Multi-Layer Structure of Neural Network Agents for Intrusion Detection

Leanid Vaitsekhovich, *Brest State Technical University*
(**31.08.2012**, Prof. Vladimir Golovko, *Brest State Technical University*)

Abstract

In this article a multi-agent model of intrusion detection system have been addressed. Three level architecture of agent hierarchy was applied. The algorithm of agent interaction can be described with a directed graph. The model is able to perform a classification of network intrusions by classes as well as by types.

1. Introduction

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

In accordance with the statistical researches prepared by Kaspersky laboratory during 2010 year [1] their *Intrusion Detection System (IDS)* repulsed 1 311 156 130 computer network attacks. The same measure for 2009 year was about 220 million incidents.

There are two main intrusion detection techniques: misuse detection and anomaly detection. Misuse detection systems (for example, STAT and IDIOT [2]), use patterns of well-known attacks or weak spots of the system to match and identify known intrusions.

Anomaly detection systems (for example, the anomaly detector of IDES [3]) flag observed activities that deviate significantly from the established normal usage profiles as anomalies, that is, possible intrusions.

2. Neural Network Agent

Network intrusions are usually generalized into four classes such as DoS, probing, U2R, R2L [4]. Each attack class consists of different attack types.

As an agent (detector) of the intrusion detection system we use the integration of *NPCA (Nonlinear Principal Component Analysis Neural Network)* and *MLP*, which are connected consequently (Fig.1) [5].

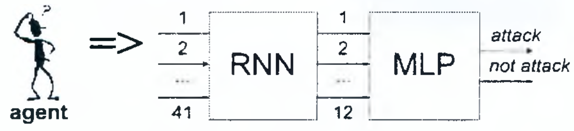

Fig.1. A single agent (detector) structure.

As an input data are used the 41 features from KDD-99 dataset, which contain the TCP-connection information [4]. NPCA transforms the 41-dimensional input vectors into 12-dimensional output vector. MLP performs the processing of the compressed data to recognize the types of attacks or normal transactions.

Such a detector in the multi-agent environment specializes in a certain type of attack.

3. Multi-Agent IDS

It is possible to reduce computational resources necessary to perform the classification by limiting number of the detectors used for a generation of a final decision. This can be done by means of predefined rules that organize strict sequences and sets of the detectors that process an input pattern.

The rules can be represented with a simple directed graph with the nodes corresponding to different types of the detectors and the edges corresponding to data transfer flows.

In this work the architecture, shown in Fig.2, was developed and underwent series of experiments.

The classification model includes three levels of abstraction. The first level node detects one of the four attack classes or normal state. Each detector at the second level represents a certain class of attack and performs a classification of input patterns as an attack type. The detectors at the third level accept or reject the decision of the detector at the second level.

4. 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. The detectors at the second level (Fig.2) allow us to determine the type of an attack.

Tab.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

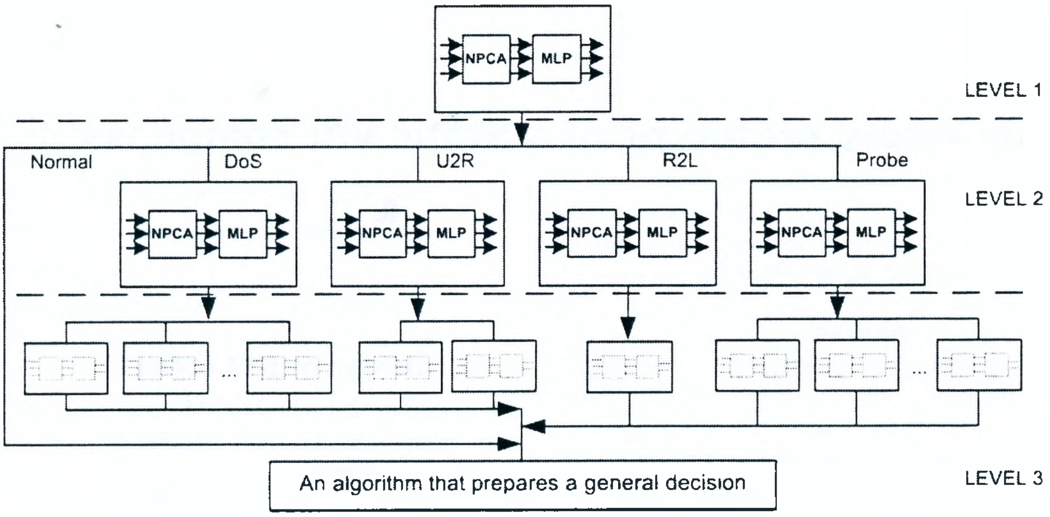

Fig.2. A structure of the multi-agent IDS represented in the form of a directed graph.

In comparison with the architectures of intrusion detection systems proposed in our earlier works [5, 6], it became possible to reduce the number of false positives as it is shown in Fig.3.

Tab.2.

Attack classification with the multi-agent system

class	count	detected	recognized
DoS	391458	391125 (99.91%)	370658 (94.68%)
U2R	52	38 (73.08%)	29 (55.77%)
R2L	1126	1068 (94.85%)	1066 (94.67%)
Probe	4107	4056 (98.75)	4056 (98.75)
Normal	97277	---	87245 (89.68%)

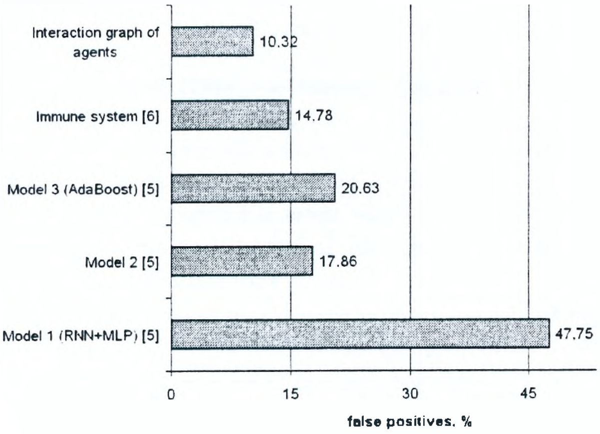

Fig.3. False positive rates for different IDS models.

5. Conclusion

In this paper we proposed a multi-agent intrusion detection system that organizes two-categorical classification process of computer network activity; reduces the number of detectors involved in generation of the final decision; cuts down false positives.

Bibliography

[1] Kaspersky Security Bulletin 2010 - Information on: http://www.securelist.com/ru/downloads /vlpdfs/k_securitybulletin_rus2_screen.pdf

[2] S. Kumar and E. H. Spafford: A software architecture to support misuse intrusion detection, In Proceedings of the 18th National Conference on Information Security, 1995, pp. 194–204

[3] T. Lunt: Detecting intruders in computer systems, In 1993 Conference on Auditing and Computer Technology, 1993

[4] 1999 KDD Cup Competition - Information on: http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html

[5] V. Golovko, L. Vaitsekhovich, P. Kochurko, U. Rubanau: Dimensionality Reduction and Attack Recognition using Neural Network Approaches, In Joint Conference on Neural Networks (IJCNN-2007), Orlando, FL, USA, 2007, pp. 2734-2739

[6] L. Vaitsekhovich, V. Golovko, U. Rubanau: Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System, In 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009), Minsk, Belarus, 2009, pp. 285-289

Author:

Leanid Vaitsekhovich
Brest State Technical University
Moskovskaja str. 267
224017 Brest, Belarus
tel. +375-162-42-63-21
fax +375-162-42-21-27
email: *vspika@rambler.ru*