International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - EEECOS 2014, ISSN : 2348 2273
Available Online at www.ijeecse.com

A Layered Approach for Intrusion Detection Using Fuzzy Artmap Neural Network Classifier

J. Sravan Kumar[1], Dr. I. Ravi Prakash Reddy[2], M. Subha Sree[3]
[1 & 3]Assistant Professor, Department of CSE, D.M.S.S.V.H.College of Engineering, Machilipatnam
[2]HOD, Department of IT, G Narayanamma Institute of Technology and Sciences, Hyderabad
[1]jnvsravankumar@gmail.com

Abstract: Intrusion Detection Systems (IDS) is a key part of system defense, where it identifies abnormal activities happening in a computer system. In general, the traditional intrusion detection relies on the extensive knowledge of security experts, in particular, on their familiarity with the computer system to be protected. To reduce this dependence, various data-mining, soft-computing and machine learning techniques have been proposed in recent years for the development of better intrusion detection systems. Many researchers used Conditional Random Fields and Layered Approach for purpose of intrusion detection. They also demonstrated that high attack detection accuracy can be achieved by using Conditional Random Fields and high efficiency by implementing the Layered approach. In the paper we propose a new method called fuzzy ARTMAP classifier (FAM) and clustering technique for effectively identifying the intrusion activities within a network. Processing huge data would make the system error prone, hence clustering the data into groups and then processing will result in having a better system. From each of the cluster, representative data is selected in the selective process for further processing. For classification process, layered fuzzy ARTMAP will have the better results when compared to other normal classifier algorithms.

Keywords: Clustering, fuzzy ARTMAP, Intrusion detection, Layered Approach.

I. INTRODUCTION

Nowadays, networks in computer face an unprecedented range of threats and vulnerabilities which created a greater risk in computer security [1]. Also intrusion events to computer systems are growing due to the popularization of the Internet and local networks. Generally, the goal of threats and attacks is to subvert the traditional security mechanisms on the systems and execute operations in excess of the intruder's authorization. These operations could include reading protected or private data or simply doing malicious damage to the system or user files. So only by building complex tool the system can be protected from malicious attacks. Intrusion detection systems are becoming increasingly important in maintaining proper network security [5, 6]. An intrusion detection system (IDS) monitors networked devices and looks for anomalous or malicious behavior in the patterns of activity in the audit stream. Intrusion Detection System is used to monitor the events occurring in a computer system or network, analyse the system events, detect suspected intrusion, and then raise an alarm.

Host-based Intrusion Detection System and Network based Intrusion Detection System are two different types of intrusion detection system. Among this the Host based Intrusion Detection system has only host based sensors and the other has network-based sensor. The basic function of Host-based technology is to determine events like what files were accessed and what applications were executed [9].

Network-based intrusion detection is the problem of detecting unauthorized use of computer systems over a network, such as the Internet. Generally a good intrusion detection system should be able to distinguish between normal and abnormal user activities. It contains any event, state, content, or behavior that is considered to be abnormal by a pre-defined standard. The intrusion detection system based on data mining can be classified according to their detection strategy. There are two main strategies in intrusion detection system such as misuse detection and anomaly detection [12]. Among this the misuse detection uses patterns of well-known attacks and anomaly detection tries to determine whether deviation from the established normal usage patterns can be flagged as intrusions. In intrusion detection system identification of camouflaged intrusions from a huge amount of normal communication activities is considered as the one of the major challenge [15]. Many Machine Learning (ML) algorithms, such as Neural Network [16], Support Vector Machine [17], Genetic Algorithm [18], Fuzzy Logic [19], and Data Mining [20], etc have been widely used to detect the attacks. Generate rules to distinguish normal behaviors from abnormal behavior by observing dataset is very important for IDSs.

In this paper we present a new clustering and classification technique in order to improve the classification accuracy of the intrusion detection system. The clustering technique is the Possibilistic Fuzzy C-Means (PFCM) and the classification technique is Fuzzy ARTMAP neural network classifier (FAM).

II. LITERATURE REVIEW

In recent times, intrusion detection has received a lot of interest among the researchers because it is widely applied for preserving the security within a network. Here, we present some of the techniques for intrusion detection. G. Gowrisona *et al.* [30] designed an intrusion detection

system to classify the network behavior with less computational complexity of O (n). The KDD Cup99 is a bench mark data used here to achieve promising classification rate. To achieve high detection rate in Intrusion Detection System (IDS), Shingo Mabu et al [31], described a fuzzy class association rule mining method based on Genetic Network Programming (GNP). GNP is used to enhance the representation ability with compact programs derived from the reusability of nodes in a graph structure. The combined method is evaluated with KDD99Cup and DARPA98 databases and showed that it provides competitively high detection rates.

However, to overcome the network based anomalies detection issue, Latifur Khan*et al.* [35] has proposed a method which was the combination of SVM and DGSOT, which starts with an initial training set and expanded it gradually using the clustering structure produced by the DGSOT algorithm. They compared the proposed approach with the Rocchio Bundling technique and random selection in terms of accuracy loss and training time gain using a single benchmark real data set. Due to the necessity of misuse and anomaly detection in a single system, M. Bahrololum*et al.* [32] proposed an approach to design the system using a hybrid of misuse and anomaly detection for training of normal and attack packets respectively. The utilized method for attack training was the combination of unsupervised and supervised Neural Network (NN) for Intrusion Detection System. By misuse approach known packets were identified fast and unknown attacks were also be detected.

For the importance of an efficient Intrusion Detection System, K.S. Anil Kumar and V. NandaMohan [33] proposed a combination of three techniques comprising two machine-learning paradigms. K-Means Clustering, Fuzzy Logics and Neural Network techniques were deployed to configure an effective intrusion detection system. This approach revealed the advantage of converging K-Means-Fuzzy-Neural network techniques to eliminate the preventable interference of human analyst in such occasions. Also, to improve the accuracy as well as efficiency of the Intrusion Detection System, Shekhar R. Gaddam*et al.*[34] presented "K-Means+ID3," a method to cascade k-Means clustering and the ID3 decision tree learning methods for classifying anomalous and normal activities in a computer network, an active electronic circuit, and a mechanical mass-beam system. Results showed that the detection accuracy of the K-Means+ID3 method was as high as 96.24 percent at a false-positive-rate of 0.03 percent on NAD; the total accuracy was as high as 80.01 percent on MSD and 79.9 percent on DED.

Vipin Kumar *et al*,[28], have analyzed NSL-KDD dataset to using K-means clustering. Clustering algorithms proves to be very useful when we have huge amount of unlabelled dataset. The study analyses the different types of attacks present in NSL-KDD. K-means Clustering applied here is able to efficiently detect new type of attacks present in dataset. K-means clustering is able to cluster the attacks present in training dataset into four major categories giving a better representation of the clusters. The main objective of the paper was to provide a complete analysis of the NSL-KDD dataset and the attacks presented. We used K-means algorithm for this purpose and also represented the distribution of instances in clusters providing better representation of the instances and making it clearer to understand.

Security is always an important issue especially in the case of computer network which is used to transfer personal information's, ecommerce and media sharing. So, Rachnakulhare and Divakar Singh, [29], have presented an intrusion detection system based on fuzzy C-means clustering and probabilistic neural network which reduced the training time and increases the detection accuracy. They evaluated the designed method based on KDD99 dataset and the simulation results showed that by selecting effective characteristics and proper training the detection accuracy rate up to 99% was achievable .

III. Proposed Intrusion Detection Based on Layered Fuzzy ARTMAP Classifier

The principle aim of the study is to create powerful system network intrusion detection system by using data mining and artificial intelligence methods. In this paper, intrusion detection system which utilizes Possibilistic Fuzzy C-Means (PFCM) clustering techniques and Fuzzy ARTMAP classifier is offered to have effective difference between the relevant data and intruded data The system consists two layers were preparing and testing of information is carried out. The block diagram of the proposed intrusion detection system utilizing both the PFCM and Fuzzy ARTMAP classifier is given in fig1.

The proposed strategy incorporates two layers of preparing and testing procedure to ascertain if the input data is attack or not. The dataset utilized here within our proposed system is the KDD cup 99 dataset. At first in proposed intrusion detection system the input KDD cup 99 dataset pre-processing is carried out with a specific to get better classification accuracy. Since the KDD cup 99 dataset utilized here has different attacks. It comprises of both symbolic and numeric esteemed qualities. So utilizing this sort of dataset will lessen the reliability of our intrusion detection system. So in pre-processing, we outline symbolic-valued attributes of KDD cup 99 dataset to numeric-valued attributes. Then the pre-processed input data is connected to a clustering method called PFCM. The PFCM cluster the input pre-processed data into N number of clusters. Further the N number clusters are prepared utilizing our proposed Fuzzy ARTMAP classifier which resolves the complex classification problems. At last after different phases of our system, the test data is given to the

trained fuzzy ARTMAP neural network classifier and test whether the input information is attack or not.

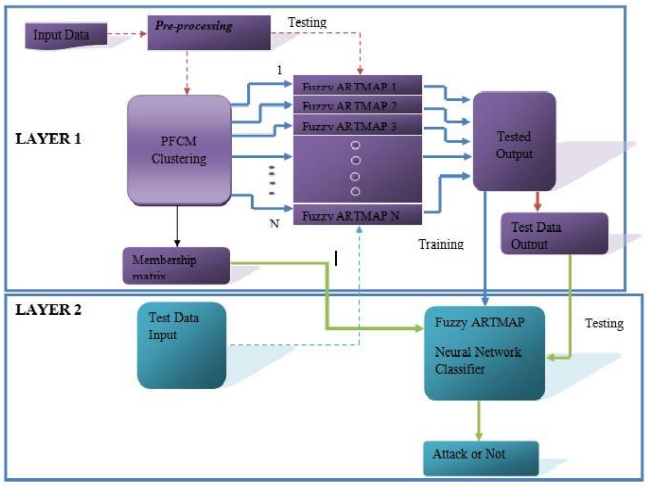

Fig.1 Proposed Intrusion detection system

IV. Clustering Using Possibilistic Fuzzy C-Means (PFCM) Clustering Algorithm

The input dataset directed to the intrusion detection system generally encompose huge amount of data which makes the processing extremely complex, hectic and time consuming. Executing this expansive number of data can additionally prompt having poor outcomes about by the increase of errors. Henceforth, it will have marked impact on the effectiveness of the system and eventually prompting diminished quality intrusion detection system. To minimal this issue, dataset is pre-processed clustering method is utilized before characterization. In pre-processing stage, we outline symbolic-valued attributes of KDD cup 99 dataset to numeric-valued attributes. Then the pre-processed input data is connected to a clustering method called PFCM. The application of Possibilistic Fuzzy C-means clustering methods will improve the clustering and accuracy of the intrusion detection system.

Step 1: Initialize $U = [u_{ik}]matrix, U^{(0)}$

Step 2: At k step: calculate the centers vectors $C^{(k)} = [v_i]withU^{(k)}$

$$v_i = \frac{\sum_{k=1}^{n}\left(u_{ik}^{m} + t_{ik}^{\eta}\right)x_k}{\sum_{k=1}^{n}\left(u_{ik}^{m} + t_{ik}^{\eta}\right)}, 1 \le i \le c.$$

Step 3: Update $U^{(k)}, U^{(k+1)}$

$$u_{ik} = \left(\sum_{j=1}^{c}\left(\frac{D_{ikA}}{D_{jkA}}\right)^{2/(m-1)}\right)^{-1}$$

Step 4: If $\left\|U^{(k)} - U^{(k+1)}\right\| < \varepsilon$, then stop; otherwise return to step 2.

V. Fuzzy ARTMAP Neural Network Classifier

Fuzzy ARTMAP is a neural network architecture which is depend on Adaptive Resonance Theory (ART). It has been used in supervised incremental learning, classification and prediction. The basic function of the fuzzy ARTMAP neural network classifier is operated by dividing the input space into a number of hyperboxes, which are mapped to an output space. The FAM has various advantages such as the classification task can be obtained by only one Fuzzy ART module and also computationally efficient. The structure of our proposed Fuzzy ARTMAP neural network classifier is shown in the figure below.

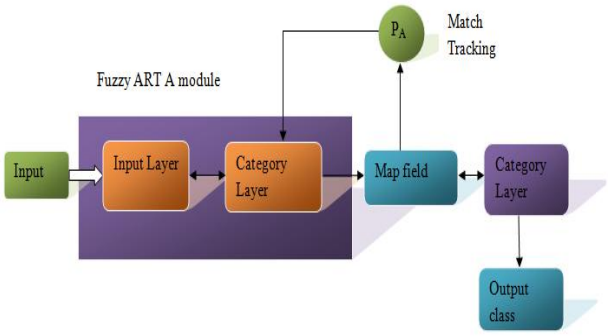

Fig.3 Fuzzy ARTMAP classifier simplified structure

In general the fuzzy ARTMAP consist of 2 largest components including fuzzy ART module map field. The important two layers for the Fuzzy ARTMAP classifier is usually input layer plus the category layer. An input layer involves several neurons that each will accept continuous signal about the range of [0,1].

Fuzzy ART map module, and significantly affects classification performance associated with Fuzzy ARTMAP system. a input vector can be normalized throughout quickly dividing their components from the norm, i.e., ones amount of absolute values of most components associated with the idea input vector. This normalizing process requires less program resources. But complement coding is selected along with applied frequently, regarding that could possibly help avoid category proliferation problem.

VI. Conclusion

Nowadays network security is one of the major worry due to various attacks and vulnerabilities in internet. As a result, intrusion detection is an important component in network security. In this paper, we proposed a new intrusion detection system using PFCM clustering and layered fuzzy ARTMAP classifier. The PFCM is a clustering method used here which provides better clustering output compared to previously used clustering method. After this the classification process is performed

using the proposed Layered fuzzy ARTMAP neural network classifier. After various stages of training process test dataset is given as input and finally the classified output is obtained.

VII. REFERENCES

[1] Witcha Chimphlee, Abdul Hanan Abdullah, Mohd Noor Md Sap,Siriporn Chimphlee and Surat Sirinoy, "A Rough-Fuzzy hybrid algorithm for computer intrusion detection", the International Arab Journal Of information technology, Vol.4, No.3, 2007.

[2] J. Allen, A. Christie, and W. Fithen, "State Of the Practice of Intrusion Detection Technologies", Technical Report, CMU/SEI-99-TR-028, 2000.

[3] B.V.Dasarathy, "Intrusion Detection", Information Fusion, Vol.4, No.4, pp.243-245, 2003.

[4] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", White Paper from Independent Study, September 11, 2003.

[5] Dr.Fengmin Gong,"Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection", White Paper from McAfee Network Security Technologies Group, 2003.

[6] Jian Pei , Jiawei Han , Laks V. S. Lakshmanan, "Pushing Convertible Constraints In Frequent Itemset Mining", Data Mining And Knowledge Discovery, Vol. 8, No.3, pp.227-252, May 2004.

[7] Cannady J, "Artificial Neural Networks for Misuse Detection", In Proceedings of the '98 National Information System Security Conference (NISSC'98), pp. 443-456, 1998.

[8] Shon T, Seo J, and Moon J, "SVM Approach with A Genetic Algorithm for Network Intrusion Detection", Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Vol. 3733, pp. 224-233, 2005, ISBN 978-3-540-29414-6.

[9] Yu Y, and Huang Hao, "An Ensemble Approach to Intrusion Detection Based on Improved Multi-Objective Genetic Algorithm", Journal of Software, Vol.18, No.6, pp.1369-1378, June 2007.

[10] J. Luo, and S. M. Bridges, "Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection", International Journal of Intelligent Systems, Vol. 15, No. 8, pp. 687-704,2000.

[11] W. Lee, S. Stolfo, and K. Mok, "A Data Mining Framework for Building Intrusion Detection Model", In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA: IEEE Computer Society Press, pp. 120-132, 1999.

[12] G. Gowrisona, K. Ramarb, K. Muneeswaranc, T. Revathic, " Minimal complexity attack classification intrusion detection system", Applied Soft Computing, vol 13, pp: 921–927, 2013.

[13] Shingo Mabu, Nannan Lu, Kaoru Shimada,KotaroHirasawa, " An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming", IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, VOL. 41, NO. 1, PP: 130-139 , 2011

[14] Latifur Khan, MamounAwad, BhavaniThuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering", The International Journal on Very Large Data Bases, Vol. 16, no. 4, October 2007.

[15] M. Bahrololum, E. Salahi and M. Khaleghi "Anomaly intrusion detection design using hybrid of unsupervised and supervised neural networks", International Journal of Computer Networks & Communications, Vol.1, No.2, 2009.

[16] K.S. Anil Kumar and Dr. V. NandaMohan, " Novel Anomaly Intrusion Detection Using Neuro-Fuzzy Inference System ", IJCSNS International Journal 6 of Computer Science and Network Security, vol.8, no.8, pp.6-11 , August 2008.

[17] Shekhar R. Gaddam, Vir V. Phoha, Kiran S. Balagani, "K-Means+ID3: A Novel Method for Supervised Anomaly Detection by Cascading K-Means Clustering and ID3 Decision Tree Learning Methods", IEEE Transactions on Knowledge and Data Engineering, Vol. 19, No. 3, pp. 345-354, 2007.

[18] Vipin Kumar, Himadri Chauhan and Dheeraj Panwar, "K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset" International Journal of Soft Computing and Engineering (IJSCE), pp. 2231-2307, Volume-3, Issue-4, September 2013

[19] Rachnakulhare and Divakar Singh, "Intrusion Detection System based on Fuzzy C Means Clustering and Probabilistic Neural Network", International Journal of Computer Applications, Vol. 74, No.2, 2013.