7th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS
Suceava, Romania, May 27 – 29, 2004

NEURAL NETWORKS FOR INTRUSIONS DETECTION IN COMPUTER NETWORKS

V. Ye. MUKHIN
National technical university of Ukraine "The Kiev polytechnic institute"
Pr. Pobedy, 37, UA-03056, Kiev, Ukraine
mukhin@comsys.ntu-kpu.kiev.ua

Abstract. *This paper describes the approach for the computer networks intrusions detection based on the artificial neural networks performing the users and processes activities identification. The offered intrusions detection system is adaptable to the different network attacks and allows improve the detection effectiveness.*
Keywords*: intrusions detection, anomaly, abusing, expert system, artificial neural network*

Introduction

The increasing volumes of the information, processed in computer networks cause the actuality for the networks security means implementation. The only one attack on the computer network may lead to the information loss, to the unauthorized using of the network resources, or to the integrity violation of the critical data. Thus, the development of the specialized tools for protection from the network attacks is rather actual.

The approaches to the intrusions detection systems realization

In general, there are two well-known methods for the attacks detection: the anomalies detection and the abusing detection. [1] The anomalies detection implies to identify those operations which are different from the templates (profiles), pre-defined for the legal users or users groups. In this method, usually, is created the database containing profiles of the inspected users activities. The second method, the abusing detection, is based on comparing of the legal users templates to the behaviour of the intruder, who wants to get the access to the system. In the first method is performed the monitoring of the critical value, that is determined as limiting level for the users and processes operations suspiciousness, and the second detection method is based on the rules analysis approach. In this approach is used the pre-defined rules set, formed by the administrator, automatically generated by the system or both variants combination. The rules describe the probable attacks scenarios, and intrusions detection mechanism identifies potential attacks if the users operations don’t coincide with the pre-defined rules.

The attacks detection with the pre-defined rules often is based on the expert systems. [2] The expert system includes the rules set, described certain knowledge of the man-expert in this field. These rules are used for the conclusions about security violation, performed on the data from the attacks detection system.

The shortcoming of this approach is necessity in permanent upgrading of the expert systems to remain them actual.

The required upgrades can either be ignored, or to be performed by security administrator in the off-line mode, that reduces the expert system effectiveness. Besides that, the expert systems cannot to detect attacks distributed in time or attacks that are performing by the several intruders simultaneously and they are hardly adapted to the new attacks scenarios. The insignificant changes in the attacks operations sequence may cause big affect on the "activity - rule" comparing process and the expert system will not detect the attack. [2]

In the past years there are offered several approaches to the attack detection based on the other means than the expert systems. One of the most perspective mechanisms for the intrusion detection systems is the neural network.

The intrusions detection systems on the neural networks

The attack detection method on pre-defined rules is effective when the precise attack characteristics are known. However, the network attacks are varied permanently, because the intruders may use the new approaches, and also due to regular changes in the software and hardware. The significant attacks variation leads to the situation, when even permanent upgrading of the expert systems rules database cannot to ensure the precise detection of the every possible attack.

Thus, the permanently varying network attacks require the adaptive securing mechanism, which provides the possibilities to analyze the big volumes of data about the users and processes activities on the less determined method, than means based on the pre-defined rules analysis. One of the effective solutions for this problem is the abusing detection system on the artificial neural network. [3]

The structure of the artificial neural network is set of the elementary nodes (neuron), linked one to each other. The nodes transform the input data set to the required output data set. The transformation result is determined by the nodes characteristics and by the links weights. The adaptation to the required output result is performed as links structure modification. Unlike the expert systems, that generate the defined conclusion about the correspondence between the certain user activities profiles and the related rules in database, the neural network provides the possibility to estimate the fact, that the input data (users profiles) are corresponded to the profiles, which network is learned to recognize. [4]

Initially, the neural network is trained to perform the correct identification of the pre-defined data domains patterns. The neural network reaction is analyzed, and then the network is adjusted to generate the correct results. Further, in addition to the initial training, neural network goes through re-training over some period.

The artificial neural networks have the large potential for the modern attacks detection means. They, actually, appear as alternative approach to statistical analysis in the anomalies detection systems. Statistical analysis implies comparing of the current events to the pre-defined standard criterions set. This method is used most frequently for detection of the deviations from the regular activities mode and identifies the activities, which may contain attacks. The neural networks are offered specially to identify the users regular activities profiles and to define statistically significant deviations from a regular mode. [4]

The realization of the safety monitoring system on the neural networks

Common principles for designing of the intrusions detection systems on the neural networks

In this paper is offered the special Neural Network Intrusion Detector (NNID) for the attacks detection in the computer networks. This Detector performs the intrusions detection in the computer networks on the analysis of the operations, that network users are running. It is well known, that various users tend to use different operations depending on their personal tasks, while the legal users run the only authorized operations. The frequencies of the certain command running can be varied for the different users. The sets of used commands and their running frequencies, thus, form the operation profile of the legal user. These sets show the users tasks and the used applications, and on this information is possible to detect the system safety violation.

The NNID designing includes the following 3 phases:

1. The training data collection. It is necessary to store the registration records for each users operation for the several days period. The vector representing the operations running frequencies for each operation is generated for all users.

2. The learning process. The neural network is learn to detect the possible intrusion on the

vectors described the operation running frequencies distribution.

3. The conclusion. Let us assume, that the network recognizes the users activities for every new vector of the operation running frequencies distribution. If the neural network made conclusion about user activity, that is different from the one for the legal user, or the network cannot reach the clear conclusion, then this certain operation is intrusion.

Further, we consider the specifics of the NNID realization, and describe the computer network configuration for the NNID testing.

The experimental researches

The offered NNID-system was tested on the local area computer network consisting from 1 server and 10 workstations. The main volume of the users information is stored on the server, therefore users regularly send requests to it. The NNID task is to recognize the possible attacks on the server.

The local area network for NNID testing has following properties:

1. The operating system is FreeBSD. This system has an option to register the users activities in audit records set, which is used for the future neural network learning.

2. The numbers of the users and the set of command, running for the certain period, in this operation system are adjustable. Thus, the offered means are tested on the real data.

3. The operating system is secured enough from the potential intruders, and all the legal users are strictly registered in system, so the main part of collected data on users activities describes the legal users operations mode (free from attacks mode).

The 30 most typical operations in computer networks were selected for the analysis, where some operations are authorized, and the other are unauthorized. The data about 89 users activities were collected within 12 days.

To provide the higher overlap between the users activities vectors, and, therefore to improve the system effectiveness, the command running frequencies are divided into intervals. It was 11 nonlinear intervals, and the representation is most precise for the lower frequencies. The first interval describe the commands, which was never used; second - the commands, which was used one or two times and so on up to the last interval, described the commands, which was used more than 500 times. The intervals were limited by values from 0.0 up to 1.0 with increment 0.1. These values, one for each command, then were assembled in 30-d dimension vector of the operations running frequencies distribution (the users operation vector), and used as input data for the neural network.

The neural network structure is based on the three-layer architecture. (Fig.1)

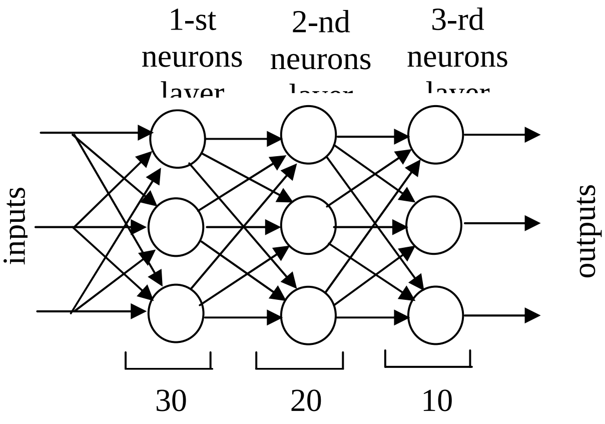

Fig. 1. A fragment of the three-layer neural network

The input layer of this neural network consist from the 30 nodes described the users activities vector, the inner layer has 20 nodes and the output layer has 10 nodes. The network is realized with the neural networks simulating environment NeuroView+.

The training of this neural network is based on errors back propagation algorithm. This algorithm is the generalization of the training procedure for the simple perceptron, known as a delta - rule, and is used the training samples. The sample consists of two vectors (input and output), and the neural network resolves weather these vectors are equal or not.

The errors back propagation algorithm is based on the gradient descent method, minimizing the summarized square-law error *E:* (1)

where $Y^N{}_{\boldsymbol{k}}$ – the real output state of the k-layer node (neuron) from N-layer neural network while on it inputs is an i-image, $Y_{i,k}$ – the ideal (desirable) output state of this node.

The main idea of this algorithm is to calculate the neuron output sensitivity to the links weights changes due to reaction on an error. First, the partial derivatives from error by links weights are calculated. The algorithm requires, that activating neuron function must be non-decreasing and had a limited derivative, so the sigmoidal activating function may be used for this operation.

The small random values are assigned to the weights of the neural network nodes links before the training will start. Every iteration of back propagation includes two phases. On the first phase (the direct pass) the network input nodes are set in the certain state according to the input vector. Then the input signals go through the network, and the output vector is generating.

On phase two, the output vector is compared to required vector (the back pass). If they coincide, there is no need in the training. Otherwise, the difference (error) between the real and required output values is calculated and is transmitted back from the output to the input layer nodes. The links weights are modified according to the information about error.

This approach allows to receive the results on the most standard neural network structure, is flexible enough and the simulation could easily be duplicated on the other neural networks variants.

The researches results

To except the re-training before the real experiments will start, several training sessions is performed to define a number of training rounds for the highest efficiency. The neural network was trained within 8 randomly selected days (65 users operations vectors), and its efficiency was checked during 4 last days (24 vectors) on 30, 50, 100 and 200 vectors, where the number 100 shows the highest efficiency.

$$E = \frac{1}{2}\sum_{k=1}^{N}\sum_{i=1}^{N}(Y_k^N - Y_{i,k})^2 \qquad (1)$$

In result 4 neural network variants was generated, and they all are tested on two tasks solving:

1. The analysis of the users operations vector for the 4 last days. If the activation of an output node representing the legal user operations, was higher, than activation of all other nodes, and also was higher, than 0.5, the user operations considered as correct.

2. The analysis of 100 randomly generated users operations vectors. If all output nodes have activation less than 0.5, the network defines this user as intruder (i.e. the user running the unauthorized operations).

All 4 variants of neural network show the similar results. On the average, the neural networks suspected 63% random users operations vectors, that leads to 96% intrusions detection. They correctly defined the legal users operations vectors in 93% situations, generating false danger warnings in 7% situations.

It should be mentioned, that all false danger situations for any neural network variants was generated for the same false accused user. The more steadfast reviewing of the users operations vectors has shown, that the data about this certain user operations were collected only for 3 days. He gets access to the system very seldom, and the neural network could not learn his activities profile. Whereas there is easy way to settle down this problem if collect more data about this user activities, we suppose, that this problem solution is difficult. It doesn’t matter, what data volumes are collected for the main users, because probably, them still may be not enough for some seldom working user. Therefore, we suppose, that the results received for this small data set, show us the real characteristic of the NNID-system.

The structure of the safety monitoring system on the neural networks

The figure 2 shows generalized structure of the safety monitoring system on the neural networks.

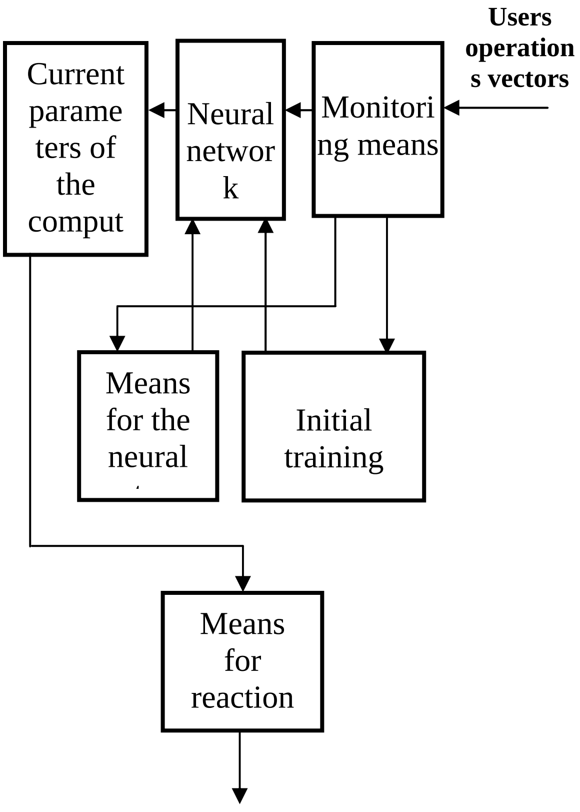

Fig. 2. The structure of the safety monitoring system on the neural networks

Any situations, that the neural network identified as attacks, are re-addressed to the computer network safety administrator or to the system for the on-line reaction on attacks.

The offered monitoring system is more effective, than system on the expert model with rules analysis, because the neural network learn the possible attacks characteristics during some period and then adjusted on them.

The advantages of the neural networks in the intrusions detection systems

The main advantage of the neural networks for the intrusion detection in the computer network is their adaptability. The neural networks can learn the intentional attacks characteristics and identify the activities, that are not similar to the registered in the network earlier, and also can analyze data even they are fuzzy, incomplete or deformed, and can perform the data analysis in a nonlinear mode. [5] These features are especially important, because, as was mentioned before, some attacks on the network can be launched the by the several intruders simultaneously.

The computer network security system requires the attacks fast detection, and the information processing rate in the neural network allows to react on the attacks in the real time and to avoid the irreparable damages to the system, that is one more advantage of the offered approach.

The neural network output data are the probabilities, and thus, the neural network provides the possibility to predict the future attacks. The abusing detection system on the neural network determines the probability that certain activities or activities series are attacks. The additional training of the neural networks improves their ability to detect the activities with attacks tags, and further this information is used for those attacks preventing. The series of the activities are analyzed, and security system launches the protective means, before the intruder will reach his goals.

The neural network can be trained to detect the known suspicious activities precisely enough. The intruders frequently use repeated fragments in the attacks, so the neural network can detect the attacks, which incompletely meet the scenarios of the previous intrusions. [6] Thus, the attack probability is estimated and the potential threat is detected, irrespective, whether or not the probability exceeds the certain critical value for the users or processes activities suspiciousness level.

The shortcomings of the neural networks applying

However, there are some shortcomings in the neural network applying for the intrusion detection. These shortcomings are caused by the fact that the neural network is "a black box". Unlike the expert systems, which operate with strictly pre-defined rules for the activities analysis, the neural networks adapt the data analysis according to their additional training. The link weights and the transmission functions of the network nodes are usually unimportant factors after the network has reached an acceptable level for the intrusions detection.

This problem is rather wide spread for the neural network implementation and is open for the further researches. Besides that, it is difficult enough to analyze effectively on the neural networks the information in the IP-datagrams in the network traffic, that is rather essential for attacks detection in the computer network. [7]

Conclusion

The effectiveness of the intrusion detection system on the neural networks can be rise if generate more correctly their internal structure and improve the neural network adaptation to the attacks detection. On the practice, the offered monitoring systems are recognized any new activities as attack with certain probability until the network not will be re-trained for more correct detection of these activities. Therefore, it is necessary to provide the additional training option for the neural network, since this feature allows react correctly to the changes in the input data. The neural network adaptability level increasing can be based on the adaptive resonance or on the self-organizing cards theories.

Thus, the intrusion detection in the computer systems and networks, is a complex problem due to big variation of the possible attacks. One of the most effective approaches for this problem solution is the neural network applying. This approach, as was shown in this paper, provides certain advantages for the computer network intrusions detection, and is perspective.

References

[1] Mukherjee, B., Heberlein, L. T., and Levitt, K. N. (1994). *Network Intrusion Detection*. IEEE Network. - pp. 26–41.

[2] Anderson, D., Frivold, T. and Valdes, (1995) *A Next-generation Intrusion Detection Expert System (NIDES): A Summary*. SRI International Technical Report SRI-CSL-95-07. -57 p.

[3] Jeremy, F. (1994). *Artificial Intelligence and Intrusion Detection: Current and Future Directions.*//Proc. of 17th National Computer Security Conference. - pp. 348-357.

[4] Hammerstrom, D. (1993). *Neural Networks At Work.* IEEE Spectrum. - pp. 26-53.

[5] Puketza, N., Chung, M., Olsson, R.A. and Mukherjee, B. (1997). *A Software Platform for Testing Intrusion Detection Systems.* //IEEE Software Vol. 14, No.5. - pp. 37-51.

[6] Ryan J., Lin M., and Miikulainen, R. (1997) *Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management.*// AAAIWokshop, Menlo Park, CA. - pp.72-79.

[7] Tan, K. (1995) *The Application of Neural Network to UNIX Computer Security.*//Proc. of IEEE International Conference on Neural Networks, Vol.1. - pp. 476-481.