ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 68 Nr kol. 1905

Anatoliy SACHENKO
Silesian University of Technology
Department of Computer Science and Econometrics

Myroslav KOMAR
Ternopil National Economic University
Research Institute for Intelligent Computer Systems

INTRUSION DETECTION SYSTEM BASED ON NEURAL NETWORKS

Summary. Designing the neural network detector of attacks using the vector quantization is considered in this paper. It's based on improved method for hierarchical classification of computer attacks and the information compression using the principal component analysis and combining the neural network detectors.

Keywords: intrusion detection system, neural networks, principal component analysis.

SYSTEM WYKRYWANIA WŁAMAŃ OPARTYCH NA SIECIACH NEURONOWYCH

Streszczenie. W artykule zaprezentowano podejście do projektowania detektora ataków komputerowych za pomocą sieci neuronowej i kwantyzacji wektorowej. Bazuje ono na ulepszonej metodzie hierarchicznej klasyfikacji ataków komputerowych i kompresji informacji za pomocą analizy głównych składowych i łączenia sieci neuronowych detektorów.

Słowa kluczowe: system wykrywania włamań, sieci neuronowe, analiza głównych składowych.

1. Introduction

Currently, the most common methods of signature analysis [1-3] for intrusion detection or statistical analysis methods [4-5] - used to identify anomalies - are not able at the proper level to ensure information security. Signature methods and statistical analysis are unable to detect new attacks, which are characterized by the lack of records in the security system [1-5].

Heuristic methods have a high likelihood of false positives. This situation stimulates the search for and development of new methods and techniques aimed at increasing the reliability of detection of computer attacks. Therefore neural network technology and other evolutionary mechanisms are increasingly used and such means proved their effectiveness in biological systems.

The analysis of well-known papers in these areas [6-10] revealed a number of disadvantages associated with: a continuous increase in the amount of memory for storage information about the invasion; the complexity of creating or selecting the necessary detectors for the detection; time-consuming to calculate; a high rate of positive errors and low rate of their detection. To speed up decision-making in such systems, as well as to improve the detection of network attacks, the authors propose to apply the neural network in combination with the method of principal components.

2. Neural network structure detector for detection of computer attacks

In [11, 12] a system of network intrusion detection is proposed basing on the method of neural networks, it consists of neural detectors that scan the network traffic to identify its abnormality. A multilayer neural network with one hidden Kohonen neurons layer [13] is considered there as the detector heart.

The first layer of neural cells is a distributor designed for the distribution of input signals to neurons in the hidden layer. Inputs signals are the network connection settings, which characterize the network traffic and provide information about the time of connection, protocol type, number of bytes transferred, number of errors during the connection, etc. The number of neural elements of the distribution layer is corresponded to the number of attributes of network traffic, $n = 41$.

The second layer of neural network consists of Kohonen neurons [13]. The Kohonen layer plays a key role in data classification and clustering, the input space images. As the result it formats clusters of different images, each of which corresponds to the definite neural element. To train the hidden layer neurons is used the principle of competitive learning accordance to the rule «winner takes all» (winner-take-all) [13-15]. The number of neurons in the Kohonen layer is equal to m, which are connected with two output layer neurons. However, the proposed feature of neural network detectors is that their number is divided into two parts: the first of Kohonen layer neurons correspond to the class of computer attacks and related to the first neuron of the output layer, and the last l neurons correspond to the class of normal network connections and connected to the second output layer neuron. Thus, the number of neurons in the hidden Kohonen layer is equal to

$$m = f + l, \tag{1}$$

where f – is the number of Kohonen layer first neurons that correspond to the class of network attack, l – is the number of Kohonen layer last neurons to activity of which characterize the class of normal, legitimate connection.

The third layer consists of two linear neural elements that use a linear function of activation [14, 15] and carry out a mapping of clusters, which are formed by a layer of Kohonen, in two classes, which characterize a normal connection or an attack. The activity of output neuron when its equal to one, is characterized by anomalous network traffic, of attack. Zero at the output describes normal, legitimate connection.

In general, the output value of the j neuron of the third layer is defined as follows:

$$Y_j = \sum_{i=1}^{m} \omega_{ij} \cdot Y_i, \tag{2}$$

where ω_{ij} – a weight between the i neuron of Kohonen layer and the j neuron of the linear layer.

If the neuron-winner in Kohonen layer has the number k, then the output value of the j neuron in the third layer is equal to

$$Y_j = \omega_{kj} \cdot Y_k. \tag{3}$$

A feature of presented detector is that the neurons in the hidden layer are divided into two groups: the first group characterizes the class of network connections related to computer attacks; the second one characterizes the class of normal connections.

3. Training the neural network detector for computer attacks identification

Since the proposed neural detector contains a hidden layer that consists of Kohonen neurons so for teaching of such network is used controlled competitive learning [14], in accordance with the rule «winner takes all». The essence of this method of learning is that during the process of learning takes place the competition between the neural elements of the Kohonen layer, which determines the neural winner element, that characterizes the membership of a given data to a particular class. To identify the neuron-winner can be used of Euclidean distance or Hamming distance, etc. During the training process, synaptic connections for the neuron-winner amplified, while other neurons are unaffected. Thus, after

training the neural network while the input image is given the activity of the neuron-winner is taken as one, and the remaining neurons are «reset» to zero.

Since the Kohonen layer is used the separation of neurons into the classes that characterize either legitimate connection or network attack, so the correct classification occurs, when to the input of the neural network are given connection parameters relating to a class of computer attacks, where the winner is one of *f* Kohonen layer's neurons, or, when to the input of the neural network are given parameters of the normal connection where the winner one of the *l* neurons of Kohonen layer. In other cases there is an incorrect classification.

As a result the Kohonen layer learning method is as follows:

1. Random initialization of weight factors ω_{ci} neurons Y_i of Kohonen layer.

2. The distribution of the input image (a vector that consists of 41 parameters of network connections) from the training set for neural network and computation of the following parameters:

a) the Euclidean distance between the input image and weight vectors of neural elements of the Kohonen layer is calculated:

$$D_i = \left|X - \omega_i\right| = \sqrt{\begin{matrix}\left(X_1 - \omega_{1i}\right)^2 + \left(X_2 - \omega_{2i}\right)^2 + \\ \ldots + \left(X_n - \omega_{ni}\right)^2\end{matrix}}, \quad (4)$$

where $i = 1, m$.

b) the neural winner element with a number *k* is determined:

$$D_k = \min_j D_j. \quad (5)$$

c) the modification of weights factors of the neuron-winner are made. Moreover, if to the input of the neural network are given parameters of network attack with the winner one of the *f* neurons, or, if to the input of the neural network are given parameters of the normal network connection, with winner one of the *l* neurons in Kohonen layer, the modification of weights factors are made according to the following expression:

$$\omega_{ck}(t+1) = \omega_{ck}(t) + \gamma(X_c - \omega_{ck}(t)), \quad (6)$$

where γ – a training step.

Otherwise, the weights factors of Kohonen layer neurons are modified according to:

$$\omega_{ck}(t+1) = \omega_{ck}(t) - \gamma(X_c - \omega_{ck}(t)). \quad (7)$$

3. The process is repeated from step 2 for all input images.

4. Training is made to the desired degree of coordination between the input and weight vectors.

To train the proposed neural network detector the training sample is used, that consisting of 80% of the connections of one of the types of attacks, and 20% of the normal connection, the ratio of attacks to normal connections is equal four to one. This ratio was obtained by experiment and it confirmed the best results of network traffic classification. Also it should be noted that detectors - in which the hidden layer neurons have the division into classes equal four to one - show the best result in the classification of network traffic.

4. Detecting the network attacks using the principal components method

The system uses the 22 detectors - one for each class of network attacks [16]. Whole network traffic is characterized by 41 connection parameters [17]. The analysis of network traffic shows that this set of parameters contains a lot of redundant information. In principle it is possible to ignore some connection parameters and to achieve at the same time increase in speed of decision taking, and due to this - to improve the quality of detection of network attacks. To find the parameters that pose the most significant information, it is suggested to use the principal component methods or Principal Component Analysis (PCA) [18], which allows to reduce the dimensionality of data with the least amount of information loss.

To determine the number of principal components is proposed to use a criterion of informativity:

$$J = \frac{\lambda_1 + \lambda_2 + ... + \lambda_p}{\lambda_1 + \lambda_2 + ... + \lambda_n} \tag{8}$$

where λ_i – the amount of information in the*i*-th component.

Using formula (8) we may analyze the distribution of the information contained per each subsequent component *n* and determine the number of principal components *p*, which should be used for further analysis without significant loss of relative informativity*J*.

Experimental studies [15] showed that one major component contains the 52.4% of information, the two main components containthe 71.7% of information, the three main components contains the 88.4% of information, and the first 12 principal components contain 99.2% of information about network connections.

It's also experimentally confirmed that successful learned detectors and analyzed network connections require th 12 principal components only, rather than 41 parameter. It allowed to reduce the dimension of the analyzed information by 3.4 times loosing the relative informativity of 0.8%.

5. Inclusive classifiers for hierarchical classification attacks

The aggregate neural network detector is a detector that consists of a set of neural detectors, each of which is trained on a particular type of attack. Since the 22 types of network attacks are indicated and they are united in four classes (DoS, U2R, R2L and Probe) let's consider the total scheme of classification for hierarchical classification based on 22 multi-neural detectors that are trained to a certain type of attack (Fig. 1) [19].

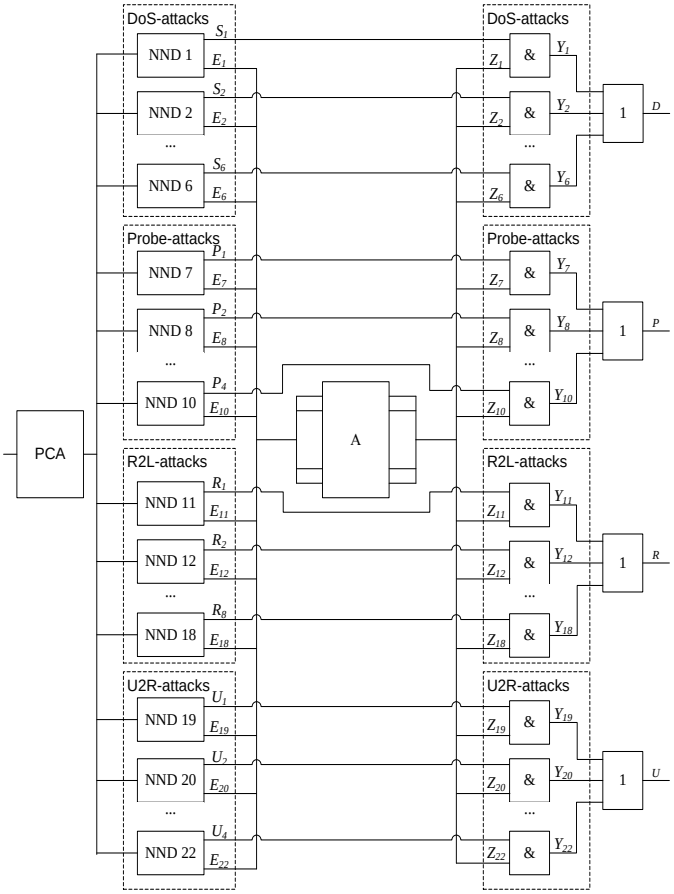

Fig. 1. Comprehensive classification scheme for hierarchical classification of computer attacks
Rys. 1. Ogólny schemat klasyfikacji hierarchicznej ataków komputerowych

A compressed set of input data with dimensionality 12 gets on neural network detectors, each of which is trained on the appropriate type of attack. If the detector detects an attack, then the output value of its first output is set into a single state. To resolve conflicts in such classifier - when several detectors are installed in the single state - a minimum Euclidean distance between the input image and weight vectors of the corresponding detector is transferred into the second output of each detector:

$$E_j = \min_j D_j = \min_i \sqrt{(x_1 - w_{1j})^2 + (x_2 - w_{2j})^2 + ... + (x_{12} - w_{12j})^2} \quad . \tag{9}$$

Information on the minimum Euclidean distance from each detector arrives at *A* referee determining the detector with the number *k*, that has minimum Euclidean metric:

$$E_k = \min E_j,\ j = \overline{1,22}. \tag{10}$$

As a result, the *k*-th output of the referee is set in single state and the other output - in zero state:

$$Z_i = \begin{cases} 1, if\ i = k \\ 0, \text{otherwise} \end{cases}. \tag{11}$$

At the output of logic elements «*I*» the type of attack is identified:

$$Y_i = F_i Z_i \tag{12}$$

where $F_i = \begin{cases} S_i, if\ i = \overline{1,6} \\ P_i, if\ i = \overline{7,10} \\ R_i, if\ i = \overline{11,18} \\ U_i, if\ i = \overline{19,22} \end{cases}$.

The output of logic elements «*OR*» defines a class of attack:

$$D = \bigvee_{i=1}^{6} Y_i,\ P = \bigvee_{i=7}^{10} Y_i,\ R = \bigvee_{i=11}^{18} Y_i, U = \bigvee_{i=19}^{22} Y_i, \tag{13}$$

where *D* – DoS-attack; *P* – Probe-attack; *R* – R2L-attack; *U* – U2R-attack.

Uniting the neural detectors, trained for a certain type of attack, the aggregated classifier allows classifying the network attacks and eliminating conflicts in the neural detectors.

6. Experimental results

The results of experimental studies (tables 1 and 2) confirmed increasing the reliability of detecting attacks that use the principal component preprocessing information about network connections.

Table 1

A comparative analysis of DoS-attacks detection

	Back, %	Land, %	Neptune, %	Pod, %	Smurf, %	Teardrop, %
with PCA	99.5	100.0	100.0	98.1	100.0	100.0
withoutPCA	99.5	90.5	100.0	98.1	100.0	100.0
Improvements	0.0	9.5	0.0	0.0	0.0	0.0

Table 2

A comparative analysis of Probe-attacks detection

	Ipsweep, %	Nmap, %	Portsweep, %	Satan, %
with PCA	65.2	100.0	99.9	99.3
withoutPCA	7.1	54.5	99.6	99.3
Improvements	58.1	45.5	0.3	0.0

It can be seen from the results above, the quality of detection is significantly increased usingthe principal component method applying to the parameters of the network traffic.

7. Conclusion

This work demonstrates: for the successful analysis of network traffic is sufficient to use the first 12 principal components, which contain more than 99% of information about network connections instead 41 parameter. It allowed to reduce the dimension of the analyzed information in 3.4 times loosing the relative informativity of 0.8%, and speed up significantly the training process as a neural network detector as well as process of analyzing the network traffic.

The scheme of hierarchical classification of attacks was designed; it consists of a set of multi-neural detectors, each of which is trained for a certain type of attack allowing determining the type and class of network attacks. The scheme eliminating the conflicts in the neural detectors was designed as well.

Since some types of attacks are not well detected by the developed system the artificial immune systems method could be explored in future work.

Bibliography

1. Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents/MueenUddin, Azizah Abdul Rehman, NaeemUddin [et al.]//International Journal of Network Security, Vol. 15, No. 2, 2013, p. 79-87.

2. Anomaly-based network intrusion detection: Techniques, systems and challenges/P. Garcia-Teodoro J., Diaz-Verdejo G., Macia-Fernandez [et al.]//Computers and Security, Vol. 28, No. 1-2, 2009, p. 18-28.
3. Salour M.: Dynamic two-layer signature-based ids with unequal databases/M. Salour, X. Su//In Fourth International Conference on Information Technology, 2007, p. 77-82.
4. Wagner D.: Intrusion detection via static analysis/D. Wagner, D. Dean//Proceedings of the 2001 IEEE Symposium on Security and Privacy, 2001, p. 156.
5. Yeung D.-Y.: Host-based intrusion detection using dynamic and static behavioral models/ D.-Y. Yeung, Y. Ding // Pattern Recognition, Vol. 36(1), 2003, p. 229-243.
6. Debar H., Becker M., Siboni D.: A neural network component for an intrusion detection system, in Proc. of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1992, p. 1-11.
7. Gaffney J. Jr, Ulvila J.: Evaluation of intrusion detectors: A decision theory approach, in Proceedings of IEEE Symposium on Security and Privacy, (S&P), 2001, p. 50-61.
8. Ragsdale D.J., Carver C.A., Humphries J.W., Pooch U.W.: Adaptation Techniques for Intrusion Detection and Intrusion Response Systems, in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Nashville, Tennessee, October 8-11, 2000, p. 2344-2349.
9. Spafford E.H., Zamboni D.: Intrusion detection using autonomous agents, in Computer Networks, Vol. 34, Issue 4, October 2000, p. 547-570.
10. Ruck D., Rogers S., Kabrisky M., Oxley M., Suter B.: The multilayer perceptron as an approximation to a Bayes optimaldiscriminant function, IEEE Transactions on Neural Networks, Vol. 1, No. 4, 1990, p. 296-298.
11. Komar M.: Methods of artificial neural networks for network intrusion detection// Proceedings of the Seventh International Scientific Conference “Internet - Education - Science – 2010”, Vinnitsa (Ukraine), 2010, p. 410-413.
12. Komar M.: System for analyzing network traffic to detect computer attacks. Herald Brest State Technical University. Physics, mathematics, computer science, No. 5, 2010, p. 14-16.
13. Kohonen T.: Sell-organised formation of topologically correct feature maps. Biological Cybernetics, No. 43, 1982, p. 59-69.
14. Golovko V.: Neural Networks: training, models and applications/V. Golovko, A. Galushkin. Radiotechnika, Moscow 2001, p. 256.
15. Komar M.: Intelligent System for Detection of Networking Intrusion/M. Komar, V. Golovko A., Sachenko S., Bezobrazov//Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011): IEEE international conference, 15–17 September 2011, Prague, Czech Republic 2011, p. 374-377.
16. Tavallaee M., Bagheri E., Wei Lu, Ali, A. Ghorbani: A Detailed Analysis of the KDD CUP 99 Data Set”/Proceedings of the 2009 IEEE Symposium on Computational

Intelligence in Security and Defense Applications (CISDA 2009). DOI: 10.1109/CISDA.2009.5356528. Publication Year 2009, p. 1-8.
17. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.
18. Gorban B., Kegl D., Wunsch A., Zinovyev (Eds.), Principal Manifolds for Data Visualisation and Dimension Reduction, LNCSE 58, Springer, Berlin – Heidelberg – New York 2007.
19. Komar M.: Method of Aggregate Classifier Construction for Hierarchical Classification of Computer Attacks/V. Golovko, O. Lyashenko, A. Sachenko//CAD in Machinery Design. Implementation and Educational Issues (CADMD 2012): international conference, 11-13 October 2012: proceedings. Lviv, Ukraine, 2012, p. 80-82.

Omówienie

W artykule zaprezentowano podejście do projektowania detektora ataków komputerowych za pomocą sieci neuronowej i kwantyzacji wektorowej, bazującej na ulepszonej metodzie hierarchicznej klasyfikacji ataków komputerowych i kompresji informacji za pomocą analizy głównych składowych i łączenia sieci neuronowych detektorów.