Performance Evaluation of Intrusion Detection Systems using ANN

Khaled Ahmed Abood Omer[1], Fadwa Abdulbari Awn[2]

[1]Computer Science and Engineering Department,
Faculty of Engineering, University of Aden, Yemen

[2]Information Technology Engineering Department
Faculty of Engineering, University of Aden, Yemen

k_abood@hotmail.com, f.awn@hotmail.com

Abstract

During the last decades, Intrusion Detection System (IDS) has attracted the attention of researchers to provide security for sensitive information that is communicated via unsecure transmission media. There are two main types of IDS based on detection process which are anomaly-based and misuse-based. In this paper, we have evaluated the performance of both IDS systems using Artificial Neural Network (ANN) where Feed Forward Neural Network (FFNN) and Back Propagation Algorithm (BPA) are used for training ANN. Selected records from KDD CUP'99 dataset are used for the training and testing both IDS systems. The obtained experimental results show that the anomaly-based IDS system outperforms the misused- based IDS system based on the classification rate, detection rate and false negative error.

Keywords: *Anomaly and misused IDS, ANN, KDD CUP'99 dataset*.

1. Introduction

Nowadays, information security becomes a major issue due to wide spread of the network and Internet that are considered as unsecure communication media. From this point of view, security participants focus their efforts to provide best method to implement information security. One of these methods is Intrusion Detection System (IDS). IDS provides protected environment for organizations that rely on Internet and networks as the principle media for communications.

An IDS is a software with the functions of detecting, identifying and responding to an unauthorized or abnormal activities on a target system [1, 2, 3]. IDS is used by organizations to provide security for the valuable information resources (information assets) and to ensure secure communications to normal users since the main purpose of IDS is to distinguish between intruders and normal users[1, 4].

There are two primary types of IDS based on events analysis to detect attacks:

- **Anomaly-based IDS**: IDS detects intrusions by searching "abnormal" network traffic [2].
- **Misuse-based IDS**: IDS detects intrusions by looking for activity that corresponds to known signatures of intrusions or vulnerabilities [5].

The first type defines a certain model of a user normal activity such that any deviation from this model is classified as anomalous, whereas the second type operates with priori prepared patterns (signatures) of known attacks that are used to identify intrusions [6]. The anomaly detection has the advantage of detecting new intrusions while misuse detection cannot detect new intrusions whose signatures are unknown. However, the anomaly detection technique may have significant number of false alarms because the legitimate user's behavior changes widely and obtaining complete description of normal behaviors is often difficult [7]. On the other hand, the misuse detection technique has high number of false negative error because the unknown attacks are considered as normal [8].

Unfortunately IDS has some errors that poorly affect the organization security. These errors are mainly classified into two types: false positive errors and false negative errors. The false positive errors occur when the IDS misclassifies normal packets or activities as an attack. This error degrades the productivity of the systems by invoking unnecessary countermeasures. On the other hand, false negative errors occur when IDS accepts an attack as a normal activity. False negative errors cause great losses for organizations which are connected to the systems by networks. The risk of false negative errors is higher than the risk for false positive errors [9].

This paper addresses the performance evaluation of IDS systems for detecting attacks by using a selected records from KDD CUP'99 dataset [10] using Artificial Neural Network (ANN). Therefore, in this work the normal traffic, known attacks and unknown attacks were applied to ANN representing both IDS systems to compare the detection efficiency of these systems. The next section reviews the related work regarding IDS and describes the used dataset based on KDD CUP'99 dataset. Section 3 discusses the experiments and the results. Finally, Section 4 concludes the work.

2. Related Work

The ANN is the most commonly used soft computing technique in Intrusion Detection Systems. Saravanakumar et. al. [11] discussed the effect of different neural network structures on IDS. They compared the performance of different methods using ANN to implement a new combination of ANN algorithm which would be efficient in detecting intrusion in a networked environment.

Muthukkumarasamy et. al. developed a security mechanism that can intelligently detect both known and unknown attacks to solve the problems of IDS [7]. The problems are inability to detect totally unknown attacks, too many false positives, and slow response time. The proposed system was based on ANN with BPA.

Alsharafat identified important input features in building IDS system to gain better Detection Rate [12]. The author implemented the IDS using ANN and used eXtended Classifier System (XCS) with internal modification for classifier generator. The experimental results show that the XCS-ANN is an effective method that can be used to improve the attack detection rate and reduce the false alarm rate.

Pradhan et. al. experimented the user behavior as parameters in IDS [13]. They introduced the Anomaly Detection System using BPA for ANN to see if ANN has the ability to classify normal traffic correctly and detect known and unknown attacks without using a huge amount of training data. They got a classification rate of 88% on known and unknown attacks.

Daejoon et. al. compared different types of errors to enhance the IDS performance [9]. They minimized the loss for an organization under an open network environment using ANN. The study analyzed the cost-effectiveness of the two types of error in order to discover which one has the great impact on the network security.

Cannady presented an approach to the process of misuse detection [14]. This approach is based on the use of rule-based expert systems to identify indications of known attacks by the means of the analytical strengths of neural networks in order to identify and classify network activity. The used prototype utilized a Multi Layers Perceptron (MLP) architecture that consisted of four fully connected layers. The final result is a two class classifier that succeeded in classification of normal and attack records in 89-91% of the cases.

Moradi et. al. [15] applied the concept of MLP for misused IDS in order to solve a multi class problem in which the type of attack is also detected by the neural network. The final result showed that the designed system was capable of classifying records with about 91% accuracy with two hidden layers of neurons in the neural network and 87% accuracy with one hidden layer.

Varma et. al. produced a 15 class classifier to implement the concept of misused intrusion detection, where 14 different types of attacks and normal user can be detected [16]. The results showed that MLP neural network has proved to implement a multiclass classification problem efficiently even with 15 classes such that the average detection rate was 86.28%.

Tesfahun et. al. presented a hybrid layered IDS by combining both misused and anomaly IDS [17]. This system detects known and unknown attacks. They used random forests classifier to detect known attacks. They built the anomaly detector by using bagging technique, to detect unknown attacks. The experimental results showed that the proposed system is very effective in improving detection rate with small false positive rate.

3. Experimentation and Results:

In this section, we discuss the dataset used to test and evaluate both IDS systems. Next we implement the two IDS systems using ANN and discuss the results.

3.1 KDD CUP'99 Dataset Description

DARPA dataset is the most popular dataset used to test and evaluate IDS systems [10]. The KDD CUP'99 dataset is a subset of DARPA dataset [18]. The dataset was preprocessed by extracting 41 features from the tcpdump data in the 1998 DARPA dataset. The KDD CUP'99 dataset consists of 41 features for each packet [18]. In order to use these records for ANN, the dataset was pre-processed to contain only numerical values, but not string values.

The KDD CUP'99 dataset consists of normal and several attacks records, where the attacks are classified based on the goals and actions of the attacker, according to that, attack type falls into one of the following four main categories:

- **Denials-of Service (DoS)** attacks have the goal of limiting or denying services provided to the legitimate users. Here the attacker tries to send some malicious packets (TCP, UDP, or ICMP) to fill up the memory or to keep the computing resource very busy. Attacks used are Smurf, Teardrop, Neptune, Land and Back.

- **Probing or Surveillance** attacks have the goal of gaining knowledge of existence or configuration of a computer system or network [6]. Attacks used are IPsweep, Mscan, Port sweep and Satan.
- **User-to-Root (U2R)** attacks have the goal of gaining root or super-user access on a particular computer or system on which the attacker already had normal user access. Attacks used are Buffer overflow and Xterm.
- **Remote-to-Local (R2L)** attack where the attacker who does not have any account on the target machine, tries to gain the access of that machine by exploiting this machine vulnerabilities. Attacks used are Warezmaster, Warezclient, Xclock, Guess_password, Snmpgetattack and Snmpguess.

3.2 Experimentation

MATLAB 7.6 [19] has been used for the implementation of FFNN network with BPA ANN. MATLAB supports a great library used for ANN to create such network and define specifications like number of layers, number of neurons in each layer and activation functions of neurons for each layer.

Both anomaly–based and misuse–based IDS systems are implemented by conducting the following steps:

- Select a random dataset as collection of random records from KDD CUP'99 dataset with 41 attributes per record. For heterogeneity in data, the data is collected randomly from two files namely 10% KDD and corrected that consist normal and attacks traffic (14 different attacks are selected).
- Preprocess the dataset, in order to use it with ANN, such that all records contain only numeric values.
- Create FFNN for 2 layers, 3 layers, and 4 layers with optimal number of neurons for each hidden layer.
- Train the network with the selected dataset using BPA [20].
- Test the network.

The 41 attributes of the selected dataset are fed as input to the created FFNN for both IDS systems such that the input layer consists of 41 neurons. The output layer of anomaly–based IDS consists of two neurons one is used to represent normal and the other is used to represent attacked traffic. If the input record is classified as normal traffic then the neuron representing normal traffic will set to one and the neuron representing attacked traffic will be zero, i.e. the output of the network would be 1 0. But if the input record is classified as an attack then the neuron representing normal traffic will be zero and the neuron representing attacked traffic will be set to one, i.e. the network output would be 0 1. The output layer of misuse–based IDS consists of fifteen neurons first one is used to represent normal and the others are used to represent and identify the attacked traffic.

We used different numbers of hidden layers to increase the classification rate of the system because increasing the number of hidden layers increases the efficiency of the system. Mean square error (MSE) is used with BPA to measure the network performance [21, 22].

The performance study of IDS is affected mainly by the overall classification rate (accuracy) and the error percentage, the following formula is used to calculate the classification rate [13]:

$$Overall\ Classification\ Rate = \frac{TP + TN}{TP + FP + TN + FN}.$$

$$= \frac{No.\ Correct\ Classification}{No.\ All\ Classification}$$

Where :

- TP (True Positive): classifying an intrusion activity as intrusion. The true positive rate is identical with *detection rate, sensitivity* and *recall*.
- FP (False Positive): incorrectly classifying normal activity as an intrusion. Also known as a *false alarm or False Positive Error*.
- TN (True Negative): correctly classifying normal activity as normal. The true negative rate is also referred to as *specificity*.
- FN (False Negative): incorrectly classifying an intrusion activity as normal. Also known as a *False Negative Error*.

In this work, we consider increasing overall classification rate and the detection rate; and decreasing the false negative errors since it has a great impact on the organization security as compared with previous work [13].

In this work, the experimentation is performed in three phases as follows:

Phase One: Train the ANN network for both IDS with normal and known attacks.

Phase Two: Test the ANN network with normal and known attacks.

Phase Three: Test the ANN network with mixed data of normal, known and unknown attacks.

Phase one: Train the ANN network with normal and known attacks

In this phase, the experiments are conducted by using 2095 records of selected dataset from KDD CUP'99 with 41 attributes per record. These records consist of normal records and different types of attack records (Snmpgetattack, Smurf, IPsweep, Satan, Portsweep, Neptune, Guess_Password, Land, Buffer _overflow, Warezmaster, Back, Warezclient, Mscan and Teardrop). This selected dataset is used for training of the neural network and for testing the neural network with known attacks.

First FFNN network is used for both IDS types anomaly-based and misuse-based that consists of 2 layers, one hidden layer and an output layer. This network is trained until sufficient result is achieved, then the network is tested with the trained dataset and the result is collected. Similarly the same steps are repeated for 3 layers and 4 layers respectively.

Figure 1 shows the detection rate with respect to the number of hidden layers for anomaly–based IDS (AID) and misuse–based IDS (MID) IDS systems. In this figure, the detection rate increases as the number of layers increases. The anomaly–based IDS (AID) performs better than misuse–based IDS (MID).

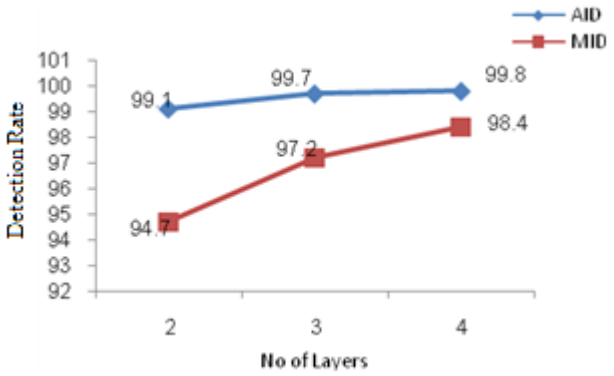

Figure1: Detection Rate of both IDS types with respect to No. of layers during training phase

In figure 2, the overall classification rate with respect to the number of hidden layers is shown. The highest overall classification rate is acquired by anomaly-based IDS.

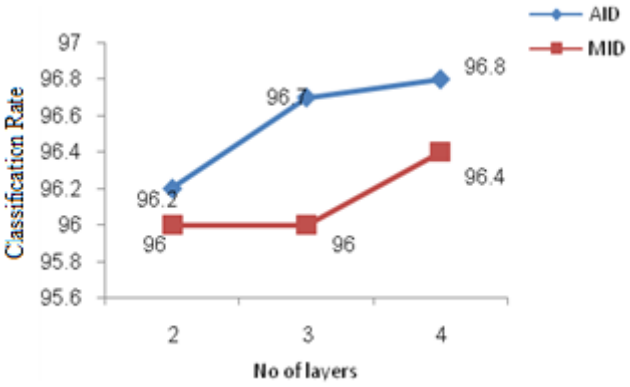

Figure 2: Classification Rate of both IDS types with respect to No. of layers during training phase

Figure 3 shows that the false negative error decreases with the increase of number of layers. Also it is clear that anomaly-based IDS outperforms misuse-based IDS system.

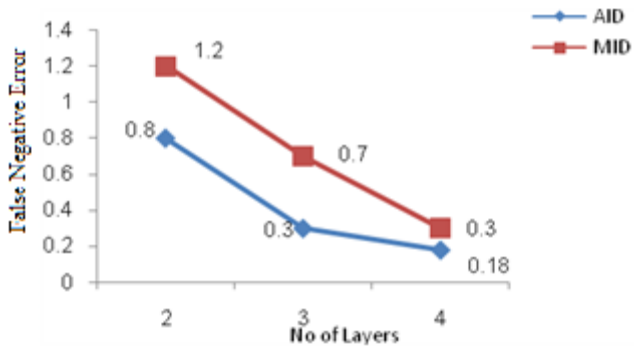

Figure 3: False Negative Error of both IDS types with respect to No. of layers during training phase

Phase Two: Test the ANN network with normal and known attacks.

In order to test the ability of the FFNN network to detect the attacks that the network was trained to detect, new dataset is used. This dataset consists of mixed data of 474 records of normal and known attacks (attacks used for training).

First the FFNN with 2 layers is tested for anomaly-based and misuse-based IDS systems. This network is trained as in phase one above, then the network is tested with the new dataset and the result is collected. Similarly the same steps are repeated the FFNN for 3 layers and 4 layers respectively.

Figure 4 shows that the detection rate increases as the number of layers increases. Also the anomaly-based IDS performs better than misuse-based IDS.

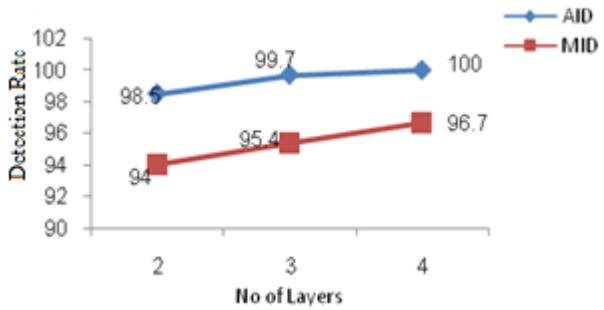

Figure 4: Detection Rate of both IDS types with respect to No. of layers during test phase

Figure 5 shows that the overall classification rate increases with the increase of number of hidden layers. Also the anomaly-based IDS performs better than misuse-based IDS.

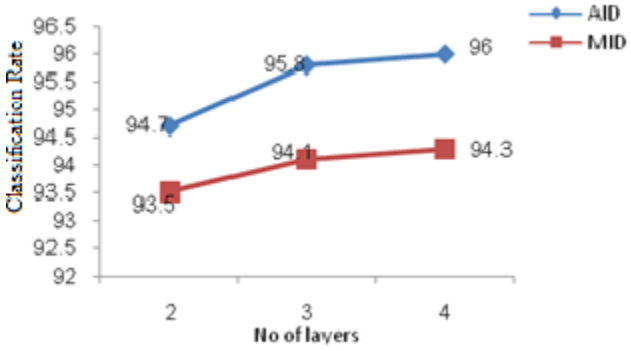

Figure 5: Classification Rate of both IDS types with respect to No. of layers during test phase

Figure 6 shows that the false negative error decreases with the increase of number of layers. Also the anomaly-based IDS performs better than misuse-based IDS system since it has small FNE percentage.

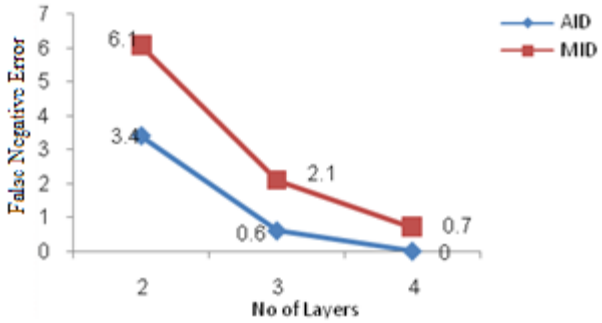

Figure 6: False Negative Error of both IDS types with respect to No. of layers during test phase

We note that the anomaly-based IDS of third network that consists of 4 layers gives the best results according to detection rate, overall classification rate and the false negative error.

Phase Three: Test the ANN network with mixed data (normal known and unknown attacks).

In order to test the ability of the FFNN network to detect new or fresh attacks, new dataset is used. This dataset consists of mixed data of normal, known and unknown attacks. This dataset contains 496 records of normal records and known attacks (attacks used for training) and three new types of attacks (xlock , xterm and Snmpguess) that our FFNN network was not trained to detect them.

First the FFNN within 2 layers is used. This network is trained as in phase one above. Then the network is tested with the new mixed dataset and the result is collected. Similarly the same steps are repeated the FFNN for 3 layers and 4 layers respectively for both IDS systems.

In figure 7, the detection rate with respect to the number of hidden layers is shown. In this figure, the detection rate increases as the number of layers increases. The anomaly-based IDS has better detection rate than that of misuse-based IDS.

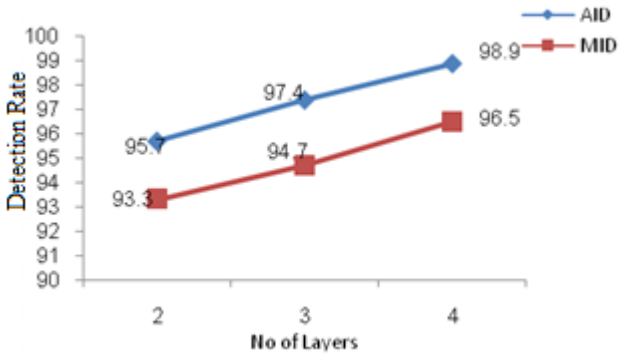

Figure 7: Detection Rate of both IDS types with respect to No. of layers during test phase with mixed data

Figure 8 shows that anomaly-based IDS outperforms misuse-based IDS. Also the overall classification rate increases with the increase of number of hidden layers.

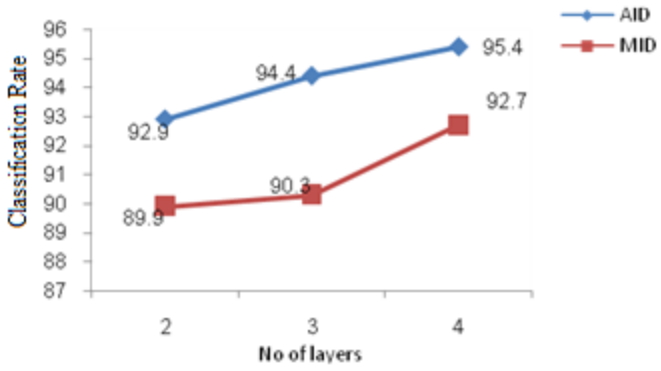

Figure 8: Classification Rate of both IDS types with respect to No. of layers for test phase with mixed data

Figure 9 illustrates that the false negative error decreases with the increase of number of layers. Also it indicates that the misuse-based IDS has high FNE values compared to that of anomaly-based IDS. Therefore, the best result is achieved with anomaly-based IDS using the third network with 3 hidden layers and 1 output layer, since it has small FNE percentage.

The anomaly-based IDS third network that consists of 4 layers gives the best results according to detection rate, overall classification rate and the false negative error. These results confirm the ability of our proposed anomaly-based IDS FFNN network with BPA to detect new attacks whose profiles are unknown.

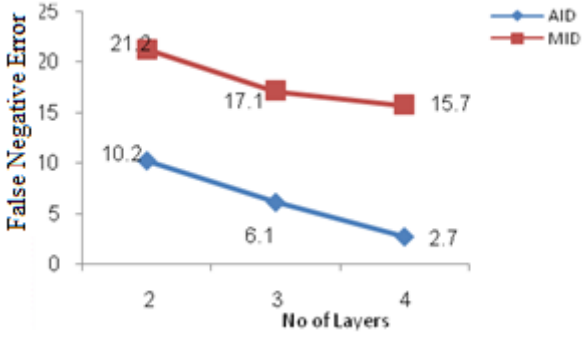

Figure 9: False Negative Error of both IDS types with respect to No. of layers for test phase with mixed data

4. Conclusion

In this work, we have evaluated the performance of anomaly-based and misuse-based IDS systems using ANN network. We have used ANN network to implement these IDS systems with selected records from KDD CUP'99 dataset. From the obtained experimental results, we have found that anomaly-based IDS system outperforms misuse-based IDS system with respect to classification rate, detection rate, and false negative error. Further, the results show that increasing the number of hidden layers with optimal number of neurons per layer, increases the performance of the network.

References

[1]. D. Denning, "An intrusion detection model ", IEEE Transactions Software Engineering, Vol. SE-13, No. 2, , February 1987, pp. 222–232.

[2]. M. Gordeev, "Intrusion Detection: Techniques and Approaches", http://www.forumintrusion.com /archive, August 2003, pp. 2 -13.

[3]. K. Richards, " Network based intrusion detection: a review of Technologies", Computer and Security, Vol. 18, 1999 pp. 671–682.

[4]. E. M. Fawwaz, M. M. Abd-Eldayem, G. Darwish, " Model-Based Clustring Framework For Intrusion Detection in Ad Hoc Networks", Egyptian Computer Science Journal, Vol. 30 No 3, 2008.

[5]. J. Planquart, "Application of Neural Networks to Intrusion Detection", SANS Institute InfoSec, 2001.

[6]. M. Panda and M. Patra , "Network Intrusion Detection Using Naive Bayes", International Journal of Computer Science and Network Security IJCSNS, Vol. 7 No. 12, December 2007, pp 253-26.

[7]. V. Muthukkumarasamy and R. Birkely, "An Intelligent Intrusion Detection System Based On Neural Network", In Proc. Int. Conf. on Applied Computing IADIS, 2004, pp. 221-228.

[8]. M. Solomon and M. Chapple, "Information Security Illuminated", Jones and Bartlett, 2005.

[9]. J. Daejoon, T. Hongb, and I. Hanc, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors", Pergamon, Expert Systems with Applications, 2003, 25, pp. 69–75.

[10]. KDD 1991 datasets. The UCI LDD Archive, http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html, Irvine, CA, USA, 1999.

[11]. S. Saravanakumar, A. Kumar, S. Anandaraj and S. Gowtham, "Algorithms Based on Artificial Neural Networks for Intrusion Detection in Heavy Traffic Computer Networks", In Proc. Int. Conf. on Advancements in Information Technology, 2011.

[12]. W. Alsharafat, "Applying Artificial Neural Network and eXtended Classifier System for Network Intrusion Detection", The International Arab Journal of Information Technology, Vol. 10, No. 3, May 2013 pp. 230-238.

[13]. M. Pradhan, S. Pradhan and S. Sahu,"Anomaly Detection Using Artificial Neural Network", International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, April 2012 pp. 29-36.

[14]. J. Cannady," Artificial neural networks for misuse detection", In Proc. Conf. on the National Information Systems Security (NISSC'98), Arlington, VA, 1998, pp 443-456.

[15]. M. Moradi and M. Zulkernine , "A Neural Network Based System for Intrusion Detection and Classification of Attacks", In Proc. IEEE Int. Conf. on Advances in Intelligent Systems- Theory & Applications, November 2004, pp. 15-18.

[16]. R. Varma & V. Kumari, "Feature Optimization and Performance Improvement of a Multiclass Intrusion Detection System using PCA and ANN", International Journal of Computer Applications, Vol. 44 No13, April 2012, pp. 4-9.

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

[18]. C. Elkan, "Results of the KDD'99 classifier learning", SIGKDD Explorating192, 2000, pp 63-64.

[19]. MATLAB online support: ww.mathworks.com/ access/helpdesk/help/techdoc/matlab.shtml., 2013

[20]. M. Negnevitsky, "Artificial Intelligent A guide to Intelligent System", 2nd ed, Addison Wesley, 2002

[21]. T. Vollmer and M. Manic, "Computationally Efficient Neural Network Intrusion Security Awareness", In Proc. Int. Symposium on Resilient Control Systems ISRCS, August 2009, pp. 25-30.

[22]. X. Xin and N. Mingxin, "BP Neural Network principle and MATLAB Simulation", http://www.paper.edu.cn,2013.