Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System

Leanid Vaitsekhovich [1], Vladimir Golovko [2], Uladzimir Rubanau [2]
Brest State Technical University, Moskovskaja str. 267, 224017 Brest, Belarus
1) vspika@rambler.ru
2) gva@bstu.by

Abstract: *In this article the artificial immune system and neural network techniques for intrusion detection have been addressed. The AIS allows detecting unknown samples of computer attacks. The integration of AIS and neural networks as detectors permits to increase performance of the system security. The detector structure is based on the integration of the different neural networks namely RNN and MLP. The KDD-99 dataset was used for experiments performing. The experimental results show that such intrusion detection system has possibilities for detection and recognition computer attacks.*

***Keywords*:** Intrusion Detection, Neural Networks, Artificial Immune System, Principal Component Analyses, Multiagent Systems.

1. INTRODUCTION

Different defense approaches exist to protect computer systems. All approaches can be divided into two main groups: organizational and technical. Technical approaches consist of network and hostbased techniques. In this article we will discuss network security tools namely intrusion detection systems.

The aim of *Intrusion Detection Systems (IDS)* is detecting inappropriate, incorrect or anomalous activity in computer systems or computer networks.

There are a lot of different means to protect computer networks: correct policy of security, gateway filters, anti-virus software etc. But as a rule IDS is assigned the role of a basic element of protection. IDS are used for early notification about network problems because generally they are allocated at a network level where suspicious actions can be found out earlier, then at higher levels. Besides IDS is able to gather necessary evidences of malicious activity as well as to reveal latent tendencies. This becomes possible due to analysis of plenty of the data.

The major problems of existing models are recognition of new attacks, low accuracy, detection time and system adaptability. The current anomaly detection systems are not adequate for real-time effective intrusion prevention. Therefore processing a large amount of audit data in real time is very important for practical implementation of IDS. It is difficult to eliminate stated disadvantages using only classical computer security methods. Therefore IDS have been closely studied recently. Researchers in this area have developed a variety of intrusion detection systems based on: statistical methods [1, 2], neural networks [3, 4], decision trees and SVMs [5], genetic algorithms and artificial immune systems [6, 7, 8, 9].

There exist two main intrusion detection methods: misuse detection and anomaly detection. *Misuse Detection* is based on the known signatures of intrusions or vulnerabilities. The main disadvantage of this approach is that it cannot detect novel or unknown attacks that were not previously defined. *Anomaly Detection* [10] defines normal behaviour and assumes, that an intrusion is any unacceptable deviation from the normal behaviour. The main advantage of anomaly detection model is the ability to detect unknown attacks.

Researches of the natural mechanism of revealing of problems in the *Human Immune System (HIS)* can be used for building of an intrusion detection system owing to the fact that major principles of functioning are similar in both cases [11]. In the HIS the mechanisms of the nonspecific protection and the innate immunity realize the misuse detection function. The HIS consists of various immune cells, chemical signals, fibers etc. Their coordinated work allows to find out deviations in an organism of a person, to classify them and to start the mechanism of the immune answer. The properties of the distribution and self-organizing (adaptation to changing conditions), incorporated in the HIS, meet the basic requirements to systems of anomaly detection. Thus, modeling of the HIS includes development of algorithms of dynamic creation and updating of signatures, and also algorithms of anomaly detection by means of comparison to the current data.

In this work we propose our own solution of *Multiagent Neural Network* that is a combination of *Artificial Immune System (AIS)* mechanisms and *Artificial Neural Networks (ANN)* to receive advantages from both approaches. We hope that such IDS will be able to perform dynamic anomaly detection and misuse detection in the real time mode.

This article is an extension of the previous work [12, 13, 14] associated with the development of intrusion detection system with the neural network classifier. Classification is the main problem in the intrusion detection domain.

The paper is organized as follows. The basic conception of an immune system functioning is given in Section 2. Section 3 deals with the neural network detector we use to build the multiagent neural network based on artificial immune system principles. Section 4 will briefly introduce the general ideas of the multiagent modeling. In Section 5 the experimental results are described. Finally, concluding remarks are made in the last section.

2. IMMUNE SYSTEM

To begin with the Artificial Immune System for the Intrusion Detection domain, let's discuss how the Human Immune System works. This description will be simplified because the aim is to consider those basic elements that can be transferred to computer networks.

If one can say so, a major principle of the human immune system is a comparison of certain "patterns" with bodies located in a human organism. Thus we can reveal foreign bodes named antigens.

In real life lymphocytes carry out the role of the mentioned patterns. They are constantly generated by a spinal cord and thymus in view of the information contained in DNA (such information is accumulated, and this process is known as evolution of genic library). The lymphocytes spread in the organism through lymphatic nodes. Each type of the lymphocyte is responsible for detection of some limited number of antigens. There is an important stage during lymphocyte generation – *negative selection*. On this stage a special test on conformity with the native cells of the organism is executed. If such conformity takes place, the lymphocyte is killed. In fact otherwise it will struggle with the own cells of the organism. Due to the negative selection the "patterns" contain the information that is absent inside the organism. If any external body fit the given pattern than it is a foreign body.

In case of the lymphocytes detect an antigen on the ground of the corresponding pattern the new antibodies are produced and destroy the antigen. There is another mechanism that is known as *clone selection*. This mechanism is similar to the natural selection: only those antibodies survive that as much as possible correspond to the detected antigen. Thus the data on the generated antibodies get to the genic library mentioned above.

The most natural domain in which to begin applying the immune system mechanisms is computer security, where the analogy between protecting a body and protecting a normally operating computer is evident.

Experts working in the area of AIS mark out three fundamental properties of the human immune system:

- Firstly, it is distributed;
- Secondly, it is self-organizing;
- And thirdly, it is not especially demanding to computer resources.

In the opinion of many experts an efficient intrusion detection system should possess all of this properties.

3. NEURAL NETWORK DETECTOR

In our intrusion detection system artificial neural network detectors perform the function of lymphocytes in the HIS. *Neural Networks (NN)* have good generalization capabilities and can be efficiently used for approximation task, classification and processing of noisy data, what is especially important for intrusion detection.

We propose to use the integration of *PCA (Principal Component Analysis neural network)* and *MLP (Multilayer Perceptron)* as for basic element of the IDS (Fig.1).

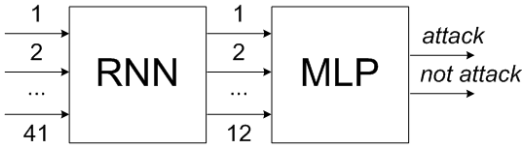

Fig.1 - Detector for immune system construction.

The 41 features from KDD-99 dataset [15] are used for input data. These features contain the TCP-connection information. The PCA network, which is also called a *Recirculation Neural Network (RNN)*, transforms 41-dimensional input vectors into 12-dimensional output vectors. The MLP processes those given compressed data to recognize type of attacks or normal transactions.

Such a detector specializes in a certain type of attack. There are two output values "yes" (when the entrance pattern relates to the given type of attack) and "no" (when the entrance pattern is not attack of the considered type).

It is also possible to use detectors of another structure (Fig.2, for details see our previous works [12, 13, 14]) but in the article we will only refer to the detector shown in Fig.1.

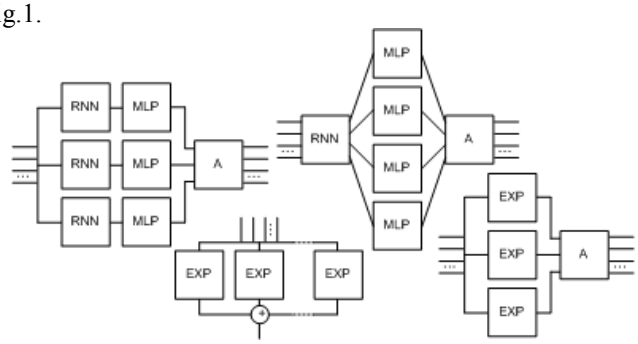

Fig.2 - Other variants of detectors.

After training of the neural networks they are ready to perform intrusion detection function.

4. MULTIAGENT NEURAL NETWORK

Multiagent neural networks use several detectors that specialize different fields of knowledge.

Real immune systems are too complicated with a lot of complex protecting mechanisms. But we need not all of them. So constructing our own multiagent system for intrusion detection we will use only the basic principles and mechanisms of the biological immune systems such as: generation and training of structurally diverse detectors, selection of appropriate detectors, ability of detectors to find out abnormal activity, cloning and mutation of detectors, forming of immune memory.

Let's consider the generalized structure of the multiagent IDS shown in Fig 3.

First of all, already known samples of normal network activity and attacks are placed into two databases of normal instances and attack instances respectively. Each sample is labeled either as an attack type or non-attack. These databases are used as a source for generation of training sets for the neural network detectors and for testing the performance of the IDS.

The next step includes creation of the detectors and the training procedure. Normal and attack samples are

randomly selected from the mentioned above databases forming a training set for an immature detector.

The periodical testing phase is necessary to control current state of the IDS for revelation of the detectors failed to train (this detectors are immediately deleted from the system) and to calculate of efficiency parameters for each detector. We can use something like this expression shown in the simplified form as for the efficiency parameter:

$$EF = count\_of\_true\_alarms - count\_of\_false\_alarms$$

A collection of the immune detectors makes up a population that circulates in a computer system and performs recognition of network attacks. It is possible to generate hundreds and thousands of the detectors each of them is responsible for a definite attack type. Availability of various input instances and element of chance during the education stage provide large quantity of the structurally different detectors. During the network traffic scan each detector performs recognition of the input vector and an overall conclusion is reported to a human operator who decides whether there is a true anomaly.

Dynamic nature of the proposed intrusion detection system is provided by regular renovation of the detectors in the population. This is a result of continuous cloning and mutation procedures; updating the set of the detectors with new members and removal of inefficient or long-life detectors.

Samples selected for the training purposes greatly influence the results of training stage and neural network generalization abilities. So preparing different training sets we can change the detector behavior and its ability to recognize certain input instances. So we can use this property of neural networks for preparing detectors with various generalization capabilities.

The cloning procedure is equal to retraining the detector with the minimal efficiency rates on the training set of the detector with the maximum performance (both detectors have to specialize in the same attack type).

The mutation procedure is related with retraining of the randomly selected detectors from the population. Besides samples for the training are renewed. So the mutation introduces into the intrusion detection system an element of randomness.

Inefficient detectors and detectors with the completed lifetime parameter are removed from the system or replaced by new randomly created detectors.

However, if a detector achieves the highest values of the efficiency among the detectors specialized in the certain attack type, it enters the immune memory to reserve here its configuration parameters (in the case of neural network detectors – a vector of its weight coefficients). These memory detectors can be easily activated, for example, in the case when overall system performance will reduce greatly.

Each detector is represented by the artificial neural network consisted of the recirculation neural network and the multilayer perceptron, which functions were already discussed above.

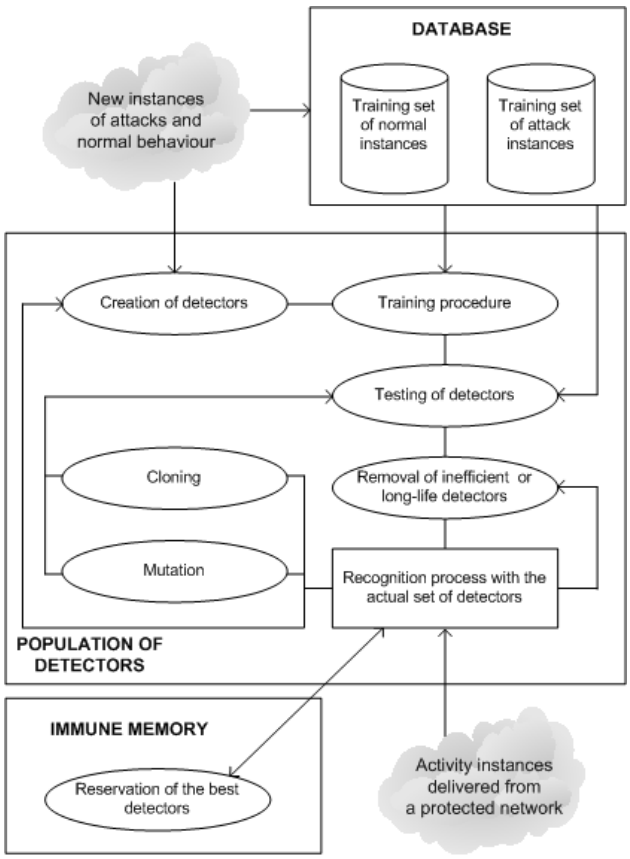

Fig.3 - Simplified multiagent NN functioning.

The detectors, which represent the same type of attack, are combined in groups from 3 to 10. Generally, all the detectors in the group give the diverse conclusions, which is the results of casual processes during the training. Theoretically, the number of detectors in the system is not limited and their number can be easily varied, but in real world problems with computational resources such as operative memory, speed etc…, arise.

Recognition process of an entrance pattern consists of the following sequence of steps:

1. Input pattern is transmitted to the multiagent system.
2. Each detector gives a conclusion about entrance activity.
3. So-called *factor of reliability* on each group of the detectors is formed. This factor reflects percent of voices in the group, given for the type of attack the group is specialized in.
4. The analysis of factors of reliability, obtained from each group, is carried out. A decision of the group with the maximum value of the factor is considered to be the final decision.

After information about new attack have been received (from a network administrator or other sources) it is appended to the database and new group of the detectors specialized on this type of attack appears. Thus new data are involved into the system work.

The obvious advantage of such an approach is, (i) Training process is made comparatively easily; (ii) Detectors are trained on a smaller number of samples than

models considered in the previous works; (iii) It allows to increase quality of their training and to considerably reduce time spent for preparation of the next detector.

5. EXPERIMENTAL RESULTS

In our work artificial immune system has been exploited for a development of multiagent IDS.

Several important questions that strongly influence the efficiency of the model arise in the course of designing multiagent structures: obtaining of the generalized decision on the basis of the set of detector opinions, selection of detectors, cloning and mutation, destruction of bad and/or irrelevant detectors.

There are a lot of random events during the multiagent system functioning. So first of all it is necessary to be convinced of the IDS stable work. Look at Fig.4. Here we can see that the detection rate and the false positive rate for some testing set appear not to exceed certain boundaries during long time functioning.

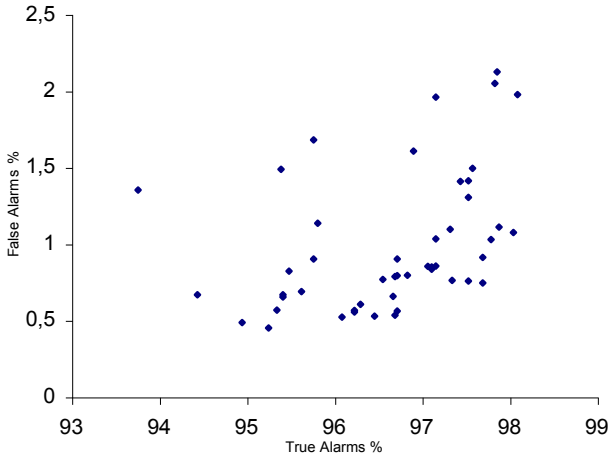

Fig.4 – Demonstration of the multiagent NN stable work.

Let's consider how such a multiagent system works from an example of a population of detectors. The population consists of 110 detectors (5 detectors in a group for each attack type from the KDD99 dataset). The results (Table 1, 2) were prepared in the same way as for the models in our previous works [12, 13, 14] so that we can compare them easily.

Table 1. Training and testing sets

	DoS	U2R	R2L	Probe	Normal	Total count
training samples	3571	37	278	800	1500	6186
testing samples	391458	52	1126	4107	97277	494020

Table 2. Attack classification with the multiagent NN

class	count	detected	recognized
DoS	391458	386673 (98.78%)	368753 (94.20%)
U2R	52	47 (90.39%)	45 (86.54%)
R2L	1126	1097 (97.42%)	930 (82.59%)
Probe	4107	4066 (99.00%)	4016 (97.78%)
Normal	97277	---	82903 (85.22%)

The second experiment (Table 3) is related with the recognition of new attacks. For this purpose, we prepared a special set of samples for testing and training. The testing samples consist of network connection records that represent some of the most popular network services taken from the KDD99 dataset (http, ftp, ftp data, smtp, pop3, telnet). As dataset for training, we generated a considerably reducing number of samples for each attack type. Also what is necessary to draw attention is that the records of some scanty attack types were entirely excluded from the training set. Therefore, only 9 types of attacks have been selected here. Accordingly, 9 groups (5 detectors in each) have been generated. So, the quantity of the population has made up 45 detectors.

Table 3. Attack detection with the multiagent NN (Step 1)

type	count	detected
Normal	75952	75269 (99.10%)
Back	2203	2157 (97.91%)
Neptune	901	899 (99.78%)
Buffer_overflow	30	28 (93.33%)
Loadmodule	9	8 (88.89%)
Guess_passwd	53	52 (98.11%)
Warezclient	1015	966 (95.17%)
Ipsweep	9	9 (100.00%)
Portsweep	15	14 (93.33%)
Satan	10	8 (80.00%)

After several iterations had passed we added few instances of "warezmaster" attack to the database. As a result 5 additional detectors appeared in the population specialized in this attack type. The results taking after this manipulations are shown in Table 4.

Table 4. Attack detection with the multiagent NN (Step 2)

type	count	detected
Normal	75952	75169 (98.97%)
Back	2203	2174 (98.68%)
Neptune	901	900 (99.89%)
Buffer_overflow	30	26 (86.67%)
Loadmodule	9	8 (88.89%)
guess_passwd	53	53 (100.00%)
Warezclient	1015	947 (93.30%)
Warezmaster *	20	18 (90.00%)
Ipsweep	9	9 (100.00%)
Portsweep	15	14 (93.33%)
Satan	10	8 (80.00%)

** - the attack that was added to the database*

The results shown in Table 5 show a lot of records corresponding to new attacks were detected and classified as an "attack". It means that multiagent systems are capable of detecting new attacks and have high generalization capacity.

Table 5. Attack detection with the multiagent NN (Step 3)

type	count	detected
Normal	75952	74340 (97.88%)
Back	2203	2169 (98.46%)
Land*	1	1 (100.00%)
Neptune	901	900 (99.89%)
Buffer_overflow	30	26 (86.67%)
Loadmodule	9	9 (100.00%)
Perl*	3	0 (0.00%)
Rootkit*	7	3 (42.86%)
ftp_write*	6	5 (83.33%)
guess_passwd	53	53 (100.00%)
Multihop*	7	5 (71.43%)
Phf*	4	0 (0.00%)
Spy*	2	0 (0.00%)
Warezclient	1015	981 (96.65%)
Warezmaster	20	19 (95.00%)
Ipsweep	9	9 (100.00%)
Nmap*	2	2 (100.00%)
Portsweep	15	15 (100.00%)
Satan	10	8 (80.00%)

** - the attacks that were absent in the training set*

6. CONCLUSION

We have discussed only the prototype of multiagent neural network that is based on artificial immune system and oriented to work on a single machine. Nevertheless, the results are promising due to the fact that many unknown records were detected. Extension of the proposed approach based on multiagent neural networks will allow us to build a real time intrusion detection system to protect local networks. Separate modules located on protected machines in different places of LAN will exchange data about their detectors what will make intrusion detection process more adaptable and quick reaction.

7. REFERENCES

[1] D.J. Marchette. A statistical method for profiling network traffic // In Proceedings of the USENIX Workshop on Intrusion Detection and Network / 1999. – P.119–128.

[2] D.J. Marchette. Computer Intrusion Detection and Network Monitoring: A Statistical View-Point // Springer - 2001.

[3] J. Cannady. Artificial neural networks for misuse detection // In Proceedings of the 1998 National Information Systems Security Conference (NISSC'98) / October 5–8 - Arlington, VA, 1998. - P. 443-456.

[4] Beghdad R. Critical study of neural networks in detecting intrusions // Comput. Secur. – 2008. - doi:10.1016/j.cose.2008.06.001.

[5] Sandhya Peddabachigari, Ajith Abraham, Crina Grosan, Johnson Thomas. Modeling intrusion detection system using hybrid intelligent systems // Journal of Network and Computer Applications – 2007 – 30. – P.114–132.

[6] Morton Swimmer. Using the danger model of immune systems for distributed defense in modern data networks // Computer Networks – 2007. – 51. – P.1315–1333.

[7] Gerry Dozier, Douglas Brown, Haiyu Hou, John Hurley. Vulnerability analysis of immunity-based intrusion detection systems using genetic and evolutionary hackers // Applied Soft Computing – 2007. – 7. – P.547–553.

[8] Mohammad Saniee Abadeh, Jafar Habibi, Zeynab Barzegar, Muna Sergi. A parallel genetic local search algorithm for intrusion detection in computer networks // Engineering Applications of Artificial Intelligence – 2007. – 20. – P.1058–1069.

[9] M. Saniee Abadeha, J. Habibia, C. Lucasb. Intrusion detection using a fuzzy genetics-based learning algorithm // Journal of Network and Computer Applications – 2007. – 30. – P.414–428.

[10] Animesh Patcha, Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks – 2007. – 51. – P.3448–3470.

[11] U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod. Danger Theory: The Link between AIS and IDS? // In Proceedings of ICARIS-2003, 2nd International Conference on Artificial Immune Systems / P.147-155.

[12] V. Golovko and L. Vaitsekhovich. Neural Network Techniques for Intrusion Detection // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2006) / Brest State Technical University - Brest, 2006. - P. 65-69.

[13] V. Golovko, P. Kachurka and L. Vaitsekhovich. Neural Network Ensembles for Intrusion Detection // In Proceedings of the 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2007) / Research Institute of Intelligent Computer Systems, Ternopil National Economic University and University of Applied Sciences Fachhochschule Dortmund - Dortmund, Germany, 2007. - P. 578-583.

[14] V. Golovko, L. Vaitsekhovich, P. Kochurko and U. Rubanau. Dimensionality Reduction and Attack Recognition using Neural Network Approaches // Proceedings of the Joint Conference on Neural Networks (IJCNN 2007) / Orlando, FL, USA – IEEE Computer Society, Orlando, 2007. - P. 2734-2739.

[15] 1999 KDD Cup Competition. - Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.