APPLICATION THE ARTIFICIAL NEURAL NETWORK IN THE INTRUSION DETECTION SYSTEM

Anna Slyvka, Rostyslav Grynyk

Lviv State University of Life Safety, Lviv, Ukraine

Defined a term "intrusion detection system" and described the main classification. Shown the general structure of the neural network. Descripted the options of neural networks usage in systems, which detect network attacks and described the main positive and negative aspects of such systems. Analyzed the advantages of using fuzzy neural networks in IDS.

Keywords: artificial neural network, fuzzy set, intrusion detection system (IDS).

Having become a sensation in the 1950s-1960s, neural networks as the embodiment of physiological and biological aspects remained in the shadow of traditional computing and were forgotten for long, but interest in neural networks (hereafter referred to as ANN) is growing rapidly these days due to the ability to use ANN in a wide variety of human activities.

Many life-sustaining activities that were within human intellect's control only as it was mistakenly considered, appeared to be susceptible to theoretical and applied computing capabilities pertaining to "artificial intelligence." ANNs are inspired by biology, since they consist of elements, which features are similar to most elementary functions of biological neurons [1]. ANNs are constructed by artificial interacting neurons that act as simple handlers of information; a figure of simple neural network is suggested by Fig. 1. Thus, creating a multiple network of artificial neurons and ensuring control of their interaction, we can perform quite complex tasks.

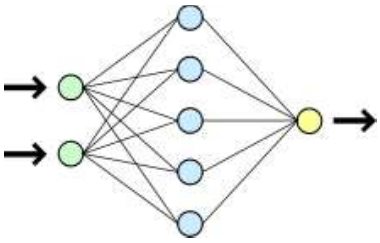

Fig. 1. The scheme of the simple neural network. Green represents the input neurons, blue - hidden neurons, yellow - output neuron

Such basic properties as educability, generalization and abstraction justify the use of neural networks in intrusion detection systems. Intrusion detection system (Intrusion) is a hardware or software tool designed to detect unauthorized attempts to access a computer system or network or unauthorized management via the Internet [2]. The number of IDS technologies have emerged. Each type has its own pros and cons in features of detection, configuration, and overall cost.

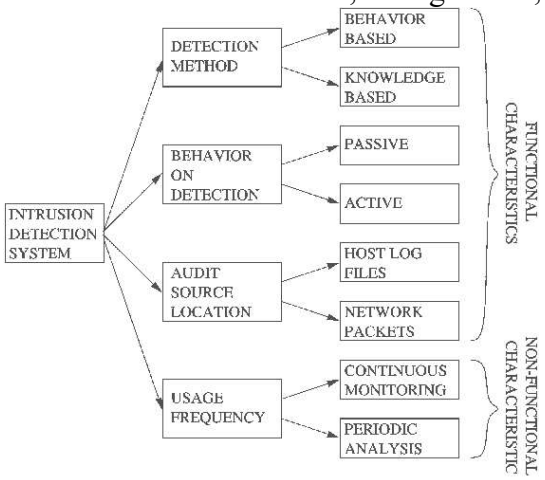

Fig. 2. Characteristics of intrusion detection system [3].

There are two types of intrusion detection systems: network IDS and host IDS. Intrusion detection process is a complex operation that consists of three main components:

• detection of patterns that indicate any violations required by security policy;
• identification of the sources that may contain the patterns of violations of security policy;
• usage the various methods of information analysis [4].

Intrusion detection systems provide an additional level of protection of information systems when combined with intrusion prevention system (IPS). Often both types operate as one, thus forming a comprehensive system of IDPS (IDS i IPS).

In modern systems of detecting network intrusion attacks (IDS) one can observe different modes of using neural networks. For example, the neural network can be used as a complement to existing expert systems aimed at filtering the inbox in order to reduce the number of false operations, which are common in most expert systems. Thus, sensitivity of the system increases as the expert system receives data only on events that are considered suspicious. If the neural network began identify new attacks as a result of training, the expert system must be updated, otherwise these attacks will be simply ignored.

If the neural network is a complete intrusion detection system, the analysis of information with regard to system-related misuse is conducted during traffic processing. Any cases that are identified as possible attacks, are processed by the automatic attack response system or redirected to the security administrator. In comparison with the previous approach, this principle possesses only one level of analysis, which greatly accelerates the speed of its work. In addition, such an intrusion detection system is highly adaptive.

One of the main drawbacks of the neural network is preconception, or "opacity" of formation of results after the analysis. However, hybrid neuro-expert or neuro-fuzzy systems allow to see the system of fuzzy rules in the structure that are automatically adjusted in neural network teaching. The adaptive property y of fuzzy neural networks enables:

• to solve separate tasks of identifying threats;
• to juxtapose the users' behavior with existing templates in the system;
• to generate new rules automatically when the new types of threats appear.

One way to optimize the intrusion detection system is to combine it with genetic algorithms. For example, to protect networks from application-governmental attacks designed to breach the availability of resources, the neural network is used to detect tokens of attacks in network traffic, identification of data formats, which are transmitted, and genetic algorithms - to get close to the best decision in managing traffic routes and parameters in the presence of non-identification attacks accuracy in terms of lack of information or information "noise". In addition, fuzzy sets can be applied to the implementation of active security audit of the system. Fuzzy neural network has the following advantages:

• distributed computing parallelism;
• adaptive neuro-fuzzy information security systems (fuzzy rules);
• the possibility of classifying threats;
• objectivity, or "transparency" of structure analysis;
• functional stability and security of the components.

Development of intellectual instruments of detection of attacks and unauthorized information processes in a network, which is built on the benefits of adaptability property, has always been a promising trend in the use of neural networks in intrusion detection systems.

Literature

1. Why artificial neural networks?. [Electronic resource] - Access: http://www.victoria.lviv.ua/html/wosserman/vstup.htm#v2
2. The system of detection of attacks. [Electronic resource] - Access https://uk.wikipedia.org/wiki/IDS
3. A Study on Recent Trends and Developments in Intrusion Detection System.- IOSR Journal of Computer Engineering (IOSR-JCE) [Electronic resource] - http://www.iosrjournals.org/
4. Intrusion detection systems and their application tools. [Electronic resource] - Access: http://5fan.ru/wievjob.php?id=3960