Intrusion Detection in KDD99 Dataset: A Review

Megha Jain Gowadiya, Anurag Jain

Abstract— With the perpetual growth in the use of network services for information and resource sharing, which makes our work easier. Sometimes extensive use of network gets compromised with different kind of threats or intrusion which may fraudulent or devastate the integrity, confidentiality and resource availability. For detecting intrusion over network system has been designed which is called Intrusion Detection System (IDS) whose purpose is to perceive a variety of anomalies and intrusions. In intrusion detection system various data mining algorithm has been applied such as ID3, KNN, K-means etc. The analysis of different feature selection approach is performed in widely used KDDCUP'99 dataset. This paper, presents the literature study of different methodologies developed by researchers with their merits and demerits.

Index Terms— Threats, Confidentiality, Network Attacks, IDS, ID3, KDDCUP'99 Dataset, Data mining, KNN, GA.

1 Introduction

COMPUTER network is extensively used technology from the past few years. This is used by several private and government organization for storing and sharing the data over the network. This incredible augmentation has created challenging subject in network and data security and exposure of security threats, generally called as intrusion, has become an exceedingly imperative and significant issue in network, data and resource security. Intrusion [1] is "whichever set of actions that endeavour to conciliate the reliability, privacy or availability of a resource. The network threats provide problems to our information hence, a system is designed which recurrently scrutinize the activity carries out over network and if any such activity is detected which may influence the performance and information of the network that must be notified or discarded such system is known as intrusion detection system (IDS). The intrusion detection system is classified according to deployment area and as per collected data. The intrusion system based on deployment area can be host- based or network based. Based on collected data an IDS is classified into two categories: Misuse based detection and anomaly based intrusion detection system. Misuse based (signature based) intrusion detection system tries to perceive malevolent activities based on prototype or signatures of known attacks [2]. If a prototype match is found, an alarm is reported to the network supervisor. Because misuse based detection system is exclusively designed for detecting notorious attacks, it produces minimum number of counterfeit alarms. On the other hand, misuse based intrusion detection systems could not distinguish fresh attacks.

Anomaly based intrusion detection mainly used to identify events that are atypical with reverence to the normal system activities [2]. If the incoming network traffic patterns do not pursue the normal network traffic activities, an alarm will be reported and such patterns are called anomalies or outliers. In spite of their potential in detecting fresh attacks anomaly based intrusion detection systems undergo from high false positive rate (FPR).

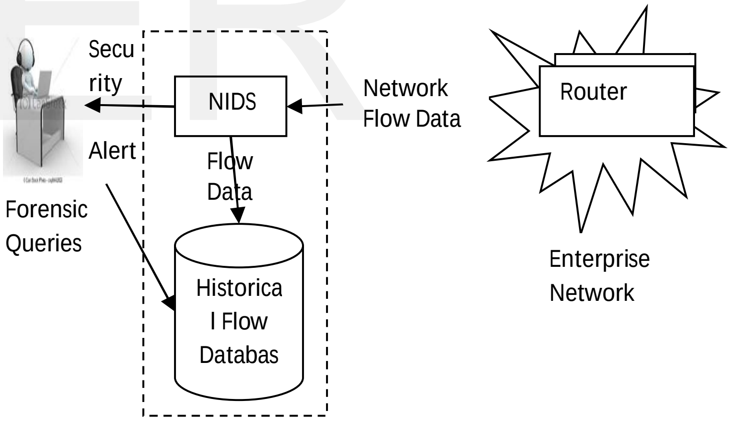


Fig. 1 Intrusion Detection System

But IDS faces problems like that's how to proficiently divide the normal activities and the abnormal activities from a large number of raw information's characteristic, and how to efficiently engender automatic intrusion rules following collected unrefined data of the network. To carry out this, unusual data mining methods must be considered, like classification, correlation analysis of data mining methods and so on [3]. The ever rising new intrusion or attacks type poses severe difficulties for their detection. The networking attack is has mainly four categories such as denial of service (DoS), probing, U2R and R2L. The human labelling of the accessible

- *Megha Jain Gowadiya is currently pursuing masters degree program in computer science and engineering in RITS, Rajiv Gandhi Prodyogiki Vishwavidyalaya Bhopal, India. E-mail: gmeghajain@gmail.com*

- *Anurag Jain is currently HOD at computer science and engineering dept. in RITS, Rajiv Gandhi Prodyogiki Vishwavidyalaya Bhopal, India. E-mail: anurag.akjain@gmail.com*

network audit information instances is generally tedious, expensive as well as time consuming. In this paper the analysis of intrusion is perform by selecting the feature in KDDCUP'99 dataset.

1.1 KDDCUP'99 DATASET

Since 1999, KDD'99 has been the most wildly used data set for the evaluation of anomaly detection methods. This data set. and is built based on the data captured in DARPA'98 IDS evaluation program. DARPA'98 is about 4 gigabytes of compressed raw (binary) tcpdump data of 7 weeks of network traffic, which can be processed into about 5 million connection records, each with about 100 bytes. The two weeks of test data have around 2 million connection records. KDD training dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack, with exactly one specific attack type [4].

1.2 NETWORK ATTACK

The data set contains a total of 23 attack, these are grouped into 4 major categories [5]:

1) Denial-of-Service (DoS)

In this type of attack, the attacker has limits or denies the service presented to the user, computer or network. Attacker tries to prevent genuine users from using a service. It is usually done by making the resources either too busy or too full and overflow.

2) Probing or Surveillance

Probing or Surveillance attacks have the main aim of gaining knowledge of the existence or configuration of a computer system or the network. The attacker then tries to harm or retrieve information about resources of the victim network.

3) User-to-Root (U2R)

User-to-root attack is attempts by an unauthorized user to gain administrative privileges. The attacker starts outs with access to a normal user account on the system (perhaps gained by sniffing password, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system.

4) Remote-to-Local (R2L)

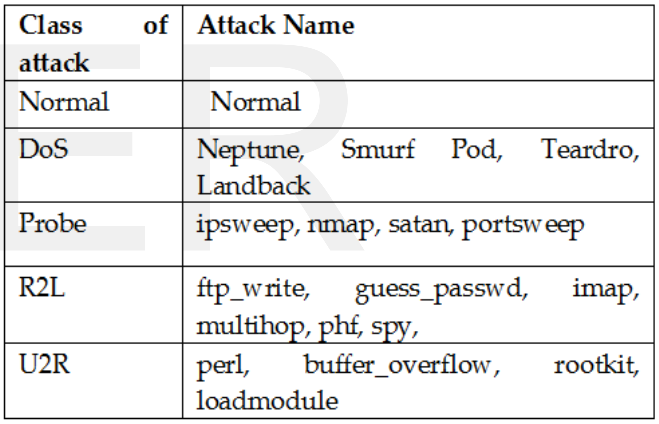
Remote-to-local attack is the kind of intrusion attack where the remote intruder consistently sends packets to a local machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine.

In training data set, 23 attack that appears which is organized into 5 major class labels those are given Table 1 below such as normal, R2L, U2R, Probe and DoS.

2 RELATED WORK

Patel et al. [6] a hybrid model is proposed that integrates Anomaly based Intrusion detection technique with Signature based Intrusion detection technique is divided into two stages. In first stage, the signature based IDS SNORT is used to generate alerts for anomaly data. In second stage, data mining techniques "k-means + CART" is used to cascade k-means clustering and CART (Classification and Regression Trees) for classifying normal and abnormal activities. The hybrid IDS model is evaluated using KDD Cup Dataset. The proposed assemblage is introduced to maximize the effectiveness in identifying attacks and achieve high accuracy rate as well as low false alarm rate.

Table: 1 Class-wise Attack on KDD dataset



Class of attack	Attack Name
Normal	Normal
DoS	Neptune, Smurf Pod, Teardro, Landback
Probe	ipsweep, nmap, satan, portsweep
R2L	ftp_write, guess_passwd, imap, multihop, phf, spy,
U2R	perl, buffer_overflow, rootkit, loadmodule

Khaing et al. [7] proposed a new approach to design the anomaly intrusion detection system using not only misuse but also anomaly intrusion detection for both training and detection of normal or attacks respectively. The utilized method is the combination of Machine Learning and pattern recognition method for Anomaly Intrusion Detection System (AIDS). The Machine Learning Algorithm, Random Forest, use as a feature selection method and the pattern recognition algorithm, k- Nearest Neighbors for detection and classification of the known and unknown attack classes. The experimental results are obtained by using through intrusion dataset: the KDD Cup 1999 dataset.

Su et al. [8] proposed the IDS with the combination of hierarchical clustering and support vector machines to increase detection accuracy. The experimental results are based on KDD 99 dataset. The result has shown better performance for detection of DoS and Probe attacks. The

BIRCH Hierarchical clustering algorithm is used and it was firstly introduced by Zhang et al. (1996) [4]. A BIRCH algorithm is used to reduce training data set so that training data set processing complexity is reduced. The SVM algorithm has high detection accuracy and low false positive rate.

Panda et al. [9] applied one of the proficient data mining technique called naïve bayes for anomaly based network intrusion detection. Experimental outcomes on the KDD cup' 99 dataset showed the uniqueness of their method in detecting network intrusion. It is examinee that the proposed technique performs recovered in terms of false positive rate, price tag, and computational time when functional to KDD'99 data sets compared to a back propagation neural network(BPNN) based approach.

Bharat et al. [10] proposed a system for intrusion detection using Particle Swarm Optimization (PSO) with Genetic Algorithm (GA) based feature selection and using Adaptive Mutation for sluggish convergence of optimization algorithm. The consequences therefore obtained were around 92% that confirms the proposed method to be reasonably efficient in intrusion detection.

Saxena et al. [11] proposed a novel method by means of data mining technique such as SVM and Particle swarm optimization for attaining privileged detection rate. PSO is an Optimization process and has a strong global search potential. The SVM-PSO Method is functional to KDD Cup 99 dataset. Free constraints are acquired by standard PSO for support vector machine and the binary PSO is used to accomplish the top probable attribute subset at building intrusion detection system. The proposed system had foremost process: Pre-processing, feature reduction using Information Gain, Training using SVM-PSO. Behind that based on the consequent training subsets a vector for SVM classification is formed and in the end, classification using PSO is executed to perceive Intrusion has happened or not. The experimental outcome illustrated that SVM-PSO acquire high detection rate than regular SVM Method algorithm.

Patel et al. [12] described about a method of intrusion detection that uses machine learning algorithms. Here they discussed about the combinational use of two machine learning algorithms called Information Gain based Feature Selection and K-means Clustering Algorithm. Dimensionality Reduction is a field in machine learning that consist of mapping high dimensional data into low dimension while preserving important features of original dataset. The experiments were conducted on the intrusion detection dataset called NSL-KDD dataset. NSL-KDD intrusion detection dataset which is an enhanced version of KDDCUP'99 dataset. The comparison of the results with and without dimensionality reduction is also done.

Bhaskar et al. [13] deliberated an effectual fusion layered intrusion detection system for identifying both formerly known and zero-day attacks. In meticulous, a two layer system that mingles misuse and anomaly intrusion detection systems is anticipated. The former layer consists of misuse detector which can notice and block known attacks and the second layer comprises of anomaly detector which can proficiently identify and block formerly unknown attacks. The misuse detector is designed based on random forests classifier and the anomaly detector is designed using bagging method with assembly of one-class support vector machine classifiers. Data pre-processing is done using involuntary feature selection and data normalization. Experimental outcomes demonstrated that the proposed intrusion detection system gives better results than other well-known intrusion detection systems in detecting both formerly known and zero-day attacks.

Dalal et al. [14] proposed an attribute based Intrusion data classification technique. The reduced feature enhanced the classification of intrusion data. The reduction procedure of feature attribute, presented by DAG function along with feature correlation factor. The proposed method work as feature reducers and classification method, from the reduction of feature attribute also reduced the execution time of classification. For assessment purposes, this model is applied on KDD'99 dataset.

Takkellapati et al. [15] proposed as the outlay of the data processing and Internet accessibility amplifies, more and more organizations are becoming susceptible to a wide range of cyber threats. Most recent offline intrusion detection systems are focused on unsupervised and supervised machine learning methods. Existing model has high error rate during the attack classification using support vector machine learning algorithm. In addition, with the study of existing work, feature selection techniques are also indispensable to progress high efficiency and effectiveness. Performance of unusual types of attacks detection should also be improved and evaluated using the proposed method. In this proposed system, Information Gain (IG) and Triangle Area based KNN are used for choosing more discriminative features by combining Greedy k-means clustering algorithm and SVM classifier to identify Network attacks. This system achieves high precision detection rate and less error rate of KDD CUP 1999 training data set.

3 INTRUSION DETECTION METHODOLOGY

Intrusion detection is serious issues in network, different authors various data mining and neural network methods has been proposed or implemented in which is this section some of them is describing below:

3.1 Radial Basis Function

Radial Basis Function (RBF) Network is a kind of Artificial Neural Network for supervised learning [16]. It uses RBF as a function which is typically Gaussian and the results are inversely proportional to the distance from the center of the neuron [17]. The conventional, RBF function network can be seen in Figure 2. MATLAB presents functions to apply RBF Network within their Neural Network Toolbox. The training function newrb() and simulation function sim() is used to train and test the network [18].

3.2 Principle Component Analysis

PCA is a widespread statistical method used in multivariate optimization harms in order to decrease the dimensionality of data while retraining an outsized fraction of the data characteristic. Primary, PCA is used to endeavor the training set onto eigen space vectors representing the mean of the data. These eigen space vectors are then used to forecast malicious connections in a workload containing normal and attack activities [19]. PCA diminish the amount of dimensions required to categorize fresh data and fabricates a set of principal components, which are ortho-normal eigen value pairs. In other words, PCA projects a set of axes which preeminent suit the data. These set of axes correspond to the normal connection data. Outlier detection occurs by mapping live network data onto these normal axes and calculating the distance from the axes. If the distance is greater than a certain threshold, then the connection is classified as an attack. The principle components are resulting from the covariance matrix. When some values are much better than others, then their corresponding eigen values have larger weights. The larger the eigen value, the more considerable its corresponding projected eigenvector. Consequently, the principal components are sorted from most to slightest considerable i.e. in descending order. If a novel data item is projected along the upper set of the noteworthy principal components, it is probable that the data item can be classified exclusive of projecting along all the principal components. The eigenvectors of the principal components represent axes which best suit a data example. Points which lie at a extreme distance from the axes would exhibit abnormal behavior. Outliers measured using the Euclidian distance are the network connections that are anomalous. Using a threshold value (t), any network connection with a distance larger than the threshold is considered an outlier.

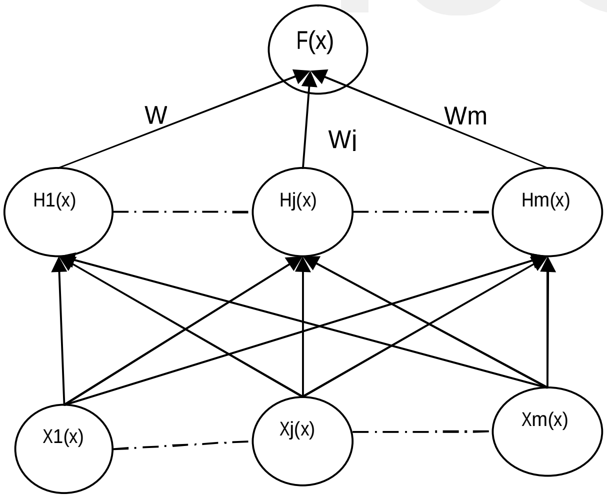


Fig. 2 Radial Basis Function (RBF) Using Single Layer

3.3 Support Vector Machine

The Support Vector Machine [20] is one of the most flourishing classification algorithms in the data mining area.SVM uses a high dimension space to discover a hyper-plane to carry out binary classification. SVM approach is a classification technique based on Statistical Learning Theory (SLT).It is based on the idea of hyper plane classifier. The goal of SVM is to find a linear optimal hyper plane so that the margin of partition among the two classes is maximized. The SVM uses a section of the data to train the system. It finds numerous support vectors that correspond to the training data. These support vectors will form a SVM model. According to this model, the SVM will classify a given unknown dataset into target classes.

A classification task engrosses training set and testing set which consist of instances. Each instance in the training set contains one “target value" (class labels: Normal or Attack) and several “attributes" (features).The objective of SVM is to construct a model which predicts target value of data instance in the testing set which is given simply attributes.

To accomplish this objective, they have used kernel functions offered with SVM. There are 3 foremost SVM kernel functions:

(i) Gaussian Kernel (Radial Basis Function)
(ii) Polynomial kernel
(iii) Sigmoid kernel

(i) Gaussian Kernel Function: The Gaussian kernel is an paradigm of radial basis function kernel.

$$K(Xi, Xj) = Exp\{-(|Xi - Xj|)/2\sigma$$

Where, **σ** stands for window width.

(ii) Polynomial Kernel Function: Such Polynomial kernel is a non-stationary kernel. Polynomial kernels are well suited for harms where all the training data is normalized. Adaptable parameters are the constant term c and the polynomial degree d.

$$K(Xp, Xj) = (Xp, Xj)^d + C$$

(iii) Sigmoid Kernel Function: Sigmoid Kernel is also called as Hyperbolic Tangent Kernel and the Multilayer Perceptron (MLP) kernel. The Sigmoid Kernel arrives from the Neural Networks field, where the bipolar sigmoid function is frequently used as an activation function for artificial neurons

$$K(Xi, Xj) = \tanh\{k(Xi, Xj) + r$$

3.4 Genetic Algorithm

Genetic algorithms [21] are employed as chromosome-like data structures. Figure 3 adopted from represent the structure and processing in a genetic algorithm. A genetic algorithm has various parameters, operators and processes which decide its arrival to an optimal solution. A short description of the parameters, operators and processes as depicted in figure 3, is as: Fitness Function: The fitness function is the measure of the superiority of a meticulous solution. The fitness function is used to conclude the mainly optimal solution from a number of solutions in a population. Selection: This process in genetic algorithms is used to opt for the most optimal solution determined by using the fitness function. The solutions which are not most favorable are discarded. Crossover: The crossover procedure in genetic algorithms is used to substitute characteristics among two dissimilar solutions. The pairs of solutions to swap characteristics are selected randomly and remain exchanging characteristics, until a completely new generation of solutions is obtained. Mutation: The mutation process in genetic algorithms transforms some random bits in a solution. The modification in the bits results in the genetic diversity of the mutated algorithms.

3.5 Bayesian-network

Reverend Thomas Bayes prepared with his work the research on the basis of cause-consequence relationships. The most significant fruit of that investigation, known as the “Bayes' theorem” [22] in his nobility, is the basis of the so-called Bayesian inference, the statistical inference system that authorizes, upon a number of clarifications, to attain or revise (if the system is previously working) the probability that a hypothesis may be true. In this manner, Bayes' theorem regulates the probabilities as novel information on evidences materializes. According to its conventional formulation, given two events A and B, the conditional probability P(A|B) that A occurs if B occurs can be obtained if we know the probability that A occurs, P(A), the probability that B occurs, P(B), and the conditional probability of B given A, P(B|A)):

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \qquad (1)$$

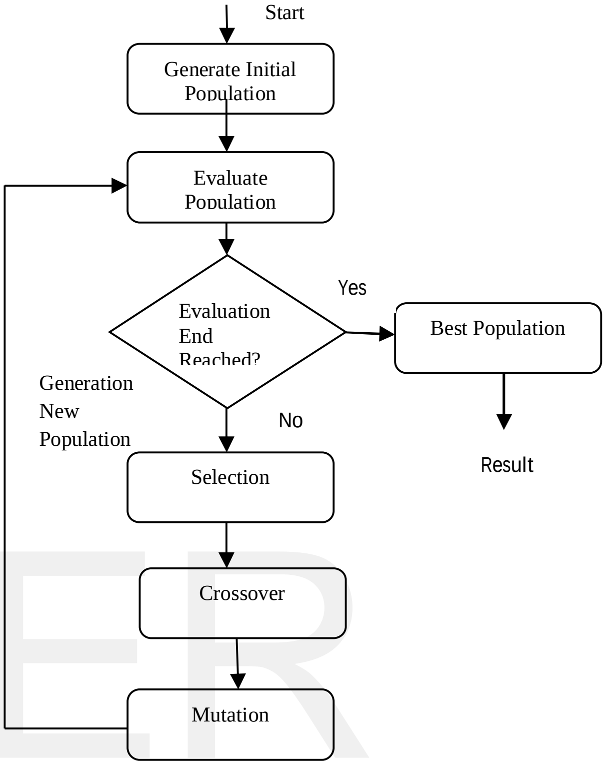


Fig. 3Structure of Genetic Algorithm

More precisely, Bayesian Networks are defined as graphical probabilistic models for multivariate analysis. Particularly, they are directed acyclic graphs (DAG) that have an allied probability distribution function. Nodes inside the directed graph correspond to predicament variables (they can be either a premise or a conclusion) and the edges signify conditional dependencies among such variables. Furthermore, the probability function illustrates the potency of these relationships in the graph (Figure 4).

Formally, let a Bayesian Network B be defined as a couple, B = (D, P), where D is a directed acyclic graph and P = {p(x1 |Ψ2), ... p (xn|Ψn)} is the set composed of n conditional probability functions (one for every variable); and Ψi is the set of parent nodes of the node Xi in D. The set P is defined as the joint probability density function:

$$P(x) = n \prod i=1 p(xi |\Psi i)$$

The most significant capability of Bayesian Networks is their capability to conclude the probability that a definite hypothesis is true (e.g: the probability of an e-mail to be spam or justifiable) given a chronological dataset.

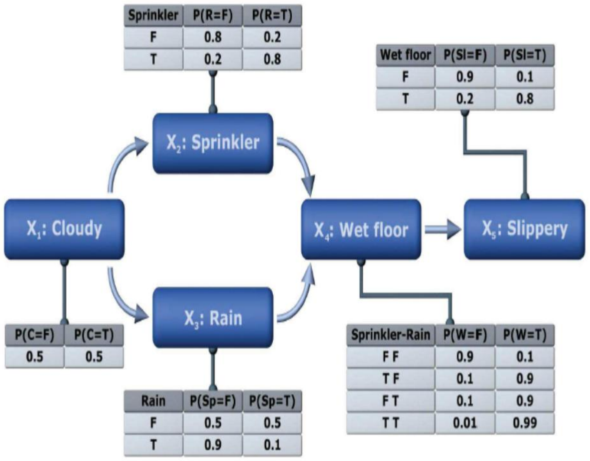


Fig. 4 Bayesian Network

3.6 Fuzzy Logic

Fuzzy Logic is derived from fuzzy set theory offering with reasoning that is fairly accurate rather than precise. They applied an enhanced algorithm of the fuzzy data mining methods to the IDS. The fuzzy data mining method is used to extort the patterns that correspond to normal behaviour for intrusion detection. They attempted classification of the data using Fuzzy logic rules [23]. Typically, an IDS uses Boolean logic in determining whether or not an intrusion is detected and the use of fuzzy logic has been investigated as an alternate to Boolean logic in the design and implementation of these systems. Fuzzy logic centered on the formal principles of fairly accurate reasoning. It presents a sound foundation to grip the mechanisms using varying degrees of truth. As boundaries are not always obviously defined, fuzzy logic can be used to recognize complex pattern or behavior variations. This is done by building an Intrusion Detection System that coalesces fuzzy logic rules with an expert system in charge of evaluating rule truthfulness. Fuzzy logic is important for the intrusion detection difficulty for two key reasons. Foremost, many quantitative features are involved in intrusion detection. Security-related data classifies the statistical measurements into four types: ordinal, categorical, binary categorical and linear categorical. Both ordinal and linear categorical measurements are quantitative features that can potentially be viewed as fuzzy variables. Two examples of ordinal measurements are the CPU usage time and the connection period. An example of a linear categorical measurement is the number of different TCP/UDP services initiated by the same source host. The second motivation for using fuzzy logic to address the intrusion detection problem is that security itself includes fuzziness. Given a quantitative measurement, an interval can be used to designate a normal value. Then, any values falling outside the interval will be considered anomalous to the same degree regardless of their distance to the interval. The similar applies to values inside the interval, i.e., all will be viewed as normal to the similar degree. The use of fuzziness in representing these quantitative features helps to smooth the unexpected separation of normality and abnormality.

Above methodology has there some merits and demerits which we are describing in table 2.

Table 2: Merits & Demerits of IDS Methodology

Methods	Merits	Demerits
Radial Basis Function (RBF)	-It has better ability in intrusion detection -Low false alarm rate	-It include high rates of incorrectness of detection intrusion
Principle Component Analysis (PCA)	-high detection rate as compare to other -minimum learning time	-High false alarm rate
Support Vector Machine (SVM)	- Low expected probability of generalization errors. -Able to detect previous unseen attack	-It requires extensive training time -High algorithmic complexity -require much memory
Genetic Algorithm (GA)	-The detection rate can be high - False alarm can be low if the fitness function is well designed	- it cannot locate the attack in audit trails - it cannot detect novel attacks as it requires more domain specific knowledge - no ability to detect multiple Simultaneous and its is complex to design.
Bayesian Network	-It readily handles incomplete data sets - Better accuracy and less false alarm rate	-It is difficult to design - time consuming
Fuzzy Logic	-false alarm rate in determining intrusive activities can be minimized. -It includes Simplicity and Flexibility	-It cannot detect novel attack -High False Positive rate To make good fuzzy classifiers to detect intrusions

4 Conclusion

Intrusion detection is a serious issue in the network technology and lots of work has been done for conforming the security. The classification of data performs by the system using misuse detection or anomaly detection. But it is not necessary that system is much efficient in classification of attack. Many data mining and soft computing techniques also proposed or applied for intrusion detection such as SVM, PCA, and RBF etc. In this research paper, literature study of different intrusion detection techniques is described with their merits and demerits. Some provides low false alarm rate or able to detect known or unknown attack and some are difficult to design. So in future, develop such system which must be more efficient than existing techniques.

5 References

[1]. R. Heady, G. Luger, A. Maccabe, and M. Servilla. The Architecture of a Network level Intrusion Detection System. Technical report, Department of Computer Science, University of New Mexico, August 1990.

[2]. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, ―Network Anomaly Detection: Methods, Systems and Tools,‖ Communications Surveys & Tutorials, IEEE press, vol. 16, no. 1, pp. 303 – 336, 2013.

[3]. M. Panda and M. R. Patra, "Ensembling Rule Based Classifiers for Detecting Network Intrusions", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, (2009), pp. 19-22.

[4]. Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", In Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009).

[5]. Vinod Rampure and Akhilesh Tiwari "A Rough Set Based Feature Selection on KDD CUP 99 Data Set", International Journal of Database Theory and Application Vol.8, No.1 (2015), pp.149-156.

[6]. Jaina Patel, Mr. Krunal Panchal "Effective Intrusion Detection System using Data Mining Technique", Journal of Emerging Technologies and Innovative Research (JETIR) June 2015, Volume 2, Issue 6, ISSN-2349-5162.

[7]. Phyu Thi Htun, Kyaw Thet Khaing "Anomaly Intrusion Detection System using Random Forests and k-Nearest Neighbor", International journal of Seventh Sense Research Group, ISSN: 2249-2615 pp: 67-71.

[8]. Shi-Jinn Horng , Ming-Yang Su , Yuan-Hsin Chen , Tzong-Wann Kao , Rong-Jian Chen , Jui-Lin Lai , Citra Dwi Perkasa ," A novel intrusion detection system based on hierarchical clustering and support vector machines ",Expert Systems with Applications 38 (2011) 306–313.

[9]. Mrutyunjaya Panda and Manas Ranjan Patra "Network Intrusion Detection Using Naïve Bayes", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007.

[10]. Bharat Rathi, Dattatray V. Jadhav "Network Intrusion Detection Using PSO Based on Adaptive Mutation and Genetic Algorithm", International Journal of Scientific & Engineering Research, Volume 5, Issue 8, August -2014, ISSN 2229 5518.

[11]. Harshit Saxena, Vineet Richaariya, "Intrusion Detection in KDD99 Dataset using SVM-PSO and Feature Reduction with Information Gain", International Journal of Computer Applications (0975 – 8887) Volume 98– No.6, July 2014.

[12]. Nupur N. Majethiya and Dipak C. Patel, "Efficient Intrusion Detection System with Reduced Dimensionality", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 4, Issue 2, March-April 2015 ISSN 2278-6856.

[13]. Abebe Tesfahun, D. Lalitha Bhaskari "Effective Hybrid Intrusion Detection System: A Layered Approach", I. J. Computer Network and Information Security, 2015, 3, 35-41.

[14]. Sunil Choudhary and Pankaj Dalal, "An Architecture for Network Intrusion Detection System based on DAG Classification", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2015.

[15]. Venkata Suneetha Takkellapati et.al "Network Intrusion Detection system based on Feature Selection and Triangle area Support Vector Machine" International Journal of Engineering Trends and Technology- Volume 3 Issue 4- 2012.

[16]. J. Mark and L. Orr, "Introduction to Radial Basis Function Networks", Technical Report, April 1996.

[17]. Z. Caiqing, Q. Ruonan, and Q. Zhiwen, "Comparing BP and RBF Neural Network for Forecasting the Resident Consumer Level by MATLAB," International Conference on Computer and Electrical Engineering, 2008 (ICCEE 2008), 20-22 Dec. 2008, pp.169-172.

[18]. A. Iseri and B. Karlık, "An Artificial Neural Networks Approach on Automobile Pricing", Expert Systems with Applications, Vol. 36 (2), March 2010, pp. 2155-2160.

[19]. Nethu B, Adaptive Intrusion detection Using Machine Learning, International Journal of Computer Science and Network Security, Vol.13 No.3, March 2013.

[20]. Yogita B. Bhavsar and Kalyani C.Waghmare, " Intrusion Detection System Using Data Mining Technique: Support Vector Machine", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459,

ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013).

[21]. Parry Gowher Majeed and Santosh Kumar” Genetic Algorithms in Intrusion Detection Systems: A Survey”, International Journal of Innovation and Applied Studies, ISSN 2028-9324 Vol. 5 No. 3 Mar. 2014, pp. 233-240

[22]. Pablo G. Bringas and Igor Santos, “Bayesian Networks for Network Intrusion Detection” in publisher of InTech. Open Scinece.

[23]. Harshna, Navneet Kaur “Fuzzy Data Mining Based Intrusion Detection System Using Genetic Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014, ISSN (Print) : 2319-5940.