The Methodology of the Ways for Increasing the Efficiency of Intrusion Detection Systems

GulomovSherzodRajaboevich
sherhisor30@gmail.com

KadirovMirhusanMirpulatovich
mirhusank@rambler.ru

TulyaganovZoxidjonYakubdjanovich
informtgtu@mail.ru

***Abstract* – This paper is considered the possibility of the modification standard gradient algorithms of the education methods, foundedto use multifunction heuristic procedures for increasing the efficiency of the operating the expert systems. The method definition of necessary parameters of decoy targets, providing most flow attacks to decoy targets is offered.The model of intrusion detection computer attacks, using in quality sign of detection position of the security policy, formalized with facility of the hardware of the hierarchical ill-defined systems.**

***Keywords* – Neural Networks, Heuristics, Decoy Targets, Flow Attacks, Automated Information System, Security Policy, Fuzzy Variables.**

I. Introduction

The problem approximation of different kinds of dependencies occurs under design of complex systems and determination of their internal characteristics. For detecting hidden patterns of problem to be solved, it can use mathematical methods, but they do not always have a universal character and are suitable for a wide range of tasks and may require large computational cost. Another direction for approximating dependence associated with the use of artificial neural networks (NN). Based on the fact that unauthorized access are universal approximate, can be identified depending on the desired in most tasks by analyzing information on the operation of systems and training on the basis of this information of neural network. In event of, when necessary to solve challenge,which containing a complex interdependencies that may vary over time, the quality of solving the problem can be improved by using NN ensembles [1]. As a result of parallel processing of a data set of NNand then combining the outputs it is probable that a solution that is superior to the results of each of the neural network, a member of the ensemble.

Under training multilayer NN most commonly used backpropagation. But this method has several disadvantages, the most significant - is indefinitely long learning process. In complex problems learning can occur for a long time, which leads to the fact that it is impossible to use a NN ensembles in intrusion detection systems, because Many of them have to work in real time. The second disadvantage - it is entering the network in a local minimum. These disadvantages allow eliminate various types of combined procedure by which to implement the small random changes weighting coefficients of the NN.

As a problem to be solved with the help of NN ensemble, consider the problem of intrusion detection in local area network. In most cases, the identification of malicious behavior detected by signatures, which compared with certain packet fields, transmitted over a network. In the case when an attacker changes the attack strategy, this method is useless until the identification and analysis will produce new attack signatures to the subsequent formation. In this case, the use of neural network ensembles can detect the attack, which is new, and the use of multiple neural networks that are part of the ensemble, can increase the probability of detection of this attack.

II. Formation of the Detection System Attacks on Bases Neural Network Associative Machines

In solving complex problems a situation may arise when trying to get an acceptable solution, even when using different algorithms, parallel processing and solving the same problem, do not give results. In this case, the association of several algorithms in the composition allows solve the problem. When solving problems using neural network methods based on the use of multiple neural networks - ensembles, the input data is processed with the help of several unauthorized access. Education each NN was carried out by the method of back propagation using combinatorial heuristics. Ensemble for solutions problems of intrusion detection consisted of three NN [2]. The first NN was trained standard algorithm back-propagation errors. Under training a second NNis used the same learning algorithm, but modified combinatorial heuristics-based look-ahead algorithm. Education the second unauthorized access conducted by the method of back propagation as long as the training error for the difference of two successive iterations is greater than a certain threshold if the error changes the value falls below the set threshold, the heuristics used. Further, the NN was trained by back propagation. The probability of the use of heuristics decreased as learning network to initially prevent the ingress of training method of back propagation of errors in a local minimum and to allow a more detailed network configuration in the final stages. Consider combinatorial heuristic algorithm look-ahead in more detail:

1. Select the neural element of the hidden or output layer of the NN. The weights of the neuron multidimensional view as the starting point x_0 with the number of component $i = 0, 1, 2, \dots N$, to the number of weights within the selected neuron. Assumed$F_{min} = f(x0)$, where F_{min} −error of training NN.
2. For each i −th component, part of the selected point, to optimize, fixing the others:

- randomly selected possible values unfixed i −th component r for forming possible combinations of weighting coefficients so that the combinations of the selected NN training error was less than x_0. If this was not achieved, repeat step 2 for the next $i+1$ components.

- determine the best combinations of r found by weighting factors and put a value equal to the minimum error training F_r.
- perform proactive search.

1) For each of the permissible combinations of the weighting factors found in step 2 (a), carry out a random selection of one of $r$the following possible values $i+1$ components, assuming that it is not fixed.
2) Select the best combinations of found and fixed the value of the components $i$as optimal.
   If $i = N$, proceed to step 3. Otherwise, follow step 2 for the component $(i+1)$.
3) Carry out a random search to determine the best value of the variable N for fixed values of other variables [3]. These points taken as a new reference point x_0, and error learning by substituting a combination found the balance of the base point for the F_{min}.
4) Go to step 2 with$i = 1$, if not satisfied the end computing conditions.

For third NN training was conducted by the method similar to the second neural network, but as a heuristic algorithm was used based on the method of complexes:

1. Select the neural element of the hidden or output layer of the neural network. Based on the weighting coefficients we construct complex consisting of P estimated allowable weighting values. For each point $p = 0, 1, 2, \ldots P$, followthese steps:

Randomly determine the admissibility of the alleged values of weighting coefficients x^r.

a) If received an invalid value, find the center of gravity of $\overline{x}$ already found the weighting values and perform the conversion for each component of the estimated values of the weighting factors:

$$x^r = x^r + 0{,}5 \cdot (\overline{x} - x^r) \ (1)$$

Repeat the procedure until, till the point will not be permitted.

b) Repeat for all other alleged weighting factors.

2. Carry out a reflection of the complex:

a) Select the estimated allowable values of weighting coefficients for the neural element, which when substituted in the neural network training error is the maximum:

$$f(x^R) = \max\big(f(x^r)\big) = F_{max} \ (.2)$$

b)Find the center of gravity $\overline{x}$and new values:

$$x^m = \overline{x} + \beta \cdot (\overline{x} - x^r) \ (3)$$

whereβ −parameter, which specifies the distance of reflection.

c) If obtained in the previous step and allowable combination $f(x^m)$greater F_{max}, it is necessary to halve the distance between the current point and the center of gravity and continue the search.

d) If the resulting combination is valid and training error is less than F_{max}, then go to step 3.

e) If obtained in the previous step invalid combination, it is necessary to reduce in half the distance to the center of gravity and continue as long as the combination does not become valid.

3. If the achieved quality of training criteria, then stop searching and to continue training using back propagation method.

For optimal functioning of the expert is necessary to form their initial states expressed preset weighting coefficients of neural networks. At the same time it should be noted that in this problem the network, not every function individually and in ensemble. Therefore it is necessary to use the principles of optimization based on cooperative co-evolution with multiple populations, taking into account the co-operation of experts. The basis of modification of populations for solutions was laid immune optimization algorithm, built on the principles of immunity of living organisms. Estimated weight NNis coded in antibodies constituting the population. As we consider the problem of antigen initialization state expert. Suppose you want to find a combination of initial states of the three experts, in which the learning process will take place in the shortest possible time and to ensure the effectiveness of co-operation. For each NN optimization process goes independently of the others. It is to produce novel antibodies using mutation operators recombination inversion and various operators. When there is a need for an expert assessment of a population, the experts, the initial states which are caused by the operation of three different populations of antibodies, combined into a single ensemble, and performed evaluation of the effectiveness and functioning of the unauthorized access of training experts from these initial states. Thus, each population of cooperative coevolution tries to find the optimal part of the overall solution. This approach allows us to break the task into subtasks, which reduces the complexity of the solution.

Evaluating the effectiveness of the given algorithms was evaluated by two parameters: the value of the error and set the time. Mismatch M −is a dimensionless [4] quantity which is a measure of the closeness to the graph optimal expert mean square error and experts trained using conventional and modified back propagation algorithm using combinatorial heuristic algorithms:

$$M = \frac{E_{st} - E_{min}}{E_{min}} = \frac{E_{st}}{E_{min}} - 1, (4)$$

whereE_{st} −stable value standard error learning, E_{min} − minimum mean square error of the expert. Mismatch with idealized model for teaching conventional back-propagation algorithm averaged 10%, using heuristics mismatch decreased to 7.35% as well as a faster convergence time of the algorithm to the optimal steady state.

Multilayer perceptron's included in the ensemble and form associative machine differ in architecture, the number of layers, the number of neurons in each layer, the initial states of the weighting factors. NN has to be sufficiently discernible to the errors that occur when searching for a NN solutions were compensated by other members of the ensemble. Following the decision of each NN all output signals are combined in a certain way, in accordance with a predetermined algorithm. The final result obtained in this ensemble of NN can exceed the quality of results from individual NN.

These basic algorithms presented multilayer perceptron, are combined in a composition with a few types of algorithmic compositions: a simple voting, weighted voting and voting by seniority. In the case of weighted voting to adjust coefficients are used the method of assessing the quality of education based on the learning process of the NN. Consider combining techniques making and receiving the resulting solutions.

The simplest example of a corrective surgery is a simple arithmetic average or vote:

$$b(x) = Q\big(b_1(x), \dots, b_T(x)\big) = 1/T \sum_{t=1}^{T} b_t(x) \ (5)$$

In the formula (2.5) $b(x)$ −the algorithmic operator, Q −corrective surgery.

Corrective surgery, which merges the basic algorithms of decisions can have free parameters that must be configured on the training set, along with the parameters of the basic algorithms. An example is a weighted average, also referred to as a linear combination of basic algorithms:

$$b(x) = F\big(b_1(x), \dots, b_T(x)\big) = \sum_{t=1}^{T} a_t b_t(x) \ (6)$$

Weights a_t express the degree of confidence in the relevant basic algorithms.

Voting by seniority called corrective surgery, which is calculated according to the algorithm: if$b_1(y) = 1$, object y is belongs to a class c_1, otherwise the right to vote is passed to the next in seniority $b_2$algorithm. If $b_2(y) = 1$, object$y$is belongs to a class c_2, and so on. Transfer of voting rights can be extended to as long as one of the basic algorithms decides. If all the algorithms return a null value, issued $c_0$response, meaning the rejection of the classification of the object.

The decision by a vote on the seniority problem selecting input data presentation about each algorithm to produce solutions and to assess its suitability. The functioning of the basic algorithm determines which algorithm will give the first answer, if the algorithm does not refuse to make a decision then the response is considered a response to the input action for the entire ensemble. In case of incorrect determination of the order of the entire ensemble can give an unacceptable solution, and the advantage of using an ensemble of several NN will be lost.

A similar problem arises in the weighted voting, since the definition of the weighting factors. The degree of confidence selected algorithm determines which contribute to the overall decision making each expert ensemble. In case of wrong selection of the coefficients, the advantage will be given to the algorithm, which is little suited to the task. To solve the problems in the NN training phase, which consists of an ensemble estimated dynamic learning process. The better the individual members of the ensemble formed, the faster they are able to perceive examples of learning sample. In the case of assessing the quality of training on the average value of the mean square error on the whole set of examples from the training set, it needs a method that can give an idea about the quality of the trained NN architecture and its conformity to the problem being solved. For each NN quality characteristics, in solving this problem, the method of least squares, through which carried out the linear approximation error training schedule individual NN of the ensemble. Using the method of least squares coefficients is linear relationship in which a function of two variables is minimum.

$$H(a,b) = \sum_{i=1}^{n} \big(y_i - (a \cdot x_i + b)\big)^2 \ (7)$$

III. A Method for Increasing the Efficiency of Detection Network Attacks

One of the most important areas in the field of information security research is to detect intrusions. Currently, there are many ways of detecting cyber-attack of various types. Among them, always emphasizes the ways that allow you to detect attacks previously unknown species [5]. To detect such attacks usually applied, the approach based on the identification of abnormal behavior in the network. Often it invited to use various heuristics to identify clearly different from normal behavior. In particular, we propose a heuristic based on the assumption that a legitimate user is not to contact him for an unknown object on the network. To use this heuristic should be placed in a network system that do not participate in other industrial processes, and not advertised as a working network services - the so-called decoy targets. Any network activity is a false target is suspicious and should consider as malicious.

The network model,which containing the decoy targets. A distinctive feature of this heuristic is that its effectiveness depends on the proportion of the total number of attacks attributable to the decoy targets. In turn, it is determined by the ratio of the number of false targets and real network and their other parameters. Let us consider the model to associate with the required efficiency parameters of false and real goals.

The basic concept of this model is the notion of purpose [6]. Under the aim will be to understand the working on the host in the network process, performing a certain code.So how often network attacks aimed at vulnerabilities in the operation of the application software, a sense of purpose can be considered reasonable. Attack in this model will be called the following steps performed by the attacker:

- select according to some rule targets for the next attack;
- checking that the appropriate target vulnerabilities;
- attempt to exploit the vulnerabilities.

As a rule, any attack is focused on a set of code vulnerabilities. Thus, it makes sense to group goals in classes on the basis of his matches. Each class will contain both real and false targets(see Fig.1).

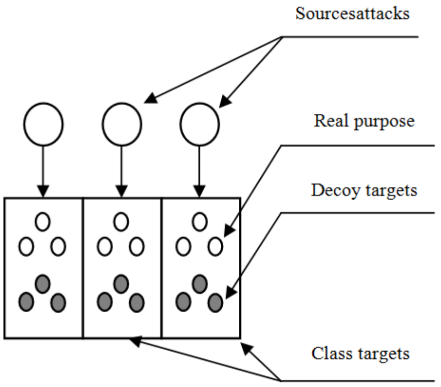

Fig.1. The scheme of interaction model components

It is believed that the attackers represented by a number of copies of malicious software, each of which carries out cyclically attempts to attack on the network. Attempts attacks occur at discrete points in time. One can assume the presence of a large number of independent sources of attacks at each time point. Consequently, we can consider the total flux attacks from these sources, considering it simple [7]. Obviously, in conditionsof changing characteristics of the external environment will change and the parameters recorded flow attacks, but it assumes that it is always possible to choose a period of time during which the flow can be considered as the simplest. In this case, it suffices to consider the state of the environment at discrete points in time intervals corresponding stationary parameters of detected attack flow. At the same time the state itself will be determined by the parameters of these flows, and the impact on the protected network attacker can be described as a set of independent streams of attacks, one for each class of targets.

Consider the probability of an attack on any false target in the network in each gap flow stationary parameter attacks. Due imposed definitions and assumptions, this probability is equal to the sum of the probabilities for all classes of targets. It has the following expression for this probability:

$$P = \sum_{i=1}^{k} P\{t \in C_i\} \frac{f_i}{f_i + r_i} \quad (8)$$

where$P\{t \in C_i\} -$ is the probability of selecting the next step of the target C_i; $f_i$and r_i −classes the number of decoy targets and real purpose, according in $C_i$class and the number ofk −class goals.

The probability of selecting targets from a particular class in practice can be determined as the ratio of the average number of attacks on the purpose of the class to the total of all attacks on the network end. These average values can be defined using the notion of intensity (I)flow attacks. The best in terms of the proposed model will be such a configuration parameter of the decoy targets in network, which will provide the maximum value of P with set limits on the number of decoy targets in each class. This is true for the fixed time.

Now suppose that the intensity of the attack effects for each class objectives change over time. If one calculates the optimum configuration of the decoy targets at each step of excluding previous changes, there is a danger that some of the decoy targets in network is embedded in a small time ago, will be removed in the next step. Obviously, this does not give them to fulfill their function and can potentially lead to their disclosure [8]. Thus, considering the dynamics of the model, it is necessary to take into account this important goal setting, as the time elapsed from the moment of its appearance, or the availability of time. Each class can be characterized by the distribution uptime availabilities goals of this class. It is possible to formulate the following limitation: time allocation available of decoy targets should not be different from the distribution of the timing of availability of RC in the same class. This restriction follows directly from the fundamental principle of the introduction of false objects in the network: to the attacker failed to disclose the fact of its misinformation, false as the object must be less different from actual.

Another limitation associated with this same principle is the need to maintain a stable set of services that are on the same host in the implementation of decoys [9]. Furthermore, there is usually a restriction on the maximum number of hosts - "carrier" decoys. Thus, it is possible to list the following options purposes, in terms of influencing the accepted model the effectiveness of heuristic:

- belonging to a class goal from the point of view of the coincidence of executable code;
- belonging to the class of real targets or decoy targets;
- time when the target became available in the network;
- host, which is the goal.

For the network as a whole are calculated parameters such as:

- the number of classes on the basis of goals matches the executable code;
- distribution target available time in each class;
- the number of real and false targets in each class, as well as the maximum possible number of hosts that carry decoys.

Formally, the model can be written as follows, taking into account:

$$\begin{cases} P = \sum_{j=1}^{k} \frac{I_j}{I} \frac{f_j}{f_j + r_j} = max \\ \sum_{i=1}^{k} \alpha_i x_i \le N, \\ P\left(\tau_j^F < \tau\right) = P\left(\tau_j^R < \tau\right) \end{cases} \quad (9)$$

where k −number of targets classes in the network; I_j −intensity of attacks on targets $C_j$class; I −intensively attacks on targets all classes; $x_j \in X$ −fixed set of target types from the set of all available configurations on the network; a_j −number of hosts with decoys corresponding x_j configuration; N −maximum number of hosts with decoys; $\tau_j^F$and τ_j^R −time availability of false and real purposes, respectively.

IV. The Method of Determining the Optimum Parameters of Decoy Targets

In whole, the method involves iteratively performing the following steps:

1. Getting the model input parameters and initial configuration of the decoy targets.
2. The calculation of the optimal configuration of the decoy targetswith solving the optimization problem defined by the model.
3. Among the possible control actions are selected such that provide maximal increase the probability of selecting an attacking of decoy targets.
4. Under change the parameters of the model the optimal configuration to be calculated again.

Development of intrusion detection model based on the provisions of the security policy. Intrusion detection system widely used as one of the most popular remedies modern automated information system (AIS). The increasing complexity of the technology of computer attacks, observed at the moment, requires the detection of the most dangerous attack complex, consisting of several stages, during which the attacker carries out malicious acts using various methods [10]. Thus, computer attacks should be viewed as attempts to violate security policy (SP) in the protected AIS, and for them to identify the necessary means to control many different parameters AIS.

Detection of complex attacks is difficult because of the need to analyze different sources of information and research the relationship between the identified simple attacks [11]. Intrusion detection system should be available to the database attributes identified ontology attacks. For intrusion detection inappropriate allocation of common features, common to all AIS as generally intension attacks varies for each AIS because it depends on the characteristics of the system to which the attack is directed. In particular, the formation of detecting signs must be taken into account especially the objectives, structure and functioning of the AIS. As a basis for the formation of signs of detection of computer attacks can be used AIS. SP allows for features and characteristics of AIS, in particular, describes a model of insider and external threats. It also includes external AIS information - model of external threats, as well as information about the role of AIS in the outside world.

The structure includes private SP, describing the parameters and criteria for the security of protected classes of AIS resources. These policies define, that is an anomaly and normal behavior for a variety of system and network settings and contain an assessment of critical deviations from normal behavior scenarios. Thus, the SP can provide the information necessary for the formation of signs detect attacks based on simple features of AIS. However, SP is a document and contains almost no quantitative characteristics of different criteria and parameters.

Thus, in achieving the objectives of the study have any problem formalization signs of intrusion detection, derived from the provisions of the positions SP, and the development of the algorithm, which allows detect complex attacks based on these signs. Also is investigated the possibility of using set of fuzzy variables and fuzzy rules for solving this problem. Let the private security policy states that users should not use the AIS resources during off-hours. Therefore, the presence of a certain number of people are outside working hours should refer to the possibility of penetration in the AIS. The simultaneous presence of a large number of active users should signal the penetration of the AIS and the possibility of the spread of the attack phase. In turn recorded the fact of penetration in turn suggests that the level of risk for AIS great [12]. In addition, the monitoring policy may indicate the need for analysis of monitoring files at least once every three days. This deviation from the monitoring policy at a high possibility of the spread of the attack must also point out that the level of risk for AIS is very high. For formalized description of the above provisions of SP advisable to write them in the form of the following rules:

R_1: if the users of the system "more" and the "outside", the possibility of the penetration of the "big";

R_2: if the users of the system "a lot", the possibility of the penetration of the "big" and the possibility of extending the "high" of attack;

R_3: if the time elapsed since the last analysis monitoring "significant" files, the violation of policy monitoring "great";

R_4:if the possibility of the penetration of the "big", the risk level of "high";

R_5: if the possibility of the spread of the attack "big" and a violation of the "big" monitoring policy, the level of risk is "very high".

In general, the premise and the conclusion of the rule can consist of any non-zero number of atomic formulas of the various logical operations. Model rules of the example shown in Fig.2.For formalizing the positions of the SP proposed to use fuzzy hierarchical construct. In accordance with the use of fuzzy sets it allows to formally define vague and open-ended terms that justifies the use of fuzzy sets and fuzzy logic for the formalization of the SP provisions and to detect deviations from normal behavior AIS.

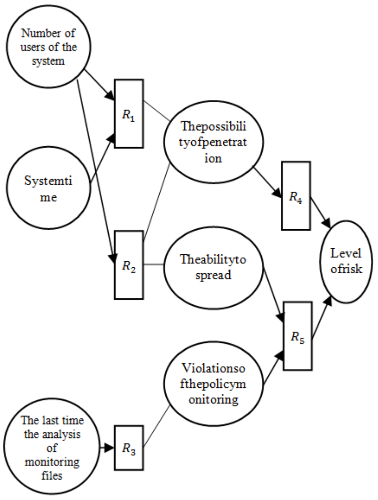
Number of users of the system
Systemti me
R_1
Thepossibili tyofpenetrat ion
R_2
Theabilityto spread
R_4
Level ofrisk
R_5
Violationso fthepolicym onitoring
The last time the analysis of monitoring files
R_3

Fig. 2. Model rules,that interpreting the positions of the SP

In the above snippet rules model, interpreting the SP position, used linguistic variables "number of users of the system", "system time", "the ability to penetrate," "the possibility of extending", "risk" and the other taking the different values of the form a "big" and "high". In this case, the input values are the variables "number of users of the system", "system time", "the last analysis of monitoring files". Other values are obtained by computing for data fuzzy rules.

Thus, the set of rules obtained by the formalization positions of the SP, is a hierarchical construct that allows for the detection of computer attacks allowing for the AIS expressed in the provisions of its SP. This construct can receive the input of the AIS quantitative indicators and using qualitative description, AIS evaluate different security settings, in particular the current level of security system, described by the linguistic variable "level of risk".

For a description of this construct and present it in a form that allows for machining, it will consider intrusion detection system ontology as a set of linguistic variables and fuzzy rules interpreting the position of the SP.For formation of values of the variables in the model we proposed to use the method of linguistic terms using statistical data, allowing on the basis of statistical data efficiently generate membership functions of linguistic variables [13]. As statistical data can be used as data obtained from the experts, and the data obtained by the experiment or observation of the operation of the AIS components in various conditions and modes.

Ontology models to detect attacks should include linguistic variable "level of risk", whose value is an estimate of the risk of security events corresponding to the identified attack. Upon detection of various attacks can be used by other variables corresponding to stages of complex attacks, such as "exploring", "penetration", "distribution" and the other showing the level of confidence in the system that the attack passes the appropriate stage. Described variables appear in the ontology as "interesting".

The set of rules and linguistic variables can be represented as a directed graph, its vertices are fuzzy rules, and the arc between the two regulations exist, if there is a linguistic variable, while participating in the conclusion of the first and in the condition of the second rule.

Taken together, the ontology of the rules should be rules cycle, type sequence of rules $R_1, R_2, \dots, R_n$such that there is a linguistic variable, occurring simultaneously in the condition rules R_{i+1} and $R_i$rights of prisoners, for $= 1, \dots, n - 1 \text{and} \mathrm{R}_1 = \mathrm{R}_\mathrm{n}$, in otherwise, the values of some linguistic variables remain uncertain. This condition is equivalent to that in said directed graph should be contours. The ontology describes the model fuzzy rules do not form a linear, as in the classical algorithm, fuzzy inference and hierarchical structure. Thus, for the implementation of the fuzzy inference rules in a given structure with classical algorithm were modified. Stages fuzzy implication and composition fuzzy inference algorithm is proposed to be carried out not in an arbitrary, and in this order, when linguistic variables that make up the rule conditions have already been defined either on the basis of fuzzification, or on the basis of the rules already in use. This procedure can be achieved, if the rules are processed in the order of topologically sorted graph rules, which will lead to the correct calculation of each subsequent linguistic variable.

Since the structure of the relevant rules of the digraph is digraph without loops, it admits a topological sorting in accordance with the algorithm [14].Attack detection algorithm in the proposed model of intrusion detection systemhas a next type:

1. Processing used fuzzy ontologies, ontology for each ordering rules in accordance with the topological sorting algorithm. Specifying that the agents must be collected in accordance with the input parameters of ontologies.
2. Preparation of input parameter values. Transfer received input parameters on modified fuzzy inference algorithm.
3. Processing of the parameters by performing a modified algorithm of fuzzy inference.
4. Assessment of the obtained values of "interesting" linguistic variables, evaluation of the level of event risk. In the case where the numerical value of "interesting" linguistic variables exceeds a certain threshold value, a decision is made about the possibility that any other attacks.
5. Repeat steps 2, 3 and 4 until the external signal the completion of the algorithm.

V. Conclusion

In conclusion, it should be noted that under proper selection of the coefficients, the sum of squared deviations from the experimental data found to be the least direct. After presentation of all the instances from training sample and correction of weight coefficients of neural network is calculated error training neural network on this iteration.

The method definition of necessary parameters of decoy targets allow maintain a configuration of decoy targets in the perimeter network, which will provide maximum flow attacks on intrusion detection system, taking into account changes in the nature of external influence on the protected network, as well as changes in its parameters.Construction the detection of signsderived from positions of the security policy is solved by providing intrusion detection system ontology as a set of linguistic variables and fuzzy rules, suitable for machine processing.

References

[1] F. Gunther, N. Wawro, and K. Bammann. Neural networks for modeling gene-gene interactions in association studies. BMC Genetics, 10:87, 2009.

[2] C. Almeida, C. Baugh, C. Lacey, C. Frenk, G. Granato, L. Silva, and A. Bressan. Modelling the dsty universe i: Introducing the artificial neural network and first applications to luminosity and colour distributions. Monthly Notices of the Royal Astronomical Society, 402:544–564, 2010.

[3] Anjali. M, B.Padmavathi«DDoS Attack Detection based on Chaos Theoryand Artificial Neural Network» 2014.

[4] Kotenko, I. Saenko, O. Polubelova, and E. Doynikova, The ontology of metrics for security evaluation and decision support in SIEM systems,” in Proc. of the 8th International Conference on Availability, Reliability and Security (ARES’13),

Regensburg, Germany. IEEE, September 2013.

[5] Hansman, S., and Hunt, R. “A Taxonomy of Network and Computer Attacks.”Computers & Security , 2004.

[6] Mandujano S. An Ontology-based Multiagent Architecture for Outbound Intrusion Detection/S. Mandujano, A. Galv6n, J. A. Nolazco // Proc. 3rd ACS/IEEE International Conference on Computer Systems and Applications, 2005.

[7] GulomovSh.R, Kadirov M.M. Guidelines for testing intrusion detection systems. Transactions of the International scientific conference «Perspectives for the development of information technologies ITPA-2015» 4-5 November, Tashkent 2015.

[8] Abraham A. and Thomas J., Distributed Intrusion Detection Systems: A Computational Intelligence Approach. // Applications of Information Systems to Homeland Security and Defense, Abbass H.A. and Essam D. (Eds.), Idea Group Inc. Publishers, USA, 2005.

[9] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., Dai, K.: An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Systems with Applications 39(1), 424–430 (2012).

[10] Tsai, C., Hsu, Y., Lin, C., Lin, W.: Intrusion detection by machine learning: A review. Expert Systems with Applications 36(10), 11994–12000 (2009).

[11] Amiri, F., Yousefi, M., Lucas, C., Shakery, A., Yazdani, N.: Mutual information-based feature selection for intrusion detection systems. Journal of Network and Computer Applications 34(4), (2011).

[12] Bosworth, S.; Kabay, M.; and Whyne,E., eds. Computer Security Handbook. Hoboken, NJ: Wiley, 2014.

[13] Slay J., and Koronios, A. Information Technology Security & Risk Management. Milton, QLD: John Wiley & Sons, Australia, 2006.

[14] ChengT., et.al. “Evasion Techniques: Sneaking Through Your Intrusion Detection/Prevention Systems.” IEEE Communications Surveys & Tutorials, Fourth Quarter 2012.

Authors' Profiles

GulomovSherzodRajaboevich

Assistant professor.
was born February 26, 1983 year in Shakhrisabz city, Republic of Uzbekistan. In 2009 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 80 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Information Security» in Tashkent University of Information Technologies.

KadirovMirhusanMirpulatovich

Senior lecturer. Was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan. In 2008 graduated “Information technology” faculty of Tashkent University of Information Technologies. Has more 63 published scientific works in the form of articles, journals, theses and tutorials.
Currently works of the department “Information technologies” in Tashkent State Technical University.

TulyaganovZoxidjonYakubdjanovich

Assistant professor. Was born September 21, 1985 year in Tashkent city, Republic of Uzbekistan. In 2009 graduated “Information technology” faculty of Tashkent University of Information Technologies. Has more 8 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department “Information technologies” in Tashkent State Technical University.