

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.245 – 250

RESEARCH ARTICLE

Soft Computing Based Intrusion Detection System

Ravi Sharma¹, Dr. Balkishan², Dr. Sunil Sikka³

¹Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, (Haryana), INDIA

²Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, (Haryana), INDIA

³Department of Computer Science & Engineering, Amity University, Gurgaon, (Haryana), INDIA

¹ roodresharma@gmail.com, ² balkishan248@gmail.com, ³ sunil.sikka@yahoo.com

Abstract --- Intrusion Detection System is used to detect the unwanted activities over the network and to design IDS soft computing techniques are used. This paper describes the role of Artificial Neural Network, Fuzzy Logic and Genetic Algorithm in Intrusion Detection System. The artificial neural network learning algorithms, data retrieval using fuzzy logic under uncertainty and power of Genetic algorithm to optimize the decision of fuzzy inference system in aspect of IDS are discussed. Main focus of the paper is to combine all the modules of the IDS and explaining the role of soft computing.

Keywords --- Intrusion Detection System; Artificial Neural Network; Fuzzy Logic; Genetic Algorithm

I. INTRODUCTION

Computing is everywhere today, and openness of the system and services lead to the security issue. Any intruder with unauthorized access lead to break the security issues. For solving security related issues an Intrusion Detection System (IDS) is maintained along with the system services. Soft computing techniques can be used to design components of IDS. IDS are used to secure the system by preventing the entrance of intrusive data to the systems. IDS are equipped with number of components especially neuro-fuzzy classifiers. Neuro-fuzzy classifiers are used to categorize the network traffic data in form of normal data and intrusive data and produce an activity output stated the output state of data. IDS is very much useful in providing the feature for detecting attacks, security violations and in documentation of intrusion threats to an organization. Documenting the threat helps the organization to understand the characteristics of the attacks so that they can understand what security measures are appropriate for network security. Human administrators are present to deal with the attacks detected by IDS. There may be the situation when no human administrators are present at the time of occurrence of attacks, in this kind of state "automated response IDSs" are used which automatically responds to attack. Whenever IDS can detect any attack in

the absence of human administrators then an IDS inform the administrator by email or pager, to stop the attack and to block the attacker permanently, this is stated as active notification [9]. Building an IDS is a complex task and its modules are build with soft computing technique. The main component of IDS is neuro-fuzzy system. Soft computing is a modern approach to constructing computationally intelligent systems. Today, number of complex problems can be solved using intelligent systems that combine knowledge, methodologies and techniques from various sources. The role model for soft computing is human mind. It is tolerant of imprecision, uncertainty, partial truth and approximation. The principal constituents of soft computing are Artificial Neural Network (ANN), Fuzzy Logic (FL) and Genetic Algorithm (GA). Real world complex problems can be solved effectively by using ANN, FL and GA in combination rather than exclusively.

Artificial neural network recognizes patterns and adapt themselves to manage with varying environment [1]. A artificial neural network is a set of simple units called neurons. A neuron is a linear automata, which realizes a weighted sum of several inputs according to a set of weights, and then computes a heavy side function or a sigmoid function to obtain an output value, called activation of the neuron. The choice of the transfer function determines whether the neuron is binary or continuously valued. To form an artificial neural network, these neurons are interconnected according to a given topology. Artificial neural network algorithms are of use in Intrusion Detection System because of its learning time series, but alone neural networks cannot adequately handle all the available data, so neuro-fuzzy technology is used [12].

Fuzzy set theory provides a major prototype in modeling and reasoning with vagueness. Fuzzy set is the advancement of crisp set. In a crisp set, an element is either a member of the set or not. For example, an orange belongs in the class of food known as fruit. Jelly bean do not. Fuzzy sets, on the other hand, allow elements to be partially in a set. Each element is given a degree of membership in a set. This membership value can range from 0 (not an element of the set) to 1 (a member of the set). It is clear that if one only allowed the extreme membership values of 0 and 1, that this would actually be equivalent to crisp set. Several researches focus on fuzzy rule learning for effective IDS. Fuzzy rules are best suited for anomaly based detection in which generated rules are able to provide better classification rate in detecting the intrusion behavior.

To model the brain, mimic human learning, and simulate biological progression an evolutionary computation is grown, of which Genetic Algorithm is a prone example. Genetic algorithms offer an attractive approach to solving the feature activity selection problem in inductive learning of neural network pattern classifiers [8]. Computer algorithms are very attractive, because they are simple to program, and not hidden in mathematical terminology. Turning these algorithms loose on a wide variety of optimization problems leads to some stunning results. GA is used in IDS's decision making module by optimizing the decision of fuzzy inference system.

The above introduced constituents of soft computing are covering the wider area in computing world. This paper illustrates the use of soft computing techniques in IDS.

Rest of the paper is divided into three sections. Section 2 discusses the concept of IDS with its implementation. Section 3 describes the role of soft computing approaches in aspect of IDS. Section 4 presents that conclusion of the paper with future plans.

II. Intrusion Detection System

The use of network is increasing day-by-day, but with the increasing use of network systems lots of security issues are also arising such as intrusion. Intrude means; Put oneself deliberately into a place or situation where one is unwelcome or uninvited. Intrusion means the action of intruding. Intrusion detection is a process of detecting an unauthorized use or attack upon a computer or a telecommunication network. There are two kinds of intrusion i.e. whether the authorized user performing unauthorized tasks or an intruder. An IDS is able to detect both the attacks by analyzing the profile of its authorized user (former) and by detecting the unwanted interruption (later). Several types of IDSs are available, they are characterized by different monitoring and analyses approaches. IDS can monitor events at three different levels: network, host and application. They can analyze these events using two detection techniques: signature detection and anomaly detection [9]. In signature detection technique pre-defined sets of known attacks are stored with the help of these stored sets, attacks are detected by comparison. In anomaly based detection technique attacks are identified by detecting unknown behavior i.e. other than the normal users. An attacker behaves differently from the normal users and thus can be detected. A number of IDSs have been proposed for a networked or distributed environment [10][11]. In network level, IDS determine the feasibility of network level monitoring, to protect network resources from attack. In distributed computing several computer nodes are participated over the network for communication. The IDS can be distributed which further consist of several IDS.

In distributed IDS agents are deployed to observe behavior of the system and users. Agents communicate via messages to advise peers when an action is considered suspect. When an agent considers an activity to be suspect, an agent with a higher level of specialization for the suspected intrusion is activated. Agents then report their findings to a centralized manager. The main drawback with these systems is that the use of one or more centralized repositories leaves at least some portion of the network exposed to malicious attacks including tampering and denial of service attacks [11].

Over the network there are three different implementation locations of IDS. i) IDS can be implemented at point of interconnection between internal and external network. ii) IDS can be built at the router. iii) IDS can be implemented after the gateway or router as a firewall.

Figure 1 shows the implementation of IDS after the router. In this place IDS can have the bulk of network traffic data and process it before entering to the system’s environment. [17]. Figure 2 shows, two IDS implemented one at external network and other at internal network for higher security. The IDS1 is used for securing the system from outsider attack i.e. unauthorized access. IDS2 is implemented inside the internal network and used for securing from the authorized user to perform the tasks which are not allowed to the user [9]. Figure 3 shows the router inbuilt IDS. Here IDS system is installed into the router such that router works as Intrusion Detection System [17].

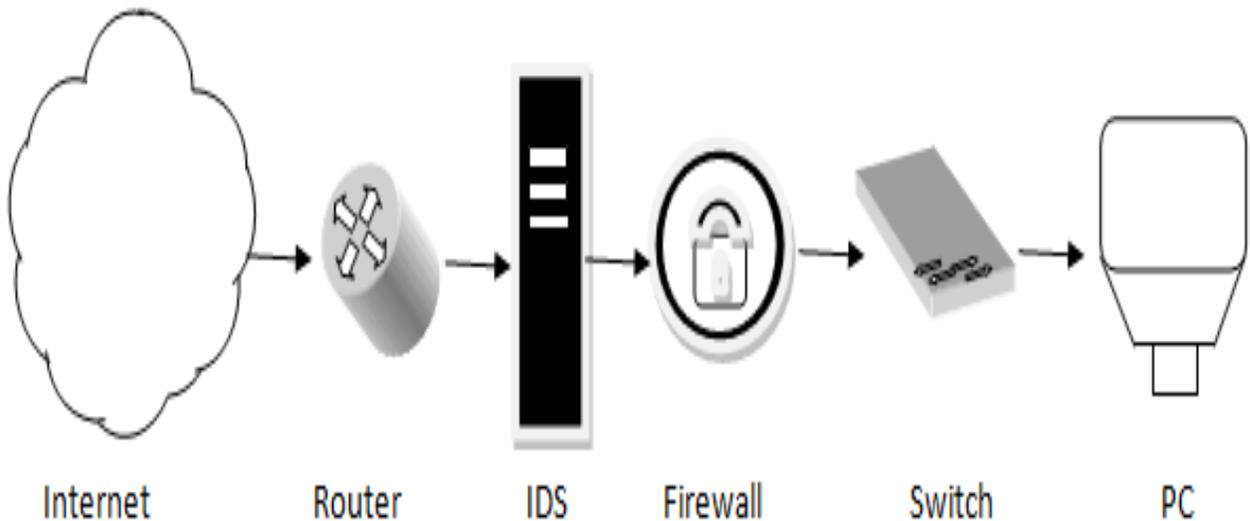


Figure 1 IDS after a router

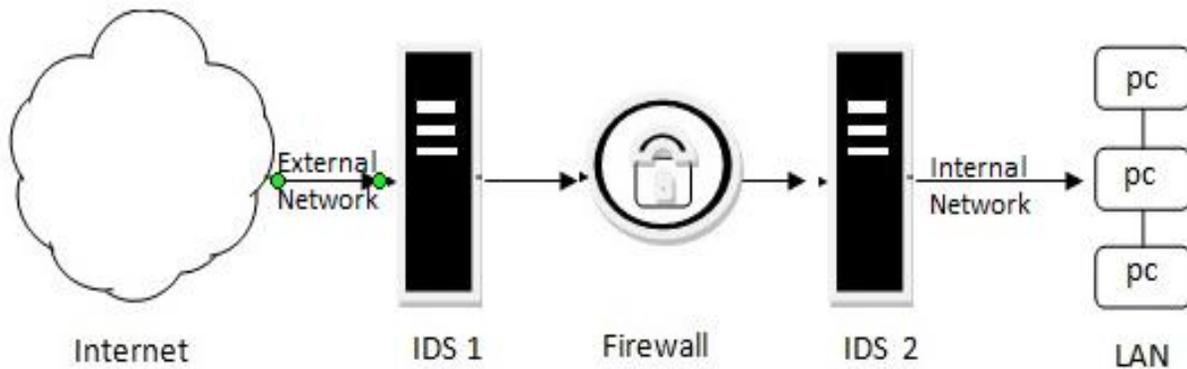


Figure 2 External and internal IDSs

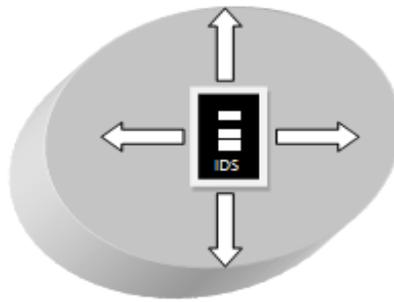


Figure 3 Router as IDS

III. Role of Soft Computing in IDS

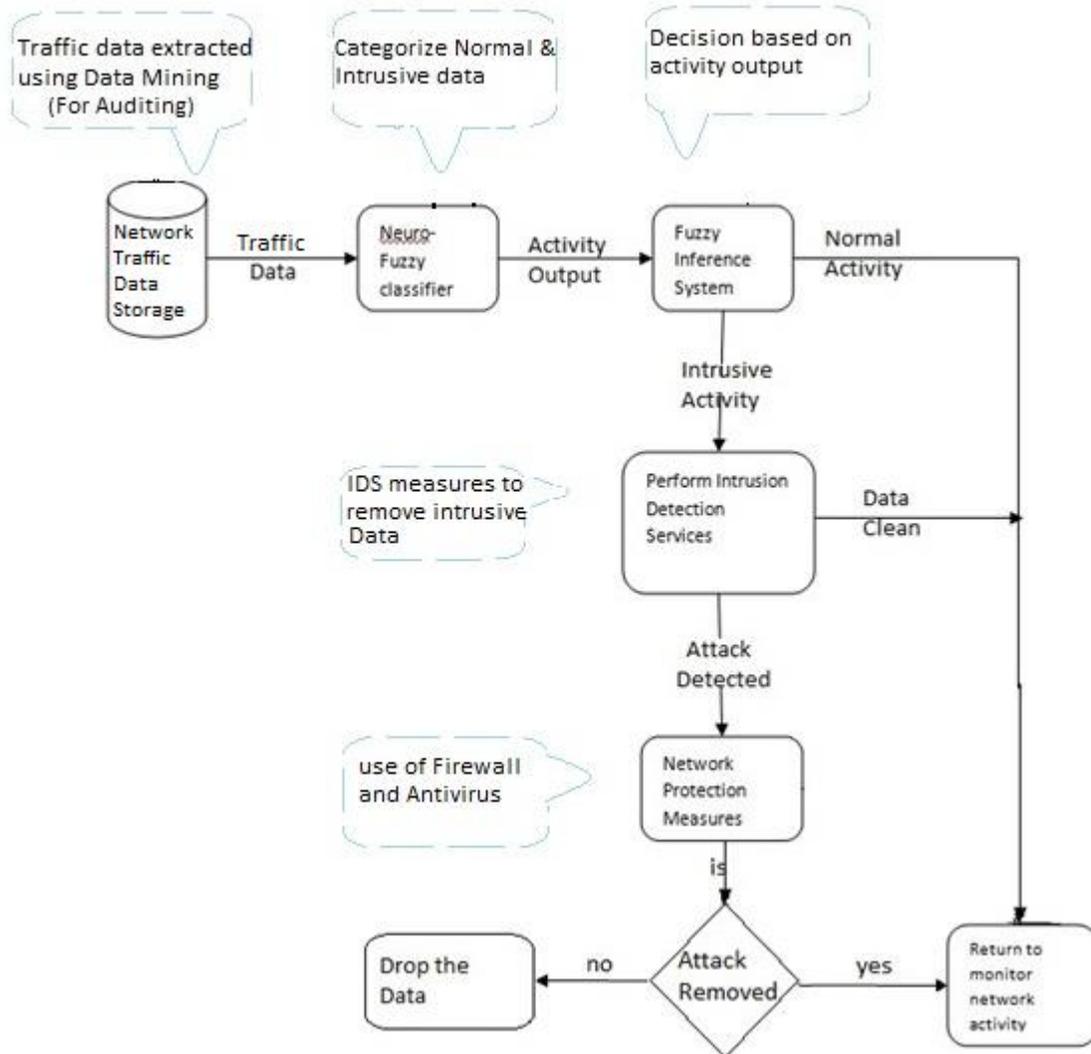


Figure 4 IDS Process State

The network traffic is vast in nature, so it is difficult to extract the data and analyze it for unknown patterns. IDS use Data Mining techniques [13] [14] [18] to discover the unknown pattern from large 'network traffic data storage' and extract the traffic data. After that the network traffic data is classified using Neuro-Fuzzy classifier. Set of parallel neuro-fuzzy classifier is used to do an initial classification. Classifier is used to categorize normal and intrusive data from the original data set [15] [19]. By strengthening the IDS we can improve the detection accuracy and performance of the IDS system. Thus, IDS is supplement with inference engine. Inference engine is decision making system for normal and intrusive data and result is optimized by using genetic algorithm. The output of the Neuro-Fuzzy classifier is then forwarded to fuzzy inference engine. Fuzzy inference engine using fuzzy set, works as the decision making system and makes the final decision that whether the activity is normal or intrusive. Inference engine core components are combination of several computing techniques, particularly unsupervised learning methods based on neural network and fuzzy logic. If the activity is normal then the IDS constantly monitor the network traffic. If the activity is intrusive then IDS protection measures are taken to remove intrusiveness and make data clean for the system. There may be the situation when data cannot be clean, thus that is the state when attack is detected. Now to protect the network, security measures are adopted and IDS is continuously monitoring the network data traffic.

IV. Conclusion

This paper discusses the concept of Intrusion Detection System and illustrates the role of soft computing constituent's artificial neural network, fuzzy logic and genetic algorithm in designing the IDS. All the modules of IDS are described with their functioning. Three different implementation areas of the IDS over the network are also discussed. Our future plan is to test the network traffic data using neuro-fuzzy classifier.

References

- [1] Soft Computing, Neural Networks, Fuzzy Logic, Genetic Algorithm, and Probabilistic Reasoning, by Ikvinderpal Singh.
- [2] S.S. Cross, R.F. Harrison, R.L. Kennedy, Introduction to neural networks The Lancet, Volume 346, Issue 8982, Pages 1075-1079
- [3] Teuvo Kohonen, An introduction to neural computing, Neural Networks, Vol. 1. pp 3-16, 1988.
- [4] Richard P. Lippmann, An Introduction to computing with neural network, IEEE, vol. 3, No. 4, pp. 4-22, April 1987.
- [5] Henrik Legind, Fundamentals of fuzzy sets and fuzzy logic, Larsen, Aalborg University Esbjerg.
- [6] Melanie Mitchell, An Introduction to Genetic Algorithm.
- [7] Randy L. Haupt, An Introduction to Genetic Algorithms for Electromagnetic, US Air Force Academy DFEE 2354 Fairchild Drive, Suite 2F6.
- [8] Jihoon Yang and Vasant Honavar, Feature Subset Selection Using A Genetic Algorithm, Artificial Intelligence Research Group, Department of Computer Science 226 Atanas off Hall Iowa State University Ames, IA 50011
- [9] Understanding Intrusion Detection System, Peter Mell, EDPACS the EDP Audit, control and security newsletter, VOL.XXIX, NO. 5, November 2001.
- [10] Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla, The Architecture of a Network Level Intrusion Detection System, NM 87131 August 15, 1990.
- [11] Ajith Abraham, Ravi Jain, Johnson Thomas, D-SCIDS: Distributed soft computing intrusion detection system, Oklahoma State University, OK 74106, USA Received 28 June 2005; accepted 28 June 2005.
- [12] Hervdebar, Monique BECKER, Didier SIBONI CSEE/DCI INT CSEE/DCI , A Neural Network Component for an Intrusion Detection System Avenue des tropiques BP80 91943 Les Ulis Cedex France INT:9,RueCharlesFourier91011 Evry Cedex France.

- [13] G.V. Nadiammal, M. Hemalatha, Effective approach toward Intrusion Detection System using data mining techniques, Tamilnadu, India, accepted 27 October 2013.
- [14] Shi-Jinn Horng a,b,*, Ming-Yang Su c, Yuan-Hsin Chen b, Tzong-Wann Kao d, Rong-Jian Chen b, Jui-Lin Lai b, Citra Dwi Perkasa, A novel intrusion detection system based on hierarchical clustering and support vector machines, 2002.
- [15] Adel Nadjaran Toosi, Mohsen Kahani, A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers Available online 24 May 2007.
- [16] Mahmoud Jazzar† and Aman Jantan††, A Novel Soft Computing Inference Engine Model for Intrusion Detection, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.
- [17] Piyakul Tillapart, Thanachai Thumthawatworn and Pratit Santiprabhob, Fuzzy Intrusion Detection System AU J.T. 6(2): 109-114 (Oct. 2002).
- [18] Susan M. Bridges, Associate Professor, Rayford B. Vaughn, Associate Professor, Intrusion Detection via Fuzzy Data Mining, Twelfth Annual Canadian Information Technology Security Symposium June 19-23, 2000, The Ottawa Congress Centre.
- [19] Jonatan Gomez and Dipankar Dasgupta, Evolving Fuzzy Classifiers for Intrusion Detection, Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2001.