Volume 5, No. 1, January 2014
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

NEURO-FUZZY BASED INTRUSION DETECTION SYSTEMS FOR NETWORK SECURITY

[1]Alka Chaudhary, [2] V. N. Tiwari, [3]Anil Kumar
[1,3]Computer Science and Engineering, Manipal University, Jaipur, India
[2]Electronics Communication and Engineering, Manipal University, Jaipur, India
[1]alka.chaudhary0207@gmail.com, [3]anil.kumar@jaipur.manipal.edu
[2]vivekanand.tiwari@jaipur.manipal.edu

Abstract: Computer networks are more vulnerable to insider and outsider attacks in recent days due to its widespread use in each field. For that aspect, numbers of security mechanism have been applied to minimize the effect of possible attacks in the network. One of very appealing concept towards network security is intrusion detection system that can able to identify the difference between normal and abnormal activities in the network. There are many intrusion detection systems have been proposed to detect the intrusion or intruders in the network. In general, soft computing techniques i.e. neuro-fuzzy based intrusion detection system make as a keystone to detect the intrusion with high detection rates. This paper is going to emphasize the proposed neuro-fuzzy based intrusion detection system and also discussed their suitability in terms of detection rates and false positives rates towards network security.

Keywords: Network security, Intrusion detection system (IDS), Soft computing (SC), Neuro- fuzzy.

INTRODUCTION

Due to the rapidly changes in the network nature, it is complex to identify the normal activities from the malicious activities. Securing our networks is very challenging issue for the researcher in these days. Many prevention based security mechanisms such as firewalls, encryption and intrusion detection systems are available to prevent the network from the vulnerabilities. However, intrusion detection systems have played a prominent role in the network security. When any unauthorized action that are trying to compromise with the attributes of security such as confidentiality, availability, repudiation and integrity then that action is known as an intrusion and detection of such intrusions is said to be the intrusion detection system (IDS) [1].

The first intrusion detection system was developed by T.F. Lunt in late 1980s which was known as intrusion detection expert system (IDES) [2]. Moreover, Bonissone accounted the used of soft computing techniques for the field of intrusion detection in 2000 [3].

Soft computing are able to construct the modern intelligent systems which are consist neural networks, fuzzy logic, genetic computing and probabilistic reasoning for new generation and also handle the robustness, tractability, low solution cost, uncertainty and partial truth. Hybrids of soft computing approaches are also possible i.e. neuro-fuzzy, fuzzy-genetic, neuro-genetic and neuro-fuzzy- genetic. One type of hybrid approach is most popular in intrusion detection field i.e. neuro-fuzzy because in this hybrid approach neural network trains the IDS in respect of possible attacks so that IDS gathers the information in regards of traffic patterns then fuzzy logic generates the rules based on that information about traffic patterns [4].

This paper is described the proposed neuro-fuzzy based IDSs for networks. The rest of the sections of this paper are follows: section II presented the work which have been done on neuro-fuzzy based IDSs in literature and section III conclude the paper in respect to the applicability of these proposed neuro-fuzzy based IDSs for network security.

WORK DONE IN NEURO-FUZZY BASED IDSs

Many neuro-fuzzy based IDSs have been presented for network security. Some of them most popular neuro-fuzzy based IDSs are discussed in this section.

For evolving fuzzy neural network (EFuNN) based intrusion detection system, [5] IDS is based on two learning paradigm: one is artificial neural network and other is fuzzy inference system. During the training phase, real time traffic analysis and packet logging on IP network by used of SNORT [6] and then a signature pattern database is built based on neuro fuzzy learning method. After that evolved IDS make a test on DARPA data set to prove the better performance. In [7], presented a comparison between evolving fuzzy neural network (EFuNN) based intrusion detection system and Artificial neural networks (ANN) and the results proved that neuro fuzzy based hybrid approach showed better performance than the ANN approach when in both case SNORT are used for training . Results shows that based on accuracy, ANN performed better because of training time for ANN in minute while for EFuNN training time in second. Secondly, in terms of interpretation of rules of EFuNN is easier than ANN.

There are also applied neuro- fuzzy based classifiers [8] in the form of binary and multi classifier to classify the normal activity from the abnormal activity in the networks. This approach is very success full in terms of detection rate than the other approaches such as RIPPER [9], SRPP [10] and EFRID [11]. In [12] also used a hybrid approach for IDS where self-organizing maps (SOM) and learning vector quantization (LVQ) used as ANN for a group of TCP flags and characterize connection type and also used fuzzy

inference system (FIS) for used as a network handshake watching but for FIS fine tuning used genetic algorithms.

CONCLUSION

As above the discussion on proposed neuro fuzzy based IDSs, It have been cleared that the hybrid approach of neuro-fuzzy in intrusion detection field is more capable to detect intrusion than separate used of approaches as ANN or Fuzzy logic. One thing is also noticed that there are many approaches based on neuro-fuzzy based IDSs but sometimes proposed approaches have the difference to each other in terms of attacks scenarios and data features when the availability of data are open source or same in manner.

REFERENCES

[1]. R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system" Technical report, Computer Science Department, University of New Mexico, August 1990.

[2]. Teresa F. Lunt , "Ides: an intelligent system for detecting intruders", in Computer security, threat and countermeasures, pp. 30-45, 1990.

[3]. Bonissone, "Hybrid soft computing systems: Where are we going?", http://www.cs.berkeley.edu/nikraves/bisc/Present/Fall0/Pieroecai2000v4.pdf(5/7/08), 2000.

[4]. Zadeh, L. , "The Roles of soft computing and fuzzylogic in the conception, design and deployment of information/intelligent systems ", In Kaynak, O., Zadeh, L.A., Turksen, B., Rudas, IJ (eds) Computational intelligence: soft computing and fuzzy-neuro integration with applications, vol 162. springer, new york 1998.

[5]. Chavan S, Shah K, Dave N, Mukherjee S , "Adaptive neuro-fuzzy intrusion detection systems", In IEEE international conference of information technology: coding and computing (ITCC'04),IEEE Computer Society Press, Los Alamitos, CA, pp. 70–74, 2004.

[6]. Kohlenberg T, Alder R Jr, Carter EF, (Skip), Foster JC, Jonkman M, Marty R, Poor M, " Snort IDS and IPS Toolkit Open Source Security", Syngress, 2007.

[7]. Shah K, Dave N, Chavan S, Mukherjee S, Abraham A, Sanyal S , "Adaptive neuro-fuzzy intrusion detection system", In IEEE international conference on ITCC'04, vol 1. pp 70–74, 2004.

[8]. A. N. Toosi, M. Kahani, R. Monsefi, "Network Intrusion Detection based on Neuro-fuzzy classification," International Conference on Computing & Informatics, (ICOCI '06), Kuala Lumpur, Malaysia, June 6-8, pp.1-5, 2006

[9]. W. Fan, M. Miller, SJ. Stolfo, Chan PK. "Using artificial anomalies to detect unknown and know network intrusions", In Proceedings of the first IEEE international conference on data mining, 2001.

[10]. M. S. Abade, J. Habibi, C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm," Journalof Network and Computer Applications, August 2005.

[11]. J. Gomez, D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," Proceeding Of 2002 IEEE Workshopon Information Assurance, United States Military Academy, West Point NY, June 2001

[12]. Copeland JA, Garcia RC, "Real-time anomaly detection using soft computing techniques", In IEEE Southeast Conference, 2001.

