# *Performance Analysis of NSL-KDD dataset using ANN*

Bhupendra Ingre
Department of Electrical Engineering
National Institute of Technology, Raipur
Raipur, C.G., India
bhupendra.ingre@gmail.com

Anamika Yadav
Department of Electrical Engineering
National Institute of Technology, Raipur
Raipur, C.G., India
ayadav.ele@nitrr.ac.in

*Abstract* –**Anomalous traffic detection on internet is a major issue of security as per the growth of smart devices and this technology. Several attacks are affecting the systems and deteriorate its computing performance. Intrusion detection system is one of the techniques, which helps to determine the system security, by alarming when intrusion is detected. In this paper performance of NSL-KDD dataset is evaluated using ANN. The result obtained for both binary class as well as five class classification (type of attack). Results are analyzed based on various performance measures and better accuracy was found. The detection rate obtained is 81.2% and 79.9% for intrusion detection and attack type classification task respectively for NSL-KDD dataset. The performance of the proposed scheme has been compared with existing scheme and higher detection rate is achieved in both binary class as well as five class classification problems.**

***Keywords – Intrusion Detection System; NSL-KDD dataset; ANN; accuracy.***

## I. INTRODUCTION

With the rapid growth in the internet technologies and smart devices, the number of intrusions also increases. Intrusion is the act of intruding or of entering into a place or virtual place without proper permission [1] [2]. For System security and confidentiality intrusion detection plays an important role. Intrusion detection system is a tool to detect intrusion when the information or secret information exchange between user and server. So for improving the system security it is essential to detect novel attacks. Firewall is also used to stop bad in, bad out but Firewall hides major parts of the system from unwanted attention. Hackers can pass malicious traffic through ports that are commonly left open by system such as SMTP, HTTP etc. So the need for sophisticated IDS arises [2]. Based on the method of detection used IDSs can be classified as signature based or misuse based IDSs in which known attacks can be classified easily, it search network traffic for malicious packet. Other one is anomaly based IDSs in these IDS the learning process involved past behavior of user. Anomaly based IDSs helps to identify newly attacks. The IDS can further be classified as host based IDS and network based IDSs according to data they process.

## II. RELATED WORK

Several studies are carried out on Intrusion Detection System since last 26 year. It is one of the imperative research area where more than 300 papers already published. M.Tavallaee [3] surveyed on anomaly based intrusion detection and published his research work during the period of 2000-08. In his research paper [3] he had mentioned that, researchers either uses their self created dataset or they uses various publically available dataset such as DARPA data [4], KDD cup'99 [5] and NSL KDD [6] dataset to identify attack or normal based on their classification accuracy, false positive rate or detection rate. Some of the researcher uses feature selection and reduction to reduce the dimensionality of dataset and it also improves the performance.

Muhammad Imran et al. [7] applied Linear Discriminant Analyis (LDA) and Genetic Algorithm for feature selection and further implemented Radial Basis Function for feature classifier. He applied cross validation on 20% of NSL KDD training dataset for training and testing. Ibrahim et al. [8] applied SOM on KDD 99 and NSL dataset and show the better result of binary classification on KDD 99 dataset then that of NSL dataset. Bhoria et al. [9] uses cart 4.5 to detect DOS attack. She applied 6 fold cross validation on 20% NSL KDD dataset for training and testing. The dataset contains 22,495 records with normal and DOS attack. Bajaj et al. [10] applied information gain model for feature selection and then applied J48, Naïve Bayes, NB tree, SVM and simple cart methods for binary classification. R.Patil et al. [11] uses Adaboost machine learning on NSL KDD dataset. Bhuyan et al [12] discussed different methods of anomaly detection on his survey paper that are statistical, classification based, clustering and outlier based, soft computing, knowledge based and combination learners. These methods applied either on training and testing dataset or cross validation is used of test the intrusion system. But the Cross validation detect accuracy only for known attack.

## III. DATASET DISCRIPTION

Numbers of dataset used for IDS, some of them are self created dataset and some are publically available. Some publically available datasets are [3]:

- DARPA datasets (1998, 1999 and 2000) generated in MIT Lincon Laboratories. Dataset is generated by introducing manually generated network based attacks. The dataset is completed in 5 week and last two week data is used for testing purpose.
- The KDD 99 intrusion data is derived from DARPA 98 dataset. Dataset contain 41 features and one more attribute for class.
- NSL-KDD dataset is offline network data based on KDD 99 dataset [9].

The proposed methodology applied on NSL-KDD dataset which having 41 attribute and one class attribute. The size of NSL-KDD dataset is less than that of KDD99 which contain redundant records. The training set of NSL-KDD does not include redundant record and hence reduce the complexity level [6]. The various advantages of NSL-KDD data set over the original KDD dataset discussed by [6]. The training is performed on KDDTrain data which contain 22 attack types and testing is performed on KDDTest data which contains additional 17 attack type. These attacks can be categories in four different types with some common properties as shown in table I for training and testing. The four categories of attacks are:

- Denial of Service (DoS) – A malicious attempt to block system or network resources and services.
- Probe – This attack collects the information about potential vulnerabilities of the target system that can later be used to launch attacks on those systems.
- Remote to Local (R2L) – Unauthorized ability to dump data packets to remote system over network and gain access either as a user or root to do their unauthorized activity.
- User to Root (U2R) – In this, attackers access the system as a normal user and break the vulnerabilities to gain administrative privileges.

TABLE I. ATTACK CATEGORIZATION FOR TRAINING AND TESTING DATASETS

| DOS | Probe | R2L | U2R |
|---|---|---|---|
| **apache2** | ipsweep | *Spy* | bufferoverflow |
| back | **mscan** | *warezclient* | loadmodule |
| land | nmap | ftp_write | perl |
| **mailbomb** | portsweep | guesspasswd | **ps** |
| Neptune | **saint** | **httptunnel** | rootkit |
| pod | satan | imap | **snmpguess** |
| **processtable** | | multihop | **sqlattack** |
| smurf | | **named** | **worm** |
| teardrop | | phf | **xterm** |
| **udpstorm** | | **sendmail** | |
| | | **snmpgetattack** | |
| | | warezmaster | |
| | | **xlock** | |
| | | **xsnoop** | |

Table I shows the attacks in NSL-KDD test and train set, bold words in the table inferred that they are new attack introduces in test set and italic words of the table present in only training data set. Table II depicts the attack classes and number of patterns falls per class. Further NSL-KDD dataset has 125973 pattern in training and 22544 in the testing set. The Proposed model also check for these 17 unknown attacks of testing set which makes model more realistic.

TABLE II. NUMBER OF PATTERNS FALLS PER CLASS

| **Training data set** | | **Testing data set** | |
|---|---|---|---|
| **Class** | **Patterns** | **Class** | **Patterns** |
| Normal | 67343 | Normal | 9711 |
| DOS | 45927 | DOS | 7458 |
| Probe | 11656 | Probe | 2421 |
| R2L | 995 | R2L | 2754 |
| U2R | 52 | U2R | 200 |
| **Total** | **125973** | **Total** | **22544** |

## IV. PROPOSED METHOD

Artificial Neural Network (ANN) used for supervised classification learning. ANN is a computational model consists of a number of simple, highly interconnected neurons [13]. The step involve in ANN based IDS is shown in fig.1.

### *A. Dataset Selection*

Number of dataset available in NSL-KDD[6] dataset repository for training and testing, from those available dataset KDDTrain+.ARFF(dataset with binary labels) is used for training and KDDTest+.ARFF is used for testing the binary category problem. And for five category KDDTrain+.TXT and KDDTest+.TXT is used for training and testing dataset respectively. The test set included additional 17 attacks which are not in the train dataset.

### *B. Data Preprocessing*

NSL-KDD dataset contain numeric and some nonnumeric attribute. Non numeric attribute like protocol_type, service and flag attribute need to convert as numeric attribute because the training input and testing input is given to ANN should be numeric matrix. And the class attribute also labeled as numeric type, starts with normal which labeled as 1, DOS labeled as 2, probe labeled as 3, R2L labeled as 4 and U2R labeled as 5. These five attacks further processed and converted in bit form as 10000 if it is normal, 01000 if it is DOS, 00100 if it is probe, 00010 if it is R2L and 00001 if it is U2R attack, one bit per row. Here position of one, corresponds with row, denote the targeted class.

### *C. Feature Reduction*

The NSL-KDD data set has 41 attribute and one class attribute. From those 41 attribute some attribute have no role and some have minimum role in detection of attack. Bajaj et al. [10] uses information gain attribute evaluation, gain ratio attribute evaluation and correlation attribute evaluation algorithm. The researcher [10] shows that attribute 9, 20 and 21 have no role and attribute 15, 17, 19, 32, 40 have minimum role in detection of attack. Observation of NSL-KDD dataset shows that features 7,8,11 and 14 have almost all zero values in dataset. Removing these entire least usable features from

training and testing set of the dataset we left with 29 features, this reduces the size of the dataset. Now the reduced dataset is passed for training and testing. Training and testing also performed with 41 features, in this case feature reduction is not performed on dataset.

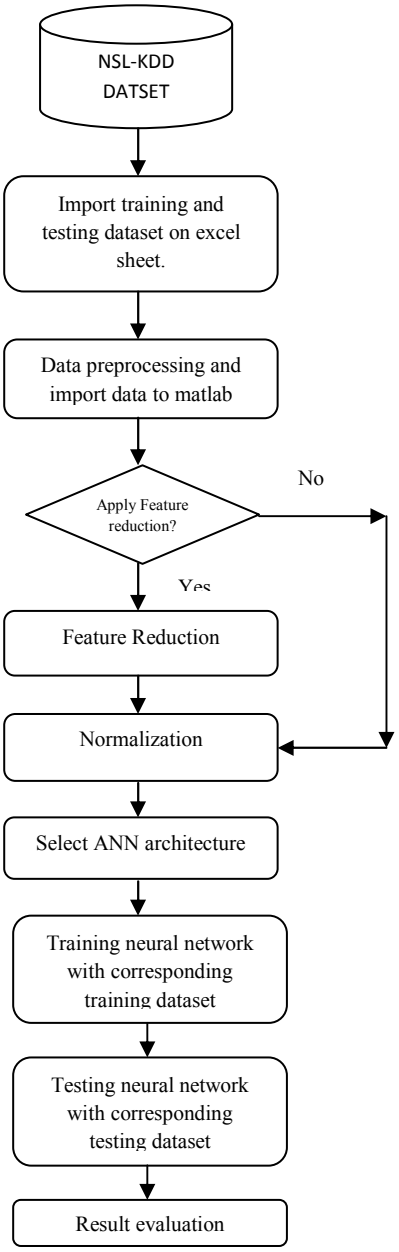


Figure 1. Flow chart of proposed IDS using ANN

### D. *Normalization*

Z-score normalization is used to normalize the attribute values. It normalizes the attribute value such that the mean and standard deviation after normalization become zero and one respectively. For this property of normalization z-score is also called as zero mean normalization. Its mathematical equation is given below.

$$a(i) = \frac{a(i) - \text{mean}(A)}{\text{std}(A)}$$

Here A is the attribute and a(i) is the $i^{th}$ value of A that is going to be updated by above equation.

### E. *Select Neural Network architecture*

There is some field in neural network which have to be selected before training process. These fields are number of neuron, number of layer in case of multilayer, algorithm and transfer function for training the neural network. Proposed method uses tansig transfer function, Levenberg-Marquardt (LM) and BFGS quasi-Newton Backpropagation (BFG) algorithm for updating weight and bias. And the learning is performed by changing the values of neuron and layers.

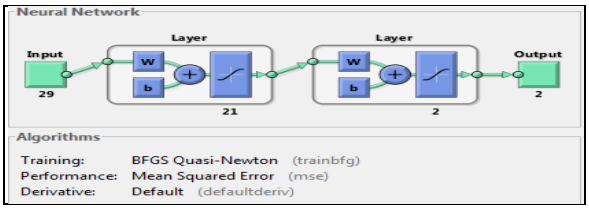


Figure 2. Architecture of neural network

Fig. 2 shows that the architecture uses trainbfg algorithm with 29 neurons (i.e. features of dataset) in input layer. Hidden layer uses 21 neurons. For binary and five class problem, output layer's neuron can be changed with 2 and 5 respectively.

### F. *Training Neural Network*

The NSL-KDD train dataset have 125973 records, table II shows that these patterns are not distributed equally. R2L and U2R have few patterns in their class. So to maintain equality and for speedup the training, 18718 patterns were selected. In these selected patterns, 17672 are chosen randomly from normal, DOS and probe class and all other from remaining classes. Training is performed on full featured dataset as well as feature reduced dataset.

### G. *Testing Neural Network*

Test set of NSL-KDD dataset having some unknown attacks, which is not present in training set. So it is main task to classify those attacks accurately. Neural network is tested against 22544 record of full test dataset with or without feature reduction as required.

### H. *Result Evaluation*

The performance of neural network can be evaluated using various parameters. Standard parameters include classification accuracy, detection rate and false positive rate, the given parameter calculated using True Positive (TP), False Negative (FN), False Positive (FP) and True Negative (TN). Confusion matrix is used to evaluate these parameters as shown in table III.

TABLE III. CONFUSION MATRIX

| Attack | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| **Actual class** | Yes | TP | FN |
| | No | FP | TN |

A good IDS should have high accuracy and detection rate but false positive rate should be low. False alarm rate is directly proportional to the misclassification rate.

$$\text{Detection Rate(DR)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{False Positive Rate(FPR)} = \frac{\text{FP}}{\text{FP} + \text{TN}}$$

$$\text{Accuracy(ACC)} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

## V. EXPERIMENTAL RESULT

The above experiment is performed on matlab using Intel(R) Core(TM)2 Duo CPU T6670@ 2.20GHz processor with 4gb RAM. Neural network with different hidden layer and algorithm is used for training 18718 selected patterns and testing 22544 pattern of NSL-KDD dataset. Training and testing performed on 41 and 29 selected features NSL dataset with various values of neural network architecture and corresponding results shown in table IV and table V for five class and binary labeled class respectively. The training and testing with 41 attribute require more time as compare to 29 selected attribute. The confusion plot for best result of testing is shown in fig 3 and fig 4. Fig 3 shows the confusion plot between testing target output and testing predicted output for five class classifications and Fig 4 shows the confusion plot between testing target output and testing predicted output for binary category. The overall training accuracy of binary classification with Levenberg-Marquardt (LM) algorithm and with 21 hidden layers is 99.3% and for five categories, with BFGS quasi-Newton Backpropagation algorithm and 23 hidden layers is 98.9%. Testing is applied on binary test data set and five categories dataset and accuracy of 81.2% and 79.9% is obtained respectively. The accuracy obtained for five class dataset doesn't include feature reduction because the accuracy obtain after feature reduction on five categories dataset, is not better than that of the accuracy without feature reduction as shown in table IV. On the other hand the accuracy of dataset with binary label with feature reduction is better as shown in table V. In fig 3, '1' represents normal, '2' represents DOS, '3' represents probe and '4', '5' represents R2L and U2R respectively.

Table VI to IX shows the confusion matrix of individual attacks, these matrixes are obtained from fig 3. The Detection rate and false positive rate for five classes is shown in table X. The confusion matrix for binary attack class is shown in table XI which is obtained from fig 4.

Binary category shows better accuracy then multi category problem that depicts from fig 3 and fig 4. Further the result of binary Intrusion Detection compared with SOM technique proposed by Ibrahim et al [8]. And it is found that the proposed techniques' accuracy is more as compare with the technique given by Ibrahim et al [8]. Table XII shows comparison of proposed method with method proposed by Ibrahim et al [8].

TABLE IV. SOME EXPERIMENTAL RESULTS FOR FIVE CLASS CLASSIFICATION

| S. No. | NN Architecture | Algorithm | No of Feature | Epoch | Accuracy |
|---|---|---|---|---|---|
| 1. | 26 | Trainlm | 41 | 17 | 76.4 |
| 2. | 25 | Trainbfg | 41 | 211 | 75.4 |
| 3. | 21 | Trainbfg | 41 | 541 | 79.3 |
| **4.** | **23** | **Trainbfg** | **41** | **771** | **79.9** |
| 5. | 19 | Trainlm | 41 | 29 | 74.5 |
| 6. | 23 | Trainbfg | 29 | 533 | 75.3 |
| 7. | 32 | Trainbfg | 29 | 394 | 76.3 |
| 8 | 21 | Trainlm | 29 | 59 | 74.8 |
| 9. | 15 | Trainlm | 29 | 140 | 73.5 |
| 10 | 18 | Trainbfg | 29 | 679 | 75.4 |

TABLE V. SOME EXPERIMENTAL RESULTS FOR BINARY CLASS CLASSIFICATION

| S. No. | NN Architecture | Algorithm | No of Feature | Epoch | Accuracy |
|---|---|---|---|---|---|
| 1. | 34 | Trainlm | 41 | 60 | 79.3 |
| 2. | 14 | Trainbfg | 41 | 469 | 76.9 |
| 3. | 17 | Trainbfg | 41 | 541 | 73.8 |
| 4. | 27 | Trainbfg | 41 | 181 | 77.8 |
| 5. | 23 | Trainlm | 41 | 178 | 80.5 |
| 6. | 25 | Trainbfg | 29 | 2466 | 78.9 |
| 7. | 17 | Trainbfg | 29 | 1212 | 78.6 |
| 8 | 17 | Trainlm | 29 | 265 | 80.5 |
| **9.** | **21** | **Trainlm** | **29** | **117** | **81.2** |
| 10 | 32 | Trainlm | 29 | 90 | 77.8 |

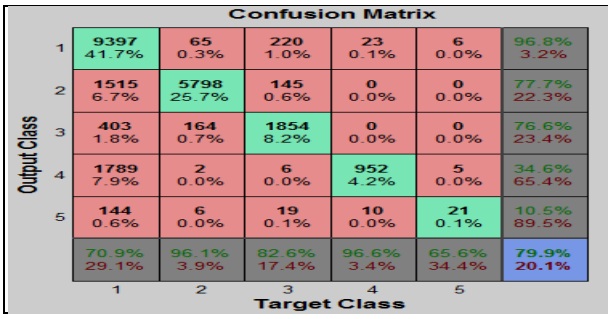


Figure 3. Five classes Test Confusion matrixes obtained after testing the neural network.

TABLE VI. CONFUSION MATRIX OF DOS

| DoS | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| **Actual class** | Yes | 5798 | 1660 |
| | No | 237 | 18022 |

TABLE VII. CONFUSION MATRIX OF PROBE

| Probe | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| **Actual class** | Yes | 1854 | 567 |
| | No | 390 | 16168 |

TABLE VIII. CONFUSION MATRIX FOR R2L

| R2L | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| Actual class | Yes | 952 | 1802 |
| | No | 33 | 17070 |

TABLE IX. CONFUSION MATRIX FOR U2R

| U2R | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| Actual class | Yes | 21 | 179 |
| | No | 11 | 18001 |

TABLE X. RESULTS OF PERFORMANCE MEASURES OF FIVE CLASS CLASSIFICATION

| Attack | FPR (%) | DR (%) |
|---|---|---|
| DoS | 1.29 | 77.7 |
| Probe | 2.35 | 76.6 |
| R2L | 0.19 | 34.6 |
| U2R | 0.06 | 10.5 |

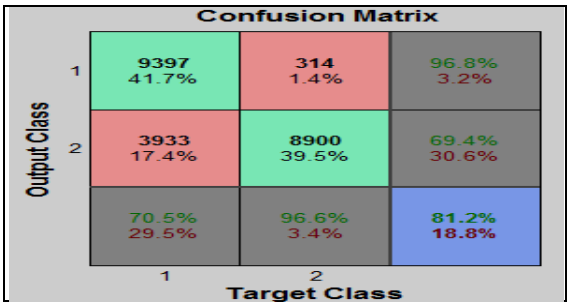


Figure 4. Binary class Test Confusion matrix obtained after testing the neural network.

TABLE XI. CONFUSION MATRIX FOR BINARY CLASSIFICATION

| Attack | | Predicted Class | |
|---|---|---|---|
| | | Yes | No |
| Actual class | Yes | 8900 | 3933 |
| | No | 314 | 9397 |

TABLE XII. COMPARISON OF PROPOSED METHOD WITH THE METHOD GIVEN BY IBRAHIM et al. [8].

| Classifier Method | Detection Accuracy | FPR(attack) |
|---|---|---|
| SOM | 75.49 | 5.77 |
| Proposed Method (binary class) | **81.2** | **3.23** |
| Proposed Method (five class) | **79.9** | - |

## VI. CONCLUSION

In this paper an ANN based Intrusion Detection System was implemented on NSL-KDD dataset. Dataset was trained and tested for binary category (normal or attack) as well as for five class attack categories. Training set having less number of patterns for R2L and U2R categories so some patterns were selected randomly from other three classes in training set. The proposed IDS system uses Levenberg-Marquardt (LM) and BFGS quasi-Newton Backpropagation algorithm for learning. Training and testing applied on dataset with full features (i.e. 41) and with reduced feature (i.e. 29). The result was evaluated based on standard parameter such as accuracy, detection rate and false positive rate and the result was compared with other reported papers. It was found that proposed technique for binary class classification gives higher accuracy of attack detection than that of other reported technique. For five class classification it was found that the system has good capability to find the attack for particular class in NSL-KDD dataset.

## REFERENCES

[1] Webster's Dictionary, Intrusion [online], available:http://www.webster-dictionary.org/definition/Intrusion. Accessed on 10/16/2013.

[2] S. Kumar, A. Yadav. Increasing Performance of Intrusion Detection System Using Neural Network. 2014 IEEE International Conference on Advanced Communication Control and Technologies (ICACCCT), pp. 1935-1939.

[3] M.Tavallaee, N.Stakhanova, and A.A. Ghorabani. Toward Credible Evaluation of Anamaly-Based Intrusion-Detection Method, IEEE Transaction on System, man, and Cybernetics- Part C: Application and reviews, vol. 40. No. 5, September 2010, pp. 516-524.

[4] MIT Lincoln Labs. DARPA intrusion detection evaluation [online], available: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/. Accessed on 10/20/2014.

[5] KDD Cup 1999.[Online] Available: http://Kdd.Ics.Uci.Edu/Databases/Kddcup99.html accessed on 8/18/2014.

[6] NSL-KDD dataset [online] available: http://nsl.cs.unb.ca/nsl-kdd/. Accessed on 7/21/2014.

[7] H. M. Imran, A. B. Abdullah, M. Hussain, S. Palaniappan, I. Ahmad. Intrusions Detection based on Optimum Features Subset and Efficient Dataset Selection. International journal of Engineering and Innovative Technology (IJEIT). Vol. 2, Issue 6, December 2012, pp. 265-270.

[8] L. M. Ibrahim, D. T. Basheer, M. S. Mahamod. A Comparison Study for Intrusion Database (KDD99, NSL-KDD) Based on Self Organization Map (SOM) Artificial Neural Network. Journal of Engineering Science and Technology, vol. 8, No.1 (2013), pp. 107-119.

[9] P. Bhoria, K. Kanwal Garg. Determining feature set of DOS attacks. International Journal of Advanced Research in Computer Science and Software Engineering, vol.3 issue 5, may 2013, pp. 875-878.

[10] K. Bajaj, A. Arora. Improving the Intrusion Detection using Discriminative Machine Learning Approach and Improve the Time Complexity by Data Mining Feature Selection Methods. International Journal of computer Applications (0975-8887) vol. 76- No.1, August 2013, pp. 5-11.

[11] D. R. Patil, T. M. Pattewar. A comparative Performance Evaluation of Machine Learning-Based NIDS on Benchmark Datasets. International Journal of Research in Advent Technology, vol.2, No. 2, April 2014. E-ISSN: 2321-9637, pp. 101-106.

[12] M. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita. Network Anomaly Detection: Methods, Systems and Tools, IEEE Communications surveys & tutorials, vol. 16, No. 1, first quarter 2014, pp. 303-336.

[13] Robert Hecht-Nielsen "Theory of the Backpropagation Neural Network" Book Neural networks for perception (Vol. 2) Pages 65-93.