International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

DETECTION OF ACCURACY FOR INTRUSION DETECTION SYSTEM USING NEURAL NETWORK CLASSIFIER

S. Devaraju[1], S. Ramakrishnan[2]
[1]*Dept. of Computer Applications, Dr.Mahalingam College of Engineering and Technology, Pollachi-3, Tamil Nadu, India*
[2]*Dept. of Information Technology, Dr.Mahalingam College of Engineering and Technology, Pollachi-3, Tamil Nadu, India*
Email: deva_sel@yahoo.com

Abstract

In recent years, the security has become a critical part of any industrial and organizational information systems. The intrusion detection system is an effective approach to deal with the problems of networks and so different classifiers are used to detect the different kinds of attacks. In this paper, the performance of intrusion detection with various neural network classifiers is compared. In this proposed research there are five types of classifiers used. They are Feed Forward Neural Network (FFNN), Elman Neural Network (ENN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN). In this problem, the feature reduction techniques are used to a given KDD Cup 1999 dataset. The performance of the full featured KDD Cup 1999 dataset is compared with that of the reduced featured KDD Cup 1999 dataset. The MATLAB software is used to train and test the dataset and the efficiency is measured. Using the above said technique, it is proved that the reduced dataset is performing better than the full featured dataset.

Keywords **- Intrusion detection, Neural networks, FFNN, ENN, GRNN, PNN, RBNN, KDD Cup, MATLAB.**

I. INTRODUCTION

In the past years, there were few intruders and so the user can manage them easily from the known or unknown attacks. In recent years the security is the most serious problem in issues of securing data or information. Because the intruders introduce a new variety of intrusion in the market, so that the user can't manage his computer system or network.

Intrusion detection attacks can be classified into two groups: Misuse or Signature based and Anomaly based. The misuse or signature based intrusion detection system detects the intrusion by comparing their parameters with its existing signature in the database. If the detecting attacks and signatures are matching, it's an intrusion. The signature based intrusions are called known attacks because the users are detecting the intrusion by matching with the signatures log files. The log file contains the list of known attacks detecting from the computer system or networks. The anomaly based intrusion detection is called as unknown attacks and this attack is observed from the network as it deviates from the normal attacks.

The intrusion detection systems are classified as Network based or Host based attacks. The network based attack may be either misuse or anomaly based attacks. The network based attacks are detected from the interconnection of computer systems.

Whenever the system is communicates with each other, the attack is sent from one computer system to another computer system by the way of routers and switches. The host based attacks are detected only from a single computer system and is easy to prevent the attacks. These attacks mainly occur from some external devices which are connected. The external devices are pen drive, CD, VCD, Floppy etc. The web based attacks are possible when systems are connected over the internet and the attacks can be spread into different systems through the email, chatting, downloading the materials etc. Nowadays many computer systems are affected by web based dangerous attacks.

In this system, it is proposed to detect the signature based intrusion using neural network classifier Feed Forward Neural Network (FFNN), Elman Neural Network (ENN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN). The various techniques are applied to solve this problem using MATLAB application for improving the performance applied to KDD Cup 1999 dataset. The performance of the full featured dataset is compared with the reduced dataset and analyzed. The Figure 1 shows the classification of proposed systems:

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

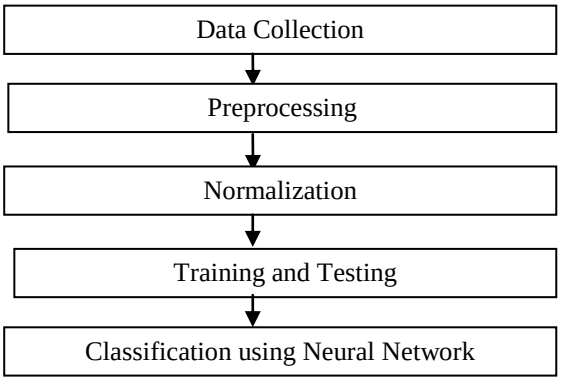

Fig. 1: Classification of Intrusion Detection

The remaining part of this paper is given as follows: In Section 2 the related work used for intrusion detection. Section 3, discusses Feed Forward Neural Network, Section 4, discusses Elman Neural Network, Section 5 discusses Generalized Regression Neural Network, Section 6, discusses Probabilistic Neural Network and Section 7, discusses Radial Basis Neural Network, Section 8, describes about the KDD Cup dataset Description. Section 9, gives our experimental results and discussion and Section 10 deals with conclusion.

II. Related Work

The field of intrusion detection system in network security has been developed for 30 years. A number of methods and techniques have been proposed and many systems have been affected by variety of intrusions. The various techniques used to detect the intrusions are data mining, neural network, and statistical methods. In this related work, the various methods and techniques are discussed.

The Multivariate Statistical Analysis methods are used to determine the anomaly detection. The statistical methods are used to compare the performance of the system [3]. The Hidden Markov Model is used to implement and determine the system call based anomaly intrusion detection [4][9]. Conditional Random Fields and Layered Approach are addressed by the two issues of Accuracy and Efficiency. This approach demonstrates the high attack detection accuracy and high efficiency using Conditional Random Fields and Layered Approach. This approach uses KDD cup '99 intrusion detection data set for detecting the attacks [5].

Anomaly detection and analysis is based on the methods which can describe the normal and abnormal traffic and accurately detect and classify various anomaly behaviors (network scanning and DDoS attacks) in network traffic using analysis method based on Correlation Coefficient Matrix [14].

The data mining techniques like decision trees are used to detecting the attacks. The KDD 99 dataset is used for training and testing the data. This model shows improvement in detecting new types of anomaly detection [11].

The Hierarchical Gaussian Mixture Model detects network based attacks as anomalies using statistical classification techniques. This model is evaluated by well known KDD99 dataset. There are six classification techniques used to verify the feasibility and effectiveness. This technique is used to reduce the missing alarm and accuracy of the attack in Intrusion Detection System [8].

The Genetic Algorithm is used to detect the intrusions in networks. It considers both temporal and spatial information of network connections during the encoding of the problem using Genetic Algorithm. The Genetic Algorithm is more helpful its identification of network anomalous behaviors [12][10]. The Rough Set Neural Network Algorithm is used to reduce a number of computer resources required to detect an attack. The KDDCup'99 dataset is used to test the data and to give better and robust result [6]. The various feature reduction techniques such as Independent Component Analysis, Linear Discriminant Analysis and Principal Component Analysis are used to reduce the computational intensity. KDD cup 99 dataset is used to reduce computation time and improve the accuracy of the systems [7].

III. Feed Forward Neural Network (FFNN)

The FFNN allows signals to travel only from input to output. The FFNN tends to be straight forward networks that associate inputs with outputs. They are extensively used in pattern recognition. The FFNN are classified into Single- layer FFNN and Multi-layer FFNN.

The single-layer neural network is the first and the simplest learning machine. The single layer is used to have only two layers such as input layer and output layer. Multi-layer feed forward networks have three layers such as input layer, hidden layer and output layers.

There are two types of phases used in multi layer FFNN, the Forward Phase is used to fix the free parameter in the network and finishes with the computation of an error signal

$$e_i = d_i - y_i \qquad (1)$$

Where d_i is the desired response and y_i is the actual output produced by the network in response to the input. In the Backward Phase, the error signal e_i is propagated through the network. During this phase adjustments are applied to the free parameters of the network so as to minimize the error e_i in a statistical sense.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

IV. Elman Neural Network (ENN)

Elman networks are feedforward networks with the addition of layer recurrent connections with tap delays. A three-layer network is used, with the addition of a set of "context units" in the input layer. There are connections from the hidden layer to these context units fixed with a weight. At each step, the input is propagated in a standard feed-forward fashion, and then a learning rule is applied. The fixed back connections result in the context units always maintaining a copy of the previous values of the hidden units, since they propagate over the connections before the learning rule is applied. Thus the network can maintain a sort of state, allowing it to perform such tasks as sequence-prediction that is beyond the power of a standard multilayer perceptron.

Both the input units and context units activate the hidden units; and then the hidden units feed forward to activate the output units. The hidden units also feed back to activate the context units. This constitutes the forward activation. Depending on the task, there may or may not be a learning phase in this time cycle. If so, the output is compared with a teacher input and backpropagation of error is used to incrementally adjust connection strengths. Recurrent connections are fixed at 1.0 and are not subject to adjustment. At the next step t+1 the above sequence is repeated. This time the context units contain values which are exactly the hidden unit values at time t.

When using the function train to train an Elman network the following occurs.

At each epoch:

1. The entire input sequence is presented to the network and its outputs are calculated and compared with the target sequence to generate an error sequence.
2. For each step, the error is backpropagated to find gradients of errors for each weight and bias. This gradient is actually an approximation since the contributions of weights and biases to errors via the delayed recurrent connection are ignored.
3. This gradient is then used to update the weights with the backprop training function chosen by the user. The function traingdx is recommended.

V. Generalized Regression Neural Network (GRNN)

The General Regression Neural Networks perform regression where the target variable is continuous. If you select a GRNN network, DTREG will automatically select the correct type of network based on the type of target variable.

DTREG also provides Multilayer Perceptron Neural Networks and Cascade Correlation Neural Networks.

GRNN networks have advantages and disadvantages compared to Multilayer Perceptron networks:

- It is usually much faster to train a GRNN network than a multilayer perceptron network.
- GRNN networks often are more accurate than multilayer perceptron networks.
- GRNN networks are relatively insensitive to outliers.
- GRNN networks are slower than multilayer perceptron networks at classifying new cases.
- GRNN networks require more memory space to store the model.

GRNN networks have four layers:

1. Input layer — There is one neuron in the input layer for each predictor variable. In the case of categorical variables, N-1 neurons are used where N is the number of categories. The input neurons then feed the values to each of the neurons in the hidden layer.
2. Hidden layer — There is one neuron for each case in the training data set. The neuron stores the values of the predictor variables for the case along with the target value. The resulting value is passed to the neurons in the pattern layer.
3. Pattern layer / Summation layer —There are only two neurons in the pattern layer. One neuron is the denominator summation unit the other is the numerator summation unit. The denominator summation unit adds up the weight values coming from each of the hidden neurons. The numerator summation unit adds up the weight values multiplied by the actual target value for each hidden neuron.
4. Decision layer — The decision layer divides the value accumulated in the numerator summation unit by the value in the denominator summation unit and uses the result as the predicted target value.

VI. Probabilistic Neural Network (PNN)

The PNN is a direct continuation of the work on Bayes classifiers. More precisely, the PNN is interpreted as a function which approximates the probability density of the distribution. The PNN consists of nodes allocated in three layers after the input layers such as pattern layer, summation layer and output layer.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

A. Pattern Layer: It is one pattern node for each training phase. Each pattern node forms a product of the weight vector and for classification, where the weights entering a node are from a particular node. After that, the product is passed through the activation function:

$$\exp\left[\left(\mathbf{x}^{\mathrm{T}} \mathbf{w}_{ki} - 1 \right) / \sigma^2 \right] \qquad (2)$$

B. Summation Layer: Each summation node receives the outputs from pattern nodes associated with a given class:

$$\Sigma_{i=1}^{Nk} \exp\left[\left(\mathbf{x}^{\mathrm{T}} \mathbf{w}_{ki} - 1 \right) / \sigma^2 \right] \qquad (3)$$

C. Output Layer: The output nodes are binary neurons that produce the classification decision

$$\Sigma_{i=1}^{Nk} \exp\left[\left(\mathbf{x}^{\mathrm{T}} \mathbf{w}_{ki} - 1 \right) / \sigma^2 \right] > \Sigma_{i=1}^{Nj} \exp\left[\left(\mathbf{x}^{\mathrm{T}} \mathbf{w}_{kj} - 1 \right) / \sigma^2 \right] \qquad (4)$$

The only factor that needs to be selected for training is the smoothing factor that is the deviation of the Gaussian functions:

- too small deviations cause a very spiky approximation which can not generalize well;
- too large deviations smooth out details.

An appropriate deviation is chosen by experiment.

VII. Radial Basis Neural Network (RBNN)

A Radial Basis Neural Network (RBNN) has an input layer, a hidden layer and an output layer. The neurons in the hidden layer contain Gaussian transfer functions whose outputs are inversely proportional to the distance from the center of the neuron. The structure is shown in Figure 2. The RBNN is viewed as a curve-fitting problem in high-dimensional space. RBF networks have three layers; Input layer, Hidden layer and Summation layer.

The RBF is applied to the distance to compute the weight (influence) for each neuron.

Weight = RBF(*distance*)

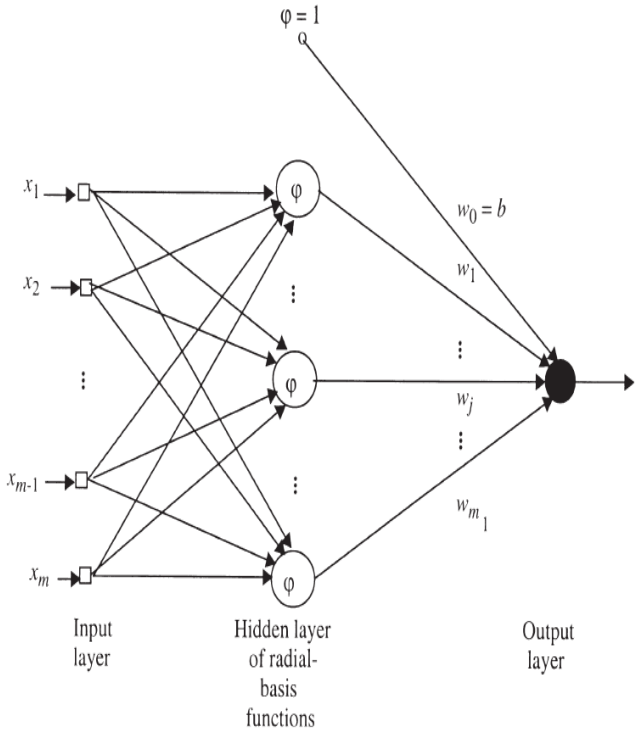

Fig. 2: Radial-basis Neural Network

The following parameters are determined by the training process:

1. The number of neurons in the hidden layer.
2. The coordinates of the center of each hidden-layer RBF function.
3. The radius (spread) of each RBF function in each dimension.
4. The weights applied to the RBF function outputs as they are passed to the summation layer.

The RBF methods have been used to train the networks. There are two types of approaches, they are K-means clustering used to find cluster centers which are then used as the centers for the RBF functions and a random subset of the training points as the centers.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

VIII. KDD CUP 1999 DATASET DESCRIPTION

The KDD Cup 1999 dataset has been used for the evaluation of anomaly detection methods. The KDD Cup 1999 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. The simulated attacks fall in one of the following four categories:

The datasets contain a total number of 24 training attack types, with an additional 14 types in the test data only.

8.1 Data Collection

KDD Cup 1999 dataset has the different types of attacks: back, buffer_overflow, ftp_write, guess_passwd, imap, ipsweep, land, loadmodule, multihop, neptune, nmap, normal, perl, phf, pod, portsweep, rootkit, satan, smurf, spy, teardrop, warezclient, warezmaster. These attacks can be divided into 4 groups [13].

The Table 1 shown the list of attacks in category wise:

Table 1
List of attacks - category wise

DoS	R2L	U2R	Probe
back	ftp_write	buffer_overflow	ipsweep
land	guess_passwd	loadmodule	nmap
neptune	imap	perl	portsweep
pod	multihop	rootkit	satan
smurf	phf		
teardrop	spy		
	warezclient		
	warezmaster		

Denial of Service (DoS) attacks: deny legitimate requests to a system, e.g. flood, User-to-Root (U2R) attacks: unauthorized access to local super user(root) privileges, e.g. various buffer overflow attacks, Remote-to-Local (R2L) attacks: unauthorized access from a remote machine, e.g. guessing password, and Probing: surveillance and other probing, e.g. port scanning [7].

The sets are named as A, B, C, D, and E respectively. The set 'A' acquires data from DoS class. The set 'B' acquires data from U2R class. The set 'C' acquires data from R2L class. The set 'D' acquires data from Probe Class. The set 'E' acquires data from Normal class. The following sets of data can be used for training and testing the data from KDD Cup 1999 dataset.

Table 2
Training and Testing Data Set

	Training Set	Testing Set
DoS	300	300
U2R	20	19
R2L	300	300
Probe	300	300
Normal	300	300
Total	**1220**	**1219**

The 41 features dataset and 13 features dataset is used to detect the attacks in KDD Cup 1999 dataset. The 41 features are listed in the website [1].

8.2 Preprocessing

The input data to the neural network must be in the range [0 1] or [-1 1]. Hence preprocessing and normalization data is required. The KDD Cup 1999 format data is preprocessed. Each record in KDD Cup 1999 format has 41 features, each of which is one of the continuous, discrete and symbolic form, with significantly varying ranges.

For converting symbols into numerical form, an integer code is assigned to each symbol. For instance, in the case of protocol_type feature, 0 is assigned to tcp, 1 to udp, and 2 to the icmp symbol and so on. Attack names are first mapped to one of the five classes, 'A' for DoS, 'B' for U2R, 'C' for R2L, 'D' for Probe and 'E' for Normal. Two features span over a very large integer range, namely src_bytes [0, 1.3 billion] and dst_bytes [0, 1.3 billion]. Logarithmic scaling (with base 10) is applied to these features to reduce the range to [0.0, 9.14]. All other features are Boolean, in the range [0.0, 1.0]. Hence scaling is not necessary for these attributes.

8.3 Normalization

For normalizing feature values, a statistical analysis is performed on the values of each feature based on the existing data from KDD Cup 1999 dataset and then acceptable maximum value for each feature is determined. According to the maximum values and the following simple formula, normalization of feature values in the range [0,1] is calculated.

If (f > MaxF) Nf=1; Otherwise Nf = (f / MaxF)
F: Feature f: Feature value
MaxF: Maximum acceptable value for F
Nf: Normalized or scaled value of F

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

8.4 Training and Testing

8.4.1 Training

300 signals from DoS, R2L, Probe and Normal class each and 20 signals from U2R class are selected for training the network. Three different neural networks are used for training the KDD Cup 1999 data. The networks are usually trained to perform tasks such as pattern recognition and decision-making. The table 2 represents the training set.

8.4.2 Testing

300 signals from DoS, R2L, Probe and Normal class each and 19 signals from U2R class are selected for testing the network. Five different neural networks are used for testing the KDD Cup 1999 data. By testing the KDD Cup 1999 data, the accuracy of the each neural networks are measured. The table 2 represents the testing set.

IX. Results And Discussion

The Intrusion Detection techniques are used to detect the intrusions based on the KDD Cup 1999 dataset. These dataset contains 41 features in various types of attacks. By reducing 41 features into 13 features the accuracy has improved by 96.23% using the Probabilistic Neural Network. These Dataset can be applied using MATLAB software and comparing these five Neural Network classifiers, the Probabilistic Neural Network proves the best accuracy [2].

9.1 Total 41 Features Dataset

The following table contains the five types of classes, five types of neural network classifiers used and the efficiency is measured. The Table 3 shows the classification of 41 featured dataset.

Table 3
Results for 41 Features Dataset

Classes/ Networks	DoS (300)	U2R (20)	R2L (300)	Probe (300)	Normal (300)	Efficiency (%)
FFNN	300	3	298	80	288	79.49
ENN	300	7	295	62	288	78.1
GRNN	294	2	38	97	285	58.74
PNN	300	3	300	300	140	85.56
RBNN	292	0	298	183	245	83.51

Based on these results, the pictorial representation is given below in chart. The figure 3 shows that the result for 41 features

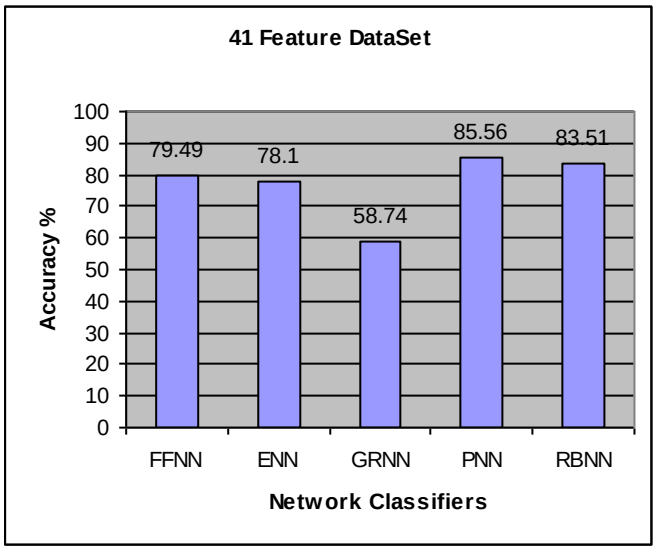

Fig. 3: Percentage of accuracy analysis for 41 features

Here the classification of KDD Cup '99 data set has been performed using 41 features dataset. The percentage of accuracy for five neural networks is listed in table 3. Here accuracy of feed forward neural networks is 79.49%; accuracy of elman neural network is 78.1%; accuracy of generalized regression neural network is 58.74%; accuracy of Probabilistic neural networks is 85.56% and accuracy of radial basic network is 83.51%.

9.2 Total 13 Features Dataset

Principal Component Analysis is one of the most widely used dimensionality reduction techniques for data analysis and compression. Because patterns can be hard to find in data of high dimensions, PCA is a powerful analysis tool. Once patterns in the data are found, the data can be compressed reducing the number of dimensions without a significant loss of information [6].

Given the data, if each datum has N features represented for instance by $x_{11}\ x_{12}\ \ldots\ x_{1N},\ x_{21}\ x_{22}\ldots x_{2N}$, the data set can be represented by a matrix $X_{n\times m}$.

The average observation is defined as

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (5)$$

The deviation from the average is defined as

$$\Phi_i = X_i - \mu \qquad (6)$$

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

Best 13 features selected after principal component analysis, the table 4 shows the classification of 13 featured dataset [13].

Table 4
Reduced 13 Features Dataset for Classification

Reduced 13 Features Dataset
0- duration -Continuous
1- flag -Symbolic
2- src_bytes- Continuous
3- dst_bytes- Continuous
4- land- Symbolic
5- wrong_fragment- Continuous
6- urgent- Continuous
7- num_failed_logins- Continuous
8- logged_in- Continuous
9- dst_host_serror_rate- Continuous
10- dst_host_srv_serror_rate- Continuous
11- dst_host_rerror_rate- Continuous
12- dst_host_srv_rerror_rate- Continuous

After selecting 13 features, the reduced dataset for classifying the neural networks is used. The Table 5 shows the classification of 13 featured dataset.

Table 5
Results for 13 Features Dataset

Classes/ Networks	DoS (300)	U2R (20)	R2L (300)	Probe (300)	Normal (300)	Efficiency (%)
FFNN	300	7	300	90	286	80.64
ENN	300	3	298	99	292	81.38
GRNN	292	1	300	300	269	95.32
PNN	300	1	300	300	272	96.23
RBNN	290	1	300	6	289	72.68

Based on these results, the pictorial representation is given below in chart. The figure 4 shows the result for 13 features.

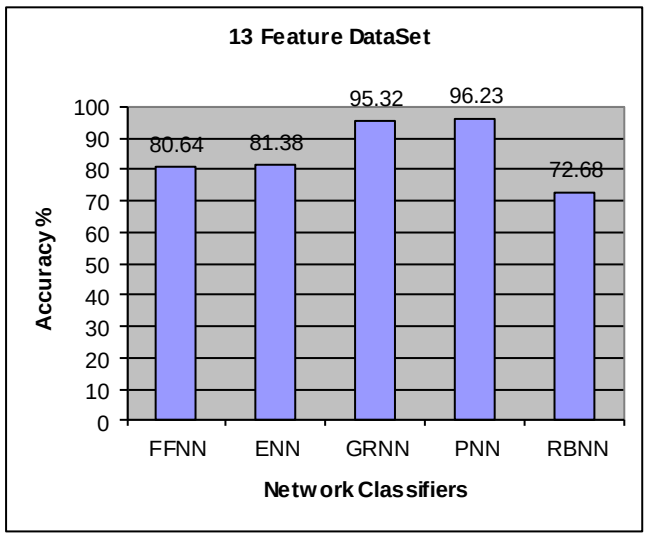

Fig. 4: Percentage of accuracy analysis for 13 features

Here the classification of KDD Cup 1999 dataset has been performed. The percentage of accuracy of five neural networks is listed in table 5. Here accuracy of feed forward neural networks is 80.64%; accuracy of elman neural network is 81.38%; accuracy of generalized regression neural network is 95.32%; accuracy of Probabilistic neural networks is 96.23% and accuracy of radial basic network is 72.68%.

X. CONCLUSION

A novel approach for detecting network intrusions using five classifiers are proposed in this paper. This study proves that the Probabilistic Neural Networks provides better accuracy over Feed Forward Neural Network, Elman Neural Network, Generalized Regression Neural Network and Radial Basis Neural Network. To enhance the results the feature reduction techniques is applied. The Principal Component Analysis is applied to the KDD CUP 1999 dataset to reduce its features and implemented using MATLAB software. PCA selects 13 features from 41 feature data set. The reduced features are used as input to different classifiers and the results are compared.

The results show the efficiency with 13 features compared to the 41 features, with reduced training and testing times. Comparing these five classifiers PNN gives better efficiency than FFNN, ENN, GRNN and RBN. The KDD Cup 1999 reduced dataset obtained with PCA shows promising results. Hence, it is proposed to consider feature reduction techniques to improve the efficiency and reduce the false alarm rate for our further research.

REFERENCES

Generic Website

[1] KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 2010.

[2] MATLAB (MATrix Laboratory) tutorials, http://terpconnect.umd.edu/~nsw/ench250/matlab.htm

Journal Papers

[3] Nong Ye, Syed Masum Emran, Qiang Chen, Sean vilbert, Multivariate Statistical Analysis of audit Trails for Host-Based Intrusion Detection, IEEE Transactions on Computers, vol.51, no.7, pp. 810-820, July 2002.

[4] Jiankun Hu, Xinghuo Yu, D. Qiu, Hsiao-Hwa Chen, A simple and efficient hidden Markov model scheme for host- based anomaly intrusion detection, Journal IEEE Network, vol. 23 iss. 1, January/February 2009.

[5] Gupta, K.K.,Nath, B.,Kotagiri, R., Layered Approach Using Conditional Random Fields for Intrusion Detection, IEEE Transactions on Dependable and Secure Computing, vol.7, iss.1, pp.35-49, Jan.-March 2010.

[6] Neveen I. Ghali, Feature Selection for Effective Anomaly-Based Intrusion Detection, IJCSNS International Journal of Computer Science and Network Security, vol.9 no.3, pp.285-289, March 2009.

[7] V.Venkatachalam and S.Selvan, Intrusion detection using an improved competitive learning lamstar neural network, IJCSNS International Journal of Computer Science and Network Security, vol.7 no.2, February 2007.

[8] Suseela T. Sarasamma, Qiuming A. Zhu, and Julie Huff, Hierarchical Kohonenen Net for Anomaly Detection in Network Security, IEEE Transactions on Systems, Man, and Cybernetics, vol. 35, no. 2, pp. 302-312, APRIL 2005.

[9] Yi Xie, Shun-Zheng Yu, A Large Scale Hidden Semi-Markov model for Anomaly Detection on User Browsing Behaviors, IEEE/ACM Transactions on Networking, vol 17, issue 1, pp. 1 – 14, February 2009.

[10] Hua Jiang, Junhu Ruan, The Application of Genetic Neural Network in Network Intrusion Detection, JOURNAL OF COMPUTERS, vol. 4, no. 12, pp. 1223 – 1230, December 2009.

[11] E. Anbalagan, C. Puttamadappa, E. Mohan, B. Jayaraman and Srinivasarao Madane, Datamining and Intrusion Detection Using Back-Propagation Algorithm for Intrusion Detection, International Journal of Soft Computing, vol. 3, iss. 4, pp. 264-270, 2008.

Conference Proceedings

[12] Wei Li, Using Genetic Algorithm for network intrusion detection, In Proceedings of the United States Department of Energy Cyber Security Group 2004 Training Conference, 2004.

[13] Devaraju S., Ramakrishnan S., Performance Analysis of Intrusion Detection System Using Various Neural Network Classifiers, IEEE Proceedings of the International Conference on International Conference on Recent Trends in Information Technology (ICRTIT 2011), 3-5, June 2011, Madras Institute of Technology, Anna University, Chennai, India.

[14] Ning Chen, Xiao-Su Chen, Bing Xiong, Hong-Wei Lu, An Anomaly Detection and Analysis Method for Network Traffic Based on Correlation Coefficient Matrix, IEEE International Conference on Scalable Computing and Communication; Eighth IEEE International Conference on Embedded Computing, pp. 238 – 244, 2009.