Implementation of Intelligent Multi-Layer Intrusion Detection Systems (IMLIDS)

Sherif M. Badr, PhD.
College of Computer science
Modern Academy, Cairo, Egypt

ABSTRACT

Intrusion Detection System (IDS) has increasingly become a crucial issue for computer and network systems. Optimizing performance of IDS becomes an important open problem which receives more and more attention from the research community.

This paper, design and develop a proposed multi-layer intrusion detection model to achieve high efficiency and improve the detection and classification rate accuracy. Also the proposed model was improved the detection rate for known and unknown attacks by training the hybrid model on the known intrusion data. Then the model applied for unknown attacks by introducing new types of attacks that are never seen by the training module.

The experimental results showed that the proposed multi-layer model using C5 decision tree achieves higher classification rate accuracy, and less false alarm rate.

Keywords: intrusion detection; Decision Tree; network security.

1. INTRODUCTION

With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. New security failures are discovered every day and there are a growing number of bad intentioned people trying to take advantage of such failures. Intrusion detection is a critical process in network security. Intrusion Detection Systems (IDS) aim at protecting networks and computers from malicious network-based or host-based attacks.Different soft-computing based methods have been proposed in recent years for the development of intrusion detection systems. Most current approaches to intrusion detection involve the use of rule-based expert systems to identify indications of known attacks. Artificial neural networks and decision trees provide the potential to identify and classify network activity.[1][2]

Most of the previous systems have some deficiencies. Some drawbacks of previous Intrusion detection systems (IDSs) are that they are unable to detect new attacks that are never seen before. Most of these systems don't identify the attack type but only specify whether the given network data is normal or attack. One of the drawbacks of IDSs that are signature-based is that they can only detect known attacks while all new unknown attacks will go unnoticed until the system is updated to be able to detect them. [3]

This work proposes a hybrid intelligent intrusion detection system to improve the detection rate for known and unknown attacks. The introduced system has the capability to learn fast, enhanced capability of detection of new unidentified attacks, and alarming the system administrator of these unseen before attacks. Unlike other systems that have one level of detection, the proposed system has three levels of detection. The first level is where the system classifies the network users to either normal or intruder. The second level is where system can identify four categories of intruders. The third level is the fine detection level, where the attack type can be identified.

The proposed model consists of multi-level based on hybrid neural network and decision tree. Different neural network and decision tree techniques were examined. Every module in each level is implemented with the different technique (Neural Network or Decision Tree) and taking the best experimental results for this module.

The experimental results with different network data, our model achieves correct classification rate of 93.64%, average detection rate about 98%; 99.8% for known attacks and 93.8% for new unknown attacks.

2. RELATED WORK

Many hybrid intrusion detection systems were designed and implemented:Neural network and C4.5 have different classification capabilities for different intrusions. Therefore, Hybrid model improves the performance to detect intrusions. Experimental results demonstrate that while neural networks are highly successful in detecting known attacks, decision trees are more interesting to detect new attacks. 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.

Pan et al. [4] presented an intrusion detection model based on hybrid neural network and C4.5. The key idea is to take advantage of different classification abilities of neural network and the C4.5 algorithm for different attacks. What is more, the model could also be updated by the C4.5 rules mined from the dataset after the event (intrusion). Neural network have high performance to DOS and Probing attacks rather than to R2L and U2R attacks. On the contrast, C4.5 can detect the R2L and U2R more accurately than neural network. [5],[6].

Peddabachigari et al. [7] presented two hybrid approaches for modeling IDS. Decision trees (DT) and support vector machines (SVM) are combined as a hierarchical hybrid intelligent system model (DT–SVM) and an ensemble approach combining the base classifiers. The hybrid intrusion detection model combines the individual base classifiers and other hybrid machine learning paradigms to maximize detection accuracy and minimize computational complexity.

Depren et al. [8] proposed a novel Intrusion Detection System (IDS) architecture utilizing both anomaly and misuse detection approaches. This hybrid Intrusion Detection System architecture consists of an anomaly detection module, a misuse detection module and a decision support system combining the results of these two detection modules. The proposed anomaly detection module uses a Self-Organizing Map (SOM) structure

to model normal behavior. Deviation from the normal behavior is classified as an attack. The proposed misuse detection module uses J.48 decision tree algorithm to classify various types of attacks. A rule-based Decision Support System (DSS) is also developed for interpreting the results of both anomaly and misuse detection modules.

Farid et al. [9] used a learning algorithm for adaptive network intrusion detection using naive Bayesian classifier and decision tree, which performed balance detections and kept false positives at acceptable level for different types of network attacks, and eliminated redundant attributes as well as contradictory examples from training data that make the detection model complex. The proposed algorithm also addressed some difficulties of machine learning such as handling continuous attribute, dealing with missing attribute values, and reducing noise in training data. Due to the large volumes of security audit data as well as the complex and dynamic properties of intrusion behaviors, several machine learning based intrusion detection techniques have been applied to network-based traffic data and host-based data in the last decades.[10].

Sabhnani and Serpen [11] evaluated performance of a comprehensive set of pattern recognition and machine learning algorithms on four attack categories as found in the KDD 1999 Cup intrusion detection dataset. Results of simulation study implemented to that effect indicated that certain classification algorithms perform better for certain attack categories: a specific algorithm specialized for a given attack category.

Consequently, a multi-classifier model that was built using most promising classifiers for a given attack category was evaluated for some categories. The proposed multi-expert classifier showed improvement in detection and false alarm rates for all attack categories as compared to the KDD 1999 Cup winner. Furthermore, reduction in cost per test example was also achieved using the multi-classifier model [12],[13].

3. GENERAL ASPECTS:

3.1 Artificial Intelligence and Intrusion Detection

There is no basic, simple, or agreed upon strict definition of artificial intelligence however as a general definition artificial intelligence is the science and engineering of making intelligent machines, especially intelligent computer programs [14].

Human's biological intelligence has inspired system security designers and researchers to build artificial intelligence system which emulates the defense mechanism of Human Immune Systems. Artificial Intelligence systems have been experienced and developed, which relies of the algorithms and intelligent techniques, combining the knowledge of past intrusions in improving the systems detection [15], [16].

Regarding the Intrusion detection, researches use different types of Artificial Intelligence methods and techniques as Neural Network & Decision Trees.

3.2 Selection of Classifier:

3.2.1 Neural Network Classifiers:

An artificial neural network is a system based on the operation of biological neural networks, in other words, is an emulation of biological neural system. Although computing these days is truly advanced, there are certain tasks that a program made for a common microprocessor is unable to perform; even so a software implementation of a neural network can be made with their advantages and disadvantages [17].

3.2.2 DECISION TREES CLASSIFIERS:

Decision trees Classifier chosen for building the new classifier that it deals with both integer and real numbers. The decision tree is a simple if then else rules that is easy to be implemented.

It is a very powerful classifier and proved to have a high detection rate as will be shown in Experimental Results section.

4. THE PROPOSED SYSTEM:

The proposed system is a modular network-based intrusion detection system that analyzes TCP dump data using data mining techniques to classify the network records to not only normal and attack but also identify attack type. The system components are shown in Figure 1.

4.1 The System Components:

4.1.1 The Capture Module:

Raw data of the network are captured and stored using the network adapter. It utilizes the capabilities of the TCP dump capture utility for Windows to gather historical network packets. It exploits the historical -user behaviors of the target system's audit trails to train its artificial training module with the most dominant features of these audit trails to identify the different types of normal and intruder profiles.

4.1.2 The Preprocessing Module:

The data must be of uniform representation to be processed by the classification module. The preprocessing module is responsible for reading, processing, and filtering the audit data to be used by the classification module. The preprocessing module handles numerical representation, normalization and features selection of raw input data. The preprocessing module consists of three phases:

4.1.2.1 Numerical Representation:

Converts non-numeric features into a standardized numeric representation. This process involved the creation of relational tables for each of the data type and assigning number to each unique type of element. This is achieved by creating a transformation table containing each text/string feature and its corresponding numeric value.

4.1.2.2 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 [12].

4.1.2.3 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.

4.1.3 The classification Module:

4.1.3.1 The Learning Phase:

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

4.1.3.2 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.

4.1.4 The Decision Module:

The basic responsibility of the decision module is to distinguish between the normal behavior and the attacks, then 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.

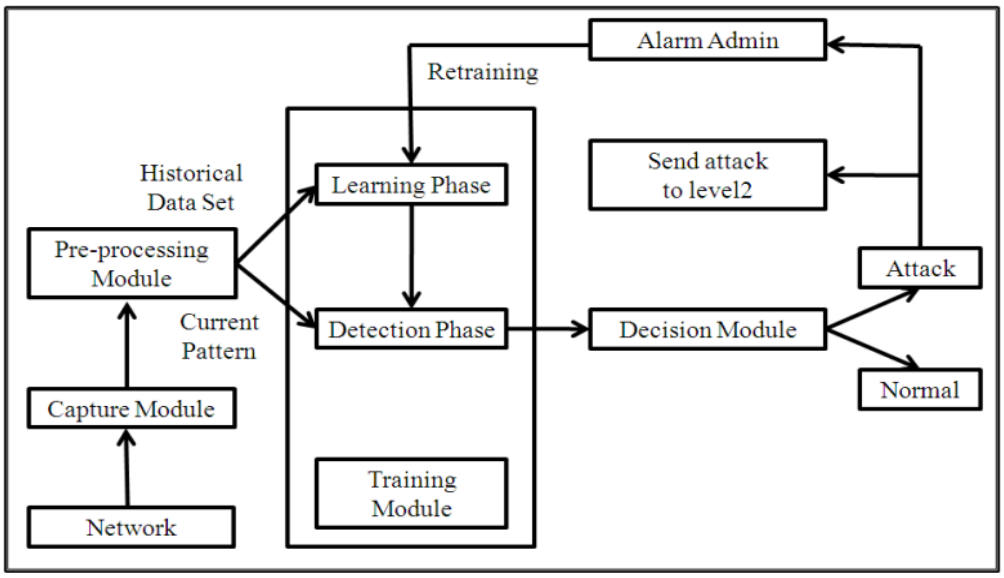

Figure 1 System Architecture

4.2 Architectures Examined:

Four system architectures were examined:

- Single Level Intrusion Detection System.
- Multi-Level Intrusion Detection System.
- Hybrid Multi-Level Intrusion Detection System.
- Enhanced Hybrid Multi-Level Intrusion Detection System.

A comparison between Single level and Multi-Level Neural Network using two types of attacks DOS (Neptune and Smurf) and Probe (Satan and Port-sweep). While Hybrid Multi-Level Intrusion detection system was examined using different machine learning techniques and larger dataset containing the four types of attacks (DOS, Probe, U2R and R2L). The results produced by the hybrid system encouraged us to develop the Enhanced Hybrid Multi-Level Intrusion detection system [7].

4.2.1 Single Level Neural Network IDS:

This experiment examines the use of the neural network to classifying normal and attack type.

4.2.2 Multi-Level Neural Network IDS:

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. That's why there's often misclassification between attacks of the same class. For that reason, a multi-stage neural network addedto identifies three levels:

- **Level 1:** is a Neural Network that identifies attacks from normal.
- **Level 2:** is a Neural Network that identifies attack category.
- **Level 3:** is a Neural Network that identifies attack type.

The data is input in the first level which identifies if this record is a normal record or attack without exhausting the network to identify the attack name. 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. If record was classified by network II to be DOS then it would be entered to the DOS network of the third level that identify attacks' type of DOS otherwise it would be introduced to the Probe network. 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.

4.2.3 Hybrid Multi-Level IDS:

The main characteristics of the proposed system:

4.2.3.1 Multilevel:

Has the capability of classifying network intruders into a set of different levels.

Level1classifies the network records to either normal or attack. The second level can identify four categories/classes. The third level identified the attack type of each class can be 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 modules 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.

4.2.3.2 Hybrid:

Modules of each level can use different machine learning techniques. A comparative study was done for examining several machine learning 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.

4.2.3.3 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.

4.2.4 Enhanced Hybrid Multi-Level IDS:

The enhanced system has a dual protection phases for Level 1 to increase the attacks detection rate. The levels of the enhanced system are shown in Fig.2. The first stage of level 1 is passing the input data through C5 Model, and then the records that are classified as normal by the C5 are passed to second stage which is MLP Model to detect some attacks that are bypassed by the C5 Model.

4.2.4.1 First Stage of Level 1:

The input data are preprocessed then entered to the C5 Model of Level 1. If the input record is classified as attack then the admin would be alarmed of the coming attack & the attack record would be input to Level 2 Model to specify its attack category [18].

4.2.4.2 Second Stage of Level 1:

If the record is classified by the first phase to be normal then it is passed to the second protection phase of Level 1 which is an MLP Model of Level 1. If the record is classified as normal by the MLP Model then it's allowed to internal network.

Otherwise if it's classified as attack the admin would be alarmed and the record would be input to the second level module to identify its attack category.The enhanced system has the advantage of higher detection rate as MLP can detect some attacks that are bypassed by the C5 Model. Meanwhile it has the disadvantage that it produce higher false alarm rate.

The two stages of Level 1 of the enhanced system are shown in Figure 3.

4.2.4.3 Data Set Description:

The new version of KDD data set is the NSL-KDD [19] dataset which consists of selected records of the complete KDD data set has the following advantages over the original KDD data set:

- It does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records.
- There are no duplicate records in the proposed test sets; therefore, the performances of the learners are not biased by the methods which have better detection rates on the

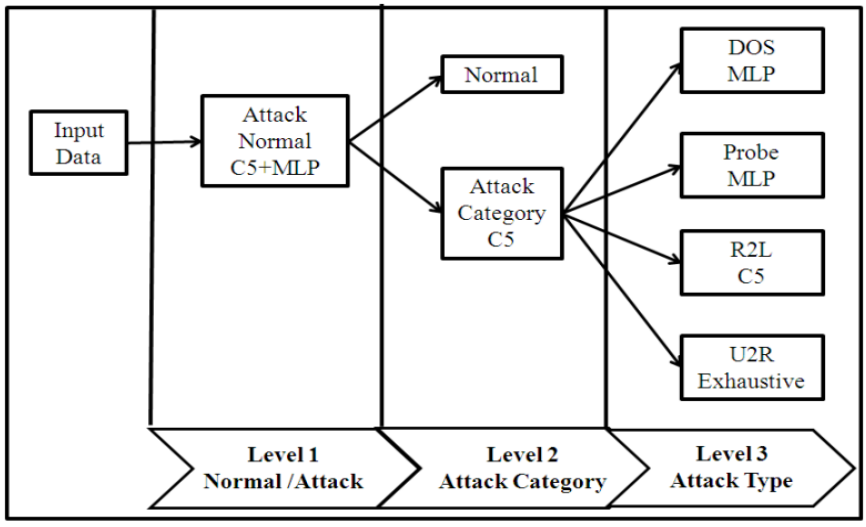

Figure 2 Levels of Enhanced Hybrid Systems

frequent records.

- The numbers of records in the train and test sets are reasonable, which makes it affordable to run the experiments on the complete set without the need to randomly select a small portion.

Consequently, evaluation results of different research works will be consistent and comparable. Although, the proposed data set may not be a perfect representative of existing real networks, because of the lack of public data sets for network-based IDSs, it is still believed that it can be applied as an effective benchmark data set to help researchers compare different intrusion detection methods [13].

The full description of the data set four attack categories, the 24 attacks types, and the three features groups are descripted in [12],[19].

4.2.4.4 Performance Measures:

To evaluate the newsystem two major indices of performance was used; the detection rate and the false alarm rate according to [20] 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.

5.EXPERIMENTS AND RESULTS:

Two experiments were performed:[21]

Experiment 1 was a comparison between using single level neural network and multi-level neural network intrusion detection system. The Single Level Neural Network examined the use of the neural network for classifying normal and attack type. The Multi- Level Neural Network 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.

Experiment 2 was to develop a hybrid multi-level intrusiondetection system. This experiment was a comparative studybetween different machine learning models and comparing theresults. The hybrid system uses multi-level as explained inexperiment 1. Each Level in the system is built with themachine learning algorithm that produced higher result for thislevel. The Hybrid Multi-Level was evolved to an EnhancedHybrid Multi-Level Intrusion Detection System which has adual protection phases in level 1.

5.1 Experiment 1:

This experiment aims to examine the difference between a multi-level MLP and single-level MLP. One of the objectives of the present experiment was to evaluate the possibility of achieving the same results with this less complicated neural network structure. Using a less complicated neural network is more computationally efficient. Therefore a single layer perception was used with no hidden layers for all the networks in this experiment. For each network 20% of the training data were set for cross validation. Early stopping criterion for validation set was applied to stop the training process to prevent over-fitting.

5.1.1 Dataset used in Experiment 1:

This experiment used neural network to check the ability of the intrusion detection system to identify attacks from different categories. There for two attacks from each DOS and

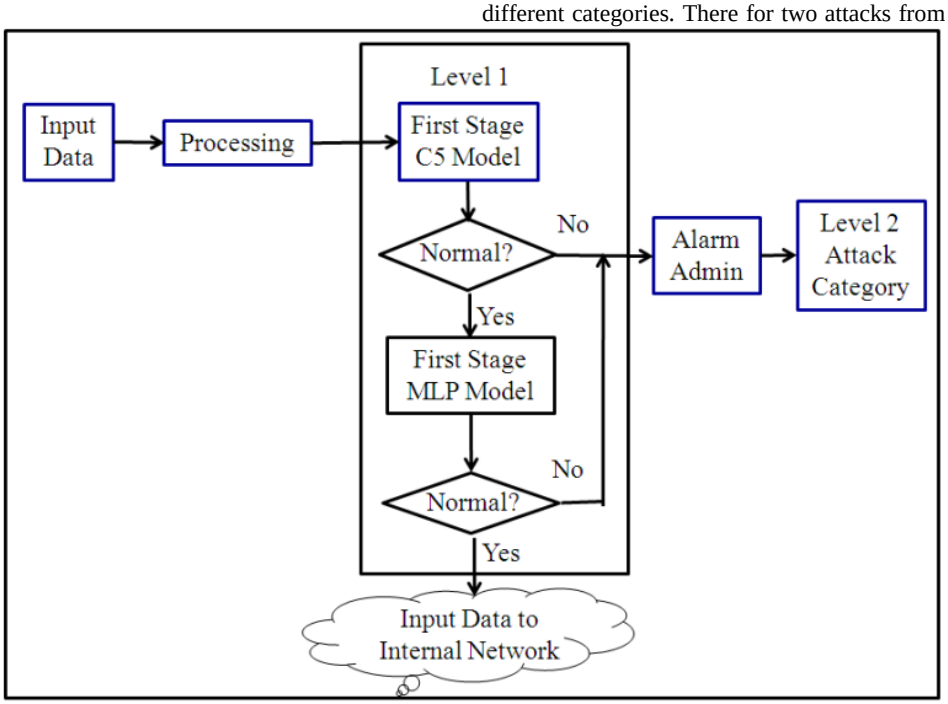

Figure 3 Dual Protection Storage of Enhanced Multi-Level Intrusion Detection System

Probe classesare used. The sample dataset contains 20000 record for training (10000 normal and 2500 for each attack type) and 1200 for testing (600 normal and 150 for each attack type).

5.1.2 Single Level Neural Network:

This network is a single layer feed-forward networks with activation function Soft-Max. The output layer of this network consists of 5 neurons (normal, Neptune, Smurf, Satan, Ports-weep).

The testing phase resulted summarized in Table 1 shows the Correct Classification Rate for each of the 5 classes and the total average classification accuracy of the single level neural network.

Table 1 single Level Classification Rate

Class Name	Training Set	Testing Set
Normal	99.4	99.3
Neptune	100	99.3
Smurf	99.8	100
Satan	100	100
Ports-weep	99.9	94.7
Average Success Rate	99.8	98.7
Error Rate	0.19	1.2

5.1.3 Multi-Level Neural Network:

All the 3 levels are a single layer perceptron feed-forward networks.The output layer of first level consists of two neurons one for normal and other for attack. The output layer of second level consists of two neurons one for DOS and other for Probe. There are two networks in level three. The first one contains two neurons one for Neptune and the other for smurf. The second network of level three consists of 2 neurons one for satan and the other for ports-weep.

The Testing results for Level 1, level 2, level 3 shown in table 2, table 3, and table4 respectively.

5.1.4 Discussion of Results of Experiment 1:

Building all the networks with a single layer perceptron with no hidden layers gave the advantage of less computation time and less complicated network. The experimental results show that using a multi-level neural network is more promising than single-level network as shown in following tables.

Table 2 Level 1 Classification Rate

Class Name	Correct Classification	
	Training Set	Testing Set
Normal	99.5	99.7
Attack	99.9	100
Average Success Rate	99.74	99.8
Error Rate	0.27	0.17

Table 3 Level 2 Classification Rate

Class Name	Correct Classification	
	Training Set	Testing Set
DOS	99.95	100
Probe	99.8	100
Average Success Rate	99.9	100
Error Rate	0.14	0

Table 4 Level 3 Classification Rate

Class Name		Correct Classification	
		Training Set	Testing Set
DOS	Neptune	100	100
	Smurf	100	100
Probe	Satan	100	98.7
	Ports-weep	100	99.3
Average Success Rate		100	99.5
Error Rate		0	0.5

Table 5 shows the Correct Classification Rate of testing dataset for each of the 5 classes for both Multi-level and single level.

Table 5 Classification Rate of Single-Level and Multi-Level

Class Name	Single-Level	Multi-Level
Normal	99.3	99.7
Neptune	99.3	100
Smurf	100	100
Satan	100	98.7
Ports-weep	94.7	99.3

5.2 Experiment 2:

The second experiment was developing a hybrid multi-level intrusion detection system. Seven distinct pattern recognition and machine learning algorithms were applied on the NSL-KDD dataset. This study was implemented using SPSS Clementine and Neuro Solution. The Hybrid Multi-Level was evolved to an Enhanced Hybrid Multi-Level Intrusion Detection System which has a dual protection phases in level 1.

5.2.1 Dataset used in Experiment 2:

Attacks from the four classes are used 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) as shown in table 5.7 & table 5.8.

5.2.2 Hybrid Multi-Level IDS*:*

The hybrid system uses algorithms in the fields of neural networks and decision trees. The examining by Neural Network used MLP, RBF and Exhaustive prune, while for decision trees used C5, CHAID, CRT and QUEST.

5.2.2.1 Level 1 output's:

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 6&table 7. C5 has a significant detection rate for known and unknown attacks but it produce higher false alarm rate compared to MLP.

Table 6 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

Table 7 Detection Rate &False Alarm Rate for Level 1

Classifier	Detection Rate	False Alarm Rate
MLP	91.4	5
RBF	78.1	9.6
Exhaustive	91.8	10.3
C5	95.6	9.4
CRT	82	15.8
QUEST	88	14.5
CHAID	85	10.4

5.2.2.2 Level 2 Output's

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 and U2R). Testing results showed that C5 & CRT (decision trees) produced best correct classification rate for second level as shown in table 8.

Table 8 Correct Classification Rate for Level 2

Classifier	Known Attacks	New attacks	Correct Classification Rate
MLP	95.1	56.3	82.8
RBF	86	50.8	74.8
Exhaustive	92.8	49.9	79.2
C5	98.4	59.3	86
CRT	96.5	62.7	85.8
CHAID	97.2	38.8	78.8

5.2.2.3 Level 3 Output's:

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.Results of Probe module showed that C5 & MLP are most efficient for detecting this type of attacks.Results of R2L module showed that C5 are most efficient for detecting this type of attacks significantly.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 9.

Table 9Attacks Classification Rate

Classifier	Correct Classification Rate			
Percentage	DOS	Probe	R2L	U2R
MLP	100	99.3	91	48.2
RBF	99.4	97.8	93	43.1
Exhaustive	99.9	97	91	54.4
C5	100	98.6	100	44.1
CRT	100	92.6	97	44.1
QUEST	99.9	94.1	96	35.3
CHAID	100	95.5	97	41.2

5.2.3 Enhanced Hybrid Multi-Level Testing Results:

The Enhanced Hybrid Multi-Level System contains a dual protection phase in level 1. The input data are input to the first protection phase which is C5 Model. Records that are classified as normal are passed to the second phase of protection which is a MLP model.Then a higher protection rate was obtained as some attacks that are bypassed by C5 are detected by the MLP whose nature differs from C5. The Statistics are shown in figure 4.

Known attacks detected by C5 = 6903

Known attacks detected by MLP = 22

Detection Rate of known attacks = (6903 + 22) / 6935 = 99.8%

Unknown attacks detected by C5 = 2784

Unknown attacks detected by MLP = 219

Detection Rate of Unknown attacks = (2784 + 219) / 3201 = 93.8 %

Total Detection Rate of Level 1 = (9687 + 241) / 10136 (Total No of Normal Records) = 97.95%

Total Correct Classification Rate of Level 1 = (8598[Normal] + 9687[C5 detected attacks] + 241[MLP detected attacks]) / (10136[TA] + 9647[TN]) = 93.65%

Total False Alarm Rate of Level 1 = (902 + 147) / 9647 (Total Normal) = 10.87%

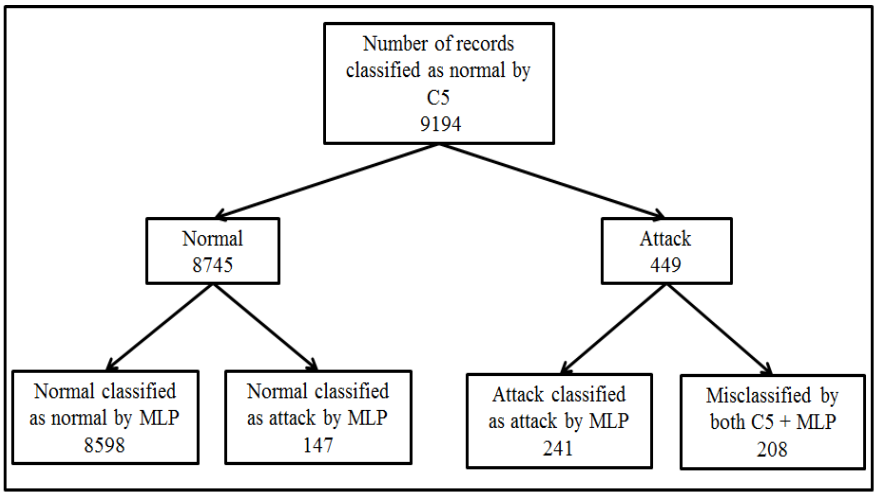

Figure 4 Summary of Results of Enhanced Hybrid Multi-Level System

5.2.4. Discussion of Results of Experiment 2:

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 multi-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, not necessary to re-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 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. The dual protection phases of first level in the Enhanced Hybrid Multi-Level Intrusion Detection System gave higher detection rate. Meanwhile it increases the false alarm rate of the proposed system.

6. CONCLUSION

In this work an Enhanced Hybrid Multi-Level Intrusion Detection System was developed. 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. The first level has dual protection phase. In the first phase of level one the data is passed through C5 Model which identifies whether the coming record is normal or 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 category of this attack.

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.

Each module is implemented with the most promising classifier that gave highest correct classification rate. Therefore, Hybrid model will improve the performance to detect intrusions.

The experimental results showed that the designed multilevel system has detection rate equal to 98% for both (known and unknown attacks). The first level is implemented by C5 decision tree & MLP Neural Network 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 Neural Network.While the neural networks are very interesting for generalization and very poor for new attacks attack 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 advantages of the proposed system is its high Detection Rate, scalability (if new attacks of specific class are added to the dataset, not necessary to re-train all the modules but only the modules affected by the new attack), adaptive (attacks that are misclassified by the IDS as normal activities or given 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), generalization ability (the proposed system outperforms previous IDSs in detecting both known and new attacks which combines the advantages of signature-based and anomaly-based IDS). Also every module can be trained on separate computer in parallel which provides less training time.

7. REFERENCES:

[1] Sherif M. Badr, *"Security Architecture for Internet Protocols", PhD thesis, Military Technical Collage*, 2001.

[2] Asmaa Shaker Ashoor, Prof. SharadGore,"Importance of Intrusion Detection System (IDS)", International Journal of Scientific & Engineering Research (IJSER), Volume 2, Issue 1, January-2011.

[3] Naelahokasha, Sherif M. Badr, Abd El Fatah Hegazy, "Towards Ontology-Based Adaptive Multilevel Model for Intrusion Detection and Prevention System (AMIDPS)", Egyptian science journal (ESC), Vol. 34, No. 5, September 2010.

[4] 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.

[5] SrinivasMukkamala, "Intrusion detection using neural networks and support vector machine", Proceedings of the IEEE International Honolulu, 2002.

[6] 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, November 15-18, 2004.

[7] S. Peddabachigari, A. Abraham, C. Grosan and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," J. Network Comput. Appl., 30: pp 114-132, 2007.

[8] OzgurDepren, Murat Topallar, EminAnarim and M. Kemal Ciliz, "An intelligent intrusion detection system for anomaly and misuse detection in computer networks," Expert Systems with Applications, Volume 29, Issue 4, pp 713-722, 2005.

[9] Dewan Md. Farid, NouriaHarbi, EmnaBahri, el "Attacks Classification in Adaptive Intrusion Detection using Decision Tree" International Conference on Computer Science (ICCS 2010), 29-31 March, 2010, Rio De Janeiro, Brazil.

[10] Mohammad SazzadulHoque, Md. Abdul Mukit and Md. Abu NaserBikas," An Implementation of Intrusion Detection System using Genetic Algorithm ", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[11] 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.

[12] KDD Cup 1999. 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] Bobor, V. "Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms", Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology, KTH/DSV, 2006.

[15] Aickelin, U., J. Greensmith, and J. Twycross. "Immune System Approaches to Intrusion Detection -A Review ", Natural Computing, Springer, 2007.

[16] Yao, J. T., S.L. Zhao, and L.V. Saxton, .A Study on Fuzzy ID. In Proceedings of the DM, ID, and Data Networks Security, SPIE, Vol. 5812, pp. 23-30, Orlando, Florida, USA, 2005.

[17] Gang, W., J. Hao, J. Ma and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," Expert Syst. Appl., 37: 6225-6232, 2010.

[18] 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.

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

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

[21] SaharSelimFouad "Implementation of Intelligent Techniques for Intrusion Detection Systems", master thesis, Egypt, 2011.