Hybrid Multi-level Intrusion Detection System

Sahar Selim, Mohamed Hashem and Taymoor M. Nazmy
Faculty of Computer and Information Science
Ain Shams University
Cairo, Egypt
Sahar.Soussa@gmail.com

Abstract— **Intrusion detection is a critical process in network security. Nowadays new intelligent techniques have been used to improve the intrusion detection process. This paper proposes a hybrid intelligent intrusion detection system to improve the detection rate for known and unknown attacks. We examined different neural network & decision tree techniques. The proposed model consists of multi-level based on hybrid neural network and decision tree. Each level is implemented with the technique which gave best experimental results. From our experimental results with different network data, our model achieves correct classification rate of 93.2%, average detection rate about 95.6%; 99.5% for known attacks and 87% for new unknown attacks, and 9.4% false alarm rate.**

Keywords-component; network intrusion detection; neural network; Decision Tree; NSL-KDD dataset

I. INTRODUCTION

Security of network system is becoming increasingly important as more sensitive information is being stored and manipulated online. It is difficult to prevent attacks only by passive security policies, firewall, or other mechanisms. Intrusion Detection Systems (IDS) have thus become a critical technology to help protect these systems as an active way. An IDS can collect system and network activity data, and analyze those gathered information to determine whether there is an attack [1].

The main objective of this work is to design and develop security architecture (an intrusion detection and prevention system) for computer networks. This proposed system should be positioned at the network server to monitor all passing data packets and determine suspicious connections. Therefore, it can inform the system administrator with the suspicious attack type. Moreover, the proposed system is adaptive by allowing new attack types to be defined.

We build the model to improve the detection rate for known and unknown attacks. First, we train and test our hybrid model on the normal and the known intrusion data. Then we test our system for unknown attacks by introducing new types of attacks that are never seen by the training module.

II. PREVIOUS WORK

An increasing amount of research has been conducted for detecting network intrusions. The idea behind the application of soft computing techniques in implementing IDSs is to include an intelligent agent in the system that is capable of disclosing the latent patterns in abnormal and normal connection audit records, and to generalize the patterns to new (and slightly different) connection records of the same class.

There are researches that implement an IDS using Multi-layer perceptron (MLP) which have the capability of detecting normal and attacks connection as in [2], [3]. Reference [4] used MLP not only for detecting normal and attacks connection but also identify attack type.

Decision Tree (C4.5 Algorithm) was explored as intrusion detection models in [5] and [6].

Neural network and C4.5 have different classification capabilities for different intrusions. Therefore, Hybrid model improves the performance to detect intrusions. [1], [7] compare the performance of Hybrid model, single Back Propagation network, and single C4.5 algorithm. Experimental results demonstrate that neural networks are very interesting for generalization and very poor for new attacks while decision trees have proven their efficiency in both generalization and new attacks detection. A multi-classifier model, where a specific detection algorithm is associated with an attack category for which it is the most promising, was built in [8].

Reference [9] developed a multi-stage neural network which consists of three detection levels. The first level differentiates between normal and attack. The second level specifies whether this attack is DOS or probe. The third detection level identifies attacks of denial of service and probe attacks.

The proposed system is a hybrid multi-level system. It consists of three levels. Each level was examined with different machine learning techniques. Each module in each level is built using the best classifier which gave best results for this level. It has the ability to identify normal and attack records and also being able to detect attack type by the next levels. This approach has the advantage to flag for suspicious record even if attack type of this record wasn't identified correctly.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

III. THE PROPOSED SYSTEM

Our system is a modular network-based intrusion detection system that analyzes Tcpdump data using data mining techniques to classify the network records to not only normal and attack but also identify attack type.

The main characteristics of our system:

- ***Multilevel:*** has the capability of classifying network intruders into a set of different levels. The first level classifies the network records to either normal or attack. The second level can identify four categories/classes. The third level where the attack type of each class can be identified.

Attacks of the same class have a defined signature which differentiates between attacks of every class/category from others, i.e. DOS attacks have similar characteristics which identifies them from attacks of Probing, R2L and U2R. That's why there's often misclassification between attacks of the same class, which gave the importance of making a multi-stage system consisting of three levels.

The data is input in the first level which identifies if this record is a normal record or attack. If the record is identified as an attack then the module would raise a flag to the administrator that the coming record is an attack then the module inputs this record to the second level which identifies the class of the coming attack. Level 2 module pass each attack record according to its class type to level 3 modules. Level 3 consists of 4 modules one for each class type (DOS, Probe, R2L, U2R). Each module is responsible for identifying the attack type of coming record.

The idea is that if ever the attack name of the third level is misclassified then at least the admin was identified that this record is suspicious after the first level network. Finally the admin would be alerted of the suspected attack type to guide him for the suitable attack response [9].

- ***Hybrid:*** Modules of each level can use different data mining technique. We made a comparative study examining several data mining techniques to find the best classifier for each level. Neural network and decision trees have different classifying abilities for different intrusions. Neural network have high performance to DOS and Probing attacks while decision trees can detect the R2L more accurately than neural network. Therefore, Hybrid model will improve the performance to detect intrusions.

- ***Adaptive:*** Attacks that are misclassified by the IDS as normal activities or given wrong attack type will be relabeled by the network administrator. The training module can be retrained at any point of time which makes its implementation adaptive to any new environment and/or any new attacks in the network.

IV. SYSTEM ARCHITECTURE

The system components as shown in Fig 1 are:

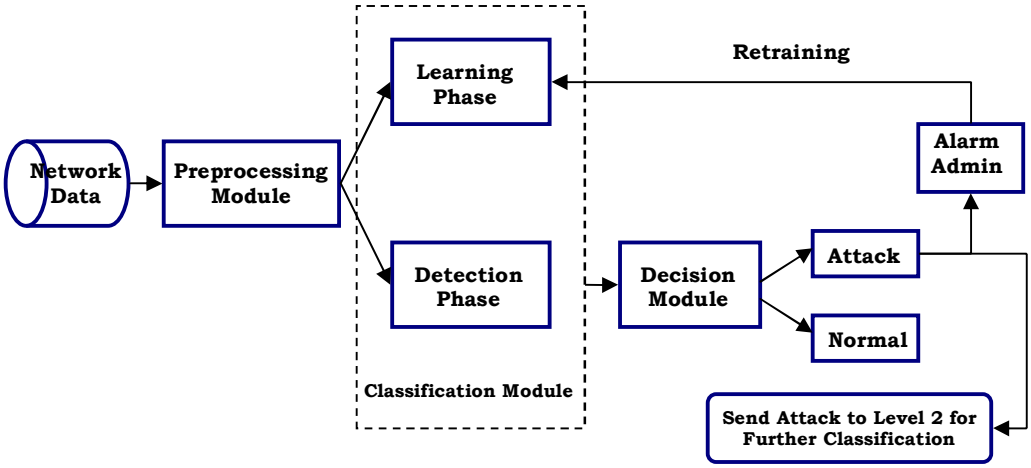

Figure 1. System architecture

A. The Capture Module

Raw data of the network are captured and stored using the network adapter.

B. The Preprocessing Module

This module is responsible for Numerical Representation, Normalization and Features selection of raw input data to be used by the classification module. The preprocessing module maps the raw packets captured from the network by the TCP dump capture utility to a set of patterns of the most Effective Selected Feature. These dominant features are then used as inputs to the training module.

The preprocessing module consists of three phases: [9]

1) Numerical Representation: Converts non-numeric features into a standardized numeric representation. This process involved the creation of relational tables for each of

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the data type and assigning number to each unique type of element. (e.g. protocol_type feature is encoded according to IP protocol field: TCP=0, UDP=1, ICMP=2). This is achieved by creating a transformation table containing each text/string feature and its corresponding numeric value.

2) Normalization: The ranges of the features were different and this made them incomparable. Some of the features had binary values where some others had a continuous numerical range (such as duration of connection). As a result, inputs to the classification module should be scaled to fall between zero and one [0, 1] range for each feature.

3) Dimension reduction: reduce the dimensionality of input features of the classification module. Reducing the input dimensionality will reduce the complexity of the classification module, and hence the training time.

C. The classification Module

The classification module has two phases of operation. The learning and the detection phase.

1) The Learning Phase

In the learning phase, the classifier uses the pre-processed captured network user profiles as input training patterns. This phase continues until a satisfactory correct classification rate is obtained.

2) The Detection Phase

Once the classifier is learned, its capability of generalization to correctly identify the different types of users should be utilized to detect intruder. This detection process can be viewed as a classification of input patterns to either normal or attack.

D. The Decision Module

The basic responsibility of the decision module is to transmit alert to the system administrator informing him of coming attack. This gives the system administrator the ability to monitor the progress of the detection module.

1) Performance Measures

To evaluate our system we used two major indices of performance. We calculate the detection rate and the false alarm rate according to [10] the following assumptions:

- False Positive (FP): the total number of normal records that are classified as anomalous
- False Negative (FN): the total number of anomalous records that are classified as normal
- Total Normal (TN): the total number of normal records
- Total Attack (TA): the total number of attack records
- Detection Rate = [(TA-FN) / TA]*100
- False Alarm Rate = [FP/TN]*100
- Correct Classification Rate = Number of Records Correctly Classified / Total Number of records in the used dataset

V. Machine Learning Algorithms Applied To Intrusion Detection

Seven distinct pattern recognition and machine learning algorithms were tested on the NSL-KDD dataset. These algorithms were selected in the fields of neural networks and decision trees.

A. Neural Networks

The neural network gains the experience initially by training the system to correctly identify pre-selected examples of the problem. The response of the neural network is reviewed and the configuration of the system is refined until the neural network's analysis of the training data reaches a satisfactory level. In addition to the initial training period, the neural network also gains experience over time as it conducts analysis on data related to the problem [2].

1) Multi-Layer Perceptron (MLP)

The architecture used for the MLP during simulations consisted of a three layer feed-forward neural network: one input, two hidden, and one output layers. Sigmoid transfer functions were used for each neuron in both the hidden layers and softmax in the output layers. The network was set to train until the desired mean square error of 0.001 was met or 10000 epochs was reached.

For the first level there were 31 neurons in the input layer (31-feature input pattern) after feature selection, 22 neurons in first hidden layer,18 neurons in second hidden layer and 2 neurons (one for normal and the other for attack) in the output layer. During the training process, the mean square error is 0.0157 at 10000 epochs. For the second level 38 in input layer, 12 in first hidden layer, 10 in second hidden layer and 4 neurons in the output layer (DOS, Probe, R2L and U2R). During the training process, the mean square error is 0.0114 at 10000 epochs. We've four networks in the third level. DOS network has layers of 28-2-2-7 feed-forward neural network. (i.e. 28 in input layer, 2 in the 1st hidden layer, 2 in the 2nd hidden layer and 7 in the output layer). During the training process, the mean square error is 0 at 1574 epochs. Probe network has layers of 24-22-14-6 feed-forward network with mean square error 0.05 at 10000 epochs. R2L network has layers of 26-17-10-5 feed-forward network with mean square error 0 at 5838 epochs. U2R network has layers of 11-9-7-5 feed-forward network with mean square error 2.33 at 10000 epochs.

2) Radial Basis Function (RBF)

The RBF layer uses Gaussian transfer functions. The learning rate was set to 0.1 for the hidden layer and 0.01 for the output layer. The alpha was set to 0.75. For the first level there were 31 neurons in the input layer, 10 neurons in hidden layer and 2 neurons (one for normal and the other for attack) in the output layer. Estimated accuracy of training was 94.4%. The second level has 37 in input layer, 10 in hidden layer and 4 neurons in the output layer (DOS, Probe, R2L and U2R) with estimated accuracy of 93.5%. We've four networks in the third level. DOS RBF network has layers of 28-20-7. (i.e. 28 in input layer, 20 in hidden layer and 7 in the output layer) with estimated accuracy 100%. Probe network has layers of 24-20-6 network with estimated

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

accuracy 98.3%. R2L RBF network has layers of 26-20-5 with estimated accuracy 98.3%. U2R network has layers of 11-20-5 with estimated accuracy 75%.

3) Exhaustive Prune

The first level there consists of 13 neurons in the input layer, 22 neurons in first hidden layer, 7 neurons in second hidden layer and 2 neurons (one for normal and the other for attack) in the output layer with estimated accuracy of training 99.8%. The second level consists of 25 in input layer, 9 in first hidden layer, 5 in second hidden layer and 4 neurons in the output layer (DOS, Probe, R2L and U2R) with accuracy of training 99.9%. We've four networks in the third level. DOS network has layers of 3-19-17-7 network with accuracy of training 100%. Probe network has layers of 10-12-5-6 network with estimated accuracy of 99.6%. R2L network has layers of 14-3-2-5 network with estimated accuracy of 100%. U2R network has layers of 1-3-2-5 network with estimated accuracy of training 81.5%.

B. Decision trees

The decision tree is a simple if then else rules but it is a very powerful classifier and proved to have a high detection rate. They are used to classify data with common attributes. Each decision tree represents a rule which categorizes data according to these attributes. A decision tree consists of nodes, leaves, and edges. A node of a decision tree specifies an attribute by which the data is to be partitioned. Each node has a number of edges which are labeled according to a possible value of the attribute in the parent node. An edge connects either two nodes or a node and a leaf. Leaves are labeled with a decision value for categorization of the data [11].

1) C5

See5.0 (C5.0) is one of the most popular inductive learning tools originally proposed by J.R.Quinlan as C4.5 algorithm (Quinlan, 1993) [11]. Single C5 acquires pruned decision tree with pruning severity 75% and winnowing attributes. First level consists of 121 nodes on train data and 20 tree depth and standard error 0.01%. Second level consists of 113 nodes and tree depth of 12 with standard error 0.05%. Third level DOS tree consists of 6 nodes and tree depth of 4 levels with standard error 0%. Probe tree consists of 69 nodes and tree depth of 10 levels with standard error 0.4%. R2L tree consists of 7 nodes and tree depth of 4 levels with standard error 0%. U2R tree consists of 9 nodes and tree depth of 4 levels with standard error 8.33%.

2) Classification and Regression Trees (CRT or CART)

CRT was set of maximum surrogates 10, minimum change in impurity 0.0 and Gini impurity measure for categorical targets. First level consists of 15 nodes and of depth 4. Second level consists of 15 nodes of tree depth 4. Third level DOS consists of 7 nodes of tree depth = 3. Probe consists of 13 nodes of tree depth 5. R2L consists of 7 nodes of tree depth 4. U2R consists of 17 nodes of tree depth 6.

3) Chi-squared Automatic Interaction Detector (CHAID)

CHAID was adjusted of Alpha splitting 0.05, alpha for merging 0.05, epsilon for convergence 0.001, using pearson chi-square method. First level consists of 35 nodes and of depth 5. Second level consists of 28 nodes of tree depth 4. Third level DOS consists of 6 nodes of tree depth 3. Probe consists of 49 nodes of tree depth 6. R2L consists of 7 nodes of tree depth 3. U2R consists of 12 nodes of tree depth 5.

4) Quick, Unbiased, Efficient Statistical Tree (QUEST)

QUEST was adjusted of maximum surrogates 5, and alpha for splitting 0.05. First Level consists of 15 nodes and of 4 tree depth. Third level DOS consists of 11 nodes of tree depth 6. Probe consists of 17 nodes of tree depth 6. R2L consists of 9 nodes of tree depth 5. U2R consists of 13 nodes of tree depth 6.

VI. EXPERIMENTS AND RESULTS

A. Dataset Description

KDDCUP'99 is the mostly widely used data set for the evaluation of these systems. The KDD Cup 1999 uses a version of the data on which the 1998 DARPA Intrusion Detection Evaluation Program was performed. They set up an environment to acquire raw TCP/IP dump data for a local-area network (LAN) simulating a typical U.S.Air Force LAN.

1) There are four major categories of networking attacks. Every attack on a network can be placed into one of these groupings [13].

a) Denial of Service Attack (DoS): is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies\ legitimate users access to a machine. e.g. apache, smurf, Neptune, ping of death, back, mail bomb, UDP storm, etc.

b) User to Root Attack (U2R): is a class of exploit in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.

c) Remote to Local Attack (R2L): occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine. e.g. perl, xterm.

d) Probing Attack: is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls. e.g. satan, saint, portsweep, mscan, nmap etc.

There are some inherent problems in the KDDCUP'99 data set [12], which is widely used as one of the few publicly available data sets for network-based anomaly detection systems. The first important deficiency in the KDD data set is the huge number of redundant records. Analyzing KDD train and test sets, it was found that about 78% and 75% of the records are duplicated in the train and test set, respectively. This large amount of redundant records in the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

train set will cause learning algorithms to be biased towards the more frequent records, and thus prevent it from learning infrequent records which are usually more harmful to networks such as U2R attacks. The existence of these repeated records in the test set, on the other hand, will cause the evaluation results to be biased by the methods which have better detection rates on the frequent records [13].

The data in the experiment is acquired from the NSL-KDD dataset which consists of selected records of the complete KDD data set and does not suffer from mentioned shortcomings by removing all the repeated records in the entire KDD train and test set, and kept only one copy of each record [13]. Although, the proposed data set still suffers from some of the problems and may not be a perfect representative of existing real networks, because of the lack of public data sets for network-based IDSs, but still it can be applied as an effective benchmark data set to help researchers compare different intrusion detection methods. The NSL-KDD dataset is available at [14].

In this study we examine using attacks from the four classes to check the ability of the intrusion detection system to identify attacks from different categories. The sample dataset contains 83655 record for training (40000 normal and 43655 for attacks) and 16592 for testing (9657 normal, 6935 for known attacks and 3202 for unknown attacks).

B. *Level 1 output*

Level 1 duty is to classify whether coming record is normal or attack. It is observed that MLP best classifies normal records while C5 is more efficient in detecting known and unknown attacks. The results of Level 1 are shown in table 1 & 2.

TABLE I. CORRECT CLASSIFICATION RATE FOR LEVEL 1

Percentage	Normal	Attacks	New Attacks	Correct Classification Rate
MLP	**95.1**	97.2	78.7	93.2
RBF	90.4	93.1	45.5	84.1
Exhaustive	89.7	97.3	86.2	91.8
C5	90.6	**99.5**	**97**	93.2
CRT	93.3	98.9	45.4	87.5
QUEST	85.5	98	67.1	86.9
CHAID	89.6	97.1	59.2	87.3

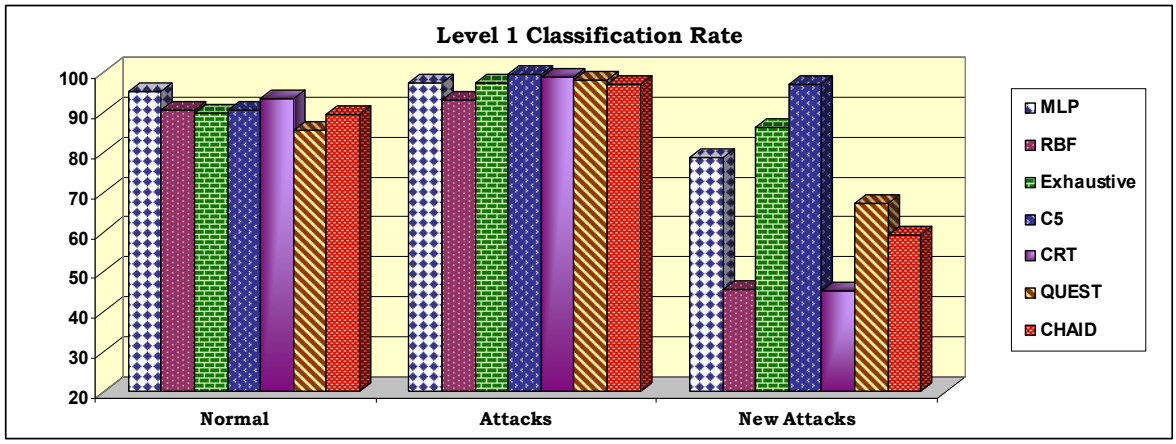

Figure 2. Level 1 Classification Rate

TABLE II. DETECTION RATE & FALSE ALARM RATE FOR LEVEL 1

Classifier	Detection Rate	False Alarm Rate
MLP	91.397	5
RBF	78.0979	9.64
Exhaustive	91.83	10.3
C5	**95.5702**	9.4
CRT	82.0343	15.8
QUEST	88.2301	14.53
CHAID	85.1322	10.44

C5 has a significant detection rate for known and unknown attacks but it produce higher false alarm rate compared to MLP.

C. *Level 2 Output*

Records classified as attacks by the first level are introduced to second level which is responsible for classifying coming attack to one of the four classes (DOS, Probe, R2L & U2R). Testing results showed that C5 & CRT (decision trees) produced best correct classification rate for second level as shown in table 3.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE III. CORRECT CLASSIFICATION RATE FOR LEVEL 2

Level 2 Classifiers	Known Attacks	New Attacks	Correct Classification
MLP	82.8202	56.2637	82.8202
RBF	74.7977	50.6717	74.7977
Exhaustive	79.2382	49.8594	79.2382
C5	**86.0174**	59.294	**86.0174**
CRT	**85.7805**	**62.6679**	85.7805
CHAID	78.7646	38.8316	78.7646

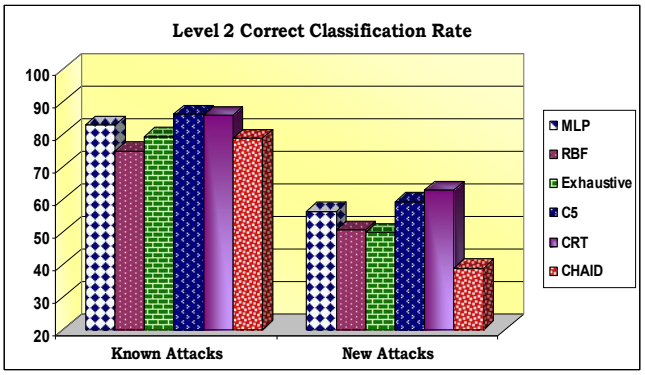

Figure 3. Level 2 Classification Rate

D. Level 3 Output

The third level consists of four modules; a module for each class. For example records that were classified by the second level to be DOS attack are sent to the DOS module of the 3rd level & so on.

Results of Denial of service modules showed that DOS attacks are easy to be correctly classified by many classifiers either neural network or decision trees as shown in table 4.

TABLE IV. DOS ATTACKS CLASSIFICATION RATE

DOS Classifier	Correct Classification Rate
MLP	100
RBF	99.3852
Exhaustive	99.9297
C5	100
CRT	100
QUEST	99.9297
CHAID	100

Results of Probe module showed that C5 & MLP are most efficient for detecting this type of attacks as shown in table 5.

TABLE V. PROBE ATTACKS CLASSIFICATION RATE

Probe Classifier	Correct Classification Rate
MLP	99.3
RBF	97.8
Exhaustive	97
C5	98.6
CRT	92.6
QUEST	94.1
CHAID	95.5

Results of R2L module showed that C5 are most efficient for detecting this type of attacks significantly as shown in table 6.

TABLE VI. R2L ATTACKS CLASSIFICATION RATE

R2L Classifier	Correct Classification Rate
MLP	91
RBF	93
Exhaustive	91
C5	**100**
CRT	97
QUEST	96
CHAID	97

U2R attacks have a very low classification rate compared to other classes. Results showed that Exhaustive prune is better than other classifiers for detecting attacks of this class as shown in table 7.

TABLE VII. U2R ATTACKS CLASSIFICATION RATE

U2R Classifier	Correct Classification Rate
MLP	48.2
RBF	43.1
Exhaustive	**54.4**
C5	44.1
CRT	44.1
QUEST	35.3
CHAID	41.2

VII. DISCUSSION

Simulation results demonstrated that for a given attack category certain classifier algorithms performed better. Consequently, a multi-classifier model that was built using most promising classifiers for a given attack category was evaluated for probing, denial-of-service, user-to-root, and remote-to-local attack categories.

While the neural networks are very interesting for generalization and very poor for new attacks detection, the decision trees have proven their efficiency in both generalization and new attacks detection. Besides the C5 has less training time than the MLP. However, none of the machine learning classifier algorithms evaluated was able to perform detection of user-to-root attack categories significantly (no more than 54% detection for U2R category).

The advantage of the proposed mutli-level system is not only higher accuracy but also the parallelism as every module can be trained on separate computer which provides less training time. Also the multi-level powers the system with scalability because if new attacks of specific class are added to the dataset we don't have to train all the modules but only the module affected by the new attack. Attacks that are misclassified by the IDS as normal activities or given

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

wrong attack type will be relabeled by the network administrator. Training module can be retrained at any point of time which makes its implementation adaptive to any new environment or any new attacks in the network.

VIII. Conclusion & Future Work

In this paper we develop a hybrid multilevel intrusion detection system. The proposed system consists of three detection levels. The network data are introduced to the module of the first level which aims to differentiate between normal and attack. If the input record was identified as an attack then the administrator would be alarmed that the coming record is suspicious and then this suspicious record would be introduced to the second level which specifies the class of this attack (DOS, probe, R2L or U2R). The third detection level consists of four modules one module for each class type to identify attacks of this class. Finally the administrator would be alarmed of the expected attack type [9].

We examined each module using different machine learning models (MLP, RBF, C5, CRT, QUEST & Exhaustive Prune). Each module is implemented with the most promising classifier that gave highest correct classification rate. Therefore, Hybrid model will improve the performance of intrusion detection.

The experimental results show that the designed multi-level system has detection rate equal to 95.6% for both (known and unknown attacks). The first level is implemented by C5 decision tree which showed significant detection rate for both known and unknown attacks. The drawback of using C5 decision tree is the high false alarm rate that it produces. The second level is implemented by C5. As for the third level DOS & Probe modules are implemented by MLP, R2L module is implemented by C5 decision tree and U2R module is implemented by Exhaustive prune.

The detection of U2R attack is more difficult because of their close resemblance with the normal connections. Our future research will be directed towards developing more accurate base classifiers particularly for the detection of U2R attacks. Also finding ways to produce less false alarm rate for the C5 Decision tree.

References

[1] Z.S. Pan, S.C. Chen, G.B Hu and D.Q. Zhang, "Hybrid Neural Network and C4.5 for Misuse Detection, " In Machine Learning and Cybernetics, pp. 2463-2467. Xi'an, 2003.

[2] J.Cannady, "Artificial neural networks for misuse detection, " Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, pp. 443-456, 1998.

[3] Srinivas Mukkamala, "Intrusion detection using neural networks and support vector machine, " Proceedings of the 2002 IEEE International Honolulu, HI, 2002.

[4] M. Moradi, and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks, " IEEE International Conference on Advances in Intelligent Systems - Theory and Applications, Luxembourg-Kirchberg, Luxembourg, November 15-18, 2004.

[5] Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman and Chowdhury Mofizur Rahman, "Attacks Classification in Adaptive Intrusion Detection using Decision Tree, " International Conference on Computer Science (ICCS 2010), 29-31 March, 2010, Rio De Janeiro, Brazil.

[6] L Prema RAJESWARI and Kannan ARPUTHARAJ, "An Active Rule Approach for Network Intrusion Detection with Enhanced C4.5 Algorithm, " International Journal of Communications, Network and Systems Sciences (IJCNS), 2008, 4, 285-385.

[7] Y. Bouzida, F.Cuppens, "Neural networks vs. decision trees for intrusion detection, " IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM), Tuebingen, Germany, 28-29 September 2006.

[8] M.R. Sabhnani and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context, " Proceedings of International Conference on Machine Learning: Models, Technologies, and Applications, Las Vegas, Nevada, 2003, pp. 209-215.

[9] Sahar Selim, M. Hashem and Taymoor M. Nazmy, "Intrusion Detection using Multi-Stage Neural Network, " International Journal of Computer Science and Information Security, Vol. 8, No. 4, 2010.

[10] S.T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchal Kohonenen Net for Anomaly Detection in Network Security," IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, 35(2), 2005, pp. 302-312.

[11] Quinlan JR. "C4.5: programs for machine learning, " Log Altos,CA: Morgan Kaufmann; 1993.

[12] KDD Cup 1999. Available on: http://kdd.ics.uci.edu/databases/kddcup 99/kddcup99.html, October 2007

[13] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[14] "NSL-KDD data set for network-based intrusion detection systems," Available on: http://nsl.cs.unb.ca/NSL-KDD/, March 2009

AUTHORS PROFILE

Sahar Selim Fouad Bachelor of Computer Science, Faculty of Computer & Information Science, Ain Shams University. Currently working for master degree. Fields of interest are intrusion detection, computer and networks security.

Mohamed Abdel-Aziz Hashem Professor in IT and Security, Ain Shams University. Currently Vice Dean of Educational & Students' Affairs, faculty of Computer and Information Science, Ain Shams University. Fields of interest are computer networks, Ad-hoc and wireless networks, Qos Routing of wired and wireless networks, Modeling and simulation of computer networks, VANET and computer and network security.

Taymoor Mohammed Nazmy Professor in Computer Science, Ain Shams University. He served before in faculties of Sciences, and education as a lecturer for over 12 years. He was the director of the university information network. Currently Vice Dean of higher studies and researches, faculty of Computer and Information Science, since 2007. Fields of interest are image processing, pattern recognition, artificial neural networks, networks security and speech signal analysis.