The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
21-23 September, 2017, Bucharest, Romania

High performance adaptive system for cyber attacks detection

Myroslav Komar, Volodymyr Kochan, Lesia Dubchak, Anatoliy Sachenko
Research Institute for Intelligent Computer Systems, Ternopil National Economic University, Ukraine, mko@tneu.edu.ua

Abstract — To increase the security of intrusion detection system, generalized structure of highly performance adaptive system for cyber attacks detection was developed. To improve its robustness, methods of artificial intelligence were proposed. Neural immune detectors were used as the main tool for identifying cyber attacks. These detectors for cyber attacks identification and classification and other vulnerable subsystems were implemented in programmable logic arrays. To provide high performance, the Mamdani fuzzy inference rules were used and relevant subsystem structures were developed.

Keywords — intrusion detection system, high performance adaptive system, cyber attacks, artificial intelligence, neural immune detector, programmable logic arrays, Mamdani fuzzy inference

I. INTRODUCTION

Today, the protection of computer systems from cyber attacks is an important and urgent issue. Specialized software is basically used to protect computer systems from cyber attacks [1-4]. However, nowadays, most malware can counteract a lot of anti-virus software. Therefore, this software is vulnerable to intrusion. Operating system functions can be intercepted during attacks. This prevents identification and malware neutralization by means of specialized software. In addition, malware can counteract specialized software running, keep track of its operations, recover deleted malicious processes, change the settings in the system registry, etc.

Nowadays, a combined method for identification and classification of cyber attacks provides relatively high efficiency of computer system protection [5-7]. Specially trained neural network is considered to be the main detector of the system for identifying intrusions. To increase the efficiency of such system, the basic principles and mechanisms of biological immune systems were also used. This approach is based on the integration of neural network detectors into the artificial immune system [8]. Due to this approach, protection system against cyber attacks can adapt to unknown intrusion, occurred as a result of cloning and mutation. Thus, this intelligent intrusion detection system uses a set of specialized detectors. Each detector is responsible for identification and classification of a certain type of intrusion and a set of such detectors are responsible for the entire system protection. However, the implementation of this method has all the disadvantages of software protection, which were mentioned above.

Thus, there is a contradiction between the robustness of computer system to intrusion and principal vulnerability of tools, providing such protection against cyber attacks. The solution to this contradiction is possible only in case of changing the paradigm of making tools, providing protection against intrusions.

II. THE PROPOSED APPROACH TO IMPROVING SECURITY OF INTRUSION DETECTION SYSTEM

In this paper, hardware is proposed to use in order to protect computer systems against cyber attacks. Hardware is not running on an infected operating system. Therefore, any of malware cannot counteract or modify the hardware operations without being identified or neutralized. All its attempts will be unsuccessful, and cyber attacks will be quickly neutralized.

To implement this approach, the hardware protection system against cyber attacks should provide meeting the following requirements:

1. High robustness to cyber attacks of the subsystem for current detection and neutralization of various types of attacks. This can be achieved only by hardware implementation of the subsystem.

2. High flexibility of the subsystem for current detection of various types of cyber attacks and their modifications. This can be achieved by periodic dynamic updates of neural detectors according to the results of the current analysis of cyber attacks.

3. For the current analysis of cyber attacks, a dedicated computer for continuous analysis of current attacks and creation of appropriate protection means, including neural detectors that built a system for cyber attacks detection, should be provided.

4. To ensure high robustness of the system (see paragraph 3) to cyber attacks, their analysis and neural network detectors training, preparation of intrusion detection and neutralization hardware for updating should be carried out on the dedicated computer that is not connected to the network. It is necessary to distinguish between the memory, containing the analyzed suspicious codes, and memory with software that carries out the analysis.

5. High performance subsystem for the current detection and neutralization of various types of cyber attacks should be provided by adaptating it to the likelihood of attacks detection.

These requirements can be met by implementing the subsystem for current detection and neutralization of cyber attacks in programmable logic arrays (PLA). In addition, PLA should be reprogrammed on dedicated computer which is used for cyber attacks analysis and it is not connected to the network. Therefore, it cannot be the subject to an attack. Computers connected to the network should not have:

- PLA's reconfiguration means, where the subsystem for current detection and neutralization of cyber attacks is implemented;
- access to PLA's outputs, controlling over its reprogramming.

It should be noted that PLAs are hardware nodes, while the subsystem for current detection and neutralization of cyber attacks has relatively high complexity. Therefore, optimization problem arises, in particular, the problem of reduction in the number of required macrocells. For this purpose, according to the analysis of the functions of the protection against cyber attacks, it is advisable to determine the functions of each subsystem. Thus, the following functions should be provided:

- current detection of the cyber threat and its classification;
- decision-making about availability of cyber attack;
- cyber attack countering;
- analysis of cyber attack modification;
- creation of the appropriate means of cyber attacks detection, that is, neural detectors;
- statistical processing of cyber attacks in order to find out their origin;
- ensuring adaptation to the likelihood of attacks.

III. Generalized Structure of High Performance Adaptive System for Intrusion Detection

Generalized block diagram of the system for detection and neutralization of cyber attacks that meets above defined requirements for the performance of its units is shown in Fig. 1. It consists of two parts. The first one is implemented in hardware and is running continuously in real time. It consists of a fuzzy address analyzer, a set of neural detectors and a subsystem of decision-making and implementing. The second one is implemented in software and represented by a dedicated computer, which is used for current attacks analysis and creation of appropriate protection means. In this part, according to the previously defined features, the subsystems for analysis and neural network training, control and statistical processing of cyber attacks data can be identified. This part includes also a dedicated buffer where suspicious code is recorded for its detailed analysis. In addition, resident software of the second part keeps track of the buffer codes in order to treat them only as data. Any of the instructions, which are included into the code, contained in dedicated buffer, cannot be performed.

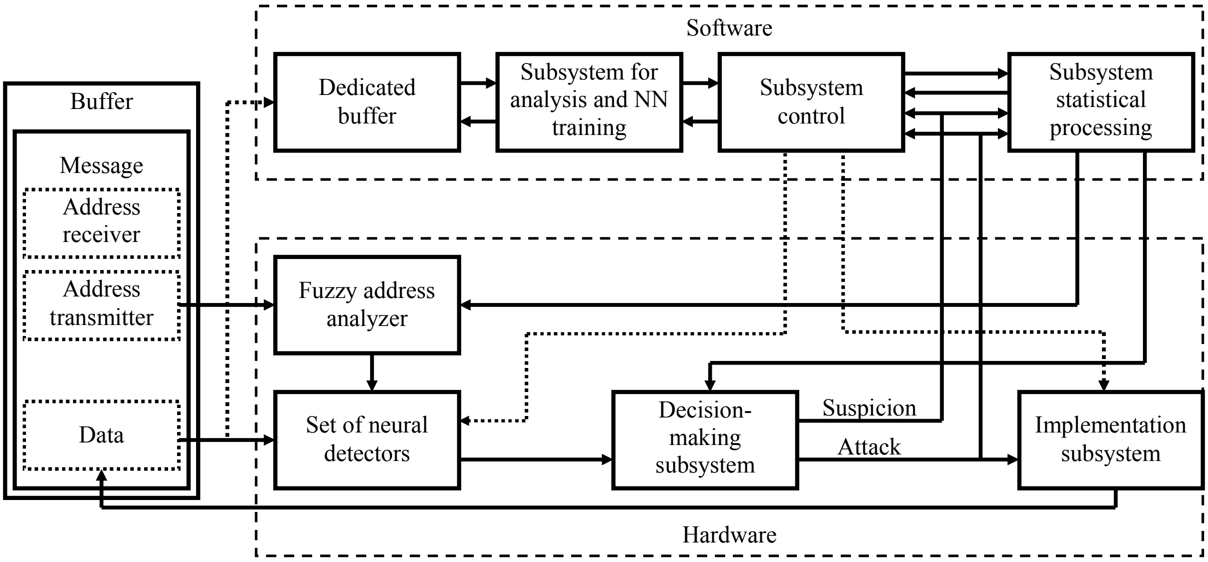

Fig. 1. Generalized block diagram of the system for cyber attacks detection and neutralization

The system for detection and neutralization of cyber attacks runs in a following way. Fuzzy address analyzer conducts continuous analysis of the current message source. Accumulated data about the history of cyber attacks, detected previously, allow to reduce the time for analysis of data, contained in the certain message. For this purpose, the results of statistical processing of the frequency of cyber attacks and their types are used. Fuzzy analyzer correspondingly arranges a set of neural detectors in order to reduce the time for analysis of buffer data. Each neural network detector produces two codes for the decision-making subsystem. One of them determines the likelihood of cyber attack. The second one determines the probability of the absence of such an attack. Such neural network detectors organization increases the efficiency of the decision-making subsystem. Due to the probabilities of availability or absence of the cyber attack and the defined level of trust in the given source of information, the decision-making subsystem can not give any signal (there is no cyber attack) or give signal "attack" (there is an intrusion) and "threat"(there is a probability of cyber attack).

Signal "attack" is received by the decision-making subsystem, which cleans the buffer and sends a certain message to the source of information. Signal "attack" is also received by the statistical processing subsystem to change the statistics on the frequency and a type of cyber attacks, referring to this source of information.

In addition to the signal "attack", the statistical processing subsystem also receives the signal "threat" in order to change the statistics on the frequency and a type of cyber attacks, referring to this source of information. But this signal is also received by the control subsystem. This subsystem initiates investigation of the suspicious code. For this purpose, hardware buffer data is rewritten into the buffer, dedicated to the analysis of cyber attacks and creation of protection means. Its subsystem for the analysis and neural networks training carries out the analysis of the suspicious code. Due to the fact that subsystems for analysis of current attacks and creation of appropriate protection means may not be running in real time, the sufficient detailed analysis can be carried out. If suspicious code is classified as a cyber attack, the control subsystem will permit to delete data in the hardware buffer (i); will learn certain neural network and create a new neural detector (ii). This neural network detector will be included in the set, located in the first part of the system for detection and neutralization of cyber attacks. This inclusion is implemented by reprogramming logic array, which contains the rest of neural detectors. Reprogramming is carried out by a computer, dedicated to the analysis of attacks and creation of appropriate protection means. Due to the fact, that this computer is not connected to computer network, there is no danger of modification of the system for detection and neutralization of cyber attacks, as a result of intrusion.

Statistical processing subsystem keeps track of identified cyber attacks as well as of their threats. As a result, characteristics of information sources, which are processed by the system for detection and neutralization of cyber attacks, are defined. These statistical data allows to adapt a set of neural network detectors to cyber attacks that are typical for the particular source of information. This can significantly reduce the time for data analysis. Statistical processing subsystem also adjusts the decision-making subsystem according to the likelihood of cyber attacks from the particular source. Thus, the time of the test for cyber attacks can be significantly reduced, that is, communication bandwidth is increased.

IV. The Main Components of the System for Cyber Attacks Detection

Fuzzy address analyzer and a set of neural detectors are the most important components of the system for cyber attacks detection. Let's consider them in detail.

The main functions of the fuzzy address analyzer can be defined as the following ones:

1. Accepting from statistical processing subsystem the corresponding functions of output belonging for each of fuzzy inference rules.

2. Accepting from statistical processing subsystem the current required values of performance, robustness to intrusion and possible storage consumption according to the estimated intrusion probability in the current channel.

3. Calculating the certain center of gravity of the final shape of functions of output belonging.

The structure of fuzzy address analyzer is shown in Fig. 2. The values of expected performance of required robustness to cyber attacks and allowable storage consumption are received at its input. However, these values are received as two options i.e. as a result of statistical processing (functions of output belonging that characterize the current information source), and as the current requirements of the system (characteristics of the current system traffic). At the output, the coordinates of the gravity centre of the figure, based on the Mamdani inference rules [9, 10] and the functions of entrance belonging, are received. This gravity centre, in its turn, determines the types of expected attacks from the certain source of information and their probability, that is, the gravity center determines which of the sets of neural detectors is sufficient for the analysis of data, received from this source of information.

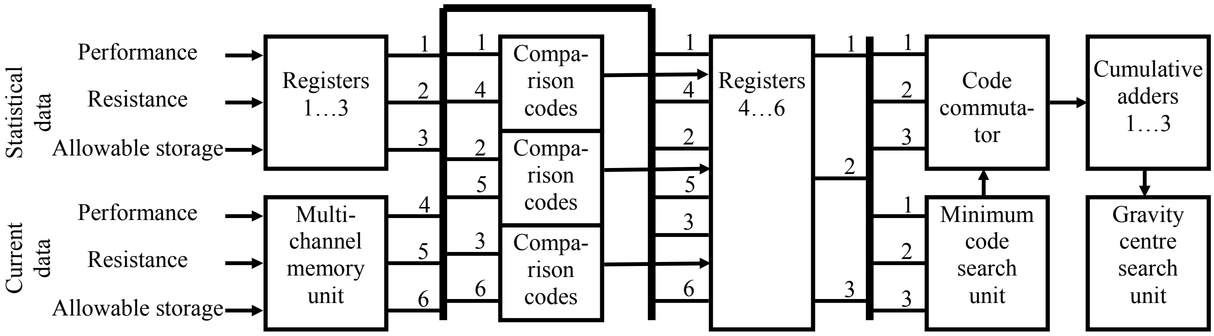

Fig. 2. The structure of fuzzy address analyzer

Fuzzy address analyzer operates in a following way. Having been received at the entrance of the analyzer, the values of both options of expected performance, necessary resistance to cyber attacks and allowable storage consumption are compared. Smaller code values are recorded in the registers 4 ... 6. Then, according to the Mamdani inference rules [9, 10], minimum code search unit identifies the rest of the minimum codes. They are transferred through the switchboard to the cumulative adders. Formula numerator and denominator are generated by these adders and gravity centre is calculated by this formula. Coordinates of the gravity centre are calculated by the gravity centre search unit. It is performed as a unit of division of values, obtained in the cumulative adders. To ensure high performance for this unit, it is advisable to construct it as a permanent storage device. In this case, the divided and divider are received at the entrances of permanent storage device address. The calculated results of division are recorded in memory cells in advance.

Another important component of the system for cyber attacks detection is a set of neural network detectors. This approach can be presented by the following set of steps [11-13]:

1. Generation of immune detectors. At this step, neural network detectors are generated with random initialization of weighting coefficients.

2. Training of immune detectors. To detect attacks of a certain type, not one trained immune neural network detector can be used, but several, by differently trained detectors, which allows diversifying the detectors and, correspondingly, improving the detection of computer attacks. As a result, a set of various detectors is created to analyze network traffic in order to detect network attacks.

3. Selection of immune detectors. To minimize the occurrence of false positives, when a normal connection is accepted as a network attack, all trained immune neural network detectors are tested for correct classification. For this, a test sample consisting of normal connection parameters is used. If the i-th detector classifies one of the test connections as an attack, it is destroyed, and a new detector is generated and trained instead.

4. Functioning of immune detectors. All network traffic received by the computer is first analyzed by a set of immune detectors, and if none of the detectors detects an anomaly, the traffic is processed by the operating system and the corresponding software. In addition, each detector is endowed with a lifetime, during which time it analyzes network traffic.

5. Activation of immune detectors. Activating detectors involves detecting a network attack by the detector. In the event that a network connection is classified by one or more detectors as a network attack, it is blocked.

6. Formation of immune memory. When a network attack is detected, it is advisable to store its parameters for the purpose of subsequent detailed analysis. In order to improve the detection quality, and also to give the intrusion detection system the flexibility, the parameters of the network connection classified as an attack are saved and entered in the training sample, thereby replenishing it with up-to-date data.

V. Conclusions

The approach of improving of the security level of the intrusion detection system is offered according to the implementation of the neural network detectors on the programmable logic arrays and introduction of the decision-making system due to Mamdani fuzzy inference rules.

Computer simulation proved that the developed high performance adaptive system for cyber attacks detection is more resistant both to well known threats and new intrusions.

References

[1] Golovko V. Neural Network and Artificial Immune Systems for Malware and Network Intrusion Detection. Studies in computational intelligence / V. Golovko, S. Bezobrazov, P. Kachurka, L. Vaitsekhovich // Springer Berlin/Heidelberg, Advances in machine learning II. – 2010. – Vol. 263. – P. 485–513.

[2] Kotenko I. Multi-agent Simulation of Attacks and Defense Mechanisms in Computer Networks / I. Kotenko // International Journal of «Computing». – 2008. – Vol. 7, no. 2. – P. 35 – 43.

[3] Bezobrazov S. Artificial immune system approach for malware detection: neural networks applying for immune detectors construction / S. Bezobrazov, V. Golovko // Inernational Journal of «Computing». – 2008. – Vol. 7, no. 2. – P. 44-50.

[4] Kachurka P. Fusion Of Recirculation Neural Networks For Real-time Network Intrusion Detection And Recognition / P. Kachurka, V. Golovko // International Journal of Computing. – 2012. Vol. 11, no. 4. – P. 383-390.

[5] Komar M. Method of detection of computer attacks by the neural network artificial immune system / M. Komar, A. Sachenko, V. Golovko, S. Bezobrazov // Pat. Number 109640 Ukraine, 2015 (In Ukrainian).

[6] 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 : Proceedings of the 6th IEEE International Conference, Prague (Czech Republic), September 15-17, 2011. - V1. - P. 374 - 377.

[7] Komar M. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications : Proceedings of the 7th IEEE International Conference, Berlin (Germany), September 12-14, 2013. - V2. - P. 665-668.

[8] Dasgupta D. Recent advances in artificial immune systems: models and applications / D. Dasgupta, S. Yu, F. Nino // Applied Soft Computing. – 2011. – T. 11. – №. 2. – C. 1574-1587.

[9] Shtovba S.D. Ensuring Accuracy and Transparency of Mamdani Fuzzy Model in Learning by Experimental Data / S.D. Shtovba // Journal of Automation and Information Sciences. – 2007. – № 39 – P. 39-52.

[10] Dubchak L. Fuzzy Data Processing Method / L. Dubchak, N. Vasylkiv, V. Kochan, A. Lyapandra. // Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications : Proceedings of the 7th IEEE International Conference, Berlin (Germany), September 12-14, 2013. – V1. - P. 373-375.

[11] Komar M. Increasing the Resistance of Computer Systems Towards Virus Attacks / M. Komar, A. Sachenko, V. Kochan, T. Skumin // Proceedings of the 36th IEEE International Conference on Electronics and Nanotechnology (ELNANO-2016). – Kyiv, Ukraine, TUU «Kyiv Polytechnic Institute», 2016. – P. 388-391.

[12] Komar M. Improving of the Security of Intrusion Detection System / M. Komar, V. Kochan, A. Sachenko, V. Ababii // Proceedings of the 13th International Conference on Development and Application Systems (DAS-2016). – Suceava, Romania, May 19-21, 2016. – P. 315–319.

[13] Komar M. Intelligent Cyber Defense System / M. Komar, A. Sachenko, S. Bezobrazov, V. Golovko // Proceedings of the 12th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer (ICTERI 2016). – Kyiv, Ukraine, June 21-24, 2016. – P. 534-549.