International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Performance Evaluation of Intrusion Detection Technique Based On Soft Computing Technique

Ravindra Kumar Gupta[1], Shailendra Singh[2]

SeniorMember, IEEE

NITTTR, Bhopal, India

ABSTRACT

Reduction and selection of intruder attribute in intrusion detection system play an important role in process of detection. The huge number of attribute in intruder induces a problem in detection process and increase more time in decision making process. In current research trend some authors used some standard technique for feature reduction such as PCA, PCNN and neural network, but these methods not consider all features for processing fixed some number of feature. In this paper we proposed a feature selection and feature reduction method based on improved ID3 algorithm. The proposed algorithm select multiple feature for reduction and the reduce feature set participant the process of detection. The reduce feature of network file classified by ID3 classification algorithm. The ID3 algorithm in the case of small data size, if sizes of data are increase the selection of attribute process raised some problem related to feature selection. For the improvement of this problem used RBF function for increasing the biased value of feature and feature subset selection. In this paper we tried to propose a very simple and fast feature selection method to eliminate features with no helpful information on them. Result faster learning in process of redundant feature omission. We also compare our proposed method with some other most successful similarity based feature selection algorithm. For the validation and performance evaluation of proposed algorithm used MATLAB software and KDDCUP99 dataset 10%. This dataset contains approx 5 lacks number of instance. the process of result shows that better classification and reduce time instead of another feature reduction reduction.

Keyword: - Feature selection, Feature reduction, Intrusion detection system, Classifier.

I.INTRODUCTION

The performance of intrusion detection system depends on classification of unknown types of attacks. The detection of unknown types of attack is very difficult due to large number of attribute and huge amount of network data. For the improvement of unknown attack feature reduction is important area of research. The reduction process reduces the large number of attribute and improved the detection of intrusion detection system. In the process of feature reduction various algorithm are used such algorithm are principle of component analysis and neural network. The reduction process used PCA method this method is static reduction technique, reduces only fixed number of attribute. The fixed number of feature reduction process not justify the value of feature it directly reduces the feature. On the consideration of computational time feature reduction is also an important aspects, the reduces feature increase the processing of detection ratio. Many methods have been proposed in the last decades on the designs of IDSs based on feature reduction technique. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more importance than ever before. Intrusion detection techniques are the last line of defenses against computer attacks behind secure network architecture design, firewalls, and personal screening. Despite the plethora of intrusion prevention techniques available, attacks against computer systems are still successful. Thus, intrusion detection systems (IDSs) play a vital role in network security. Symantec in a recent report uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise, going from 9 million attacks in June2013 to over 33 millions in less than a year. One solution to this is the use of network intrusion detection systems (NIDS) that detect attacks by observing various network activities. It is therefore crucial that such systems are accurate in identifying attacks, quick to train and generate as few false positives as possible.

An Intrusion Detection System (IDS) inspects the activities in a system for suspicious behavior or patterns that may indicate system attack or misuse. There are two main categories of intrusion detection techniques; Anomaly detection and Misuse detection. The former analyses the information gathered and compares it to a defined baseline of what is seen as “normal” service behavior, so it has the ability to learn how to detect network attacks that are currently unknown. Misuse Detection is based on signatures for known attacks, so it is only as good as the database of attack signatures that it uses for comparison. Misuse detection has low false positive rate, but cannot detect novel attacks. However, anomaly detection can detect unknown attacks, but has high false positive rate.

An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. In other words, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a system/network. Traditionally, intrusion detection systems have been classified as a signature detection system, an anomaly detection system or a hybrid/compound detection system. A signature detection system identifies patterns of traffic or application data presumed to be malicious while anomaly detection systems compare activities against a “normal” baseline. On the other hand, a hybrid intrusion detection system combines the techniques of the two approaches. Both signature detection and anomaly detection systems have their share of advantages and drawbacks. The primary advantage of signature detection is that known attacks can be detected fairly reliably with a low false positive rate. The major drawback of the signature detection approach is that such systems typically require a signature to be defined for all of the possible attacks that an attacker may launch against a network. Anomaly detection systems have two major advantages over signature based intrusion detection systems. The first advantage that differentiates anomaly detection systems from signature detection systems is their ability to detect unknown attacks as well as “zero days” attacks. This advantage is because of the ability of anomaly detection systems to model the normal operation of a system/network and detect deviations from them. A second advantage of anomaly detection systems is that the aforementioned profiles of normal activity are customized for every system, application and/or network, and therefore making it very difficult for an attacker to know with certainty what activities it can carry out without getting detected. However, the anomaly detection approach has its share of drawbacks as well. For example, the intrinsic complexity of the system, the high percentage of false alarms and the associated difficulty of determining which specific event triggered those alarms are some of the many technical challenges that need to be addressed before anomaly detection systems can be widely adopted. Section-II gives the information of about feature of face image. In section III discuss the method of face recognition. In section IV discuss the proposed method. In section V comparative result finally, in section VI conclusion and future scope.

II.TYPES OF IDS TECHNIQUES

There are two primary approaches to analyze events to detect attacks, namely misuse detection and anomaly detection. Misuse detection is based on the extensive knowledge of known attacks and system vulnerabilities provided by a human expert, looking for hackers who attempt to perform these attacks and/or to exploit known vulnerabilities. Although misuse detection can be very accurate in detecting known attacks, it cannot detect unknown and emerging cyber threats this shortcoming makes them vulnerable to the reactivity of attackers. In other words, when attackers change their behavior in response to detection techniques, these techniques become useless and need major redesign. One solution for this problem would be to use adaptive approaches which are inherently designed to be resilient to small changes in the environment and adapt easily. On the other hand, anomaly detection is based on the analysis of profiles that represent normal behavior of users, hosts, or network connections. Anomaly detectors characterize normal “legitimate” computer activity using different techniques and then use a variety of measures to detect deviations from defined normal behavior. The major benefit of anomaly detection algorithms is their potential to recognize unforeseen attacks. However, the major limitation is the possibly high false alarm rate. Note that deviations detected by anomaly detection algorithms may not necessarily represent actual attacks as they may simply be new or unusual but still legitimate network behavior. Anomaly detection techniques fall into the following five groups: statistical methods, rule-based methods, distance-based methods, profiling methods, and model-based approaches. It should be mentioned that many IDSs, such as snort, use both misuse detection and anomaly detection to benefit from their respective advantages. There are two general categories of intrusion detection systems (IDSs): misuse detection and anomaly based. Misuse detection systems are most widely used and they detect intruders with known patterns. The signatures and patterns used to identify attacks consist of various fields of a network packet, like source address, destination address, source and destination ports or even some key words of the payload of a packet. These systems exhibit a drawback in the sense that only the attacks that already exist in the attack database can be detected, so this model needs continuous updating, but they have a virtue of having very low false positive rate. Anomaly detection systems identify deviations from normal behavior and alert to potential unknown or novel attacks without having any prior knowledge of them. They exhibit higher rate of false alarms, but they have the ability of detecting unknown attacks and perform their task of looking for deviations much faster. Application and development of specialized machine learning techniques is gaining increasing attention in the intrusion detection community. Soft computing is a collection of methodologies, which aim to exploit tolerance for imprecision, uncertainty and partial truth to achieve tractability, robustness and low solution, cost. As soft-computing techniques can also be used for machine learning, different soft-computing techniques have been used for intrusion detection (Fuzzy Logic, Artificial Neural Networks, Genetic Algorithms), but their possibilities are still under-utilized. In this work we have realized a misuse detection system that is based on Genetic Algorithm (GA). We have exploited both possibilities, either to classify network traffic as normal or abnormal, or to further classify the attacks by their type. Many features of GA make it very suitable for intrusion detection. Like robustness to noise, self learning capabilities and the fact that initial rules can be built randomly so there is no need of knowing the exact way of attack machinery at the beginning. Further classification of the attacks is not very important for intrusion detection, but it is important for network forensics because knowing the exact type of a threat and the way it performs its attack, the recovery after an attack would be more successful.

III.FEATURE SELECTION

Feature selection is an essential data processing step prior to applying a machine learning algorithm. It is a process of determining whether a feature is relevant or not for a particular problem. Using effective features to design classifier not only can reduce the data size but also can improve the performance of the classifier and enhances data understanding or visualization [15]. One of the major problems in feature reduction is to select effective attributes that have the best discrimination ability between the classes. There are two common approaches for feature reduction: Wrapper and Filter. A Wrapper method selects feature subset based on the performance of the learning algorithm that is going to be used. Wrapper method is totally dependent on the learning algorithm. On the other hand Filter methods evaluate features according to statistical characteristics of the data only without the involvement of any learning algorithm. The wrapper approach is generally considered to produce better feature subsets but runs much more slowly and requires more computing resource than a filter.

Different techniques have been used to tackle the problem of feature selection. feature ranking algorithms to reduce the feature space of the DARPA data set from 41 features to the six most important features. They used three ranking algorithms based on Support Vector Machines (SVMs), Multivariate Adaptive Regression Splines (MARSs), and Linear Genetic Programs (LGPs) to assign a weight to each feature. Experimental results showed that the classifier's accuracy degraded by less than 1 percent when the classifier was fed with the reduced set of features. Sequential backward search was used in [8], [9] to identify the important set of features: starting with the set of all features, one feature was removed at a time until the accuracy of the classifier was below a certain threshold. Different types of classifiers were used with this approach including Genetic Algorithms ,Neural Networks , and Support Vector Machines.

IV.ATTRIBUTES SELECTION FROM DATASET

Effective input attributes selection from intrusion detection datasets is one of the important research challenges for constructing high performance IDS. Irrelevant and redundant attributes of intrusion detection dataset may lead to complex intrusion detection model as well as reduce detection accuracy. This problem has been studied during the early work of W.K. Lee [5], research on KDD99 benchmark intrusion detection dataset, where 41 attributes were constructed for each network connection. The attribute selection methods of data mining algorithms identify some of the important attributes for detecting anomalous network connections. Attributes selection in intrusion detection using data mining algorithms involves the selection of a subset of attributes d from a total of D original attributes of dataset, based on a given optimization principle. Finding a useful attribute subset is a form of search. Ideally, attribute selection methods search through the subsets of attributes, and try to find the best one among the completing 2N candidate subsets according to some evaluation function. Therefore, building IDS based on all attributes is infeasible, and attributes selection becomes very important for IDS. In KDD99 intrusion detection dataset, there are total 494021 examples in the 10% training dataset. The KDD99 dataset contains 22 different attack types that could be classified into four main categories namely Denial of Service (DoS), Remote to User (R2L), User to Root (U2R) and Probing. There are 41 attributes for each network connection that have either discrete values or continuous values. The attributes in KDD99 dataset can be divided into three groups. The first group of attributes is the basic features of network connection, which include the duration, prototype, service, number of bytes from source IP addresses or from destination IP addresses, and some flags in TCP connections. The second group of attributes in KDD99 is composed of the content features of network connections and the third group is composed of the statistical features that are computed either by a time window or a window of certain kind of connections. The attributes selection in KDD99 dataset has been widely used as a standard method for network-based intrusion detection learning, and it was found that all 41 attributes of KDD99 dataset are not the best ones for intrusion detection learning. Therefore the performance of IDS may be further improved by studying new attribute selection methods.

V.NETWORK DATA MINING

NDM may serve two different purposes. First, knowledge about the analyzed monitoring data is generated. This allows determining dominant characteristics and identifying outliers within the data records that can be considered as anomalous or suspicious. Secondly, NDM can be deployed to define rules or patterns that are typical for specific kinds of traffic, e.g. normal web traffic or traffic observed during a denial of service (DoS) attack. These rules and patterns can be used to analyze new sets of monitoring data and to check if these show similar properties and characteristics as the original data. Obvious applications profiting from such rules and patterns are network-based intrusion detection systems (NIDS) and traffic analyzers that characterize and classify traffic flows.

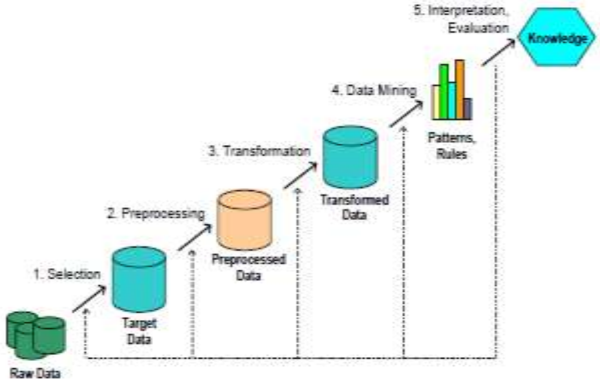

Figure 1: Knowledge Discoveries in Databases.

The data mining approach to intrusion detection was first implemented in mining audit data for automated models for intrusion detection (MADAMID) The data mining process of building intrusion detection models is depicted in below figure. Raw data is first converted into ASCII network packet information, which in turn is converted into connection level information. These connection level records contain within connection features like service, durati on etc. Data mining algorithms are applied to this data to create models to detect intrusions. Data mining algorithms used in this approach include rule based classification algorithm (RIPPER), Meta classifier, frequent episode algorithm and association rules.

VI.CLASSIFIER CONSTRUCTION

Classifier construction is another important research challenge to build efficient IDS. Nowadays, many data mining algorithms have become very popular for classifying intrusion detection datasets such as decision tree, naïve Bayesian classifier, neural network, genetic algorithm, and support vector machine etc. However, the classification accuracy of most existing data mining algorithms needs to be improved, because it is very difficult to detect several new attacks, as the attackers are continuously changing their attack patterns. Anomaly network intrusion detection models are now using to detect new attacks but the false positives are usually very high. The performance of an intrusion detection model depends on its detection rates (DR) and false positives (FP). DR is defined as the number of intrusion instances detected by the system divided by the total number of the intrusion instances present in the dataset. FP is an alarm, which rises for something that is not really an attack. It is preferable for an intrusion detection model to maximize the DR and minimize the FP. For DR, we can modify the objective function to 1-DR. Therefore classifier construction for IDS is another technical challenge in the field of data mining.

VII.SUPPORT VECTOR MACHINE

Support Vector Machines (SVMs) are also a good candidate for intrusion detection systems which can provide real-time detection capability, deal with large dimensionality of data. SVMs plot the training vectors in high dimensional feature space through nonlinear mapping and labeling each vector by its class. The data is then classified by determining a set of support vectors, which are members of the set of training inputs that outline a hyper plane in the feature space. SVM is a technique for solving a variety of learning, Classification and prediction problems. The basic SVM deals with two-class problems in which the data are separated by a hyper plane defined by a number of support vectors. Support vectors are a subset of training data used to define the boundary between the two classes. In situations where SVM cannot separate two classes, it solves this problem by mapping input data into high-dimensional feature spaces using a kernel function. In high-dimensional space it is possible to create a Hyper plane that allows linear separation. Compared with the ANN, the SVM have two advantages. Firstly, the global optimum can be derived. Secondly, the over fitting problem can be easily controlled by the choice of a suitable margin that separates the data. Empirical testing has shown that the SVM performance is better than that for the ANN in classification and regression problems. Support Vector Machine is a popular topic based on statistical machine learning. In a nutshell, a SVM is an algorithm that works as follows. It uses a nonlinear mapping to transform the original training data into a higher dimension. Within this new dimension, it searches for the linear optimal separating hyper plane (that is, a “decision boundary” separating the tuples of one class from another). With an appropriate nonlinear mapping to a sufficiently high dimension, data from two classes can always be separated by a hyper plane. The SVM finds this hyper plane using support vector (training tuples) and margins (defined by the support vectors). Especially in high-dimensional data space, the effective overcome of the dimension disaster and excessive learning problems are very important. SVM has widely been applied in pattern recognition fields. Network connection includes much information of user behavior. The traditional SVM-based intrusion detection methods are rarely taken into considering the differences among different network protocols. They found SVM by adopting unified data formats. That takes much time and leads to low efficient.

VIII.NEURAL NETWORKS

An artificial neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the characteristics of the elements and the weights associated with the interconnections among them. By modifying the connections between the nodes the network is able to adapt to the desired outputs. Unlike expert systems, which can provide the user with a definitive answer if the characteristics which are reviewed exactly match those which have been coded in the rule base, a neural network conducts an analysis of the information and provides a probability estimate that the data matches the characteristics which it has been trained to recognize. While the probability of a match determined by a neural network can be 100%, the accuracy of its decisions relies totally on the experience the system gains in analyzing examples of the stated problem. A neural network contains no domain knowledge in the beginning, but it can be trained to make decisions by mapping exemplar pairs of input data into exemplar output vectors, and adjusting its weights so that it maps each input exemplar vector into the corresponding output exemplar vector approximately. A knowledge base pertaining to the internal representations is automatically constructed from the data presented to train the network. Well-trained neural networks represent a knowledge base in which knowledge is distributed in the form of weighted interconnections where a learning algorithm is used to modify the knowledge base from a set of given representative cases. A generic form of a neural network intrusion detector is presented in the below Figure. The system use the input labeled data (normal and attack samples) to train a neural network model. The resulting model is then applied to the new samples of the testing data to determine the corresponding class of each one, and so to detect the existing attacks. Using the label information of the testing data, the system can compute the detection performances measures given by the false alarms rate, and the detection rate. A classification rate can also be computed if the system is designed to perform attacks multi classification.

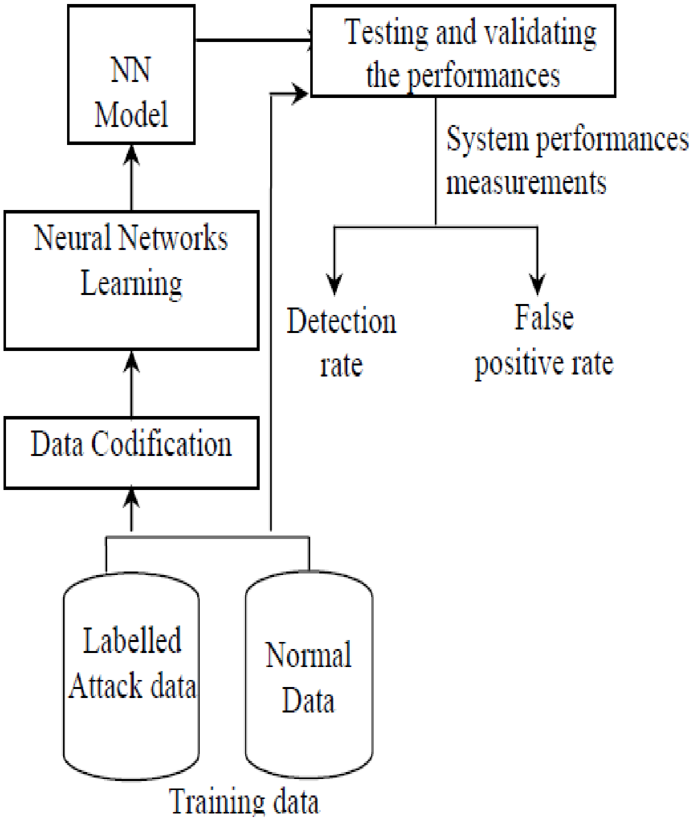

Figure 2: A generic form of a NN-base intrusion detection system.

IX.RELATED WORK

In this section we describe the literature survey on the basis of optimization and classification techniques for the intrusion and unknown detection. A rich literature of intrusion detection focuses on feature reduction using soft computing and neural network. Many of these techniques are based on principal of component into a set of class classification problems. Despite the success of these techniques reported in different domains for various types of applications, such as text document classification, and speech recognition, most of these techniques are mainly proposed for learning from relatively balanced training data. However, in much application, the training data can be often intrusion, where some classes of data have a small number of samples compared to the other classes, and in which it is important to accurately classify the minority cases. In survey, numbers of anomaly detection systems are study based on many different machine learning techniques. Some studies apply single agent learning technique, such as neural networks, genetic algorithms, support vector machines, etc.

[1] In this paper author tried to propose a very simple and fast feature selection method to eliminate features with no helpful information on them. Result faster learning in process of redundant feature omission. We compared our proposed method with three most successful similarity based feature selection algorithm including Correlation Coefficient, Least Square Regression Error and Maximal Information Compression Index. After that we used recommended features by each of these algorithms in two popular classifiers including: Bayes and KNN classifier to measure the quality of the recommendations. There are varieties of attacks that IDS tries to detect. Some of these can be detected by scanning the packets to find signature of specific attacks.

[2] In this paper author described the feature reduction method with using classifier and the details are Synthetic Minority Oversampling Technique (SMOTE) is applied to the training dataset. A feature selection method based on Information Gain is presented and used to construct a reduced feature subset of NSL-KDD dataset. Random Forests are used as a classifier for the proposed intrusion detection framework. Empirical results show that Random Forests classifier with SMOTE and information gain based feature selection gives better performance in designing IDS that is efficient and effective for network intrusion detection. They used random forests classifier for developing efficient and effective IDS. For improving the detection rate of the minority classes (R2L and U2R) in imbalanced training dataset we used Synthetic Minority Oversampling Technique (SMOTE) and we picked up all of the important features of the minority class using the minority classes attack mode.

[3] In this paper author discussed the techniques for intrusion detection which are based on the data mining techniques and the details are an intrusion detection system (ids) is the fundamental part of the security infrastructure, since it ensures the detection of any suspicious action. Although the detection of intrusions and attacks is the ultimate goal, the huge amount of generated alerts cannot be properly managed by the administrator. In order to improve the accuracy of sensors, we adopt a two-stage technique. The first one aims to generate meta-alerts

through clustering and the second one aims to reduce the rate of false alarms using a binary classification of the generated meta-alerts. For the first stage we use two alternatives, self-organizing map (SOM) with K-means algorithm and neural gas with fuzzy c-means algorithm. For the second stage we use three approaches, SOM with K-means algorithm, support vector machine and decision trees.

[7] In this paper, a new learning approach for network intrusion detection using naïve Bayesian classifier and ID3 algorithm is presented, which identifies effective attributes from the training dataset, calculates the conditional probabilities for the best attribute values, and then correctly classifies all the examples of training and testing dataset. Most of the current intrusion detection datasets are dynamic, complex and contain large number of attributes. Some of the attributes may be redundant or contribute little for detection making. It has been successfully tested that significant attribute selection is important to design a real world intrusion detection systems (IDS).

[8] In this paper, author use a genetic algorithm to select a subset of input features for decision tree classifiers, with a goal of increasing the detection rate and decreasing the false alarm rate in network intrusion detection. We used the KDDCUP 99 data set to train and test the decision tree classifiers. The experiments show that the resulting decision trees can have better performance than those built with all available features. Machine Learning techniques have recently been extensively applied to intrusion detection. Example approaches include decision trees ,Genetic Algorithm and Genetic Programming, naive Bayes, KNN and neural networks A key problem is how to choose the features (attributes) of the input training data on which learning will take place.

[9] Author proposed here a using SOM for reduce alarm in IDS and described as an Intrusion detection systems aim to identify attacks with a high detection rate and a low false alarm rate. Classification-based data mining models for intrusion detection are often ineffective in dealing with dynamic changes in intrusion patterns and characteristics. Consequently, unsupervised learning methods have been given a closer look for network intrusion detection. Traditional instance-based learning methods can only be used to detect known intrusions, since these methods classify instances based on what they have learned. They rarely detect new intrusions since these intrusion classes has not been able to detect new intrusions as well as known intrusions. Author proposed a soft Computing technique such as Self organizing map for detecting the intrusion in network intrusion detection.

[12 Author presents a novel approach for detecting network intrusions based on a competitive learning neural network. In the paper, the performance of this approach is compared to that of the self-organizing map (SOM), which is a popular unsupervised training algorithm used in intrusion detection. While obtaining a similarly accurate detection rate as the SOM does, the proposed approach uses only one fourth of the computation times of the SOM. Furthermore, the clustering result of this method is independent of the number of the initial neurons. This approach also exhibits the ability to detect the known and unknown network attacks. The experimental results obtained by applying this approach to the KDD-99 data set demonstrate that the proposed approach performs exceptionally in terms of both accuracy and computation time.

[14] Author proposed here a novel method for IDS using RBFNN and the detailed as a Neural Network model combined with prototype clustering and classification for fast and accurate detection of intrusion in host based system. Previous RBF suffered from grouping of pattern of intrusion, now this problem are reduced using Distance variable ensemble cluster classification and increase the rate of detection of infected data in host system. Our methodology test in KDD CUP 99 and calculate the rate of detection Accuracy, Precision, Recall, False positive rate, false negative rate, true positive rate, True negative rate. In this paper Author proposed a prototype classifier based on neural network RBF model.

X.PERFORMANCE EVALUATION FOR EXPERIMENTAL RESULT

In this section we discuss the comparative result analysis based on instant based learning and data mining approach and optimization algorithm for intrusion detection. The rate of intrusion detection finds on given method of author and used KDDCUP99 dataset for analysis. The analysis of comparative detection rate evaluate on the basis of detection rate. The result of all these method given below in table 1.

Method	**Algorithm applied**	**Detection Rate (%)**
Neural Network [1]	RBF network	89-90
Markov Model [3]	HMM	85-86
ART [7]	Adaptive theory	86-91
Prototype Classification [9]	ECCS	91-93
Optimization [12]	ANT	92-93
AIS [21]	DT(danger	90-92

	theory)	
GA [17]	Genetic Algorithm	88-91
PCA [19]	Principal component analysis	89-93
LPDA [23]	LPDA	90-93
ACO [13]	Ant colony optimization	91-94

Table 1: Shows the comparative result analysis of data mining approach, neural network and Optimization Algorithm for detection of intrusion on given KDDCUP99 dataset.

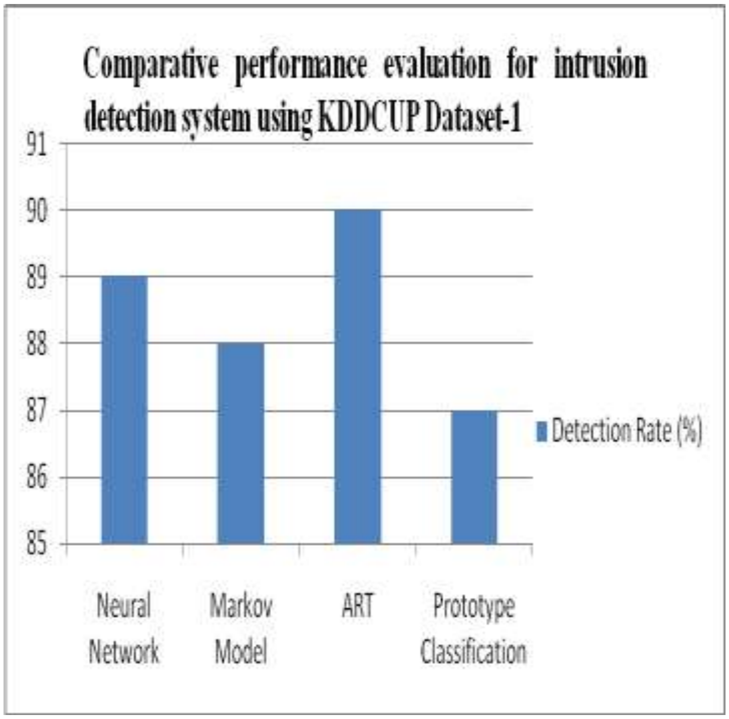

Figure 3: Shows that the comparative performance evaluation using data mining and neural network method for IDS.

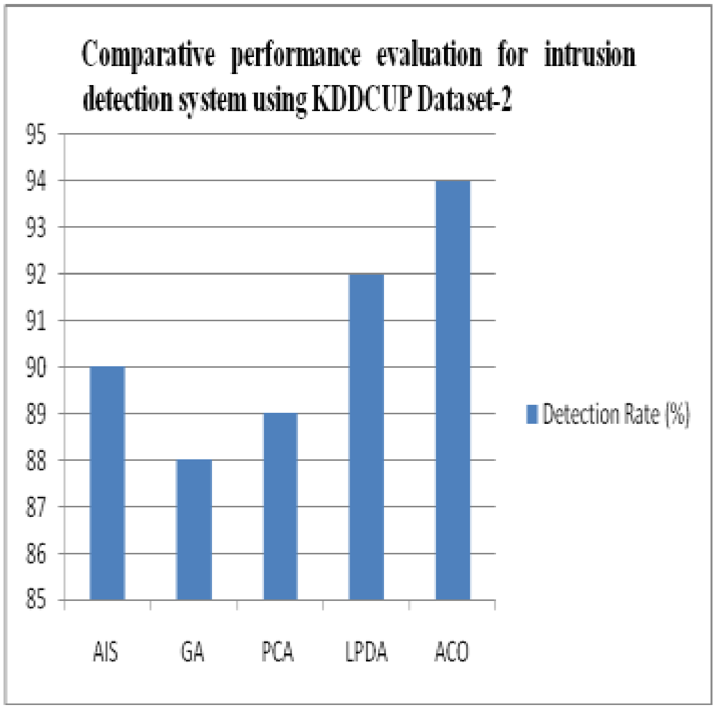

Figure 4: Shows that the comparative performance evaluation using optimization algorithms for IDS.

XI. CONCLUSION AND FUTURE WORK

In this paper presents the empirical evaluation of feature reduction and feature optimization technique for intrusion detection system. In intrusion detection process the traffic size and number of attribute is very large. Due to large size of feature and attribute the process of intrusion detection is suffered. Now in current decade various authors and researchers used feature reduction and optimization technique for the reduction of feature attribute and traffic size. Soft computing and neural network play an important role for feature reduction. The process of neural network reduces the feature and impart as classifier for the process of classification. In future proposed a hybrid model for feature reeducation and classification for intrusion detection system.

REFERENCES

[1] Shafigh Parsazad, Ehsan Saboori, Amin Allahyar "Fast Feature Reduction in Intrusion Detection Datasets" MIPRO 2012, Pp 1023-1029.

[2] Abebe Tesfahun, D. Lalitha Bhaskari “Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction” International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013. Pp 127-132.

[3] Hachmi Fatma, Limam Mohamed “A two-stage technique to improve intrusion detection systems based on data mining algorithms” IEEE, 2013. Pp 1-6.

[4] Shailendra Singh, Sanjay Silakari “An Ensemble Approach for Cyber Attack Detection System: A Generic Framework” 14th ACIS, IEEE 2013.

[5] Li Chen “Using Genetic Algorithm for Network Intrusion Detection” Proc. the United States Department of Energy Cyber Security Group 2004 Training Conference, May 2004.

[6] Jain , Upendra “An Efficient intrusion detection based on Decision Tree Classifier using feature Reduction”, International Journal of scientific and research Publications , Vol. 2, Jan. 2012.

[7] Dewan Md. Farid, Jerome Darmont, Nouria Harbi, Nguyen Huu Hoa, Mohammad Zahidur Rahman “Adaptive Network Intrusion Detection Learning: Attribute Selection and Classification” 2008. Pp 1-5.

[8] Gary Stein, Bing Chen, Annie S. Wu, Kien A. Hua “Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection” 2556. Pp 1-6.

[9] Ritu Ranjani Singh a, Prof. Neetesh Gupta “To Reduce the False Alarm in Intrusion Detection System using self Organizing Map” in International journal of Computer Science and its Applications.

[10] Z. Xue-qin, G. Chun-hua, L. Jia-jin “Intrusion detection system based on feature selection and support vector machine” Proc. First International Conference on Communications and Networking in China (ChinaCom '06), Oct. 2006.

[11] Zhang , M. Zulkernine “Network Intrusion Detection using Random Forests” School of Computing Queen’s University, Kingston Ontario, 2006.

[12] John Zhong Lei and Ali Ghorbani “Network Intrusion Detection Using an Improved Competitive Learning Neural Network” in Proceedings of the Second Annual Conference on Communication Networks and Services Research IEEE.

[13] P. Jongsuebsuk , N. Wattanapongsakorn and C. Charnsripinyo “Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks” in IEEE 2013.

[14] Deepak Rathore and Anurag Jain “a novel method for intrusion detection based on ecc and radial bias feed forword network” in Int. J. of Engg. Sci. & Mgmt. (IJESM), Vol. 2, Issue 3: July-Sep.: 2012.

[15] Wing w. Y. Ng, rocky k. C. Chang and daniel s. Yeung “dimensionality reduction for denial of service detection problems using rbfnn output sensitivity” in Proceedings of the Second International Conference on Machine Learning and Cybernetics, Wan, 2-5 November 2003.

[16] Anshul Chaturvedi and Prof. Vineet Richharia “A Novel Method for Intrusion Detection Based on SARSA and Radial Bias Feed Forward Network (RBFFN)” in international journal of computers & technology vol 7, no 3.

[17] Mohammad Behdad, Luigi Barone, Mohammed Bennamoun and Tim French “Nature-Inspired Techniques in the Context of Fraud Detection” in ieee transactions on systems, man, and cybernetics part c: applications and reviews, vol. 42, no. 6, november 2012.

[18] Alberto Fernandez, Maria Jose del Jesus and Francisco Herrera “On the influence of an adaptive inference system in fuzzy rule based classification system for imbalanced data-sets” in Elsevier Ltd. All rights reserved 2009.

[19] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez and E.Vazquez “Anomaly-based network intrusion detection: Techniques, Systems and challenges” in Elsevier Ltd. All rights reserved 2008.

[20] Terrence P. Fries “A Fuzzy-Genetic Approach to Network Intrusion Detection” in GECCO 08, July12–16, 2008, Atlanta, Georgia, USA.

[21] Zorana Bankovic, Dusan Stepanovic,Slobodan Bojanic and Octavio Nieto-Taladriz “Improving network security using genetic algorithm approach” in Published by Elsevier Ltd 2007.

[22] Mrutyunjaya Panda and Manas Ranjan Patra “network intrusion detection using naive bayes” in IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007.

[23] Animesh Patcha and Jung-Min Park “An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends” in Computer networks 2007.

[24] Ren Hui Gong, Mohammad Zulkernine and Purang Abolmaesumi “A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection” in IEEE 2005.

[25] Jonatan Gomez and Dipankar Dasgupta “Evolving Fuzzy Classifiers for Intrusion Detection” in IEEE 2002.

[26] Francisco Herrera “Genetic fuzzy systems: taxonomy, current research trends and prospects” in Springer-Verlag 2008.

[27] Adel Nadjaran Toosi and Mohsen Kahani “A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers” in Elsevier B.V. All rights reserved 2007.

[28] C. Phua, V. C. S. Lee, K. Smith-Miles, and R.W. Gayler “A comprehensive survey of data mining-based fraud detection research” CoRR,”, pp. 1–14, 2010.

[29] E. Blanzieri and A. Bryl “Asurvey of learning-based techniques of email spam filtering” Artif. Intell. Rev., vol. 29, no. 1, pp. 63–92, 2008.

[30] D. Sculley and G. Cormack “Filtering email spam in the presence of noisy user feedback” in Proc. 5th Email Anti-Spam Conf., 2008, pp. 1– 10.