following key features:

– possibility to create a new class of recognition vectors in case of discrepancy of an input vector to any existing class;

– lack of the need for full network retraining to add new information;

– only one image, received as a result of allocation of general image properties of a training selection, is stored in the weight of each neuron of the recognition layer.

5. Application of ART-2 network to detect network attacks

The paper describes some experiments using KDD'99 test selections based on the above-mentioned approach. The ART-based neural network was trained using test selection of 489296 data vectors. Table 1 shows the quantity of data vectors for each group of network status in the training and full selections and a group belonging to a class of network status. It also specifies the recall ratio of training selection concerning all tested vectors. The recall ratio is the relation of vectors in the training selection to vectors in test selection.

Table 1. Number of training and test data vectors for every type of attack

Group of network status	Class of network status	Number of vectors in training selection	Number of vectors in test selection	Recall ratio
normal	normal	93480	640216	0.15
smurf	dos	280790	1295481	0.22
ipsweep	probe	1244	3701	0.34
multihop	r2l	4	2	1
guess_passwd	r2l	53	52	1
buffer_overflow	u2r	22	12	1
portsweep	probe	1038	6361	0.16
pod	dos	264	87	1
phf	r2l	4	3	1
warezmaster	r2l	2	20	0.1
perl	u2r	3	2	1

satan	probe	1586	15762	0.10
nmap	probe	231	1998	0.12
rootkit	u2r	9	7	1
neptune	dos	107031	387229	0.28
loadmodule	u2r	6	8	0.75
imap	r2l	12	2	1
back	dos	2203	101	1
teardrop	dos	979	397	1
land	dos	21	6	1

The experiment was made on a test selection of 2351447 vectors in size. Table 2 shows the general results of an experiment on network status recognition. In case the system detected an attack, but did not indicate the correct group to which it belongs, then it was considered that the attack is not detected correctly.

Table 2. Results of experiment on network status recognition

Network status	Recall ratio	Recognition rate
Normal status	0.14	0.96
Attack status	0.09	0.98

Table 3 shows the detailed results of an experiment on network status recognition. The results demonstrate that not all classes of attacks were sufficiently recognized. It should be noted that such attacks as multihop, guess_passwd, buffer_overflow, perl, rootkit, loadmodule, imap total to approximetely 0.003% of selection, and correspondingly they are also present in the training selection. Thus, there were not enough samples for network training to recognize these types of attacks; however, due to their rarity a mistake in their recognition could be neglected.

Dos attacks formed the main group of attacks in test selection. The attacks of this group were detected and correctly classified with an error of a mere 0.15%. The next group of network states following in value is the normal state - the error of its recognition reached 3.6%.

Table 3. Detailed results of experiment on network status recognition

Group	Class	Recall ratio	Recognition rate
normal	normal	0.15	0.96
smurf	dos	0.22	0.99
ipsweep	probe	0.34	0.74
multihop	r2l	1	0
guess_passwd	r2l	1	0.01
buffer_overflow	u2r	1	0
portsweep	probe	0.16	0.87
pod	dos	1	0.11
phf	r2l	1	0

warezmaster	r2l	0.1	0.48
perl	u2r	1	0
satan	probe	0.10	0.01
nmap	probe	0.12	0.07
rootkit	u2r	1	0
neptune	dos	0.28	0.99
loadmodule	u2r	0.75	0
imap	r2l	1	0
back	dos	1	0.03
teardrop	dos	1	0.11
land	dos	1	0.76

Paper [6] describes the experiment with Kohonen networks and a two-layer perceptron using the same test selection (KDD'99). However, the authors ensured network training using the entire test sample, which is confirmed by the recall ratios of experiments. Table 4 shows comparative results of recall ratios and recognition rate for some classes of attacks.

Table 4. Recognition rate for some classes of attacks and recall ratios of a test sample in experiments with various neuron networks

Group of network status	Class of network status	ART, recall ratio	ART, recognition rate	Two-layer perceptron, accuracy	Kohonen network, accuracy
normal	normal	0.15	0.96	0.9998	0.9969
smurf	dos	0.22	0.99	1	1
neptune	dos	0.28	0.99	1	1
portsweep	probe	0.16	0.87	0.9341	0.9987
land	dos	1	0.76	0.8947	1
ipsweep	probe	0.34	0.74	0.9271	0.99
warezmaster	r2l	0.1	0.48	0.0884	1
teardrop	dos	1	0.11	0.9975	1
nmap	probe	0.12	0.07	0.7694	0.6871
back	dos	1	0.03	0.8743	0.7224

In most cases the recall ratio of the training selection described in [6] was 10 times higher than in the experiment conducted within the present study. At the same time, the recognition rate of attacks for the most widespread classes using ART-2 network turns to be much lower than the Kohonen network and the two-layer perceptron. Low indicators for teardrop, nmap and back attacks are explained by a small number of such attacks both in test and complete samples.

6. Conclusions

The study covered an approach to the intrusion detection system of network attacks using neural networks based on adaptive resonant theory. Experiments with the ART-2 network to detect and classify the attacks from KDD'99 test selection were made. The general results of an experiment and their comparative analysis with results of similar experiments using the two-layer perceptron and Kohonen network show that the ART-2 network can be applied to detect and classify the network attacks within the data network analysis module of the intrusion detection system.

The major challenge of this task is the definition of parameters. The study used the network traffic parameters in KDD'99 selection, but due to fast variability of transfer systems in computer networks, the definition of new parameters is advisable. Thus, the development of approaches to definition of network traffic parameters remains urgent.

It is planned to increase the recognition rate of input data vectors, rarely occurring in the training selection.

7. Acknowledgments

The article was prepared within the development program of the Flagship Regional University on the basis of Belgorod State Technological University named after V.G. Shukhov, using the equipment of High Technology Center at BSTU named after V.G. Shukhov; under the support of the Foundation for Assistance to Small Innovative Enterprises in Science and Technology (UMNIK Program) and RFBR grant № 16-07-00487.

References

[1] Key tendencies of cyberattacks 2015 according to Positive Technologies URL: http://www.securitylab.ru/news/476333.php
[2] Melnikov D A 2015 Information security of open systems. (Litres)
[3] Marenkov A N and Ajmuhamedov I M 2011 *Bulletin of the Astrakhan State Technical University* **1** 137-140
[4] Markov R A 2015 *Young Scientist* **23** 55-60
[5] Golovko V A and Bezobrazov C V 2011 *Open semantic technologies for the design of intelligent systems* (OSTIS-2011) pp. 185-196
[6] Emelyanova Y G 2011 *Software systems: theory and applications* **2(3)** 3-15
[7] KDD-99 International Conference on Knowledge Discovery and Data Mining. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[8] Bukhanov D G and Polyakov V M 2016 *Science and Technology. Telecommunications* **3** 35-41
[9] Risso F and Degioanni L 2001 *Computers and Communications. Proceedings. Sixth IEEE Symposium on – IEEE* pp. 686-693
[10] Watson R N M, Peron C S J and Summit F D 2007 *FreeBSD Developer Summit* pp. 12
[11] Bukhanov D G, Polyakov V M, Uskov D A and Daeef F 2016 *ISJ Theoretical & Applied Science* **1(21)** 139-144
[12] Carpenter G A, Grossberg S and Rosen D B 1991 *Neural networks* **4(4)** 493-504