International Journal of Computer Applications Technology and Research
Volume 5– Issue 9, 556 - 560, 2016, ISSN:- 2319–8656

A Study of Intrusion Detection System Methods in Computer Networks

Mohammad Hossein Karamzadeh
Islamic Azad University, Bushehr Branch,
Computer Group, Bushehr, Iran

Reza Sheibani
Islamic Azad University, Mashhad branch,
Computer Group, Mashhad, Iran

Abstract: Intrusion detection system (IDS) is an application system monitoring the network for malicious or intrusive activity. In these systems, malicious or intrusive activities intrusion can be detected by using information like port scanning and detecting unusual traffic, and then they can be reported to the network. Since intrusion detection systems do not involve predefined detection power and intrusion detection, they require being intelligent. In this case, systems have the capability of learning. They can analyze packages entering the network, and detect normal and unusual users. The common intelligent methods are neural networks, fuzzy logic, data mining techniques, and genetic algorithms. In this research, the purpose is to study various intelligent methods.

Keywords: Intrusion Detection, Normal Network, Genetic Algorithm, Computer Networks

1. INTRODUCTION

Public and private organization and institution increasingly use internet world wide network and the various services. In this world networks, millions of computers are connected to each other, and provide different services for millions of users. The important challenge of organizations is accessibility, control of users, internal and external, to network information and services. Users may endanger the security of network information. By information security, we mean integrity, confidentiality or availability of information. Intrusion refers to any set of actions that do not compromise one of these principles. In order to confront with systems intruders, intrusion detection systems are designed. These systems are located over a host or network, and detect intrusion on the basis of detecting misuses, unusual behavior or a combination of them [1]. Information security, intrusion and attack are defined. Then, intrusion detection systems are introduced. Also, performance, architecture and their techniques are presented. In addition, intrusion detection methods are introduced. Finally, two high-applicable methods of implementation are presented on the basis of fuzzy logic and neural networks.

2. INTRUSION DETECTION

Intrusion refers to actions that are not legally allowed, and endanger, three principles of information security involving confidentiality, integrity and availability. The intrusion to network is usually considered as an attack. The reason of these attacks can begin with a simple curiosity, and it continues to malicious and destructive objectives. In order to present, detect and stop the attacks, we must be able to detect time and the position of an intruder at first so that damages of organization information resources are minimized. Intrusion detection systems are responsible for detecting illegal misuses of the system or damages by both internal and external users. Intrusion detection systems are created as software and hardware, and each one has its own special advantages and disadvantages, speed and accuracy are advantages of hardware systems. Lack of security failure occurring by intruders is another advantage of such systems. Easy application of software, flexibility capability in software conditions and the difference of various operating systems dedicate more generality to software systems, and such systems are generally more appropriate options.

2.1 The history of intrusion detection systems

By increasing speed, efficiency, and connection of computers in 1970s, security systems are highly required. During 1977-1976, standard international organization held a meeting between governmental and inspection organs of EDP (Electronic Data Processing). The result was preparing a report in terms of security conditions, inspection and systems control. At this time, U.S.A ministry of power performed a research about inspection and security of computer systems because this country was concerned about security of its own systems. James P. Anderson was responsible for this mission. Anderson was the first person who presented an article about the necessity of automatic inspection of systems security. Anderson's report prepared in 1980 can be introduced as initial core of intrusion detection concepts. In this report, some mechanisms are introduced for systems security inspection. Also, it was shown how to control the system when a failure occurs.

During 1984-1986, Dorotty Denning and peter Neumann performed a research about the security of computer systems. The result was to create a real-time intrusion detection system performing as expert systems. This system was called IDES (Intrusion Detection Expert System). In this project, misuses detection was investigated. The idea proposed in this project was used as a base for many intrusion detection systems.

2.2 Intrusion Detection

- Audit analysis project

During 194-1985, a group began performing a project in Sytek with the command of America navy. The purpose of this project was presenting an automatic method to collect shell data for Unix operating system. Then, collected data are analyzed. In this project, separating desirable behavior from undesirable behavior is demonstrated [2].

- Discovery

Discovery is a system based on expert systems, and it is created to detect and prevent the problems in information bank of TRW Credit Company, this system is different from intrusion detection systems of that time. Unlike intrusion detection systems investigating operating system activities, this system investigated logs of information banks. The purpose of discovery is to prepare a report of unhallowed performances in information bank. In this project, statistical models are used to analyze data, and they are written in Cobol language [3].

- Haystuk

This project was performed by Haystack laboratory (1989-1991) and Tractor applied science (1987-1989) with the request of America Navy, The purpose of Haystack implementation was to provide an opportunity for security officers to detect misuses of SBLC (Standard Base Level Computer) computers of air force. These computers were mainframes 1100/60, and vintage operating system was performed in these computers. Processor motor of this system uses written to SQL and ANSIC language. This system can detect anomalies by using batchmode. In this case, information is continuously collected, and processed [4].

- MIDAS

MIDAS (Multics Intrusion Detection Alerting system) was implemented by NCSC (National Computer Security Center), and the purpose was to investigate Dockmaster systems (for which Hnoywell DPS 870 operating system is applied). In this system, information is collected and classified. Then, information of each class showing a connection and relation is compared with users' behavior. According to this comparison, they could detect false and unusual behaviors. MIDAS was implemented by LISP language. In this system, expert systems are used for processing [3].

- NADIR

NADIR was implemented by computer laboratory of Los Alamos, and it was used to investigate individuals performance on ICN network (Integrated Computing Network). ICN network is the main network of Los Alamos, and more than 9000 users use it. NADIR investigates the network by using collected information. In this system, statistical methods and expert systems are used for information processing [5].

- NSM

NSM (Network System Monitor) was implemented by California University. This system can be considered as the first intrusion detection system, and it uses information network as information resource. Previously, other intrusion detection systems performed their own tasks on the basis of information collected from operating system or programs' logs. Then, NSM performance and efficiency was used in most products.

3. GENERAL NERAL ARCHITECTURE OF INTRUSION DETETION SYSTEMS

An intrusion detection system generally involves the following parts.

- Information collection or sensor

This part is responsible for collecting information. For example, this part must create detect changes occurring in system file or network performance, and must collect required information.

- System Review

Each intrusion detection system should involve a part investigating the system itself in terms of its performance and efficiency so that accuracy and performance of the system can be assured.

- Information storage or information bank

Each intrusion detection system stores its own information in a place. This place can be a simple text or information bank.

- Control management

The user can create connection with intrusion detection system, presents necessary orders and commands.

- Analysis

This part of intrusion detection system is responsible for investigating collected information.

Architecture structure of IDS is observed in figure 1.

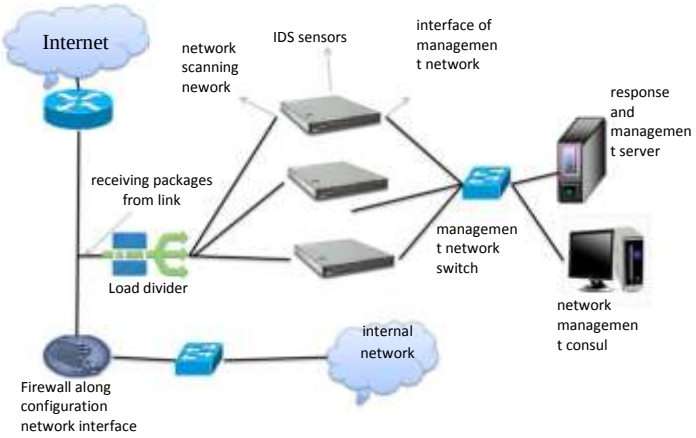

Figure 1: IDS architecture [5]

4. INTRUSION DETECTION

These techniques are used in misuses and anomaly detection systems. some of them are reviewed in this research.

4.1 Biological immune system

In this method, security in computer systems is proposed. The question is that "how a set of computers protect themselves?". In order to response it, similarities between biological immune system and compute immune system must be investigated. In a biological system, protection is performed by investigated. In a biological system, protection is performed by investigating finer factors like amino acids, proteins and etc. This can be true for intrusion detection systems. In this case, system calls can be considered as the first and detailed information resource. In this way, the order of system calls execution is statistically maintained for different users. If a program is executed, then execution order of system calls must accommodate with stored information. The alarm is presented if a difference is observed.

4.2 Genetic algorithm

One of intrusion detection methods is using genetic algorithm. According to genetic algorithm, intrusion detection process involves definition of a vector for information occurrences; that is, the related vector shows that occurrence is on intrusion or not.

At first, a hypothetical vector is considered, and its accuracy is investigated. Then, another hypothesis is proposed.

It is on the basis of test result, in previous hypothesis. Genetic algorithm involves two steps. The first step involves solution encoding as binary strings, while the second step involves finding a function to investigate binary string. GASSATA is a system performing the basis of it.

In GASSATA, system occurrences are classified on the basis of set of vectors. H (a vector for each string for occurrence) and n (the number of known attacks) are defined as follows. If it is equal to 1, than an attack occurs; otherwise, it is reserved if it is o. The function involves two parts. In the first part, danger probability of attack in a system is multiplied by the vector value. Then, its result is used to detect the error on the basis of second order function. In this way, false hypothesis are deleted. This step shows the difference between different attacks. The result of processing is to optimize the result analysis [7].

4.3 Statistical models in intrusion detection

Statistics is used in intrusion detection systems that are based on anomalies. Most of these systems have simple measurement tools, and determine attacks on the basis of changes in relation to a specified threshold limit. NID, of SRI apply expert statistical algorithm by using X2-like test of similarity measurement between short-term and long-term profiles. In our present statistical model, the algorithm similar to NIDES is used, but it has some differences. Therefore, some basic and main information about statistical algorithm of NIDES is introduced. The user profile is shown by the number of probability density function in IDES. S is considered as the sample space of random variable, and E1, E_2,…E_n events are considered in S sample space. suppose that

$$Q = N \times \sum_{i=1}^{k} \frac{(\acute{p}_i - p_i)^2}{p_i} \qquad (1)$$

Where pi is the probability of accruing Ei event. Also, imagine that pi is iterated continuously in specified time interval. N indicates the number of all events. In statistical algorithm of NIDES, X^2 like test is used to determine the similarity between the real and attack traffic.

When N is large, and E_1,E_2,…,E_n events care independent, Q is X^2 of (k-1) degree. since application programs cannot be immediately guaranteed, Q does not experimentally follow X^2.

NIDES solves this problem by using probability distribution function for Q updated daily in immediate operations.

Since we use neural networks to detect intrusion, we are not concerned about real Q distribution. The network traffic is not fixed, and it may be attacked in various times ranging from several seconds to some hours, so we require an algorithm for network traffic monitoring with different time window. According to observations, we use a window of static model layer (figure 1). Each model layer corresponds with time cut. Events occurring at present must be stored in layer buffer. 1. Stored events are compared with reference model of that layer. The result is transferred to neural network to detect the network position. When buffer of time event is full, it becomes empty, and then stored events are transferred to buffer of layer event 2. The similar processing is performed until reaching the highest level recursively. Events are easily removed after processing in the highest level. Similarity-meatering-algorithm whom we use is as follows:

$$Q = f(N).\left[\sum_{i=1}^{k} |\acute{p}_i - p_i| + \max_{i=1}^{k}(|\acute{p}_i - p_i|)\right] \qquad (2)$$

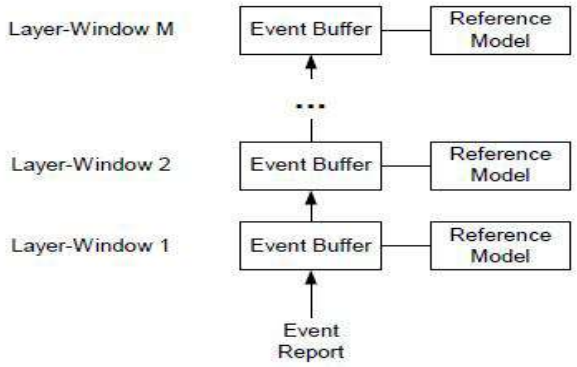

Figure 2: Statistical model [8]

f(N) is a function used to compute the number of all events occurring in a range of window. In addition to similarity measurements, we designed an algorithm to update the color of reference model. We consider P_{old} as the resource model before updating. P_{new} is considered as a reference model after updating, and P_{obs} is taken into account as the activity of a user in time window.

Updating formation of reference model is as follows:

$$\bar{p}_{new} = s \times a \times \bar{p}_{obs} + (1 - s \times a) \times \bar{p}_{old} \qquad (3)$$

In this formula, a is predefined adaptation rate, and s is the value produced by neural network. Suppose that output value of neural network is a continuous value between 1 and -1.In this case, -1 means absolute intrusion, and 1 is lack of absolute intrusion. Different values show related absolute levels. Computation function of S is as follow:

$$S = \begin{cases} t & if\ t \geq 0 \\ 0 & otherwise \end{cases} \qquad (4)$$

4.4 Neural networks

Neural networks are widely used as effective methods of patterns classification, but application programs are altered due to high volume of computations and long learning cycles.

BP neural networks are used by [4] and [7] to detect activity anomaly. In [2], we extend the example of hybrid neural network called hybrid backward perceptron network. This network is a combination of perceptron neural networks and small backward network. In order to understand neural network better, we tested five types of neural networks involving perceptron, RBF , FUZZY MAP, PBH and BP. Perceptron [9] of figure (3) is an sample of neural network used to classify linearly separable patterns. It only involves a neuron with setting threshold limit and connection. We use perceptron neural networks as a base to evaluate efficiency and performance of other neural networks.

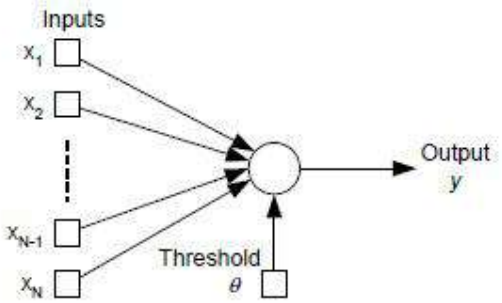

Figure (3) perceptron and architecture

Backward networks [9] or BP (figure 4) is a multi-layer forward network involving an input layer, on output layer and a hidden layer. BPs have higher production power, and they are used to solve some diverse and difficult problems. We tested BP network by some hidden neurons in range of 2-8.

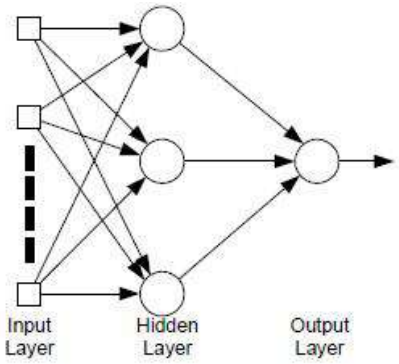

Figure (4): BP architecture [8]

Hybrid backward perceptron [6] or BPH (figure 5) is a combination of perceptron and small backward network. BPH networks have capability of linear and nonlinear detection and discovery, and they depend on input stimulus vectors and output values. We tested BPH neural networks in range of 1-8 of hidden neuron.

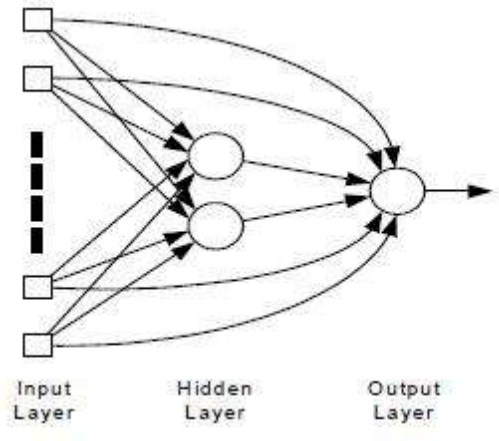

Figure (5): BPH architecture [8]

FUZZY ARTMAP [10] involves two fuzzy art networks: ART_a and ART_b. F2 layers are connected by subsystems introduced as match tracking system.

We used ARTMAP system [11]. Figure (6) is used to classify the problems. We tested ARTMAP neural networks with 1-8 neurons.

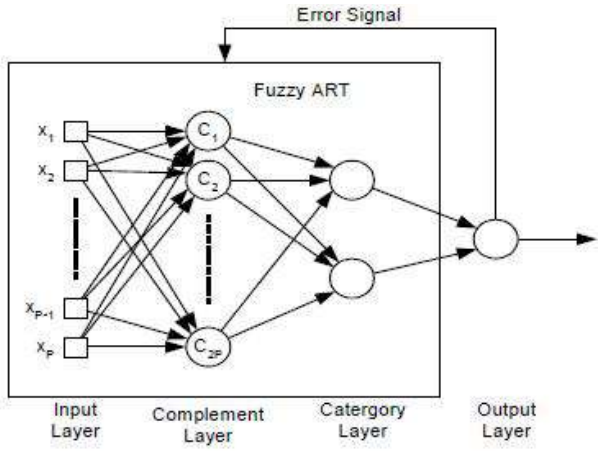

Figure (6): Fuzzy ARTMAP architecture

Racbal-basis network [9] or RBT (figure 7) involves three input layers. Input layer is constituted of resource nodes. The second layer is a hidden layer with enough large size, and presents different purposes of BP network. Output layer provides network replay to activation patterns applied to input layer. We tested RBT networks for hidden neurons in range of 2-8 [9].

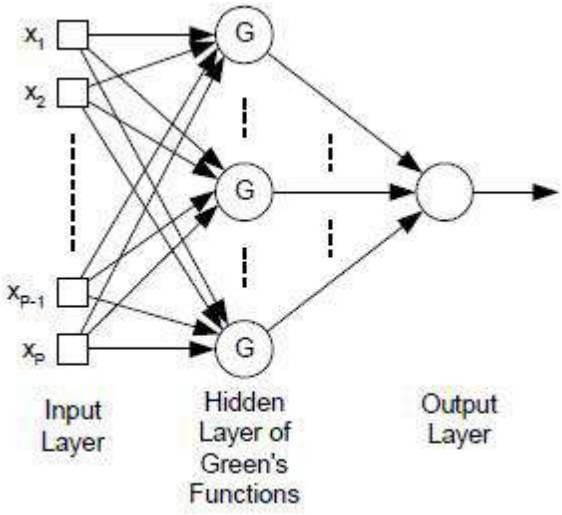

Figure (7): RBT architecture [8]

In our experiments, we used professional neural works of II/PLUSTM to generate all neural networks discussed earlier.

5. SUMMARY AND CONCLUSION

Intrusion detection systems are one of used tools to create security of computer networks. These systems can be classified according to two views. The first view is related to information resource, while the other one is the method of intrusion investigation. According to intrusion investigation method, two classes of systems can be considered such as the method of detecting misuses and anomalies. The research shows that IDS systems are very efficient to detect intrusion in network.

6. REFERENCES

[1] Crosbie, M., &Spafford, G. (1995, November).Applying genetic programming to intrusion detection.InWorking Notes for the AAAI Symposium on Genetic Programming.MIT, Cambridge, MA, USA: AAAI, pp. 1-8.

[2] Gong, R. H., Zulkernine, M., &Abolmaesumi, P. (2005, May). A software implementation of a genetic algorithm based approach to network intrusion detection. In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks.SNPD/SAWN 2005. Sixth International Conference on, pp. 246-253.

[3] Hashemi, V. M., Muda, Z., &Yassin, W. (2013). Improving Intrusion Detection Using Genetic Algorithm.Information Technology Journal, 12(5), pp. 2167-2173.

[4] Li, W. (2004,May). Using genetic algorithm for network intrusion detection.InProceedings of the United States Department of Energy Cyber Security Group 2004 Training Conference,pp. 24-27.

[5] Lu, W., &Traore, I. (2004). Detecting new forms of network intrusion using genetic programming. Computational IntelligenceJournal, 20(3), pp. 475-494.

[6] Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. Network IEEE, 8(3), pp. 26-41.

[7] Ojugo, A. A., Eboka, A. O., Okonta, O. E., Yoro, R. E., &Aghware, F. O. (2012). Genetic algorithm rule-based intrusion detection system (GAIDS).Journal of Emerging Trends in Computing and Information Sciences, 3(8), pp. 1182-1194.

[8] Shaveta, E., Bhandari, A., &Saluja, K. K. (2014,March).Applying Genetic Algorithm in Intrusion Detection System: A Comprehensive Review.In5th International Conference on Recent Trends in Information,Telecommunication and Computing(ITC 2014.India:ACEEE, pp. 102-112.

[9] Xia, T., Qu, G., Hariri, S., &Yousif, M. (2005, April). An efficient network intrusion detection methodbased on informationtheory and genetic algorithm. InPerformance, Computing, and Communications Conference, 2005 .IPCCC 2005. 24th IEEE International.IEEE, pp. 11-17.