Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPARATIVE STUDY OF CLASSIFICATION MODELS FOR DETECTION IN IP NETWORKS INTRUSIONS

[1]ABDELAZIZ ARAAR, [2]RAMI BOUSLAMA
[1]Assoc. Prof., College of Information Technology, Ajman University, UAE
[2]MSIS, College of Information Technology, Ajman University, UAE
E-mail: [1] araar@ajman.ac.ae , [2]bouslamar@gmail.com

ABSTRACT

Intrusion detection is an essential mechanism to protect computer systems from many attacks. We presented a contribution to the network intrusion detection process using six most representative classification techniques: decision trees, BayesNet, NaïveBayes, Rules, SVM, and Perceptron multi-layer network. In this paper, we presented a feature selection using random forest technique, towards two dimensional dataset reductions that are efficient for the initial and on-going training. The well known KDD'99 Intrusion Detection Dataset is tremendously huge and has been reported by many researchers to have unjustified redundancy, this makes adaptive learning process very time consuming and possibly infeasible. 20 attributes are selected based on errors and time metrics. Performance and accuracy of the six techniques are presented and compared in this paper. Finally, improvement of supervised learning techniques is discussed for detecting new attacks. The different results and experiments performed using the principal component analysis and the enhanced supervised learning technique are thoroughly presented and discussed. We showed that J48 is the best classifier model for IDS with reduced number of features. Finally, avenues for future research are presented.

Keywords- *IDS, KDD99, Feature Selection, Classification, Decision Trees, Rules, Bayesnet, Naïvebayes, SVM, And Perceptron Multi-Layer Network*

1. INTRODUCTION

Internet is largely used in government, military and commercial institutions. The new emerging protocols and new network architectures permit to share, consult, exchange and transfer information from any place all over the world to any other one situated in different country. Despite the above progress, the actual networks are becoming more complex and are designed with functionality while security is not considered as a main goal. The concept of Intrusion Detection System (IDS) proposed by Denning (1987) is useful to detect, identify and track the intruders. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. 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. The host based attacks are detected only from a single computer system and is easy to prevent the attacks. Data mining can help improve intrusion detection by adding a level of focus to anomaly detection [2]. It helps in to classify the attacks to measure the effectiveness of the system.

Classification is the process of finding the hidden pattern in data. With the use of classification technique it is easy to estimate the accuracy of the resulting predictive model, and to visualize erroneous predictions. The goal of classification is to accurately predict the target class for each case in the data.

The term data mining refers to the process of extracting useful information from large databases to find unsuspected relationship and to summarize the data in novel ways that are both understand-able and useful to data owner. It typically deals with the data that have already been collected for some useful purpose other than data mining analysis.

Experimental results using WEKA show that by using the feature selection on KDD, it can decrease the time for building a model, also increases TP rate and accuracy when compared with 6 cluster algorithms.

2. INTRODUCTION DETECTION TECHNIQUES

In general IDSs may be analyzed as misuse/anomaly detection and network-based/host-based systems.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1. Misuse detection

Misuse detection depends on the prior representation of specific patterns for intrusions, allowing any matches to them in current activity to be reported. Patterns corresponding to known attacks are called signature-based. These systems are unlike virus-detection systems; they can detect many known attack patterns and even variations; thereof but are likely to miss new attacks. Regular updates with previously unseen attack signatures are necessary [3].

2.2. Anomaly detection

Anomaly detection identifies abnormal behavior. It requires the prior construction of profiles for normal behavior of users, hosts or networks; therefore, historical data are collected over a period of normal operation. IDSs monitor current event data and use a variety of measures to distinguish between abnormal and normal activities. These systems are prone to false alarms, since user's behavior may be inconsistent and threshold levels will remain difficult to fine tune. Maintenance of profiles is also a significant overhead but these systems are potentially able to detect novel attacks without specific knowledge of details. It is essential that normal data used for characterization are free from attacks [3].

2.3 Data collection

Intrusion detection is defined to be the process of monitoring the events occurring in a computer system and detect computer attacks and misuse, and to alert the proper individuals upon detection. In this paper, we use WEKA for the purpose of statistical analysis and feature selection on the KDD'99 dataset [4].

There are totally 4,898,431 connections recorded, of which 3,925,650 are attacks. For each TCP/IP connection, 41 various quantitative and qualitative features were extracted.

2.4 Type of attacks

The simulated attack fall in one of the following four categories [5]:

i- Denial of Service Attack (DOS): Attacks of this type deprive the host or legitimate user from using the service or resources.

ii- Probing or Surveillance Attack: These attacks automatically scan a network of computers or a DNS server to find valid IP addresses.

iii- Remote to Local (R2L) Attack: In this type of attack an attacker who does not have an account on a victim machine gains local access to the machine and modifies the data.

iv- User to Root (U2R) Attack: In this type of attack a local user on a machine is able to obtain privileges normally reserved for the super (root) users.

Each connection record consisted of 41 features and falls into the four categories are shown in Table 1. The training set consists of 5 million connections.

Table 1: Basic characteristics of the KDD 99 intrusion

	Anomaly		**Misuse**		**Normal**
Dataset	DOS	Probe	U2R	R2L	
10% KDD	391458	4107	52	1126	97277
Corrected KDD	229853	4166	70	16347	60593
Whole KDD	3883370	41102	52	1126	972780

On the KDD'99 Dataset: Statistical Analysis for Feature information about network of computers for the apparent purpose of circumventing its security. Table 2 shows the distribution of intrusion types and their frequencies in datasets among attacks.

Table 2: Distribution of intrusion types in datasets

Normal (97277)	**Probing** (4107)	**DOS** (391458)	**R2L** (1126)	**U2R** (52)
Normal (97277)	Nmap (231)	Land (21)	Spy (2)	Buffer_over flow (30)
	Portsweep (1040)	POD (264)	Phf (4)	Rootkit (10)
	Ipsweep (1247)	Teardrop (979)	Multihop (7)	Loadmodule (9)
	Satan (1589)	Back (2203)	ftp_write (8)	Perl (3)
		Neptune (107201)	Imap (12)	
		Smurf (280790)	Warezmaster (20)	
			Guess- passwd (53)	
			Warezclient (1020)	

KDD CUP 1999 dataset have 41 different features shown in table 3. These features had all forms of continuous and symbolic with extensively varying ranges falling in four categories: basic, content, time-based traffic and host-based traffic features [6].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Attributes/Features from the Selected 10% KDD Dataset

No	Feature Name	No	Feature Name
1	Duration	22	is_guest_login
2	protocol_type	23	Count
3	service	24	srv_count
4	flag	25	serror_rate
5	src_bytes	26	srv_serror_rate
6	dst_bytes	27	rerror_rate
7	land	28	srv_rerror_rate
8	wrong_fragment	29	same_srv_rate
9	urgent	30	diff_srv_rate
10	hot	31	srv_diff_host_rate
11	num_failed_logins	32	dst_host_count
12	logged_in	33	dst_host_srv_count
13	num_compromised	34	dst_host_same_srv_ rate
14	root_shell	35	dst_host_diff_srv_rate
15	su_attempted	36	dst_host_same_src_ port_rate
16	num_root	37	dst_host_srv_diff_host_rate
17	num_file_creations	38	dst_host_serror_rate
18	num_shells	39	dst_host_srv_serror_rate
19	num_access_files	40	dst_host_rerror_rate
20	num_outbound_ cmds	41	dst_host_srv_rerror_ rate
21	is_hot_login		

3. RELATED WORK

Our literature survey reveals many results; In [7], they presented a survey on intrusion detection techniques, they identified strengths but also overcome the drawbacks. In [8], they evaluated the performance of two well known classification algorithms for attacks. Bayes net and J48 algorithm are analyzed. In [9], they compared the performance measure of five machine learning classifiers such as Decision tree J48, BayesNet, OneR, Naive Bayes and ZeroR. The results are compared and found that J48 is excellent in performance than other classifiers with respect to accuracy. In [10], they claimed for proper selection of SVM kernel function such as Gaussian Radial Basis Function, attack detection rate of SVM is increased and False Positive Rate (FPR) is decrease. In [11], they discussed about the combinational use of two machine learning algorithms called Principal Component Analysis and Naïve Bayes classifier. In [12], they presented a new classification method using Fisher Linear Discriminant Analysis (FLDA). They claimed that the approach achieves good classification rate for R2L and U2R attacks. In [13], important features of KDD Cup 99 attack dataset are obtained using discriminant analysis method and used for classification of attacks. They show that classification is done with minimum error rate with the reduced feature set. In [14], based on their results, best algorithms for each attack category is chosen and two classifier algorithm selection models are proposed. They identified the best algorithms for each attack categories. In [15], they reduced the dimensions of NSL-KDD data set. Features are reduced 33 attributes; they suggested machine learning algorithm after selection process is SimpleCart for the intrusion detection that leads to improve the computer security alerts. In [16], they presented the relevance of each feature in KDD '99 intrusion detection dataset to the detection of each class. Rough set degree of dependency and dependency ratio of each class were employed to determine the most discriminating features for each class. Empirical results show that seven features were not relevant in the detection of any class. In [17], they analyzed two learning algorithms (NB and BayesNet) for the task of detecting intrusions and compared their relative performances. BayesNet with an accuracy rate of approximately 99% was found to perform much better at detecting intrusions than NB with 11 features. In [18], two significant enhancements are presented to solve these drawbacks. The first enhancement is an improved feature selection using sequential backward search and information gain. The second enhancement is transferring nominal network features to numeric ones by exploiting the discrete random variable and the probability mass function to solve the problem of different feature types. In [19], they classified the NSL-KDD dataset with respect to their metric data by using the best six data mining classification algorithms like J48, ID3, CART, Bayes Net, Naïve Bayes and SVM to find which algorithm will be able to offer more testing accuracy. Principal component analysis (PCA) technique for reducing the dimensionality of the data is used. With 41 and 23 features, the SVM algorithm showed the highest accuracy compared with rest of the algorithms. However, they used only one metric for comparison. In this paper, we showed 20 features can lead to high performance with respect to many metrics.

4. FEATURE SELECTION

Due to the large amount of data flowing over the network real time intrusion detection is almost impossible. Feature selection can reduce the computation time and model complexity.

4.1 Random forests

Random Forests (RF) is a special kind of ensemble learning techniques and robust concerning the noise and the number of attributes. In [20], they proposed an approach of feature selection using random forest to improve the performance of intrusion detection systems. The evaluation metrics

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is conducted on 41 features and its selected subsets 3, 5, 10 and 15 features.

Feature selection processes involve four basic steps in a typical feature selection method shown in Figure 1[21]. First is generation procedure to generate the next candidate subset; second one is an evaluation function to evaluate the subset and third one is a stopping criterion to decide when to stop; and a validation procedure to check whether the subset is valid.

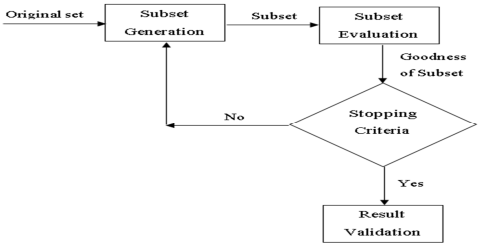

Figure 1: Four key steps of Feature Selection

To find out a subset out of 41 attributes listed Table 3, whose performance is equal to or greater than the performance given by the 41 attributes. For this purpose, we used the RRF (regularized random forest) package of r-tool [22,23] to rank the features with the help of their significance. We applied the feature selection of RRF package on the kddcup'99 dataset. Due to which we get the information gain for each feature of kddcup'99 dataset and we ranked the features according to their significance. After that we used the random forest classifier of WEKA [24,25] tool to classify the feature set and check their performance.

4.2. Information gain attributes evaluation:

Information Gain Attribute evaluates the worth of an attribute by measuring the information gain with respect to the 23 classes [26].

$$\text{Info}(G) = -\sum_{i=1}^{23} p_i \log_2(p_i) \qquad (1)$$

Here Information gain G is computed by calculating p_i the probability of occurrence of class i over total classes in the dataset. A feature *F* with values $\{ f_1, f_2, \ldots, f_{41} \}$ can divide the training set into s_{ij} which is a sample of class *i* contains feature *j*. The information gain of each feature is as follows:

$$\boldsymbol{E(\text{fj}) = \sum_{i=1}^{23} \frac{Sij}{S} * Info(G)} \quad \text{j=1,..,41} \quad (2)$$

(1) and (2) are used to sort the features in decreasing order based on their information gains.

4.3 Performance Measurement Terms

Table 4 shows different attributes selection with respect to some criteria. Detection of attack can be measured by following metrics [27]:

- True Positive rate (TP): Corresponds to the number of detected attacks and it is in fact attack.
- False Positive rate (FP): or false alarm, Corresponds to the number of detected attacks but it is in fact normal.
- Correctly classified instances (%): Performance is computed by asking the classifier to give its best guess about the classification for each instance in the test set. Then the predicted classifications are compared to the actual classifications to determine accuracy.
- Root mean squared error RMSE: It is the most used and it is expressed in the same units as actual and predicted attacks.
- A kappa statistic of 1 indicates perfect agreement between actual and predicted attacks. Higher kappa is better.

Table 4: Evaluation metrics of Random Forest for feature selection

Total no of features	(41)	(3)	(5)	(10)	(15)	(20)	(25)	(30)	(35)
TP Rate	1	0.998	0.999	0.999	0.999	1	1	1	1
FP Rate	0	0	0	0	0	0	0	0	0
Time taken to build model (sec)	101.12	34.95	34.98	48.02	62.16	67.92	75.64	75.88	87.64
Correctly classified Instances (%)	99.9649	99.8017	99.8678	99.9083	99.9434	99.9607	99.9637	99.9595	99.9702
Incorrectly Classified Instances (%)	0.0351	0.1983	0.1322	0.0917	0.0566	0.0393	0.0363	0.0405	0.0298
Kappa statistic	0.9994	0.9966	0.9978	0.9984	0.999	0.9993	0.9994	0.9993	0.9995
Mean absolute error	0.0001	0.0002	0.0002	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
Root mean squared Error	0.0049	0.0119	0.0095	0.0079	0.0063	0.005	0.0051	0.0052	0.0049
Relative absolute error (%)	0.123	0.4814	0.3076	0.2321	0.1642	0.1175	0.1325	0.1212	0.1195
Root relative squared error (%)	3.083	7.4223	5.9296	4.9264	3.9558	3.1251	3.2092	3.2274	3.0646

The following figures are constructed for TP rate and time taken to build a model with different attribute numbers form the sorted table.

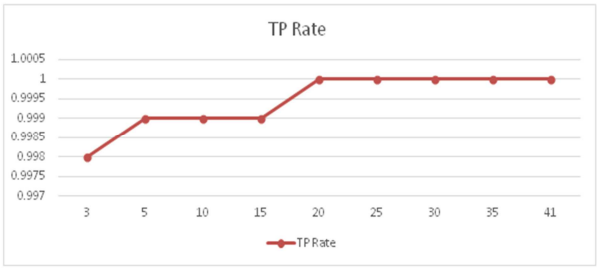

Figure 2 TP rates

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

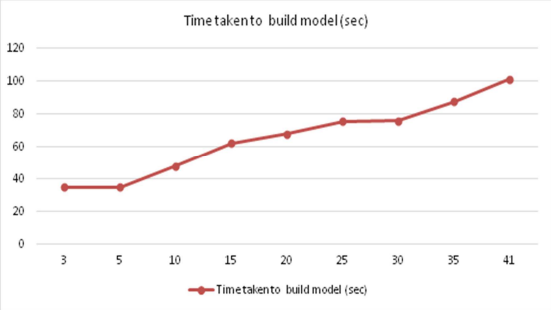

Figure 3: time to build a model

In Figure 2, the value of TP converges to 1 from 20 attributes, while in Figure 3, the time for building a model is less than other values above 20. Table 5 shows the information gains of the selected 20 features which have value above zero.

Table 5: The selected 20 attributes for training data

N0	Attribute#	Attribute name	Info Gain
1	5	src_bytes	1.4384029
2	23	count	1.3902034
3	3	service	1.3552348
4	24	srv_count	1.0977182
5	36	dst_host_same_src_port_rate	1.0961848
6	2	protocol_type	1.0159265
7	33	dst_host_srv_count	0.9054253
8	35	dst_host_diff_srv_rate	0.8997895
9	34	dst_host_same_srv_rate	0.8713826
10	30	diff_srv_rate	0.7844647
11	29	same_srv_rate	0.7773695
12	4	flag	0.7645689
13	6	dst_bytes	0.5820167
14	38	dst_host_serror_rate	0.5662843
15	25	serror_rate	0.5449353
16	39	dst_host_srv_serror_rate	0.5438835
17	26	srv_serror_rate	0.521429
18	12	logged_in	0.4364079
19	32	dst_host_count	0.3470899
20	37	dst_host_srv_diff_host_rate	0.3060166

5. IDS CLASSIFICATION METHODS AND RESULTS

Figure 3 shows a summary of the methodology presented in this paper. A comparison among classifiers is conducted.

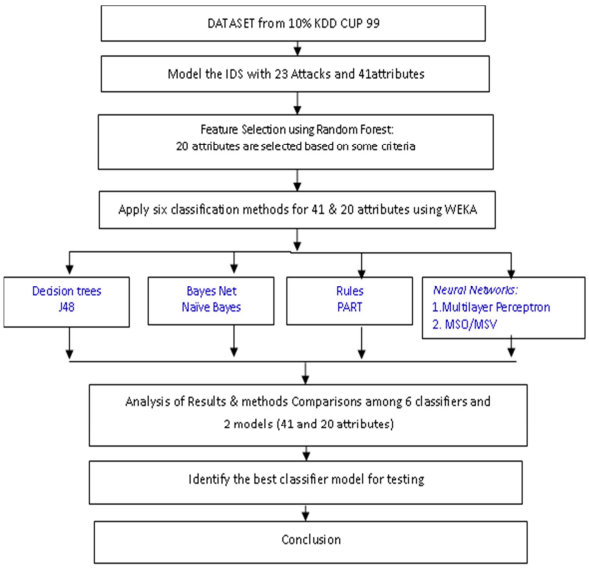

Figure3: Simplified methodology

Table 7 shows the performance of each classifier for 2 models with respect to errors and kappa. Figures 4 and 5 visualize the 2 models with respect to kappa and RMSE. J48 and PART have the superiority over the other classifiers.

Table 7: Comparison of classifiers with respect to error

Classification Algorithms	Error Names	Test with 41 Features	Test with 20Features
J48	Kappa statistics	0.9992	0.9994
	Mean absolute error	0.0001	0
	Root mean squared error	0.0064	0.0056
BayesNet	Kappa statistics	0.9944	0.994
	Mean absolute error	0.0003	0.0004
	Root mean squared error	0.0152	0.0158
NaïveBayes	Kappa statistics	0.8802	0.9214
	Mean absolute error	0.0063	0.0042
	Root mean squared error	0.0774	0.0621
Rule PART	Kappa statistics	0.9993	0.9992
	Mean absolute error	0	0
	Root mean squared error	0.0056	0.0062
Multilayer Perceptron	Kappa statistics	0.9986	0.9906
	Mean absolute error	0.0002	0.0007
	Root mean squared error	0.0082	0.0195
SVM	Kappa statistics	0.9986	0.9909
	Mean absolute error	0.0794	0.0794
	Root mean squared error	0.1961	0.1961

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

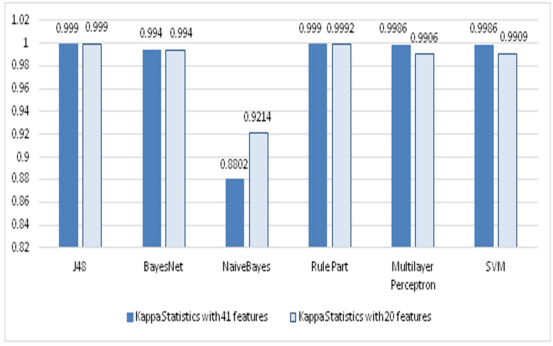

Figure 4: Kappa statistics comparison

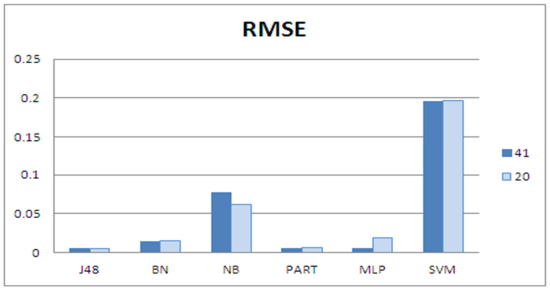

Figure 5: Root mean squared error comparison

A large set of machine learning and pattern classification algorithms trained and tested on KDD intrusion detection data set failed to identify most of the *U2R* and *R2L* attacks, as reported by many researchers in the literature. Table 8 exposes the deficiencies and limitations of the KDD data set to argue that this data set should not be used to train pattern recognition or machine learning algorithms for misuse detection for these two attack categories. Analysis results clearly suggest that no pattern classification or machine learning algorithm can be trained successfully with the KDD data set to perform misuse detection for *U2R* or *R2L* attack categories. From Table 8, J48 and rule PART have higher accuracy for normal and anomaly attack with 20 attributes.

Table 8: Accuracy comparison

Classification Algorithms	Class Names	Test Accuracy with 41 Features	Test Accuracy with 20 Features
J48	Normal	99.9	100
	Probe	98.7	98.4
	DOS	94.7	96.9
	U2R	31.8	26.5
	R2L	51.6	44.1
BayesNet	Normal	98.9	98.8
	Probe	83.7	84.3
	DOS	98.9	99.3
	U2R	44.3	13.6
	R2L	50.4	37.4
NaiveBayes	Normal	64.9	77.9
	Probe	83.1	81.5
	DOS	94.2	90.7
	U2R	59.8	29.1
	R2L	66.2	57.8
Rule PART	Normal	99.9	99.9
	Probe	99.0	98.9
	DOS	94.8	94.7
	U2R	45.4	13.6
	R2L	57.4	38.4
Multilayer Perceptron	Normal	99.9	99.1
	Probe	98.1	80.2
	DOS	82.2	70.9
	U2R	0	11.3
	R2L	35.2	33.8
SVM	Normal	99.9	99.8
	Probe	98.1	87.5
	DOS	98.8	83.0
	U2R	36.3	11.3
	R2L	45.7	45.3

Figure 6 to 8 illustrate comparisons on normal and anomalies. J48, PART and SVM-SMO are the best classifiers for normal detection.

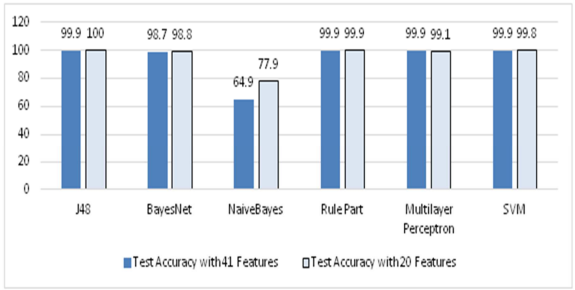

Figure 6: Test Accuracy of Class Normal Comparing with 41 & 20 Features

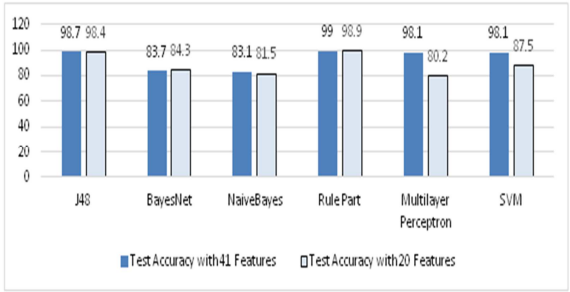

Figure 7: Test Accuracy of Class probe attack Comparing with 41 & 20 Features

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

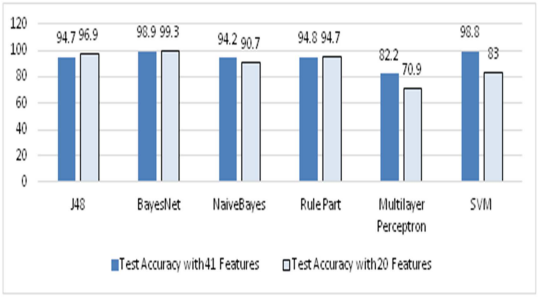

Figure 8: Test Accuracy of Class DOS attack Comparing with 41 & 20 Features

The J48 algorithm with 20 attributes can be used as a training model for IDS [29]. The following figure summarizes the intrusion process.

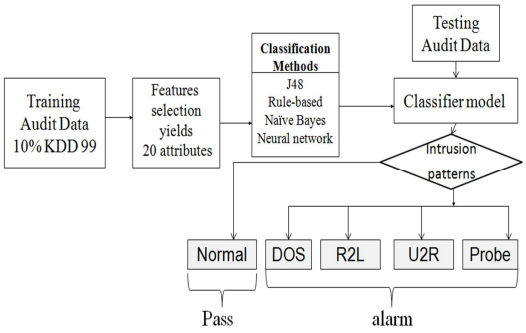

Figure 9: Proposed System for Intrusion Detection

6. CONCLUSION AND FUTURE WORK

In this paper, a comparative analysis has been done on the basis of detection rate, computational time and root mean square error. 20 attributes as feature set is used for the classification of the entire dataset with normal and attack record. It is found that this analysis gives good classification rate and minimum error rate when compared to the classification done using the full feature set, thereby reducing the burden of the IDS in working with a large feature set. To increase the classification rate of *U2R* and *R2L* attacks, we strongly recommend the following:

(1) All researchers stop using the KDD Cup '99 dataset,

(2) The KDD Cup and UCI websites include a warning on the KDD Cup '99 dataset webpage informing researchers that there are known problems with the dataset, and

(3) This data set must not be used for network-intrusion detection. It does not reflect reality; it's simulated and old data.

In our future work, we suggest the following: 1. additional measures including more statistical tools will be employed.

2. Other data mining tools than WEKA can be used for the analysis.

3. A framework of hybrid intrusion detection system uses the snort and a selected training classification model to predict the type of attack for new dataset.

REFERENCES

[1] Denning, D. "An Intrusion Detection Model". *IEEE Transactions on Software Engineering*, 13(2), 1987, 222–232.

[2] Sneha Kumari, Maneesh Shrivastava, "A Study Paper on IDS Attack Classification Using Various Data Mining Techniques" *International Journal of Advanced Computer Research,* Volume-2 Number- 3 Issue-5 September-2012

[3] T. Verwoed and R. Hunt, "Intrusion Detection Techniques and Approaches," Elsevier: *Computer Communications*, Vol.25, No.10, 2002, pp: 1356- 1365

[4] T. Eldos, M. Siddiqui and A. Kanan "On the KDD'99 Dataset: Statistical Analysis for Feature Selection", *Journal of Data Mining and Knowledge Discovery*, ISSN: 2229-6662 & ISSN: 2229-6670, Volume 3, Issue 3, 2012

[5] A. Balon-Perin, "Ensemble-Based Methods for Intrusion Detection", Master thesis, Norwegian University of Science and Technology, Dept. of Computer and Information Science, July 2012

[6] Devendra Kailashiya et al, "Improve Intrusion Detection Using Decision Tree with Sampling", *Int. Journal Computer Technology & Applications*,Vol 3 (3), 2012, 1209-1216

[7] Sonawane S. , Pardeshi S. and Prasad G.," A Survey on Intrusion Detection Techniques",World *Journal of Science and Technology* 2012, 2(3):127-133, ISSN: 2231 – 2587 Available Online: www.worldjournalofscience.com

[8] N.S. Chandolikar & V.D.Nandavadekar, "Comparative Analysis of two Algorithms for Intrusion attack Classifications using KDD CUP Dataset", *International Journal of Computer Science and Engineering*, V1, Issue 1, 81-88 2012

[9] Upendra and Y. K. Jain, "An Empirical Comparison and Feature Reduction Performance Analysis of Intrusion Detection", *International Journal of Control Theory and Computer Modeling* (IJCTCM) Vol.2, No.1, January 2012

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] Yogita B. Bhavsar, Kalyani C.Waghmare " Intrusion Detection System Using Data Mining Technique: Support Vector Machine", *International Journal of Emerging Technology and Advanced Engineering* V3, I3, March 2013

[11] Neethu B, "Classification of Intrusion Detection Dataset using Machine Learning Approaches", *International Journal of Electronics and Computer Sciene Engineering*, ISSN 2277-1956/V1,N3 2012

[12] P. Gifty Jeya, M. Ravichandran, C. S. Ravichandran, "Efficient Classifier for R2L and U2R Attacks", *International Journa l of Computer Applications (0975 – 8887),* Volume 45– No.21, May 2012

[13] S.Siva Sathya, R.Geetha Ramani, K.Sivaselvi, " Discriminant Analysis based Feature Selection in KDD Intrusion Dataset", *International Journal of Computer Applications* (0975 – 8887) Volume 31– No.11, October 2011

[14] Huy Anh Nguyen and Deokjai Choi, "Application of Data Mining to Network Intrusion Detection: Classifier Selection Model", APNOMS 2008, LNCS 5297, pp. 399–408, 2008. Springer-Verlag Berlin Heidelberg 2008

[15]Karan Bajaj, Amit Arora, **"**Dimension Reduction in Intrusion Detection Features Using Discriminative Machine Learning Approach*", International Journal of Computer Science Issues,* Vol. 10, Issue 4, No 1, July www.IJCSI.org

[16] A A.Olusola., A S.Oladele and D. O.Abosede, "Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features", *Proceedings of the World Congress on Engineering and Computer Science* Vl WCECS 2010, San Francisco, 20-22, 2010

[17] Y. K. Jain and Upendra, "Intrusion Detection using Supervised Learning with Feature Set Reduction", International *Journal of Computer Applications* (0975 – 8887) Volume 33– No.6, November 2011

[18] Maher Salem and Ulrich Buehler, "Mining Techniques in Network Security to Enhance Intrusion Detection Systems", International Journal *of Network Security & Its Applications*, Vol.4, No.6, November 2012

[19] S Mallissery, S Kolekar, R Ganiga, "Accuracy Analysis of Machine Learning Algorithms for Intrusion Detection System using NSL-KDD Dataset ",Proc. of the Intl. Conf. on Future Trends in Computing and Communication, FTCC 2013

[20] Sneh Lata Pundir and Amrita, " Feature Selection using Random Forest in Intrusion Detection System", *International Journal of Advances in Engineering & Technology,* Vol. 6, Issue 3, pp. 1319-1324 , July 2013.

[21] M. Aggarwal and Amrita, "Performance Analysis of Different Feature Selection Methods In Intrusion Detection", *International Journal of Scientific & Technology Research* V 2, N6, June 2013

[22]B.Azhagusundari, Antony Selvadoss Thanamani, "Feature Selection based on Information Gain", *International Journal of Innovative Technology and Exploring Engineering* ISSN: 2278-3075, Volume-2, Issue-2, January 2013

[22] P. T. Htun and K. T. Khaing, "Detection Model for Daniel-of-Service Attacks using Random Forest and k-Nearest Neighbors", *International Journal of Advanced Research in Computer Engineering & Technology* V 2, No5, May 2013

[24] Kesavulu, E., Reddy, V. N. and Rajulu, P. G. "A Study of Intrusion Detection in Data Mining". Proceedings of the World Congress on Engineering, IIIWCE 2011,London, 2011

[25] P. T. Htun and K. T. Khaing, "Important Roles Of Data Mining Techniques For Anomaly Intrusion Detection System", *International Journal of Advanced Research in Computer Engineering & Technology* V2,No 5, May 2013

[23] Y B. Bhavsar, K C.Waghmare "Intrusion Detection System Using Data Mining Technique: Support Vector Machine", International *Journal of Emerging Technology and Advanced Engineering,* Volume 3, Issue 3, March 2013

[26] S. Singh , S. Silakari "An Ensemble Approach for Feature Selection of Cyber Attack Dataset", *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, 2009

[27]Sanjay Kumar Sharma, Pankaj Pandey and M. S. Sisodia, "Anomaly Based Network Intrusion Detection by using Data Mining", *International Journal of Advanced Research in Computer Science and Electronics Engineering,* V1, Issue1, March 2012

[28] Sabhnani M., Serpen G., "Why Machine Learning Algorithms Fail in Misuse Detection on KDD Intrusion Detection Data Set", *Journal of Intelligent Data Analysis*, 2004

[29] Rami Bouslama ," A Study of Classification Models for Anomaly Detection in IP Networks intrusions", Master thesis, IT College, Ajman University, UAE, 2014