ISSN 22773061

A Review of Feature Reduction in Intrusion Detection System Based on Artificial Immune System and Neural Network

Uma Vishwakarma[1], Prof. Anurag Jain[2], Prof. Akriti jain[3]

Uma2011cse01@gmail.com[1], anurag.akjain@gmail.com[2]

Department of computer Science & Engg[1, 2]

RITS, Bhopal, INDIA

ABSTRACT

Feature reduction plays an important role in intrusion detection system. The large amount of feature in network as well as host data effect the performance of intrusion detection method. Various authors are research proposed a method of intrusion detection based on machine learning approach and neural network approach, but all of these methods lacks in large number of feature attribute in intrusion data. In this paper we discuss its various method of feature reduction using artificial immune system and neural network. Artificial immune system is biological inspired system work as mathematical model for feature reduction process. The neural network well knows optimization technique in other field. In this paper we used neural network as feature reduction process. The feature reduction process reduces feature of intrusion data those are not involved in security threats and attacks such as TCP protocol, UDP protocol and ICMP message protocol. This reduces feature-set of intrusion improve the classification rate of intrusion detection and improve the speed performance of the intrusion detection system. The current research going on fixed and static number of feature reduction, we proposed an automatic and dynamic feature reduction technique using PCNN network.

Keywords: - intrusion detection, feature reduction, artificial immune system and neural network.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 9, No 3

editor@cirworld.com

www.cirworld.com, member.cirworld.com

INTRODUCTION

Due to the rapid increase in the illicit network activities, intrusion detection system (IDS) as a component of defense-in-depth is very necessary because traditional firewall techniques cannot provide complete protection against intrusion[1]. Currently, the greatest threat against the security of networks and information systems, are attack on the network infrastructure. Intrusion Detection (ID) is an active and important to explore area network security [2]. There are several methods for intrusion detection expert systems such as statistical analysis and state transition implementation approaches, etc., and these several approaches on the immune system have been proposed in recent years [10,11]. The goal of intrusion detection is to detect unauthorized access or misuse of computer systems by insiders of the system and external access and secure system integrity, privacy, usability and availability. Reduction unit means an important role in intrusion detection system [12,13]. The performance of intrusion detection reports large amount of functionality. The various authors and encounters contribute data in the reduction of the function of penetration. The feature space with limited features that really contributes to the classification which reduce the cost of pre-processing and minimizes the impact of "peak" phenomenon in the classification[9]. Through this improve the overall performance of intrusion detection systems based on classifiers. In recent years, with computer systems, using the principles of the human immune system for intrusion [3] detection. For half a century, some quite successful IDS have been implemented, but were marred by problems of high false positives surrounding a mismatch and short self-directed. A promising solution to the human immune system (HIS) is inspired to respond to this difficult problem. HIS protects the body from damage caused by a large protects the body from damage caused by a large number of harmful bacteria and viruses caused, and provides the body with a high degree of protection against invading pathogens, to a robust manner, itself organized and distributed. So we can learn from SA to meet the challenges in computer security. Artificial neural network (ANN) is a new data-mining approach in intrusion detection on an ANN comprises a number of processing elements which are strongly connected to each other, and transformation of a set of inputs to a set of expected results. Neural networks are both in the detection of intrusion into the abnormality detection signal and the penetration of abuse used. The system learns to predict entered on a preceding sequence of instructions from a user for the next command [14]. Here is a moving window of w is used as a recent command. The predicted user with the actual control of the user command, and comparing a deviation is reported as the engagement. The size of the window W given an important role, because if w is too small, there are many false alarms will be and if it is too large, attacks cannot be detected. Intruder detector in a neural network (NNID) identifies the distribution operations of commands used by the user [15].

The reaming part of paper is arranged as follows. In section II describe related work of feature reduction and intrusion detection. In section III describe the artificial immune system and neural network. In section IV feature reduction technique in intrusion detection. Section V describes problem formulation in feature reduction. In VI describe survey result of feature reduction technique. Finally conclude in section VII.

II RELATED WORK

In this section we discuss some related work to intrusion detection and feature reduction based on artificial immune system and neural network. These methods also contribute for feature reduction process.

In [1] author uses an Dendritic Cell Algorithm (DCA) and Dempster Belief Theory(DBT) in order to minimize the rate of the generation of intrusion detection system, false positive rate and improve correlation factor in the designed IDS, Which is a new technique for intrusion detection that is based on Artificial immune system called DCA and DBT, With this dual detection method we minimize the false positive as well as false negative rate but also improve the correlation factor and decrease the intrusion rate in the system.

In [2] author uses an Agent-based artificial immune system to apply intrusion detection systems. A multi agent-based IDS inspired by the danger theory of human immune. ABAIS is an intelligent system with learning and memory capabilities. The intelligence behind ABIDS is based on the functionality of dendrites cells in human immune systems and the danger theory, while dendrites cells agents are emulated for innate immune subsystem and artificial T-cell agents are for adaptive resistant system. Opposite gens selection are profiles of system calls while resultant behaviors are regarded as signals.

In [3]authors describe the Intrusion technique for detection of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or in the offing terrorization of abuse of computer security policies, acceptable use policies, or security standard. Their immune-based intrusion response model depending on the self-learning and diversity of AIS can predict mysterious attacks and categorize them.

In [4] in the field of intrusion detection author improved an intrusion detection technique as it applies artificial immune theory to the intrusion detection model. It used the dynamic equation of the node cell and storage cell, and sets up a kind of dynamic match Algorithm. Dynamic match algorithm adopts the method, which regulate the match degree dynamically and control the evolving speed. By using Dynamic match algorithm they improve the efficiency and accuracy of artificial immune system.

In [5] Author describes Immune based Adaptive IDS Model for Enhanced Fast Adaptive Clustering Algorithm and Algorithm of Mining Fuzzy Associate. The Immune based Adaptive IDS Model would be accurate, low in false alarms, The Self and non self sets can update automatically and always. So IAIDSM improve the capacity of detecting new type intrusions and the adaptability of the system. But using this approaches the result obtained is not and real time efficient.

In [6] Authors describe negative clone selection algorithm for intrusion detection, but in real time application IDS suffered from selection problem of attributes. With this problem resolved by danger theory, danger theory gives a entropy based concept for separating different attributes. The separation of attribute in danger applied a negative selection algorithm for intrusion detection.

In [7]author describe a four-layer model based on DT and AIS for IDS, which consists of four layers, each of them works independently and interacts with each other. In the third layer-IRL a mechanism of reasoning with uncertainty is presented to increase the detection accuracy.

In [8] authors describe a method of immune system for intrusion detection. The process behind work is defined two different centers of intrusion data. One intrusion data are placed as target value and another data of intrusion use as test data and find the difference of both these data. The difference of both these data work as intruder and attack attribute of IDS.

III ARTIFICIAL IMMUNE SYSTEM AND NEURAL NETWORK

Immune system and neural network in current environment play important role in reduction of data dimension and feature reduction. Various authors used immune and neural network for reduction of feature and optimization of data. The size of network file is large due to maximum number of attribute. The maximum number of attribute compromised the rate of detection and speedup of network. Now we discuss artificial immune system and neural network.

Artificial Immune System (AIS) is a new bio-divine model, which is applied to resolve various problems in the field of information security. Artificial immune systems (AIS) are adaptive systems, stimulated by hypothetical immunology and experiential resistant methods, theory and models, which are applied to detection process. Its two important attribute terms plays a vital role in Human immune system Antigens and antibodies. Antigens are foreign molecules on 'intruders' - that is, epitomes that are recognized by the immune system as foreigners. Antibodies are a part of immune system which is responsible for detecting and binding to the antigens. The number of antibodies is very less than the number of antigens. In fact, the possible number of antigens is close to infinite; but the possible number of antibodies is not [7]. Inspired by the success of biological immune systems, AIS-based systems also use the concept of Antigen and antibodies. In which, a small number of antibodies can detect large number of antigens. Like HIS which protects the human body against the foreign pathogens, the AIS suggest a multilayered protection structure for protecting the computer networks against the unauthorized attacks. There are various kinds of harmful living things in our living surroundings. Including bacteria, viruses, and parasites [9].

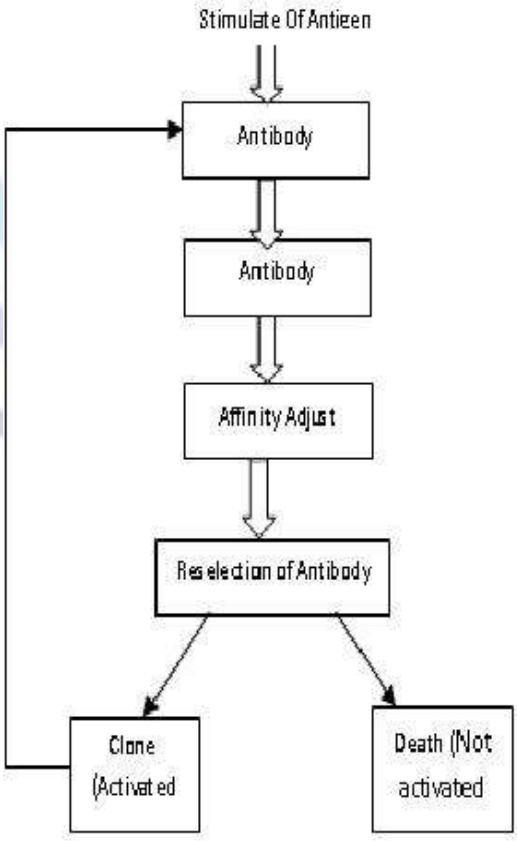

Figure 1Flow chart of artificial immune system

We call them pathogens. They enter our body through food, respiration or damaged part of our body. In this case, we can still keep our health due to passive barriers such as slum and mucus membranes, physiological conditions such as pH and temperature, and immune system in our body

ANN is one of pattern recognition technique that has the capacity to adaptively model user or system behavior. This algorithmic technique can built a useful model of user or system behavior relying on a reduced amount of network data. Thus; it is useful for IDS where experimented hacker can sometimes alter system or applications log files to hide their mounted attacks. Moreover, ANN technique has been employed in modeling anomalous data and detection of attacks signs in intrusive data. In [4, 14] ANN was capable to autonomously learn attack signature. In addition, it is able to detect learned attacks (encountered in training data) and relying on its generalization capacity it is able to identify and learn new unseen attacks ANN is a powerful technique for modeling complex relationship between input and output data. It consists of a network of computational units that implement a mapping function to approximate the desired output relying on attaining data set. The network units or neurons are highly interconnected. Each unit receives weighted inputs to compute its activation and feeds a single output to other neurons that perform the same task. Each connection between two processing units has a weight which can be updated from iteration to another to adapt the network to the desired outputs. In neural network, processing units are organized into layers. The input layer is the first layer the network structure. Neurons in this layer don't perform any task rather than feeding input data to other neuron layers. The number of neurons of this layer depends on the dimensionality of logged network traffic data. The structure of ANN disposes a single input layer which is connected to the first hidden layer of neurons and may be to other layers in specific architectures (Recurrent Neural Network).

IV FEATURE REDUCTION TECHNIQUE

The feature reduction of anomaly and intruder file are play great role in intrusion detection system. They reduces features of anomaly increase the efficiency of intrusion detection algorithm and method. In this paper we discuss a hybrid method for feature reduction using artificial immune system and neural network A combination of artificial immune system and neural network reduces number of attribute without learning of parameter work a complete system and reduces feature of anomaly file. PCNN neural network is itself a hybrid model of network play an important role in feature reduction technique. Feature extraction is an important issue in intrusion detection. Of the wide number of features that Can Be Monitored for intrusion detection purpose, which all are truly useful, All of Which are less significant, or All Which May Be useless? The elimination of useless features enhances the accuracy of detection while speeding up the computation, ANN Improving the overall performance of IDS. Pulse Coupled Neural Network (PCNN), Expired called the third generation of artificial neural network, is the neural network mathematic model Applied synchronous pulse fracture occurrence in the visual cortex of mammals. It has important budding in feature reduction and has been widely applied to intrusion detection etc. It is based on Elkhorn's model, and derives from the phenomena of synchronous pulse bursts in mammals' (cats, monkeys, etc.) visual cortex When PCNN is used in feature reduction; it is a monolayer two dimensional array of laterally linked neurons. The number of neurons in the network is able to that of attributes in the input file. Conversation association exists between file attribute and neurons. Each attribute is connected to an only one of its kind neuron and each neuron is connected with its closest neurons. Feature reduction includes feature structure, space dimensionality reduction, sparse representation, and feature selection. Although such problems have been tackled by

ISSN 22773061

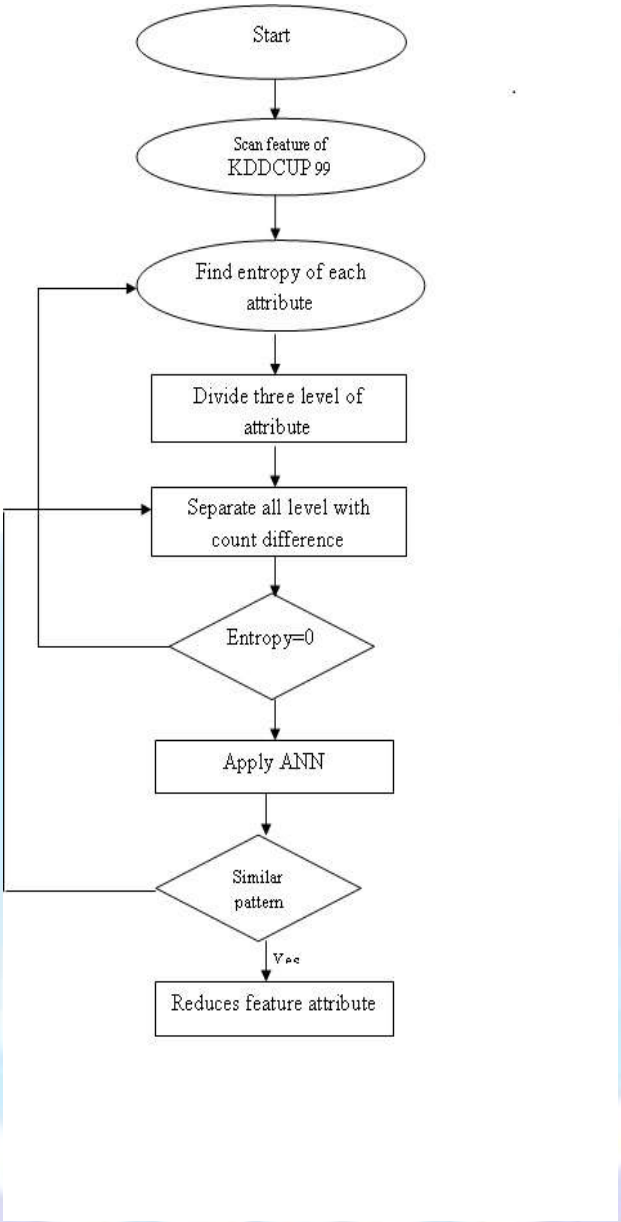

Figure 2 process block diagram of feature reduction process using neural network

V PROBLEM FORMULATION IN FEATURE REDUCTION

The current scenario of intrusion detection system suffered from detection rate and false alarm generation. The useless features induce a problem of detection and alert generation applies to large a large number of feature attribute in network data. The current review of feature reduction algorithm based on artificial immune system work directly on dynamic feature reduction of intruder file [16]. The feature reduction is important issues in improving of classification rate of intrusion detection system action, so we reduce those attribute and improve the efficiency of method of intrusion detection system. Some problem given below found in survey [2, 5, 6, 7, 8, 16]

1. Dynamically feature attribute are not reduces.
2. All scanning method of data are sequentially, due to this reason detection time overhead are increase.
3. The rate of false alarm generation is high.
4. The detection of signal in DCA algorithm is ambiguous.
5. Entropy based intrusion detection system suffered by high false rate.
6. Belief function not correctly recognised PAM signal of DCA.

VI SURVEY RESULT OF FEATURE REDUCTION

In this section we discuss the comparative feature reduction analysis based on neural network and data mining approach for intrusion detection. The rate of feature reduction finds on given method of author and used KDDCUP99 dataset [17] for analysis. The analysis of comparative reduction rate evaluate on the basis of number of reduces feature and reduction process nature. The result of all these methods given below in table I.

Algorithm applied	Total number of Feature	Number of reduces Features	Reduction process
DT[7]	41	10	slow
DNID[14]	41	12	slow
Improved Competitive Learning Lamstar Neural Network[18]	41	9	fast

Table I shows the comparative feature reduction analysis of data mining approach and neural network for reduction of feature of intrusion on given KDDCUP99 dataset.

VII CONCLUSION AND FUTURE WORK

In this paper we give a review of feature reduction technique for intrusion detection system. The process of feature reduction technique in network data is very challenging due to variable length and mixed structure of data. Various authors developed a method of feature reduction such as LDPA and PCA for reduction of feature of network data. This method reduces fixed number of feature for intruder data. But in review process we found that artificial immune system and neural network uses as automatic feature reduction process. The reduction of features is great advantage over normal feature selection process. The process of feature reduction improves the efficiency of classification and detection algorithm.

REFERENCES:-

[1] Anurag Jain ,Swati Dongre and Kalpana Kumari, “Intrusion Detection Technique based on Dendritic Cell Algorithm & Dempster Belief Theory,” International Organization of Scientific Research (IOSR), vol. 1, Issue 5, May-June 2012.

[2] Chung-Ming Ou, Yao- Tine Wang and C.R. Ou” Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems ” in IEEE International Conference on Fuzzy Systems in 2011.

[3] Li Rui, Luo Wando “Intrusion Response Model based on AIS” in Information Technology and Applications (IFITA), 2010 International in 2010.

[4] By YUAN Hui, LIU Jian-yong “Intrusion Detection Based on Immune Dynamical Matching Algorithm” in E-Business and E-Government (ICEE), 2010.

[5] Lei Deng De- yuan Gao “ Research on Immune based Adaptive Intrusion Detection System Model” in IEEE 2009

[6] Junmin Zhang, Yiwen Liang “A Novel Intrusion Detection Model Based on Danger Theory” in IEEE 2008.

[7] Haidong Fu , Xiuo Yuan and Liping Hu, “Design of a Four-layer Model Based on Danger Theory and AIS for IDS in IEEE 2007.

[8] Baoyi WANG Shaomin ZHANG “ New Intrusion Detection Method Based on Artificial Immune System” in IEEE 2007.

[9]S.Devaraju, Dr.S.Ramakrishnan: “analysis of intrusion detection system using various neural network classifiers”1033-1038,IEEE 2011.

[10]K kr.Gupta, B Nath,R Kotagiri” Layered Approach Using Conditional Random Fields for Intrusion Detection” 1545-5971/10 2010 IEEE.

[11] Jiankun Hu and Xinghuo D. Qiu, Hsiao-Hwa Chen, ” A Simple and Efficient Hidden markov model Scheme for Host-based anomaly Intrusion Detection” 0890-8044/09/ 2009 IEEE.

[12] Chunyu Miao and W Chen “A Study of Intrusion detection System Based on Data Mining” 978-1-4244-6943-7/10/26.00 2010 IEEE.

13] Nong Ye, Syed M Emran, Qiang Chen, and Sean Vilbert” Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection” 2002 IEEE.

[14] ACMSIGKDD, Liwei (Vivian) Kuang” DNIDS: A Dependable Network Intrusion Detection System” in IEEE, 2007.

[15] Lei Li, De-Zhang Yang, Fang-Cheng Shen “A Novel rule-based Intrusion Detection System by”2010.

[16] Y I Shakhatreh, K A Bakar " A Review of Clustering Techniques Based on Machine learning Approach in Intrusion Detection Systems" IJCSI Vol.8 2011.

[17] P. Natesan a, P. Balasubramanie a; G. Gowrison b " Improving Attack Detection Rate in Network Intrusion Detection Using Adaboost Algorithm with Multiple Weak Classifiers" Journal of Information & Computational Science 2239–2251.2009.

[18] V.Venkatachalam S.Selvan ," Intrusion Detection using an Improved Competitive Learning Lamstar Neural Network" IJCSNS VOL.7 2007.