Journal of Computer Science, 9 (3): 391-403, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.391.403 Published Online 9 (3) 2013 (http://www.thescipub.com/jcs.toc)

Hybrid of Fuzzy Clustering Neural Network Over NSL Dataset for Intrusion Detection System

[1]Dahlia Asyiqin Ahmad Zainaddin and [2]Zurina Mohd Hanapi

[1]Department of Industrial Electronic,
Faculty of Computer and Network Technology, German Malaysian Institute, Malaysia
[2]Department of Communication Technology and Network,
Faculty of Computer Science and Information Technology, University Putra Malaysia, Malaysia

Received 2012-10-01, Revised 2013-04-26; Accepted 2013-05-04

ABSTRACT

Intrusion Detection System (IDS) is one of the component that take part in the system defence, to identify abnormal activities happening in the computer system. Nowadays, IDS facing composite demands to defeat modern attack activities from damaging the computer systems. Anomaly-Based IDS examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies. These technique identifies activities which degenerates from the normal behaviours. In recent years, data mining approach for intrusion detection have been advised and used. The approach such as Genetic Algorithms , Support Vector Machines, Neural Networks as well as clustering has resulted in high accuracy and good detection rates but with moderate false alarm on novel attacks. Many researchers also have proposed hybrid data mining techniques. The previous resechers has intoduced the combination of Fuzzy Clustering and Artificial Neural Network. However, it was tested only on randomn selection of KDDCup 1999 dataset. In this study the framework experiment introduced, has been used over the NSL dataset to test the stability and reliability of the technique. The result of precision, recall and f-value rate is compared with previous experiment. Both dataset covers four types of main attacks, which are Derial of Services (DoS), User to Root (U2R), Remote to Local (R2L) and Probe. Results had guarenteed that the hybrid approach performed better detection especially for low frequent over NSL datataset compared to original KDD dataset, due to the removal of redundancy and uncomplete elements in the original dataset. This electronic document is a “live” template. The various components of your paper [title, text, tables, figures and references] are already defined on the style sheet, as illustrated by the portions given in this document.

Keywords: Artificial Neural Network, Fuzzy Clustering, Intrusion Detection System, KDDCup 1999, NSL KDDCup, Data Mining

1. INTRODUCTION

One of the components in security that suit the ‘defense in depth’ model is known as Intrusion Detection System (IDS) (Chung, 2011). An IDS is capable of sending early alarm upon risk exposure caused by any attack. This is to alert the system administrators to execute corresponding response measurements, thus to reduce the possibility of bigger losses.

A growing interest in investigation of anomaly detection sparks from the ability of the approach to detect unknown attacks and to evaluate unforeseen vulnerability. Nonetheless, current anomaly detection technique suffers from high false alarm rate. Similarly, machine learning, that is being one of the most promising advancements in solving intricate data classification problems with accuracy also suffers from the same drawback (Sandeep, 2008). In view of this, this

Corresponding Author: Dahlia Asyiqin Ahmad Zainaddin, Department of Industrial Electronic, Faculty of Computer and Network Technology, German Malaysian Institute, Malaysia

research proposes a new hybrid mining approach to improve current anomaly detection capabilities in IDS that would be an essential component of a security arsenal to fit the 'defense in depth' architecture in securing an information infrastructure.

Detection precision and detection stability are two key indicators to evaluate intrusion detection systems (Wang *et al*., 2010) that refer to the accuracy for each class of attack and stability the detetction in each class respectively. Recently, there has been exhaustive effort in improving the existing anomaly detection techniques due to significantly high false alarm as well as moderate accuracy and detection rate. In addition, there is lacking in performance of single classifier, which has resulted in high tendency for wrong classification during detecting unknown attacks (John *et al*., 2000).

Even Artificial Neural Network (ANN) as one of the widely and successfully used techniques and has been successful in solving many complex practical problems, however, there are main drawbacks of ANN-based IDS existing in two aspects (Wang *et al*., 2010; Ritu *et al*., 2011); Lower detection precision, especially for low-frequent attacks, for example: Remote to Local (R2L), User to Root (U2R) and weaker detection stability.

In specific, there are three types of ANN based IDS, which known as Supervised ANN-based IDS, Un-Supervised ANN based IDS and Hybrid ANN-based IDS (Giuseppina *et al*., 2004; Al-Wesam *et al*., 2010). Several studies shows that, unlike hybrid ANN, single classifier of Artificial Neural Network (supervised and un-supervised) produced low detection precision and low stability level. The motivation for using the hybrid ANN is merely to overcome the limitations of individual ANN.

Supervised ANN-based IDS forms input-output pair examples to build an external relationship between the input and output. But since in practice the number of training set is very large and the distribution of training set is imbalanced, the MLFF neural networks is easy to reach the local minimum and thus stability is lower. Un-Supervised ANN-based IDS: classify input data and separate normal behaviors from abnormal or intrusive ones (Endorf *et al*., 2004). The main advantage of unsupervised ANN in IDS is that it can improved the analysis of new data without retraining. Just like using supervised learning ANN, the performance of unsupervised ANN is also lower. Especially for low-frequent attacks, unsupervised ANN also gets lower detection precision (Rachid, 2008). The last category is hybrid ANN. It can be formed by combining supervised ANN and unsupervised ANN, or combine the ANN with other data mining techniques to detect intrusion (Ritu *et al*., 2011; Borji, 2007). Horeis (2003) introduced a combination of SOM and Radial Basis Function (RBF) networks. The system offers generally better results than IDS based on RBF networks alone. Chen *et al*. (2007) proposed hybrid flexible neural-tree-based IDS based on flexible neural tree, evolutionary algorithm and Particle Swarm Optimization (PSO). Empirical results indicated that the proposed method is efficient. Different ways to construct hybrid ANN will highly influence the performance of intrusion detection. Different hybrid ANN models should be properly constructed in order to serve different aims.

The main objective of this research is to test the stability of detection precision for low-frequent attacks and weaker detection stability using the current hybrid approach of Intrusion Detection System (IDS) (Wang *et al*., 2010) with NSL dataset instead of using standard KDDCup 1999 dataset. In current approach, the aggregation of clustering and classification has been applied. The clustering techniques are required to cluster each and every data according to their group behavior. Next, the classifier techniques are applied to these arrangements in order to classify the data into the right categories.

The scope of this research is focused on hybrid mining approaches which later, the validation will be based on precision percentage, recall percentage and f-value.

The exists Fuzzy Clustering and Neural Network approach which was being tested using KDD Cup '99 dataset (Rachid, 2008) will be evaluate again with NSL dataset where the datasets represents four type of attacks (Probe, User to root, Root to Local, Dos) and normal behaviour data.

1.1. Background

IDS has been introduced as a forefront security to detect various attacks (Kartit *et al*., 2012). In cyber world, any set of action which tends to compromise the Confidentiality, Integrity, or Availability (CIA) of resources are addressed as an "Intrusion". In other words, any violation with existing established policy, which attempts to break into or misuse the system such as the network medium, servers or firewall are also considered as an intrusion (Lodin, 1998; Stallings, 2006).

Anderson *et al*. (1980) has introduced IDS and his work has been improved by (Dorothy, 1987). According to their experiment, user behaviors are translated using some computer audit mechanism and other statistical detection methods to detect masqueraders who illegally access the system. Hence, IDS is the process of supervising and monitoring events that are happening in computer system or network system. Data instances are continuously examined for sign of intrusions before an alarm is sent out to inform associated personnel for possible risks.

In recent years, data mining algorithms have been applied as intrusion detection methods in finding new intrusion patterns (Dorothy, 1987; Nicholas *et al*., 1996; Kusum *et al*., 2010; Ali and Len, 2011; Mehdi and Mohammad, 2012). Clustering is an anomaly detection method that is able to detect novel attack and is capable to find natural grouping of data based on similarities among the patterns.

In IDS, clustering is an anomaly detection method that is able to detect novel attack and is capable to find natural grouping of data based on similarities among the patterns. Clustering is a type of unsupervised learning (Ashwin and Avinash, 2009). The Fuzzy C-Means (FCM) based algorithms are the most popular fuzzy clustering algorithms in practice (Muna *et al*., 2009; Jakir *et al*., 2011; Suguna and Selvi, 2012). FCM clustering allows one piece of data to belong to two or more clusters. FCM initially proposed by (Dunn, 1973) and generalized by (James, 1981) and other authors such as (Fukuyama and Sugeno, 1989). Usually, membership functions are defined based on a distance function, such that membership degrees express proximities of entities to cluster centers (i.e., prototypes). By choosing a suitable distance function different cluster shapes can be identified.

Classification is a type of supervised learning that is used to classify data into specific category. Under classification methods, there exist a variety of classifiers which have been widely cited, reviewed and used by other researchers such as by (Ozgur *et al*., 2005; Xindong *et al*., 2008; Chih-Fong *et al*., 2009). Different classifiers have attract researcher's interest in recent years, such as OneR (Robert, 1993), Support Vector Machine (Vladimir, 1995), Random Forest (Leo, 1999), Naïve Bayes (George, 1995) and Neural Networks (Sang-Jun and Sung-Bae, 2005). Neural computing refers to a pattern recognition methodology for machine learning. ANN is a biologically inspired form of distributed computation (Anderson, 1995; Simon, 1999). It is composed of simple processing units and connections between them. ANN is the most popular used approaches in Intrusion Detection Systems (Mehdi and Zulkernine, 2011).

In this study, classic feed-forward neural network with back-propagation algorithm or known as Multilayer Perceptron (MLP), will be used to predict intrusion. A few limitation of MLP method has been discover (Alpaydin, 2010), which: (1) the convergence obtained from backpropagation learning is very slow, (2) the convergence in backpropagation learning is not guaranteed and (3) backpropagation learning requires input scaling or normalization.

In particular, when at least two learning techniques combined together, it's become hybrid learning. A few hybrids of Neural Networks based technique were practices for Intrusion Detection. Tie-Jun (2008) used the backpropagation network with Genetic Algorithms to enhance backpropagation. KDD dataset was being used in the experiment. The detection rate for Guess-password, Satan and Peral was 85.60, 90.97 and 90.79 respectively. The overall accuracy of detection rate is 91.61 with false alarm rate of 7.35. Srinivas *et al*. (2005) used Back Propagation Neural Network with variety of learning algorithm. The performance of the network is 95.0. The overall accuracy of classification for RPBRO is 97.04 with false positive rate of 2.76% and false negative rate of 0.20. Novikov *et al*. (2006) used Radial Based Function (RBF) Neural Network together with Multilayer Perceptron to classify five types of attacks, the accuracy rate of classifying attacks is 93.2 using RBF and 92.2 using MLP Neural Network and the false alarm is 0.8%. KDD dataset was used for anomaly dataset and the result of accuracy of classification was 92.2% using MLP Neural Network and 93.2% using RBF Neural Network.

Recently, a lot of learning techniques have been explored in clustering and classification for the task of anomaly detection, for example, as studied by (Wang *et al*., 2010; Muna *et al*., 2012). Hybrid concept is gaining popularity as the approach promises better flexibility in detecting malicious traffic.

1.2. Methodology

For this study, precision, recall and f-value play the important role in achieving the research objective. **Figure 1** shows method of experiment that have been executed to achieve the research objective. Each step is briefly explained as follows (Wang *et al*., 2010).

1.3. Artificial Neural Network

In Step 1, instances will be clustered by using Fuzzy C-Means approach in order to assign membership function to each of them. In this step, each training and testing is clustered into the corresponding group behavior using clustering techniques before a classifier is applied to each group. The highest degree of membership function appointed to each intances refer to the cluster they belongs. In Step 2, each of the resulted cluster will be train with multilayer perceptron to get different based models. During step 3, we will use the whole instances to simulate with the model produced from step 2 previously, in order to reduce error for each model. In step 4, the output produced from step 3 respectively will be use to aggregate with membership function value which was raised throughout step 1. Step 5, use another neural network model by using output calculated from step 4 previously as input for final classification to achieve precision, recall and f-value.

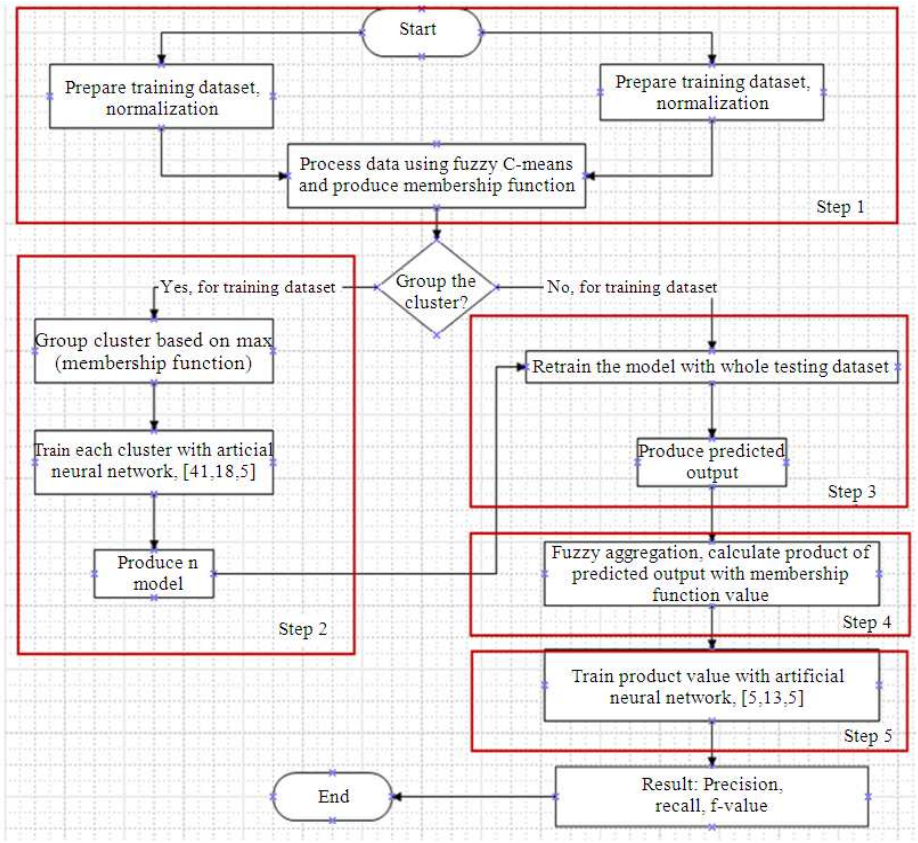

Fig. 1. Step of experiment

1.4. Artificial Neural Network

Classic feed-forward neural networks trained with the backpropagation algorithm to predict intrusion was employed in the experiment. This is how to create different base model ANN*i* with different training subsets from the clustered instances previously. A feed-forward neural network has an input layer, an output layer, with one or more hidden layers in between the input and output layer.

Each node i in the input layer has a signal x*i* as network's input, then it was multiplied by a weight value between the input layer and the hidden layer, Equation (1):

$$In(j) = \theta_j + \sum_{i=1}^{n} x_{iwij} \quad (1)$$

Then passed through the bipolar sigmoid activation function of Feed-forward algorithm, which will proceed through the numbers of hidden layers, Equation (2):

$$f(x) = \frac{2}{(1 + \exp(-x))} - 1 \quad (2)$$

After that, Backpropagation algorithm was applied in order to update weight as to become input for Feed-forward algorithm in next iteration, Equation (3):

$$w(t+1) = w(t) - \frac{\eta \partial E(t)}{\partial w(t)} + \propto \quad (3)$$

The output of the activation function *f* (In(j)) is then broadcast all of the neurons to the output layer. The output value will be compared with the target; in this study, we used the mean absolute error as error function, Equation (4):

$$E_m = \frac{1}{2n} \sum_k \sqrt{(T_k - Y_k)^2} \quad (4)$$

When n is the number of training patterns, Y_k and T_k are the output value and the target value, respectively. Structure of ANN (input, hidden layer and output) in ANN module referred as (Mukhopadhyay, 2011; Wang *et al*., 2010; Anderson, 1995) respectively.

1.5. Fuzzy Aggregation Module

The aim of fuzzy aggregation module is to aggregate different ANN's result and reduce the detection errors as every ANNi in ANN module only learns from the subset TRi.

First, Let the whole testing set TS as data to input the every trained ANNi and get the outputs, Equation (5):

$$Y_J^{TR} = \left\lfloor y_{J1}^{TS}, y_{J2}^{TS}, ..., ..., y_{Jk}^{TS} \right\rfloor, j = 1,2,..n \quad (5)$$

Then, form the input for new ANN, Equation (6):

$$Y_{input} = [Y_1^{TS}.U_1^{TS}.Y_2^{TS}.U_1^{TS}, ..., Y_n^{TS}.U_n^{TS}] \quad (6)$$

where, U_n^{TS} is TS^n belonging to C_{TS}.

Finally, the new ANN is trained. We can use Y_{input} as input and use the whole testing set TS's class label as output to train the new ANN, Equation (6). Through above three steps, the new ANN can learn the errors which caused by the individual ANNi in ANN module. At this stage, structure for fuzzy aggregation module referred as (Anderson, 1995; Dorothy, 1987), respectively.

1.6. Implementation

A series of experiments were conducted to compare the performance of single classifier and previous approaches against the proposed hybrid approach using a standard benchmark dataset, KDDCup 1999. NaiveBayes (NB), Tree (J48) and BackPropagation Neural Network (BP) has been chosen as the group of single classifiers. BackPropagation Neural Network will be combined with Fuzzy C-Means clustering to form hybrid approach known as Fuzzy C Neural Network (FCNN).

The steps of experiment on **Fig. 1** explained as below:

Stage I: For an arbitrary data set DS, it is firstly divided into normalized training set TR and testing set TS. Then the different training subsets TR_1; TR_2; . . . ; TR_k are created from TR with fuzzy clustering module.

Stage II: As for ANN model, ANN*i*, (i = 1; 2; . . . ; k) is trained by the specific learning algorithm to formulate k different base ANN models, where each training subset TR*i* : i = 1; 2; . . . ; k.

Stage III: Then all selective training set TR was used in next simulation to reduce the error for every ANN*i* and get the results. The membership grades are used, which were generated by fuzzy clustering module, as to combine the results. Subsequently, we train another new ANN using the combined results.

KDD dataset covered four major categories of attacks. In order to demonstrate the abilities to detect different kinds of intrusions, the training and testing data covered all classes of intrusion categories as listed in the following as adopted from the KDD Dataset 1999, **Table 1**.

Random selection has been used in many applications to reduce the size of the dataset. In this study, we randomly select 18,285 records similar to prior research (Rachid, 2008), for training dataset and 10% of testing dataset with 41 attributes (**Table 2**).

The NSL KDD Cup was choosen apart of KDD datset to test the stability of the existing Fuzzy C-Means approach. NSL dataset is currently become the popular dataset used nowadays (Mrutyunjaya *et al*., 2010; Shilpa *et al*., 2010; Bhavin and Bhushan, 2012). NSL dataset is actually based on KDD Cupp '99 dataset with reduction of instances. NSL-KDD dataset, developed by (Tavallaee *et al*., 2009), an enhanced version of KDDCup 1999 benchmark intrusion detection dataset because of the inherent problems. The first important limitation in the KDDCup 1999 dataset is the huge number of redundant records in the sense that almost 78% training and 75% testing records are duplicated, as shown in **Table 3**. Even, (John, 2000) had discussed that the NSL KDD data set still loses from some of the problems and may not be a good example of existing real networks, due to the lack of public data sets for network-based IDSs, but (Tavallaee *et al*., 2009) insist that it still can be applied as an effective benchmark data set to help researchers compare different intrusion detection methods instead of using the random data.

The number of records in the NSL-KDD train and test sets are acceptable. This advantage makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of dissimilar research work will be coherent and comparable.

The final step is to analyze the final result from classification using different techniques and concludes the findings upon observed, collected results. The experimental results are evaluated by comparing results from the proposed approach against results from the previous works. The categories of data behavior in IDS data was generally defined as follows:

- True Positive (TP): Actual attack instances detected as attack instances
- True Negative (TN): Normal instances detected as normal instances
- False Positive (FP): Normal instances detected as attack instances
- False Negative (FN): Attack instances detected as normal instances

Table 1. Type of attack

Type of attack	Description
Denial of service (Dos)	Memory resources too busy to accept legitimate users access these resources. Examples of attacks are Smurf, Mailbomb, SYN Flooding, Ping Flooding, Process table, Teardrop, Apache2, Back and Land
Probe (Prb)	Scanning port and host to gather information or find known vulnerabilities. Examples of attacks are Nmap, Satan, Ipsweep, Mscan.
Remote to local (R2L):	Unauthorized access from a remote machine in order to exploit machine's vulnerabilities. Examples of attacks are Ftp_write, Imap, Named, Phf, Sendmail and SQL Injection.
User to root (U2R)	Unauthorized access to local super user (root) privileges using system's susceptibility. Examples of attacks are Loadmodule, Perl, Fdformat.

Table 2. Dataset selection for KDDCup 1999

Connection type	Training dataset	(%)	Testing dataset	(%)
Normal	3000	16.415	60,593	19.48
Dos	10,000	54.69	229,853	73.89
PRB	4107	22.46	4166	1.34
R2L	1126	6.16	16,189	5.2
U2R	52	0.28	288	0.09

Table 3. Redundant record in KDD 1999 training and testing dataset

	Redundand records in KDD 1999 training dataset		
	Original records	Distinct records	Reduction rate (%)
Normal	972,781	812,814	16.44
Anomaly	3,925,650	262,178	93.32
Total	4,898,431	1,074,992	78.05
Normal	60,591	47,911	20.92
Anomaly	250,436	29,378	88.26
Total	311,027	77,289	75.15

1.7. Performance Evaluation

Precision, Recall and F-Value rate for single classifiers as well as hybrid approaches were evaluated by using Equation (7-9):

$$\text{Precision} = \frac{TP}{TP + FP} \quad (7)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (8)$$

$$F - \text{value} = \frac{1 + \beta^2 * \text{Recall} * \text{Precision}}{\beta^2(\text{Recall} + \text{Precision})} \quad (9)$$

Precision, Equation (7), is a measure of the accuracy provided that a specific class has been predicted. Recall, Equation (8), is a measure of the ability of a prediction model to select instances of a certain class from a data set. F-value, Equation (9), is the harmonic mean of precision and recall, which measure the quality of classifications.

10 experiments has been performed followed the existing approach developed from the previous work and produced similar results as it become the baseline to show the comparison betweeen the result of KDD and NSL dataset afterward.

Figure 2a-c illustrates the Precision, Recall and F-value results respectively across all category classes obtained from J48, Bayes, BP and FCNN. Generally, the proposed hybrid approach of FCNN performed better than the single classifier in detecting Normal, Dos, R2L and U2R instances. **Figure 2a** proved that FCNN is considered to more efficient in correctly classifying low frequent attack such as R2L and U2R attack classes. **Figure 2b** shows that FCNN produced slightly better improvement for Normal instances. While the performance for, Dos and Probe instances are almost similar to each other. As for **Fig. 2c** describes that single classifers performed less efficient than the FCNN for low type of attack, while no much different for Normal, Dos and Probe.

1.8. Comparison Over NSL Dataset

As to test the stability of FCNN framework, another dataset has been used; NSL dataset. NSL dataset origins from KDDCup 1999 dataset where all ambuigities and redundant instances has been removed. For analysis, Precision, Recall and F-Value also become the measurement for all instances. Another 10 experiments have been conducted and average result were present as follows:

1.9. Precision Comparison for Standard Dataset over NSL Dataset

Figure 3, shows that hybrid approach of FCNN with NSL dataset performed better for probe attack and have slightly improvement on low frequent type of attack. It looks like FCNN not seems stable in recognizing probe attack on different type of dataset, because the FCNN framework only bother to low frequent type of attack; U2R and R2L, since these two types of attack consume most damages compared to others.

1.10. Recall of FCNN againts NSL-FCNN

Table 4 summarized the experimental results which evaluate the Recall value of the proposed approach using standard dataset against againts NSL dataset.

Table 4. Recall for FCNN using standard dataset Vs NSL dataset

Recall for standard dataset Vs NSL dataset on FCNN framework	Type of attack				
	Normal (%)	Dos (%)	Probe (%)	R2L (%)	U2R (%)
FCNN	99.5	97.9	88.0	46.8	87.9
NSL-FCNN	98.2	99.1	94.1	78.0	89.0

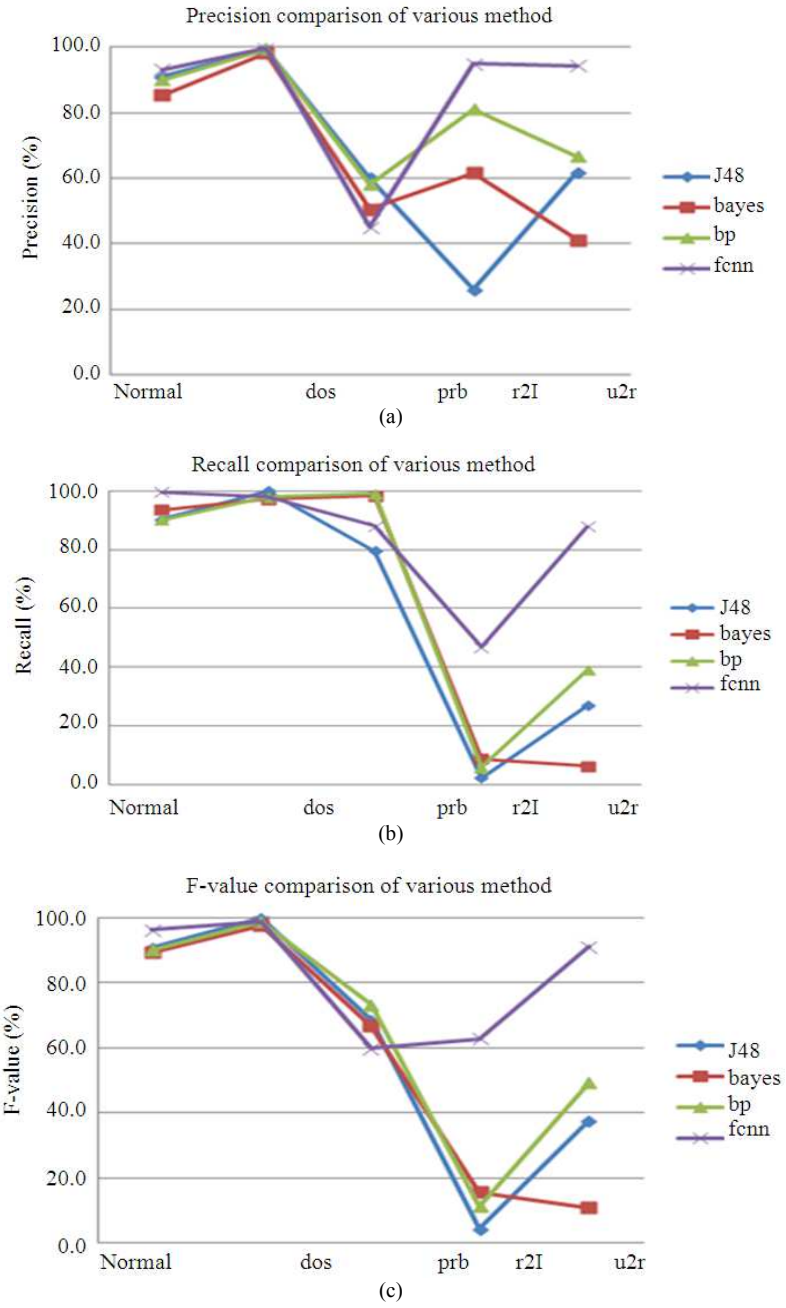

Fig. 2. (a) Precision Comparison (b) Recall Comparison (c) F-Value Comparison

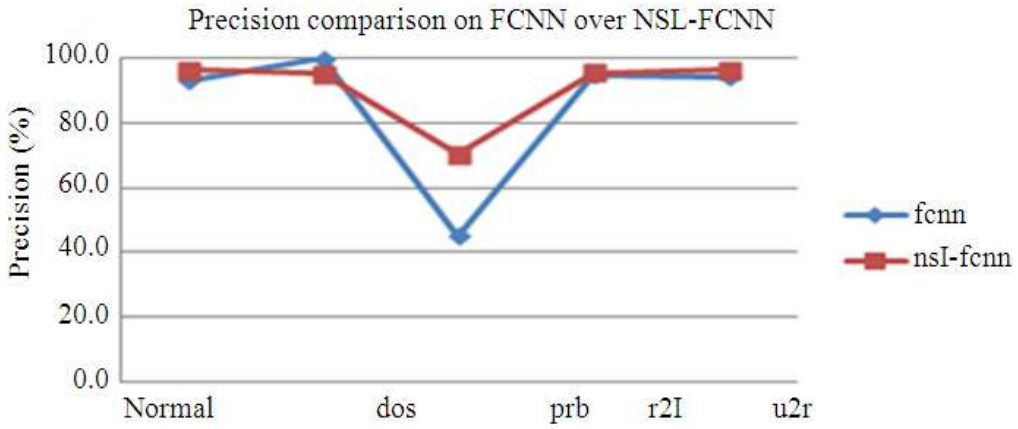

Fig. 3. Precision Comparison for standard dataset over NSL dataset

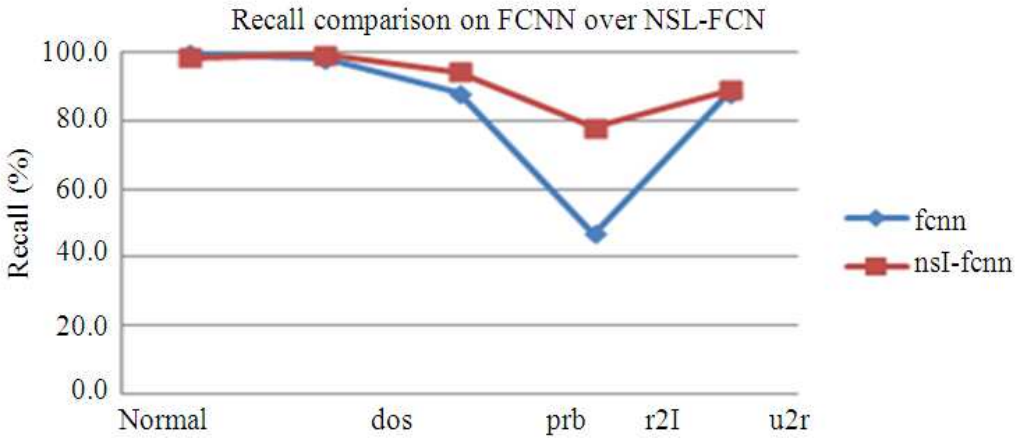

Fig. 4. Recall comparison for standard dataset over NSL

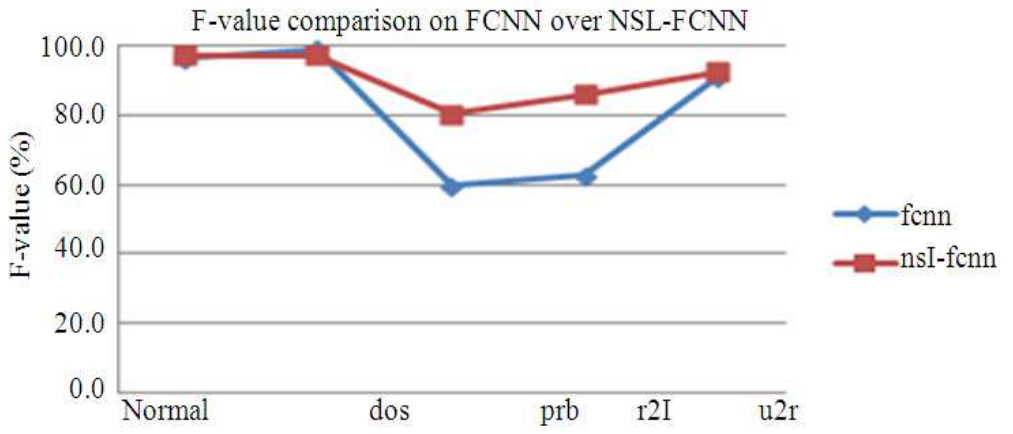

Fig. 5. F-Value Comparison for standard dataset over NSL dataset

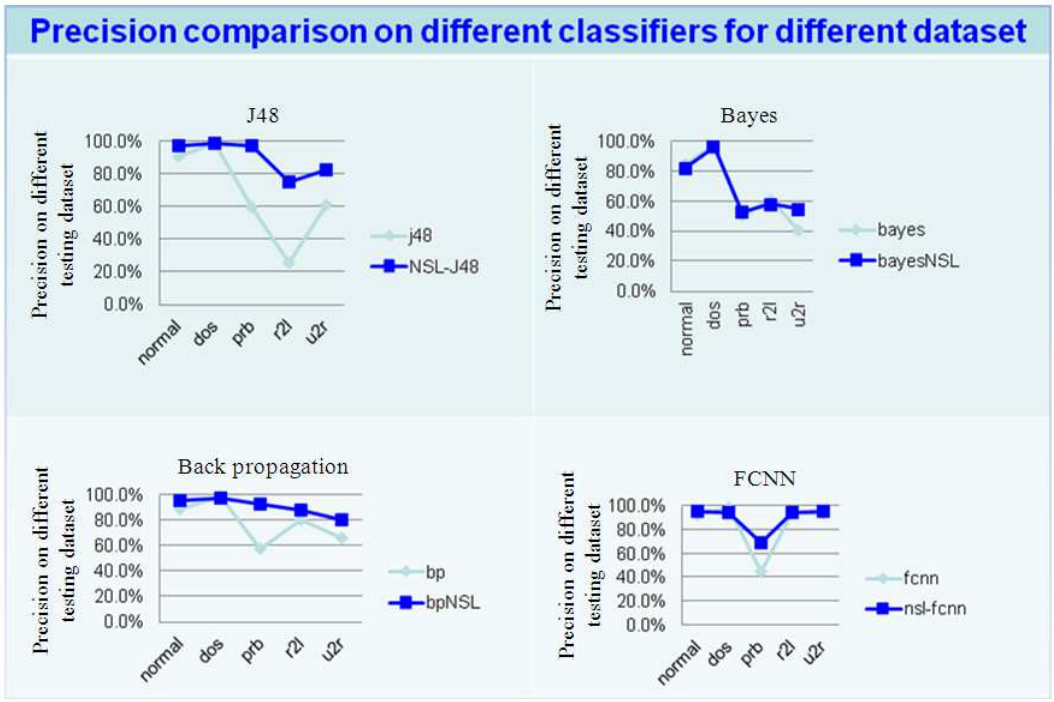

Fig. 6. Precision Comparison for Different Classifiers on standard dataset over NSL dataset

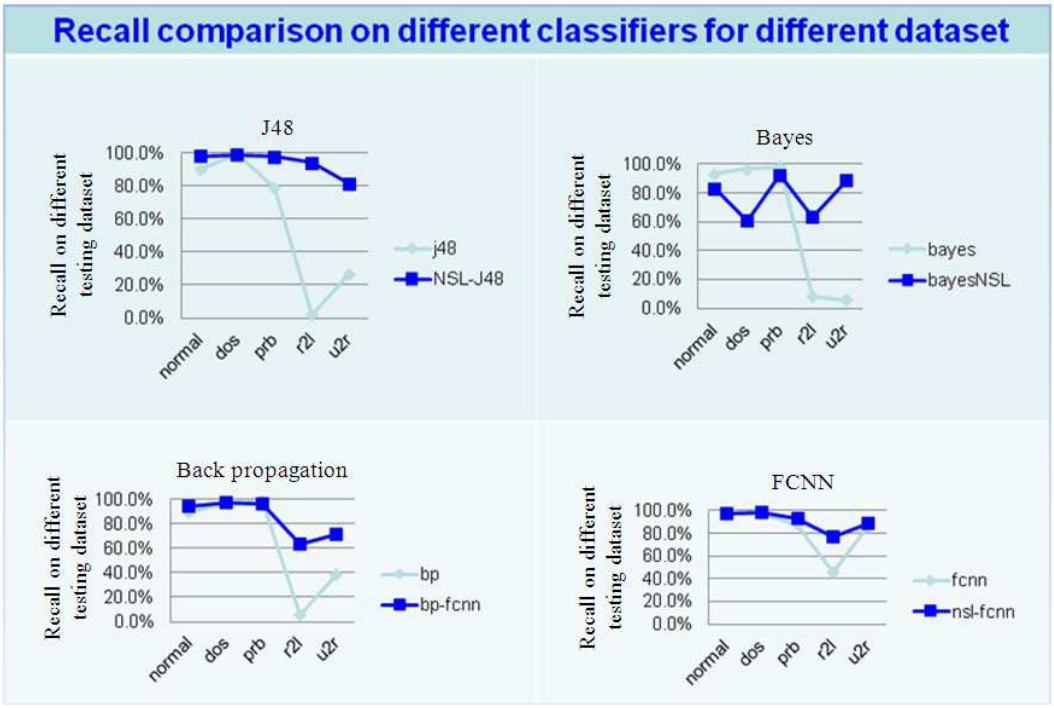

Fig. 7. Recall comparison for different classifiers on standard dataset over NSL dataset

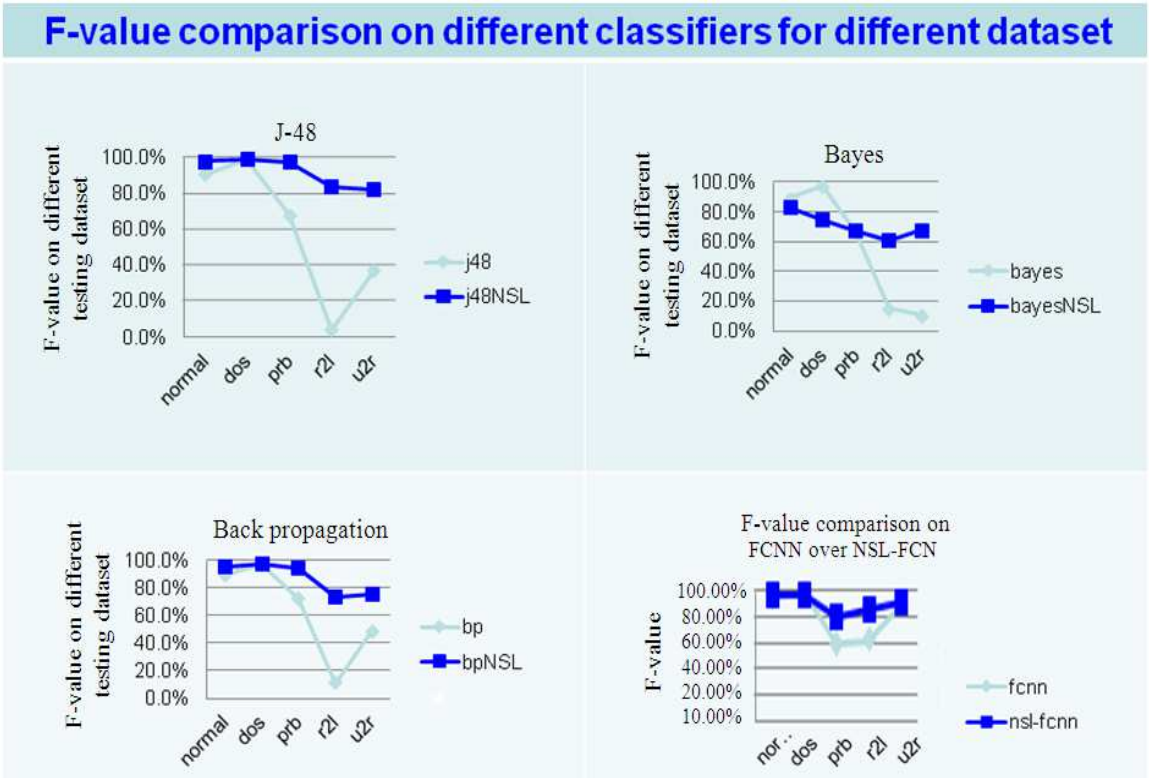

Fig. 8. F-Value comparison for different classifiers on standard dataset over NSL dataset

1.11. Recall Comparison for Standard Dataset over NSL Dataset

As for **Fig. 4 and 5** Recall value for hybrid approach of FCNN with NSL dataset performed a slightly better for U2R type of attack and have improvement for probe and R2L type of attack. There are few records that fall under R2L and U2R type of attack to be train and enormous redundant records in the testing KDDcup 1999 dataset, had prevent FCNN from recognizing rare attack records that fall under U2R and R2L categories. Since dimensionality of reduction have been applied on NSL dataset, it has remove until 78% reduction rate in training dataset and up to 75% reduction rate on testing dataset over compared to the standard dataset.

1.12. F-Value Comparison for Standard Dataset over NSL Dataset

1.12.1. Precision Comparison on Different Classifiers for Different Dataset (Standard KDDCup Dataset Againts NSL Dataset)

We also conduct experiment by using NSL dataset with single classifier; J48, Naive Bayes and Backpropagation Neural Network to support the increasing result found by the FCNN framework previously.

As mentioned earlier, NSL dataset has removed the redundancy exists in the KDD dataset. By using the same aproach of the experiment, we found better result which at the same time supports the strenght of the previous framework. **Figure 6-8** shows the result of Precision, Recall and F-value respectively for NSL dataset using four different approaches. It does really shows that most of all single classifiers itself also perform outstanding result for each measurement, especially for low frequent type of attack; R2L and U2R if compared with KDD datasets result, **Fig. 2-2c** previously. Tavallaee *et al*. (2009) defines that the redundancy in KDD dataset caused the problem of learning algorithm that biased towards the most frequent records, which at the same time the evaluation results also biased by the methods (usually for records that fall under U2R and R2L categories) which have better detection rates on the frequent records.

2. CONCLUSION

In this study, we have proposed the used of NSL dataset instead of KDD dataset implementation over the existing framework of Fuzzy Clustering Neural Network, as a new variant to classify anomalous and normal activities compared to single classifiers. Nonetheless, the initial problem to deal with high poor accuracy and low detection rate has been resolved by the proposed hybrid technique. Using NSL dataset with hybrid mining approach, achieved detection of precision higher than 90% while keeping the recall rate on average higher than 80%. As for harmonic mean value NSL dataset shows increament over 90%, compared to original KDD dataset.

In general, the technique of existing Fuzzy Clustering Neural Network showed good result in order to overcome the limitation of single Neural Network classification especially to detect the low frequent attack. By applying NSL dataset using the approach, there are increments in the detection, because the redundancy and uncertain data in the original KDD dataset has been remove.

3. REFERENCES

Alpaydın, E., 2010. Introduction to Machine Learning. 2nd Edn., MIT Press, Cambridge, ISBN-10: 9780262012430 pp: 584.

Al-Wesam, K., R. AL-Rashdan, W. Naoum, S. Al_Sharafat and M.K. Al-Khazaaleh, 2010. Novel network intrusion detection system using hybrid neural network (hopfield and kohonen som with conscience function). Int. J. Comput. Sci. Network Security, 10: 10-13.

Anderson, J.P., 1980. Computer security threat monitoring and surveillance.

Anderson, J.P., 1995. An introduction to neural networks. 3rd Edn., MIT Press, Cambridge, ISBN-10: 0262011441, pp: 672.

Ashwin, K. and K. Avinash, 2009. Rough set approach for overall performance improvement of an unsupervised ann-based pattern classifier. J. Adv. Comput. Intell. Intell. Inform., 13: 434-440.

Bhavin, S. and H.T. Bhushan, 2012. Artificial neural network based intrusion detection system: A survey. Int. J. Comput. Appli., 39: 13-18. DOI: 10.5120/4823-7074

Borji, A., 2007. Combining heterogeneous classifiers for network intrusion detection. Proceedings of the 12th Asian computing science conference on Advances in computer science on Computer and Network Security, (ASIAN' 07), Springer-Verlag Berlin, Heidelberg, pp: 254-260.

Chen, Y., A. Abraham and B. Yang, 2007. Hybrid flexible neural-tree-based intrusion detection systems. Int. J. Intell. Syst., 22: 337-352. DOI: 10.1002/int.20203

Chih-Fong, T., H. Yu-Feng, L. Chia-Ying and L. Wei-Yang, 2009. Intrusion detection by machine learning: A review. Expert Syst. Appli., 36: 11994-12000. DOI: 10.1016/j.eswa.2009.05.029

Chung, A., 2011. On testing of implementation correctness of protocol based intrusion detection systems. Proceedings of the 9th International Conference onSoftware Engineering Research, Management and Application, Aug. 10-12, IEEE Xplore Press, Baltimore, MD., pp: 171-174. DOI: 10.1109/SERA.2011.26

Dorothy, E.D., 1987. An intrusion-detection model. IEEE Trans. Software Eng., 13: 222-232. DOI: 10.1109/TSE.1987.232894

Dunn, J.C., 1973. A fuzzy relative of the isodata process and its use in detecting compact well-separated clusters. J. Cybernetics, 3: 32-57. DOI: 10.1080/01969727308546046

Endorf, C., E. Schultz and J. Mellander, 2004. Intrusion Detection and Prevention. 1st Edn., McGraw-Hill, California, ISBN-10: 0072229543, pp: 386.

Fukuyama, Y. and M. Sugeno, 1989. A new method of choosing the number of clusters for the fuzzy c-means method. Proceedings of the 5th Fuzzy System Symposium, (FSS' 89).

George, H.J., 1995. Estimating continuous distributions in bayesian classifiers. Proceedings of the Eleventh conference on Uncertainty in Artificial Intelligence, (UAI' 95), Morgan Kaufmann Publishers Inc. San Francisco, CA, USA., pp: 338-345.

Giuseppina, G., M.C. Viorel and C. Konig, 2004. Combining unsupervised and supervised artificial neural networks to predictaquatic toxicity. J. Chem. Inform. Comput. Sci., 44: 1897-1902. DOI: 10.1021/ci0401219

Horeis, T., 2003. Intrusion detection with neural network-Combination of selforganizing maps and redial basis function networks for human expert integration.

Jakir, H., A. Rahman, S. Sayeed, K. Samsuddin and F. Rokhani, 2011. A modified hybrid fuzzy clustering algorithm for data partitions. Australian J. Basic Applied Sci., 5: 674-681.

James, C.B., 1981. Pattern Recognition with Fuzzy Objective Function Algorithms. 1st Edn., Plenum Press, New York, pp: 256.

John, M., 2000. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Trans. Inform. Syst. Security, 3: 262-294. DOI: 10.1145/382912.382923

John, M., A. Christie and J. Allen, 2000. Defending yourself: The role of intrusion detection systems. IEEE Software, 17: 42-51. DOI: 10.1109/52.877859

Kartit, A. A. Saidi, F. Bezzazi, M. El Marraki and A. Radi, 2012. A new approach to intrusion detection system. J. Theoretical Applied Inform. Technol. Network Security, 36: 1817-3195.

Kusum, K., S.S. Bharti and S. Jain, 2010. Intrusion detection system using clustering. Proceedings of the International Conference, (IC' 10).

Leo, B., 1999. Random forests. University of California, Berkeley.

Lodin, S., 1998. Intrusion detection product evaluation criteria. CiteSeerX.

Mehdi, B. and B. Mohammad, 2012. An overview to software architecture in intrusion detection system. Int. J. Soft Comput. Software Eng. DOI: 10.7321/jscse.v1.n1.1

Mehdi, M. and M. Zulkernine, 2011. A Neural Network Based System for Intrusion Detection and Classification of Attacks. University of British Columbia.

Mrutyunjaya, P., A. Abraham and M.R. Patra, 2010. Discriminative multinomial Naïve Bayes for network intrusion detection. Proceedings of the Sixth International Conference Information Assurance and Security, Aug. 23-25, IEEE Xplore Press, Atlanta, GA., pp: 5-10. DOI: 10.1109/ISIAS.2010.5604193

Mukhopadhyay, I., 2011. Back propagation neural network approach to intrusion detection system. Proceedings of the International Conference on Recent Trends in Information Systems, Dec. 21-23, IEEE Xplore Press, Kolkata, pp: 303-308. DOI: 10.1109/ReTIS.2011.6146886

Muna, M., T. Jawhar and M. Mehrotra, 2009. Design network intrusion system using hybrid fuzzy neural network. Department of Computer Science, Jamia Millia Islamia New Delhi.

Muna, M., T. Jawhar and M. Mehrotra, 2012. A hybrid FCM clustering-neural network for intrusion detection. Department of Computer Science, Jamia Millia Islamia New Delhi.

Nicholas, J., P.K. Zhang, M. Chung, B. Mukherjee and R.A. Olsson, 1996. A Methodology for testing Intrusion Detection System. IEEE Trans. Software Eng., 22: 719-729. DOI: 10.1109/32.544350

Novikov, D., V.Y. Roman and L. Reznik, 2006. Anomaly detection based intrusion detection. Proceedings of the Third International Conference on Information Technology: New Generations, Apr. 10-12, IEEE Xplore Press, Las Vegas, NV., pp: 420-425. DOI: 10.1109/ITNG.2006.33

Ozgur, D., M. Topallar, E. Anarim and M.K. Ciliz, 2005. An intelligent Intrusion Detection System (IDS) for anomaly and misuse detection in computer networks. Expert Syst. Applications, 29: 713-722. DOI: 10.1016/j.eswa.2005.05.002

Rachid, B., 2008. Critical study of neural networks in detecting intrusions. Comput. Sec., 27: 168-175. DOI: 10.1016/j.cose.2008.06.001

Ritu, R.S., N. Gupta and S. Kumar, 2011. To reduce the false alarm in intrusion detection system to reduce the false alarm in intrusion using self organizing map. Int. J. Soft Comput. Eng.

Robert, C.H., 1993. Very simple classification rules perform well on most commonly used datasets. Mach. Learn., 11: 69-90. DOI: 10.1023/A:1022631118932

Sandeep, V.S., 2008. Computer security: Machine learning approach. Department of Mathematics Royal Holloway, University of London.

Sang-Jun, H. and C. Sung-Bae, 2005. Evolutionary neural networks for anomaly detection based on the behavior of a program. IEEE Trans. Syst. Man Cybernetics 36: 559-570. DOI: 10.1109/TSMCB.2005.860136

Shilpa, L., S. Joseph and B. Verma, 2010. Feature Reduction using Principal Component Analysis for Effective Anomaly–Based Intrusion Detection on NSL-KDD. Int. J. Eng. Sci. Technol., 2: 1790-1799.

Simon, H., 1999. Neural Networks: A Comprehensive Foundation. 2nd Edn., Prentice Hall, ISBN-10: 0132733501, pp: 482.

Srinivas, M., H.S. Andrew and A. Abraham, 2005. Intrusion detection using an ensemble of intelligent paradigms. J. Network Comput. Applic., 28: 167-182. DOI: 10.1016/j.jnca.2004.01.003

Stallings, W., 2006. Cryptography and Network Security: Principles and Practices. 4th Edn., Prentice Hall, Upper Saddle River, N.J., ISBN-10: 0131873164, pp: 680.

Suguna, J. and A.M. Selvi, 2012. Ensemble fuzzy clustering for mixed numeric and categorical data. Int. J. Comput. Appli., 42: 19-23. DOI: 10.5120/5673-7705

Tavallaee, M., E. Bagheri, W. Lu and A.A. Ghorbani, 2009. A detailed analysis of the KDD CUP 99 data set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, Jul. 8-10, IEEE Xplore Press, Ottawa, ON., pp: 1-6. DOI: 10.1109/CISDA.2009.5356528

Tie-Jun, Z.Z., 2008. The research of intrusion detection based on genetic neural network. Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition, Aug. 30-31, IEEE Xplore Press, Hong Kong, pp: 276-281. DOI: 10.1109/ICWAPR.2008.4635789

Vladimir, N.V., 1995. The Nature of Statistical Learning Theory. 2nd Edn., Springer, New York, ISBN-10: 0387945598, pp: 188.

Wang, G., J. Hao, J. Ma and L. Huang, 2010. A new approach to intrusion detection using Artificial Neural networks and fuzzy clustering. Expert Syst. Appli., 37: 6225-6232. DOI: 10.1016/j.eswa.2010.02.102

Xindong, W., V. Kumar and J.R. Quinlan, 2008. Top 10 algorithms in data mining. Knowl. Inform. Syst., 14: 1-37. DOI: 10.1007/s10115-007-0114-2