ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ ДАННЫХ СОВРЕМЕННЫЕ ПРОБЛЕМЫ РОБОТОТЕХНИКИ АНАЛИЗ И МОДЕЛИРОВАНИЕ СЛОЖНЫХ СИСТЕМ

UDK 004.9

COMPUTER NETWORK SECURITY APPROACH BASED ON MULTI-AGENT DYNAMIC RECOGNITION

Leanid Vaitsekhovich
Intelligent Information Technology Department, Brest State Technical University, Brest

In this article a multi-agent model of intrusion detection system have been addressed. The integration of an Artificial Immune System and Neural Networks in the role of detectors permits to increase flexibility and overall performance of the system. The detector structure is based on two different neural networks namely NPCA and MLP. The model is able to perform a classification of network intrusions by classes as well as by types.

Keywords - Intrusion Detection, Neural Network, Artificial Immune System, Principal Component Analyses, Multi-agent System.

Introduction

Computer network security is one of the most significant problems today. Its importance is growing with the development of Internet and computer computational power.

There are two main intrusion detection techniques: misuse detection and anomaly detection. Misuse detection systems (for example, STAT and IDIOT [1]) use patterns of well-known attacks.

Anomaly detection systems [2] flag observed activities that deviate significantly from the established normal usage profiles as anomalies, that is, possible intrusions.

Neural Network Agent

Network intrusions are usually generalized into four classes such as DoS, probing, U2R, R2L [3]. Each attack class consists of different attack types.

As an agent (detector) of the Intrusion Detection System (IDS) we use the integration of NPCA (Nonlinear Principal Component Analysis Neural Network) and MLP (Multilayer perceptron), which are connected consequently (figure1) [4].

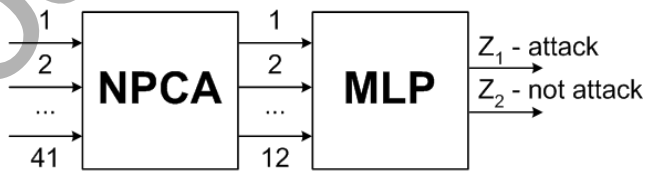

Figure 1 – A single agent (detector) structure

41 features from KDD-99 dataset are used as an input instance. Each input contains TCP-connection information [3]. NPCA transforms the 41-dimensional input vectors into the 12-dimensional output vector. MLP performs the processing of the compressed data to recognize attacks or normal transactions.

Artificial immune system

Experts working in the area of Artificial Immune Systems (AIS) mark out a few fundamental properties of the approach:

- Firstly, AIS are distributed;
- Secondly, AIS are self-organizing.

Biological immune systems are too complicated with a lot of complex protecting mechanisms. But constructing a multi-agent system for intrusion detection only the basic principles and mechanisms can be used 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 a generalized structure of the multi-agent IDS shown in figure 2.

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.

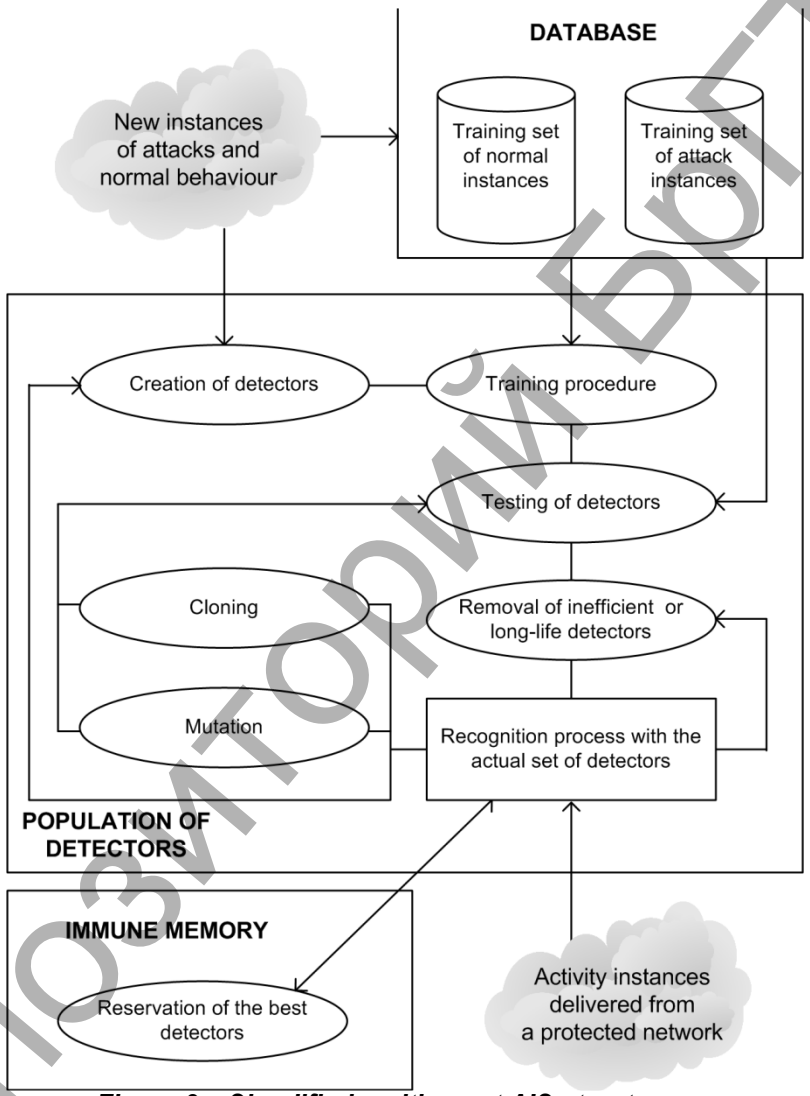

Figure 2 – Simplified multi-agent AIS structure

The procedure of building and performance of the neural network immune system can be represented as follows:

1. Generate an initial population of the detectors. It should be noted that each detector represents a neural network with random weights:

$$D = \left\{ D_i, \quad i = \overline{1,r} \right\}, \tag{1}$$

where D_i is *i*-th neural network immune detector, *r* is the number of detectors.

2. Train the neural network immune detectors. A training data set is generated by random way from normal and attack instances from the database. After the training a certain amount of the detectors is obtained, which is used in the testing stage.

3. Select the best neural network detectors. The goal of this process is to eliminate bad (unsuitable) detectors that are insufficient for detection and recognition. Each detector is verified using a test data set. As a result the total mean square error E_i is determined for each single detector. The detectors with zero mean square error should be selected:

$$D_i = \begin{cases} 0, & if\ E_i \neq 0 \\ D_i, & otherwise. \end{cases} \quad (2)$$

where *0* characterizes deletion of a detector.

4. Each detector get lifetime and is chosen when the next input instance is supplied to be inspected.

5. Each detector scans the instance. As a result the output values of the detectors Z_{i1}, Z_{i2}, where $i=1…r$, are defined.

6. If *i*-th detector does not detect an attack in a scanning instance, i.e. $Z_{i1}=0$ and $Z_{i2}=1$, then it chooses the next instance for inspection. If the lifetime of a detector is ended, it is eliminated from the detectors set and a new detector is created.

7. If *i*-th detector detects an attack in the input, i.e. $Z_{i1}=1$ and $Z_{i2}=0$, then it activates alarm. In this case cloning and mutation of the given detector is performed. As a result a set of clones is generated and each clone is trained by using the detected intrusion. Finally we can get a set of clones, which is aimed to detect the given activity.

8. Select the best clone detectors, which are most suitable to detect this malicious activity. The mean square error for each clone is calculated, using the detected attack. If $E_{ij}>E_i$, then a detector has passed selection. Here E_{ij} – means a square error for *j*-th clone of *i*-th detector.

9. Creation of the immune memory. The best neural network detectors are defined, which have shown perfect results during detection of given computer attacks. The detectors of the immune memory exist in the system for a long time and provide the protection against repeated attacks.

Theoretically, the number of the detectors in the system is not limited and their number can be easily varied, but in the real world problems with computational resources such as operative memory, speed etc…, arise.

Experimental results

The results of experiments are discussed in this section. We used data presented in table 1 for training and testing. Table 2 shows the classification results.

In comparison with architectures of intrusion detection systems proposed in our earlier works [4, 5], it becames possible to increase the accuracy of the proposed architecture to 0.92 as it is shown in table 3.

Table 1 – The training and testing sets

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

Table 2 – Attack classification with the multi-agent system

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%)

Table 3 – Some common characteristics

true positive rate	true negative rate	accuracy
0.94	0.85	0.92

Conclusion

In this paper we propose a multi-agent intrusion detection system that organizes joint work of a set of the neural network detectors on the bases of the artificial immune system mechanisms. The detector structure is represented by the integration of two different neural networks namely NPCA and MLP. The model is able to perform a classification of network intrusions by classes as well as by types and cuts down false positives.

Bibliography

1. A software architecture to support misuse intrusion detection / S. Kumar, E.H. Spafford // In Proceedings of the 18th National Conference on Information Security. 1995. – P. 194–204.
2. Animesh, Patcha An overview of anomaly detection techniques: existing solutions and latest technological trends / Patcha Animesh, Park Jung-Min // Computer Networks – 2007. – № 51. – P. 3448–3470.
3. 1999 KDD Cup Competition - Information on: http://kdd.ics.uci.edu/database/kddcup99/kddcup99.html.
4. Golovko, V. Dimensionality Reduction and Attack Recognition using Neural Network Approaches / V. Golovko, L. Vaitsekhovich, P. Kochurko, U. Rubanau // In Joint Conference on Neural Networks (IJCNN-2007). – Orlando, FL, USA, 2007. – P. 2734–2739.
5. Vaitsekhovich, L. Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System / L. Vaitsekhovich, V. Golovko, U. Rubanau // In 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009). – Minsk, Belarus, 2009. – P. 285–289.

УДК 004.8.032.26

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОБРАБОТКИ ЭЛЕКТРОЭНЦЕФАЛОГРАММ ДЛЯ ДИАГНОСТИКИ ЭПИЛЕПСИИ

Артеменко С.В.
Брестский государственный технический университет, г. Брест

Введение

Разработано множество методов для изучения и анализа сигналов электроэнцефалограмм (ЭЭГ) с целью выявления патологических изменений мозга во время эпилептических припадков [1, 2]. Многие из этих методов уже используются в клиниках, однако являются малоэффективными. Для автоматического обнаружения эпилептической активности по сигналам ЭЭГ в основном используются линейные (частотно-временные, математические и статистические) методы, в которых не учитывается нелинейность исследуемого сигнала.

Несмотря на проведение широких исследований в области анализа ЭЭГ, самым эффективным считается метод визуальной оценки. При этом даже опытные врачи расходятся во мнении, принимая один и тот же паттерн за аномальную активность либо за артефакт.

Исследования ЭЭГ сигналов показали, что они являются нестационарными и хаотическими [3]. ЭЭГ описывает поведение сложной динамической системы, и характер нормальной активности сигналов является хаотическим, поэтому применение линейных методов анализа является малоэффективным [3].

1. Методы выявления патологической активности в ЭЭГ сигналах

Существующие методы детектирования эпилептической активности в сигналах ЭЭГ можно разделить на несколько основных категорий:

Метод визуальной оценки. Несмотря на проведение широких исследований в области анализа ЭЭГ, самым распространенным является метод визуальной оценки [1]. Однако такая методология не лишена субъективности.