computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

FUSION OF RECIRCULATION NEURAL NETWORKS FOR REAL-TIME NETWORK INTRUSION DETECTION AND RECOGNITION

Pavel Kachurka, Vladimir Golovko

Brest State Technical University
Moskovskaya str. 267, 224017, Brest, Republic of Belarus
e-mail: paulermo@gmail.com, gva@bstu.by
http://www.bstu.by

Abstract: *Intrusion detection system is one of the essential security tools of modern information systems. Continuous development of new types of attacks requires the development of intelligent approaches for intrusion detection capable to detect newest attacks. We present recirculation neural network based approach which lets to detect previously unseen attack types in real-time mode and to further correct recognition of this types. In this paper we use recirculation neural networks as an anomaly detector as well as a misuse detector, ensemble of anomaly and misuse detectors, fusion of several detectors for correct detection and recognition of attack types. The experiments held on both KDD'99 data and real network traffic data show promising results.*

Keywords: *Intrusion detection, classification, artificial neural networks.*

1. INTRODUCTION

An increasing role of network information technologies in human activities leads to a rising level of attention to such technologies from evildoers. The average level of expenses of legitimate users in case of successful attack increases too. Every second organization has been attacked during 2009-2010 years and 45% of them were victims of targeted attacks [1]. The global damage from computer attacks in 2011 is expected to be higher than $250 billion [2].

In popular proprietary or open source intrusion detection systems (IDS) mostly signature search and rule-based analysis [3–6] is used. Its shortcoming is the insufficient flexibility at detection of the modified and unknown attacks. A large number of methods for analyzing network activity by means of various technologies of data mining exist. Researchers widely use decision trees [7], Bayesian networks [8], hidden Markov models [9], fuzzy logic [10], artificial immune systems [11], support vector machines [12] and other techniques.

One of the technologies with promising results bases on the use of artificial neural networks (ANNs). ANNs have been declared alternatively to components of the statistical analysis of systems of anomaly detection. Neural networks have been specially suggested to identify typical characteristics of users of system and statistically significant deviations from the established operating mode of the user. Many different ANN architectures can be used to detect and classify the intrusions. Comparative studies [13–14] researchers conclude that every architecture has its own advantages and disadvantages but Adaptive Resonance Theory (ART) networks and Multi-layer Perceptrons (MLP) show better results most often. Recent researches try to utilize classic NN architectures [15] or PCA neural networks [16–17], to create hierarchical ANN-based IDS [18–22], to combine different ANNs with other approaches [23–24], incl. flow traffic analysis [25].

Different approaches are compared using wide known KDD'99 database [26] from processed DARPA 1998 Intrusion detection evaluation database. It contains more than 4 million records describing TCP-connections. The given data base includes normal connections and the attacks of 22 types belonging to four classes: DOS – «denial-of-service» – refusal in service, for example, a Syn-flood; U2R – not authorized access with root privileges on the given system, for example, various attacks of buffer overflow; R2L – not authorized access from the remote system, for example, password selection; Probe – analysis of the topology of a network, services accessible to attack, carrying out search of vulnerabilities on network hosts.

Table 1 shows that mentioned techniques show good results as in detection of known attacks. But

during the detection of new attacks the FNR and FPR can raise up to 30-50% [24]. The quality of attack class recognition is shown in Table 2. You can see that ANN-based approaches operate better than others.

Table 1. Best Results In Attack Detection

Approach	FNR, %	FPR, %
Flexible Neural Tree [17]	1,2	0,3
MLP [22]	5,8	0,8
Clasterisation[12]	7	10
K-NN [12]	9	8
SVM [12]	2	10

Table 2. Best Results In Attack Recognition

Approach	dos, %	probe, %	r2l, %	u2r, %
Gaussian classifier	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Decision Trees [18]	99,8	50,0	33,3	50,0
Bayesian Networks [18]	99,7	52,6	46,2	25,0
Flexible Neural Tree [17]	98,8	99,3	98,8	99,9
Fuzzy NN [19]	100,0	100,0	99,8	40,0
MLP [18]	99,9	48,1	93,2	83,3
RBF [20]	98,8	98,0	97,2	–
Hierarchy of PCA Networks [21]	100,0	100,0	97,2	–
PCA Networks & SOM [21]	99,0	75,2	77,0	–
Hierarchy of SOM [20]	96,9	81,3	0,0	1,1

Most of IDS techniques use only anomaly detection or only misuse detection. The combination of this approaches can show better results than the systems using them separately. The goal of this study is to build IDS capable to 1) detect and recognize known attacks with the accuracy comparable to the best shown above; 2) detect previously unseen attacks with low false positive and negative rates; 3) combine anomaly and misuse detection in one technique.

In this paper the neural network based approach to anomaly and misuse detection on the basis of the analysis of the network traffic is described. The algorithm of IDS functioning is discussed and the building of working prototype is described.

The paper is organized as follows. The anomaly detectors based on recircular neural networks (RNNs) are described in the section 2. The misuse detectors are described in the Section 3. The joint functioning of anomaly and misuse detectors in one ensemble is discussed in the Section 4. Section 5 presents the fusion classifier bsed on previously discussed detectors. Test results of presented approaches on KDD'99 dataset are presented in Section 6. The structure of IDS prototype and its testing on real data are presented in Section 7. The conclusion is made in Section 8.

2. RNN-BASED ANOMALY DETECTORS

There are two technologies in intrusion detection: anomaly detection and misuse detection. Their basic difference consists that at use of the first the normal behavior of the subject is known and deviations from this behavior are searched while at use of the second attacks which are searched and distinguished among normal behavior. Both techniques eliminate each other's defects, owing to what the best results of detection can be reached only applying them simultaneously, within the limits of different IDS subsystems or with use of the combined detection methods.

It is proved [27], what the best results at classification (even a question – «attack or not?» is definition of an accessory to a class of attacks or a class of normal connections; not speaking already about definition of a class of attack) give classifiers independent from each other. There are much more abilities for construction of a cumulative estimation of the general classifier at use of independent detectors of the identical nature.

Recirculation neural networks (see Figure 1) differ from others ANNs that on the input information in the same kind is reconstructed on an output. They are applied to compression and restoration of the information (direct and return distribution of the information in the networks «with a narrow throat»), for definition of outliers on a background of the general file of entrance data.

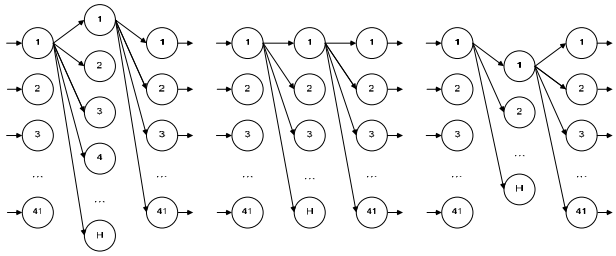

Fig. 1 – 3-layered RNN Architecture

Nonlinear RNNs have shown good results as the detector of anomalies: training RNN is made on normal connections so that input vectors on an output were reconstructed in themselves, thus the connection is more similar on normal, the less reconstruction error is:

$$E^k = \sum_j (\bar{X}_j^k - X_j^k)^2, \qquad (1)$$

where X_j^k – j-th element of k-th input vector, $\overline{X}_j^k$ – j-th element k-th output vector. Whether $E^k > T$, where T – certain threshold for given RNN

connection admits anomaly, or attack, differently – normal connection (see Figure 2). Thus there is a problem of a threshold T value determination, providing the most qualitative detection of abnormal connections. It is possible to get threshold value minimizing the sum of false positive (FP) and false negative (FN) errors, basing on cost characteristics of the given errors – FN error seems to be more expensive, than FP error, and its cost should be higher.

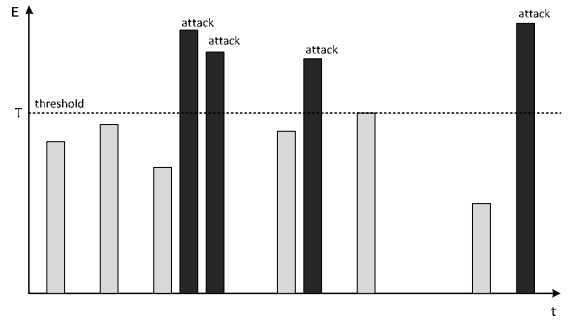

Fig. 2 – RNN-based anomaly detection

3. RNN-BASED MISUSE DETECTORS

The described technique of definition of an input vector accessory to one of two classes – "normal" or "attacks", that is "not-normal" – it is possible to use in opposite way. If at training the detector of anomalies we used normal vectors which were restored in itself, and the conclusion about their accessory to a class "normal" was made, training the detector on vectors-attacks which should be restored in itself, it is possible to do a conclusion about their accessory to a class of "attack". Thus, if during functioning of this detector the reconstruction error (1) exceeds the certain threshold, given connection it is possible to carry to a class "not-attacks", that is normal connections. As training is conducted on vectors-attacks the given approach realizes technology of misuse detection, and its use together with previous technique is righteous.

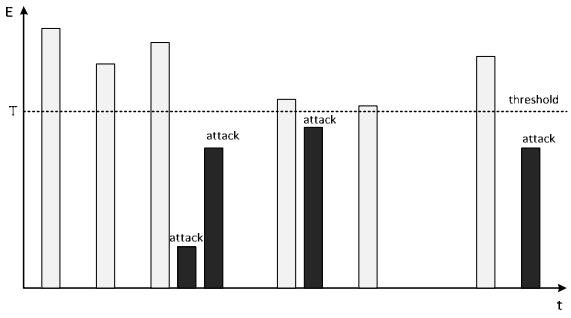

Fig. 3 – RNN-based misuse detection

Thus, one RNN can be applied to definition of an accessory of input vector to one of two classes – to on what it was trained or to the second class, to which outliers correspond.

4. ENSEMBLE OF RNN-BASED ANOMALY AND MISUSE DETECTORS

As it was mentioned above anomaly detectors can function with high False Positive Rate while the misuse detectors can skip targets not belonging to training database. The use of two approaches within one system helps to avoid the disadvantages of each technology without losing their dignity. This will reduce I-type and II-type errors increasing accuracy of prediction.

If anomaly and misuse detectors base on different approaches then the problem of the complexity of final decision exists. The biggest problem in such approach is to make decision when the attack was detected only by one detector.

Ensemble made of two RNN-based detectors – anomaly detector and misuse detector described above – lets to analyze not only binary vectors of their decisions but to construct the decision basing on their output data. In the terms of RNN-based detectors it means that we can compare reconstruction errors of anomaly and misuse detectors (see Figure 4):

$$\begin{cases} X \in A_N, \ \ если \ \ E_{\text{A}} \le E_3, \\ X \in A_P, \ \ если \ \ E_A > E_3, \end{cases} \tag{2}$$

where E_A – reconstruction error on the anomaly detector, E_3 – reconstruction error on the misuse detector, A_N – normal connections (negative), A_P – attacks (positive).

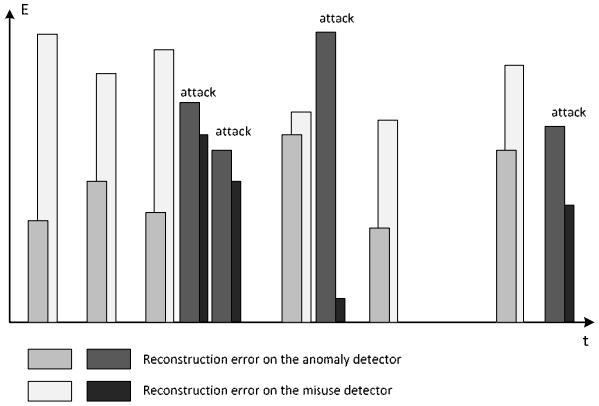

Fig. 4 – RNN ensemble-based intrusion detection

This approach requires equal quantity of synaptic connections in the detectors and equal MSE achieved during the training phase. Opposite reconstruction errors can become incomparable that leads to decision making basing on the private decisions of every detector.

5. FUSION OF RNN-BASED CLASSIFIERS

As it was told above the best classification results can be achieved using several independent classifiers of the identical nature because construction of the general estimation from private can be made by greater number of methods. We shall unite the private detectors trained in the previous section in one general.

The main idea of this approach is that every new detector can be trained using the data samples not recognized by the operating detectors. In such a way general classifier can grow from one normal detector to many parallel neural detectors (see Figure 5).

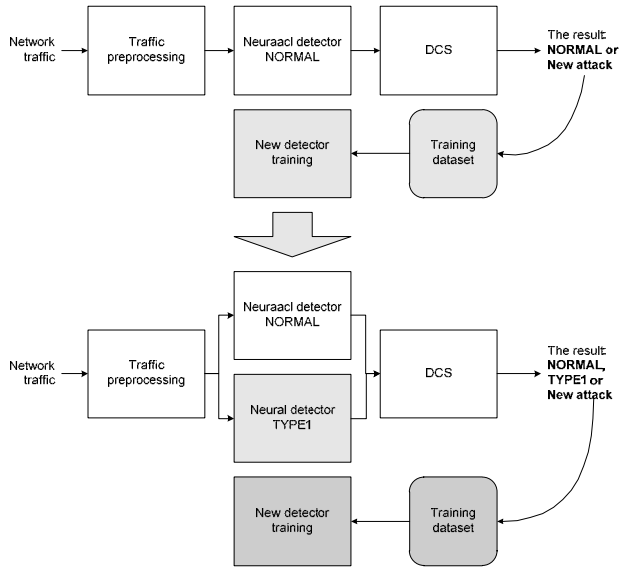

Fig. 5 – General Classifier Generation

The general classifier consists from N private detectors, each of which has a threshold T. To make estimation values comparable it is enough to scale reconstruction error on a threshold to get the relative reconstruction error:

$$\delta_i^k = \frac{E_i^k}{T_i}. \qquad (3)$$

Thus, than less δ_i^k is, the probability of accessory of an input image X^k to a class A_i is higher.

6. RNN-BASED APPROACH TESTING ON KDD'99 DATASET

KDD'99 dataset [26] contains almost 5 million connection records and only 20% of them represent normal network traffic. As for the main test dataset ("ALL") we shall use 10%-sample of KDD database. It contains 494020 connections including attacks of 22 types.

For validation of the possibility to detect unknown attacks we shall add test dataset "ALL-NEW" made of records from the KDD'99 testing data set. It includes 32 types of attacks and normal connections which are absent in the KDD'99 training dataset.

RNNs will be trained using layered training method using training data sets described in Table 3.

Table 3. Datasets description

Dataset	*P* No. of attacks	*N* No. of normal	No. of connection types	
			K Total	No. of attack types
Testing data sets				
ALL	396743	97277	23	22
ALL-NEW	250436	60592	33	32
Training data sets				
Normal connections	*0*	500	1	0
Attacks	4400	0	22	22

To train anomaly detectors on the normal traffic 500 random normal connections are selected as well as to train misuse detectors – 200 random connections for each attack type are selected.

The training and testing phases where made on several 3-layer and 5-layer RNNs with different count of neurons in hidden layer. Test results show that the architecture of the neural networks does not affect the accuracy of prediction almost. In the Table 4 the test results of the 3-layer RNNs with 41 input and output neurons and 25 neurons in hidden layer are shown.

Table 4. Attack detection results on the KDD dataset

	FPR, %	FNR, %	ACC, %
ALL data set			
Anomaly	10,88	0,10	**97,78**
Misuse	0,10	2,73	**97,79**
Ensemble	0,03	1,83	**98,52**
ALL-NEW data set			
Anomaly	7,43	19,56	**82,80**
Misuse	0,17	19,56	**84,22**
Ensemble	0,00	12,33	**90,07**

As it can be seen from the Table 4, (1) the RNN ensemble-based approach detects attacks on benchmark KDD dataset with high accuracy; (2) ensemble performs better than every detector separately; (3) ensemble can detect unknown attacks.

Let's test the ability of the fusion of RNN-based classifiers to correctly detect and recognize attacks. The results are shown in the Table 5.

The results show that 97% of attack can be correctly recognized by the fusion of RNN detectors. The accuracy of prediction of such an approach is high enough.

Table 5. Results of attack detection and recognition by RNN-fusion on the KDD dataset

FPR, %	FNR, %	ACC, %	CR, %
12,50	0,01	97,53	97,41
dos, %	**probe, %**	**r2l, %**	**u2r, %**
99,87	96,76	99,73	98,08

7. RNN-BASED IDS TESTING ON THE REAL NETWORK DATA

Our IDS prototype is implemented for the operating system GNU/Linux using open source software BroIDS, mawk, bash, tee, gcc. For the training and testing purposes we have conducted the attacks of the following types: (1) *tcpscan* – the attack of Probe class, scans the open ports of the victim using TCP-connections; (2) *synflood* – DoS-attack, tries to flood the victim with the SYN packets of TCP connections; (3) *udpflood* – DoS-attack, floods the victim with UDP packets. The training datasets contain 500 collected connections for each class.

Data Preprocessing. IDS receives a records of all network connections formed with the help of Bro IDS from host's traffic. Bro is an open source intrusion detection system which performs a modified script for obtaining records of the connections which include the following fields: timestamp, duration of connection in seconds; source's and destination's IP-address; name of the service used; port numbers; the number of bytes transferred; the result flag of the connection.

Bro consistently generates connection strings which are piped to the pre-processing module (see Figure 6). Further, the obtained connection lines are handled consistently by several scripts in awk, which form the records similar to KDD database [26] records, encode categorical parameters and normalize input data. The resulting row of numbers is used as the input vector to RNN-based detectors.

```
61.674526 192.168.2.20 74.125.10.225 http 51450
80 tcp 989 20105 SF X ShADadfFR
↓
61 tcp http 989 20105 SF 0 0 0 1 0 0 0 1 1 1
↓
61 1 20 989 20105 1 0 0 0 1 0 0 0 1 1 1
↓
0.85635375 0.50000109 0.78600832 0.95235664
0.98665665 0.50000109 0.0066928509 0.0066928509
0.0066928509 0.50000109 0.0066928509
0.0066928509 0.0066928509 0.50000109 0.50000109
0.50000109
```

Fig. 6 – Data Preprocessing

Neural Detectors' Training. Each particular detector is a nonlinear recirculation neural network with one hidden layer. Learning algorithm and the functioning of RNN is implemented in C and as a result IDS has speed adequate to assess the functioning of the prototype system in real time.

RNNs are trained using the method of layer-learning. Then the initial threshold value for a particular detector is set equal to the value at which 5% of the images of the training sample gives a reconstruction error above the threshold. After this threshold adjustment neural detector is able to determine the membership of its class with up to 95% in real time mode.

Time and quality of training depends on the number of images in the training set. Table 6 shows the results of thresholds setting for the detectors of the three classes when applied to the input detector images of the training sample.

Table 6. Threshold Adjustment Results

Class A_i name	DR_i, %	Threshold T_i
Normal	94,6	0.819415
tcpscan	94,8	0.835775
synflood	94,8	0.785963

Private Detectors Functioning and Generation. Trained and configured neural detectors calculate the relative reconstruction error and conclude probability of belonging of the input image to the class.

The result of the private detector is a string containing a timestamp to identify a specific connection; the name of the class, which is responsible for this detector; the absolute error of reconstruction of input images; the relative error of reconstruction of the input image, which will be used to decide to witch class image belongs. If the relative error of reconstruction is greater than 1, then the image is saved for possible future participation in new detector training.

Table 7 shows the results of the analysis of three classes by private detectors. Every connection was fed to the detectors of two classes to which this connection does not belong. The successful decision in this case is result more than 1 on every detector. It shows that this algorithm can be successfully used for anomaly and unknown attack detection.

Table 7. Anomaly Detection Quality

Real / Predicted	normal	tcpscan	synflood
normal		100,00%	31,00%
tcpscan	98,20%		84,00%
synflood	99,40%	94,40%	

At the beginning of its operation IDS has only one source of data: normal network traffic. Neural detector trained on this traffic begins to detect anomalies in network connections. For example, all tcpscan connections were correctly identified as an

anomaly (see Table 8), and saved for new detector training like a training sample.

As seen from Table 5 quality of detection of synflood images as anomalies at the normal-detector is quite low – only 31%. But in the opposite synflood- detector detects anomalies in normal connections with an accuracy of 99.4%. By combining these detectors into a single system in accordance with Section 3, we can obtain a significant increase in quality of recognition.

Nevertheless, we can conclude that the quality of anomaly detection and therefore – detection of unknown attacks by private normal-detector is high enough.

In case none of detectors operating in the IDS predicted input image as belonging to its class IDS accumulates image for a training of new detector.

Attack Recognition. This module accumulates the results of analysis of input image by all currently functioning private detectors. It is worth noting that the detectors operate in parallel mode. If all the relative errors are greater than 1 it is concluded that the connection may not belong to either of these classes. Mode of recognition of a new class can be turned off and then even among relative errors greater than 1 the smallest one will be chosen.

Table 8 and 9 show the quality of attack detection and recognition on the training datasets and in the real-time testing.

Table 8. Attack Detection and Recognition on the Training Datasets

	W/out new class gen.			With new class gen.		
	FN_K,%	FN_U,%	FP,%	FN_K,%	FN_U,%	FP,%
normal tcpscan	0,40	87,60	1,60	0,00	63,00	2,40
normal synflood	0,00	90,80	0,60	0,00	0,00	40,20
normal synflood tcpscan	0,04		1,80	**0,00**		**8,60**

Table 9 Attack Detection and Recognition in Real-Time Mode

	W/out new class gen.			With new class gen.		
	FN_K,%	FN_U,%	FP,%	FN_K,%	FN_U,%	FP,%
normal					7,68	1,22
normal tcpscan	0,20	100,0	0,98	0,28	10,70	1,22
normal synflood	14,72	33,32	0,73	4,72	0,10	7,82
normal synflood tcpscan	1,09	48,44	1,22	**1,09**	**0,01**	**8,81**

8. CONCLUSION

The results of experiments presented in Section 6 and Section 7 let us to make the following conclusions.

RNN-based anomaly and misuse detectors separately perform with good accuracy but the best accuracy can be achieved when used both of them. The use of RNN-based ensemble of anomaly and misuse detector allows to detect known attacks with superior accuracy 98% and to detect previously unseen attaks with good accuracy 90%.

The fusion of RNN-based classifiers is the evolution of the ensemble. Fusion classifier allows not only to detect but also to recognize the attack. Like an ensemble it can detect and recognize network intrusions previously seen in the training dataset (see Figure 7) and totally unknown and the quality of recognition is high enough. Unlike an ensemble where the decision is made by the absolute reconstruction error in the fusion classifier decision is made by the relative reconstruction error. It allows to tune classifier's accuracy using methods of threshold selection.

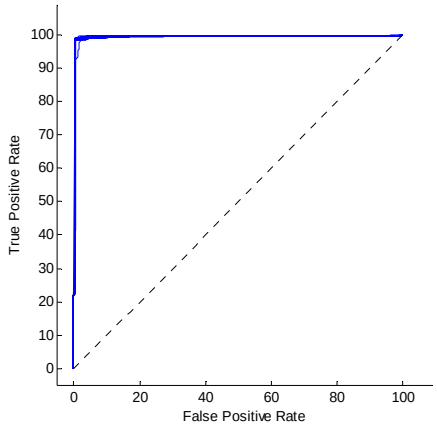

Fig. 7 – ROC of Known Attack Detection Using RNN-based Ensemble

Tests on the real network data prove that this technique can be used for building real-time intrusion detection systems. The main promising result of presented technique is that both anomaly and misuse detection simultaneously can successfully detect known and previously unseen network intrusions.

9. REFERENCES

[1] CSI Computer Crime and Security Survey 2010 [Electronic resource] Mode of access: http://gocsi.com/survey. – Date of access: 11.01.2011.

[2] Proposal for a Regulation of the European Parliament and Council concerning the European Network and Information Security Agency (ENISA) [Electronic resource] Mode of access: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf. – Date of access: 11.01.2011.

[3] J. Beale and Caswell. *Snort 2.1. Intrusion Detection*. – 2-nd ed. – Syngress Publishing, Inc. 2004.

[4] Prelude SIEM. [Electronic resource] Mode of

access: http://www.prelude-technologies.com/en/welcome/index.html. – Date of access: 12.01.2011.

[5] Cisco Intrusion Detection [Electronic resource] Mode of access: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml. Date of access: 12.01.2011.

[6] Bro Intrusion Detection System [Electronic resource] Mode of access: http://www.bro-ids.org/. Date of access: 12.01.2011.

[7] J. Frank, Artificial intelligence and intrusion detection: Current and future directions, The 17th National Computer Security Conference, Baltimore, MD, 1999 / National Institute of Standards and Technology (NIST). – 1999.

[8] C. Srilatha, A. Ajith, Th. Johnson, Feature deduction and ensemble design of intrusion detection systems, *Computers & Security*, (24) (2005), pp. 295-307.

[9] T.D. Lane, *Machine Learning Techniques for the Computer Security Domain of Anomaly Detection,* Ph. D. Thesis, Purdue Univ., West Lafayette, IN, 2000.

[10] J.E. Dickerson, J.A. Dickerson, Fuzzy intrusion detection, *IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conf.: proceedings*, Vancouver, Canada, July, 2001. – North American Fuzzy Information Processing Society (NAFIPS), (Vol. 3), (2001), pp. 1506-1510.

[11] S.A. Hofmeyr, S. Fo, Immunizing computer networks: Getting all the machines in your network to fight the hacker disease, The 1999 IEEE Symp. on Security and Privacy: proceedings, Oakland, CA, 1999. – IEEE Computer Society Press, 1999.

[12] E. Eskin, A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data, *Data Mining for Security Applications*; Eds.: D. Barbar, S. Jajodia, Boston, Kluwer Academic Publishers, 2002.

[13] A. Iftikhar, A. Azween, A. Alghamdi, Towards the selection of best neural network system for intrusion detection, *International Journal of the Physical Sciences*, (5) 12 (2010), pp. 1830-1839.

[14] A. Ali, A. Saleh, T. Badawy, Intelligent adaptive intrusion detection systems using neural networks (comparative study), *International Journal of Video & Image Processing and Network Security*, (10) 1 (2010).

[15] M. Pradhan, S.K. Pradhan, S.K. Sahu, Anomaly detection using artificial neural network, *International Journal of Engineering Sciences & Emerging Technologies,* (2) 1 (2012), pp. 29-36.

[16] Kh. Al-Nafjan, M.A. Al-Hussein, A.S. Alghamdi, M. Amanul Haque, and I. Ahmad, Intrusion detection using PCA based modular neural network, *International Journal of Machine Learning and Computing*, (2) 5 (2012), pp. 583-587.

[17] A. Jahanbani, H. Karimi, A new Approach for detecting intrusions based on the PCA neural networks, *Journal of Basic and Applied Scientific Research*, (2) 1 (2012), pp. 672-679.

[18] G. Liu, Z. Yi, S. Yang, A hierarchical intrusion detection model based on the PCA neural networks, *Neurocomputing*, 2007.

[19] L.O. Anyanwu, L. Keengwe, G.A. Arome, Scalable intrusion detection with recurrent neural networks, *International Journal of Multimedia and Ubiquitos Engineering*, (6) 1 (2011).

[20] H.G. Kayacik, A.N. Zincir-Heywood, M. Heywood, A hierarchical SOM-based intrusion detection system, *Engineering Applications of Artificial Intelligence*, 9 (2006), pp. 439-451.

[23] G. Liu, Z. Yi, S. Yang, A hierarchical intrusion detection model based on the PCA neural networks, *Neurocomputing*, 2007, pp. 1561-1568.

[24] T. Novosad, J. Platos, V. Snasel, A. Ajith, Fast intrusion detection system based on flexible neural tree, *proceedings of Sixth International Conference on Information Assurance and Security (IAS)*, USA, 2010, pp. 142-147.

[25] G. Wang, J. Hao, J. Ma, L. Huang, A new approach to intrusion detection using Artificial Neural Networks and fuzzy clastering, *Expert Systems with Applications*, (2) (2010).

[26] M.J. Muna, M. Mehrotra, Design network intrusion detection system usin hybrid fuzzy-neural network, *International Journal of Computer Science and Security*, (4) 3 (2010), pp. 258-294.

[27] A. Yousef, Z. Jovanovic, Flow-based anomaly intrusion detection system using neural network, *Proceedings of International Conference on Internet Computing, Informatics in E-Business and applied Computing (ICIEACS 2012)*, Bur Dubai, UAE, 2012.

[28] KDD Cup'99 Competition, 1999, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[29] G. Giacinto, F. Roli, L. Didaci, Fusion of multiple classifiers for intrusion detection in computer networks, *Pattern Recognition Letters*, 24, 2003, pp. 1795-180.

[30] S. Saravanakumar, Umamahchwari, D. Jayalakshmi, R. Sugumar, Development and

implementation of artificial neural networks for intrusion detection in computer network, *International Journal of Computer Science and Network Security*, (10) 7 (2010).

[31] P. Kachurka, V. Golovko, Neural network approach to real-time network intrusion detection and recognition, *Proceedings of The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, (15-17 September 2011), Prague, 2011, pp. 393-397.

Pavel Kachurka *was born in Belarus in 1982. He received PhD degree in 2012 from the Belarusian State University of Informatics and Radio-electronics. At present he works as an assistant professor at the Department of Intelligent Informational Technologies, Brest State Technical University (Belarus). His research interests include computer network security, data-mining, artificial intelligence and neural networks, networking and operating systems.*

Prof. Vladimir Golovko *was born in Belarus in 1960. He received M.E. degree in Computer Engineering in 1984 from the Moscow Bauman State Technical University. In 1990 he received PhD degree from the Belarus State Technical University and in 2003 he received doctor science degree in Computer Science from the United Institute of Informatics problems national Academy of Sciences (Belarus). At present he work as a head of Intelligence Information Technologies Department and Laboratory of Artificial Neural Networks of the Brest State Technical University. His research interests include Artificial Intelligence, neural networks, autonomous learning robot, signal processing, chaotic processes, intrusion and epilepsy detection. He has published more than 200 scientific papers, including books and chapters of books.*