Erroneous Classified Attack: A Time-Bomb

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

ABSTRACT
Over the past several years, the Internet environment has become more complex and un-trusted. Enterprise networked systems are inevitably exposed to the increasing threats posed by hackers as well as malicious users internal to a network. Intrusion Detection System (IDS) technology is one of the important tools used now-a-days, to detect such threats, which is a predictable element of the computer network system. Various IDS techniques has been proposed, which identifies and alarms for such threats or attacks. Data mining provides a wide range of techniques to classify these attacks. Today's IDS faces a number of key challenging issues. The challenges like detect malicious activities of the large amount of network traffic. The main challenging if some attacks were sneaking as normal connection. [1]
This paper provides a proposed system which performs well when compare to other IDS also introduce a comparative study of strong and weak points with other system on the attack detection rate of these existing classification techniques.

Keywords: Intrusion detection; data mining; network security.

1. INTRODUCTION
The study of security in computer networks is a rapidly growing area of interest. This activity has been fueled by several recent network attacks. Consequently, network attacks or intrusions such as eavesdropping on information meant for someone else, illegally accessing information remotely, breaking into computers remotely, inserting erroneous information into files and flooding the network thereby its effective channel capacity are not uncommon. To overcome these problems, several proposals suggest the deployment of new, secure, and possibly closed systems by using methods that can prevent network attacks, e.g., encryption technique. But this solution is not suitable for infrastructure of open data networks, also it cannot protect against stolen keys or legitimate users misusing their privileges.

Network Intrusion Detection System (NIDS) and Prevention Systems (NIPS) serve a critical role in detecting and dropping malicious or unwanted network traffic. These have been widely deployed as perimeter defense solutions in enterprise networks at the boundary between a trusted internal network and the un-trusted Internet. This traditional deployment model has largely focused on a single-vantage point view of NIDS/NIPS systems, placed at manually chosen (or created) chokepoints to provide coverage for all suspicious traffic.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

The main objective of this work is to design and develop security architecture (an intrusion detection system) for computer networks. This proposed system should be positioned at the network server to monitor all passing data packets and determine suspicious connections. The proposed system should have a pre-knowledge about normal users behaviors as well as the different types of attacks. Therefore, it can inform the system administrator with the suspicious attack type. Moreover, the proposed system should allow new attack types to be defined, i.e. the proposed system should have an adaptive capability.

Finally, a comparative study with other system has done showing the main difference between the two systems focusing on the fetal mistake of the other system. [2]

Challenges to Intrusion Detection
There are many challenges to doing intrusion detection:

- False positives: Administrators can be totally bogged down by false positives which are essentially warnings about things.
- Learning curves: Intrusion detection can be a technically challenging environment that may require a substantial learning curve.
- Large Logs: Logs of events are useless unless that are looked at via some mechanism.
- Placement of IDS: Where do you place your IDS in order to effectively catch intrusion attempts?

2. RELATED WORK
Intrusion detection (ID) is a major research problem in network security, where the concept of ID was proposed by Anderson in 1980. ID is based on the assumption that the behavior of intruders is different from a legal user. The goal of intrusion detection systems (IDS) is to identify unusual access or attacks and raises an alarm whenever a suspicious activity is detected to secure internal networks. Several machine-learning techniques including neural networks, fuzzy logic, support vector machines (SVM) have been studied for the design of IDS. In particular, these techniques are developed as classifiers, which are used to classify whether the incoming network traffics are normal or an attack. [3]

There are researches that implement an IDS using Multilayer perceptron (MLP) which have the capability of detecting normal and attacks connection also MLP not only for detecting normal and attacks connection but also identify attack type.

Some researches apply Decision Tree (C4.5 Algorithm) as intrusion detection models.

Others discuss the use of artificial neural networks for network intrusion detection. Though the neural networks can work effectively with noisy data, they require large amount of data for training and it is often hard to select the best possible architecture for a neural network.

Some authors proposed a simple practical layered approach to intrusion be computation. They discussed that such a system would decrease computational intensive and be more accurate. They proposed a three layer system to ensure complete security viz. availability, integrity and confidentiality, each layer corresponding to one aspect of security. The first layer or the connection establishment layer corresponds to the packet level features such as source and destination IP address, number of connections to the host, source and destination port number, user ID etc. and is optimized to detect attacks exploiting the availability aspect such as DOS attacks, probes, etc. the second layer which is the privacy layer ensures data confidentiality and refers to features such as files accessed, data retrieved etc. The third layer or access control layer ensures integrity of data and is more concerned with the file modifications, user privileges etc.

Other authors discussed layered approach and compared the proposed Layered Approach with the decision tress, naive Bayes classification methods. Their syste**m is based upon serial layering of multiple hybrid detectors.**

3. GENERAL ASPECTS

The proposed system is a modular network-based intrusion

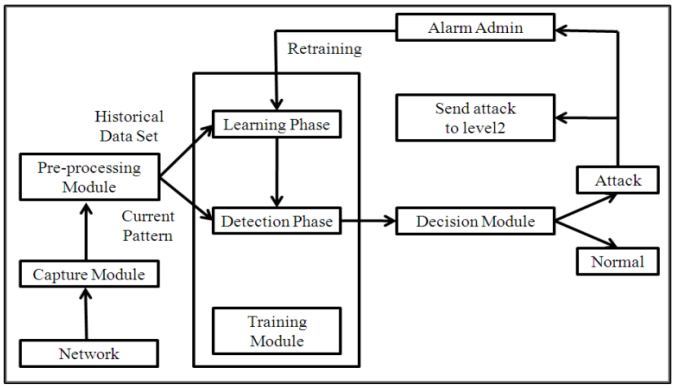

Figure 1 System Architecture

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.

3.1. The System Components:

3.1.1. 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.

3.1.2. 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:

3.1.2 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.

*3.1.2.2. 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.

3.1.2.3. 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.

*3.1.3. The classification Module***:**

3.1.3.1 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.

3.1.3.2 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.

3.1.3.4. 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.

3.2 Data 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 environment to acquire raw TCP/IP dump data for a local area network (LAN) simulating a typical U.S. Air Force LAN [8].

There are some inherent problems in the KDDCUP'99 data set, which is widely used as one of the few publicly available data sets for network-based anomaly detection systems

The data in the experiment is acquired from the NSLKDD 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. 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 [8].

We used attacks from the four classes to check the ability of the intrusion detection system to identify attacks from different categories. The two approaches are examined by two techniques:

1) Test with New Attack: The sample dataset contains 83644 record for training (40000 normal and 43644 for attacks) and 19784 for testing (9647 normal, 6935 for known attacks and 3202 for unknown attacks).
2) Test by Data Partitioning: The sample dataset contain 103427 records is partitioned by 10% (10156 records) for training and 90% (93271 records) for testing.

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.

3.3 Performance Measure:

To evaluate our system we used two major indices of performance. We calculate the detection rate and the false alarm rate according to 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.

There are four major categories of networking attacks. Every attack on a network can be classified into one of these groupings.

1) 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.
2) 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.
3) 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.
4) Probing Attack: is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls.

For our results, we give the Precision, Recall, and F-Value and Accuracy. Achieving very high accuracy is very easy by carefully selecting the sample size but if we use accuracy as a measure for testing the performance of the system, the system can be biased and can attain very high accuracy. However, Precision, Recall, and F-Value are not dependent on the size of the training and the test samples.
They are defined as follows:

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F-Value} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision} + \text{Recall}}$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Where TP, FP, FN and TN are the number of True Positives, False Positives, False Negatives and True Negative, respectively, and corresponds to the relative importance of precision versus recall and is usually set to 1.
We divide the training data into different groups; DOS, Probe, U2R, and R2L. Similarly, we divide the test data.

3.4. Machine Learning Algorithms Applied to Intrusion Detection:

Three distinct machine learning algorithms were tested on the NSL-KDD dataset. These algorithms are C5.0 decision trees, Multi-Layer Perceptron neural networks, and Naïve Bayes.

3.4.1. C5.0 Decision Trees:

Decision trees have also been used for intrusion detection]. 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. Each decision tree represents a rule which categorizes data according to these attributes. A decision tree consists of nodes, leaves, and edges.
See5.0 (C5.0) is one of the most popular inductive learning tools originally proposed by J.R.Quinlan as C4.5 algorithm.
C5.0 can deal with missing attributes by giving the missing attribute the value that is most common for other instances at the same node. Or, the algorithm could make probabilistic calculations based on other instances to assign the value. Single C5 acquires pruned decision tree with pruning severity 75% and winnowing attributes.

3.4.2. Multi-Layer Perceptron (MLP) Neural Networks:

The neural network gains the experience initially by training the system to correctly identify pre-selected examples of the problem.
The most popular static network is the MLP .MLP are feed-forward neural networks trained with the standard back propagation algorithm. They are supervised networks so they require a desired response to be trained. They are widely used for pattern classification. With one or two hidden layers, they can approximate virtually any input–output map.

3.4.3. Naïve Bayes:

Naive Bayes classifiers have also been used for intrusion detection. However, they make strict independence assumption between the features in an observation resulting in lower attack detection accuracy when the features are correlated, which is often the case for intrusion detection.

4 THE PROPOSED MODELS AND RESULTS

The proposed model was implemented through three steps (papers) each one dealing with a problem to take judgment then turn into the next step till getting the final shape:

4.1 Layered-Model Approach for intrusion detection systems:

In this step we compared the results of 2 different approaches of intrusion detection system (Phase and Level Approach). Phase Approach consists of three detection phases. The data is input in the first phase which identifies if this record is a normal record or attack. If the record is identified as an attack then the module inputs this record to the second phase which identifies the class of the coming attack. The second phase module passes each attack record according to its class type to phase 3 modules. Phase 3 consists of 4 modules one for each class type (DOS, Probe, R2L, U2R) as shown in figure 2.

Each module is responsible for identifying the attack type of coming record, while the Level approach consists of 3 independent detection levels. The First Level is to detect normal or attack profiles. The Second Level is to detect normal records and classify the attacks into four categories independently on the results of the first level. The third Level is to classify each attack type and normal records [4], [5].

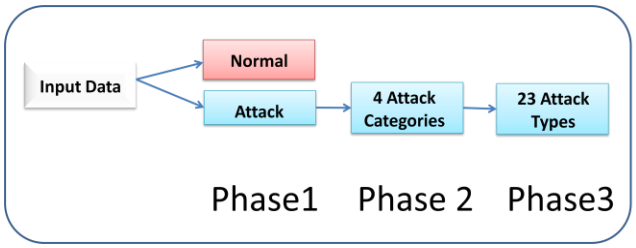

Fig 2: Layered-Model Approach System

We examined each model approach using different decision trees modules (C5, CRT, QUEST and CHAID). Each module is implemented by applying 2 techniques (New Attacks and Data Partitioning Techniques) .First, New Attacks Technique is to add new attacks in testing. Second, Data Partitioning Technique is to divide the dataset into 10 %for training and 90% for testing.

New Attacks technique is more realistic than Data Partitioning technique as in real life we are exposed to new attacks every second which we can't expect.

The results show that C5 decision tree has the most significant detection rate for both phase and level approaches. CRT & CHAID have promising results in Data Partitioning technique for both phase and level approaches as shown in table 1, 2.

Quest has high classification rate when adding new attacks in the second level.

Table 1 Classification Rate of Phases with New Attacks

Classifier	Correct Classification Rate		
	Phase 1	Phase 2	Phase 3
C5	100%	85.34 %	99.32%
CRT	100%	83.62 %	97.55%
Chaid	100%	85%	98.73%
Quest	100%	73.11 %	93.48%

Table 2 Classification Rate of Phase with Data Partitioning

Classifier	Correct Classification Rate		
	Phase 1	Phase 2	Phase 3
C5	100%	99.98 %	99.49%
CRT	100%	99.97%	97.02%
Chaid	100%	99.79%	97.38%
Quest	100%	93.74%	93.25%

The experimental results showed that Phase Model approach has Higher Classification Rate in New Attacks and Data Partitioning Techniques than Level Model approach. Therefore, the phase approach is more realistic than Level approach as in real life we are exposed every second to new attacks that we don't expect.

The next will be directed towards finding ways to prevent propagating errors in phase model, also using other Machine learning techniques in our experiments for detecting more types of intrusions.

4.2 Enhanced Layered-Model Approach for Intrusion Detection Systems:

A multi-Layer intrusion detection system has been developed to achieve high efficiency and improve detection and classification rate accuracy. The proposed system consists of two stages. First stage is for attack detection and the second stage is for attack classification. The data is input in the first Stage which identifies if this record is a normal record or attack [3].

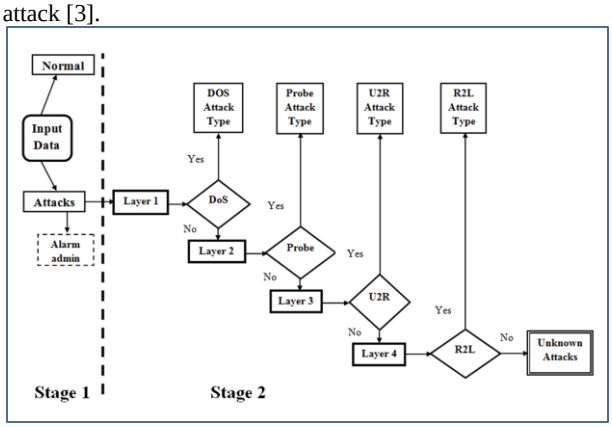

Fig 3: Enhanced Layered-Model Approach System

If the input record was identified as an attack then the administrator would be alarmed that the coming record is suspicious and then introduced to the second stage which consists of four sequential layers that specifies the class of this attack (DOS, Probe, U2R or R2L). Finally the administrator would be alarmed of the expected attack type as shown in figure 3.

We examined each layer using different machine learning models (C5, MLP & Naïve Bayes) then we implemented our system with gain ratio feature selection technique for selecting the best features for each layer based on the attacks' type that the layer is trained to detect rather than using all the 41 features.

The advantage of the proposed multi-layer system is not only the higher accuracy but also the multi-layers improve scalability as when new attacks of specific class are added to the data set; there is no need to train all the layers but only the layer affected by the new attack. Attacks that are misclassified by the IDS as normal instances or given wrong attack class / type will be relabeled by the network administrator as the

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 .In addition, Our proposed system propagates errors as to simulate the real system and results be more accurate and real.

Table 3 Detection Rate & False Alarm Rate for Stage 1

Classifier	Detection Rate	False Alarm Rate
C5.0	100	0
MLP	93.38	9.5
Naïve Bayes	98.58	16.78

Table 4 Performance Measure for Stage 1

Classifier	Precision (%)	Recall (%)	F-Value (%)	Accuracy (%)
C5.0	100	100	100	100
MLP	90.41	92.86	91.62	91.89
Naïve Bayes	83.22	98.21	90.18	91.1

Our experimental results show that C5 is very effective in improving the attack detection rate and classification rate with low False Alarm Rate as shown table 3, 4.
Feature selection using Gain Ratio and implementing the Layered Approach reduce the time required to train and test the model significantly. Most of the present methods for intrusion detection fail to reliably detect R2L and U2R attacks, while our proposed system can efficiently detect and classify such attacks.

Table 5 Performance Measure for Dos Layer

Classifier	Precision %	Recall %	F-Value %	Accuracy %
C5.0	100	100	100	100
MLP	97.29	87.34	92.04	88.97
Naïve Bayes	83.5	88.5	85.9	81.74

Table 6 Performance Measure for Probe Layer

Classifier	Precision %	Recall %	F-Value %	Accuracy %
C5.0	100	100	100	100
MLP	74.5	83.49	78.21	70.92
Naïve Bayes	84.1	99.6	91.2	88.86

Table 7 Performance Measure for U2R Layer

Classifier	Precision %	Recall %	F-Value %	Accuracy %
C5.0	100	100	100	100
MLP	80	32.65	44.84	96.17
Naïve Bayes	100	100	100	100

Table 8 Performance Measure for R2L Layer

Classifier	Precision %	Recall %	F-Value %	Accuracy %
C5.0	100	100	100	100
MLP	66.67	2.11	4.1	88.21
Naïve Bayes	100	100	100	100

The experimental results also show that C5 decision tree has significant detection and classification rate for both stages as shown in tables 5,6,7,8. Using Gain Ratio significantly enhances the accuracy of U2R and R2L for the three machine learning techniques (C5, MLP and Naïve Bayes). It was shown that MLP has high classification rate when using the whole 41 features in DOS and Probe layers.

4.3 Adaptive Enhanced Layered-Model Approach for Intrusion Detection Systems:

The purpose of this step was to enhancement of the previous work in section 4.2., where If the output record of second step 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 stage which consists of four fixed sequence of layers that specifies the class of this attack (layer 1 for DOS, layer 2 for probe, layer 3 for U2R or layer 4 for R2L), otherwise if the attack not classified as one of known attack classes, our model classify it as unknown attack. Finally the administrator would be alarmed of the expected attack type [6], [7].
The new modification for the model of section 4.2., was how to make the model adapted by changing the sequence of the 4 layer classification to get the optimum combination for highest classification rate.

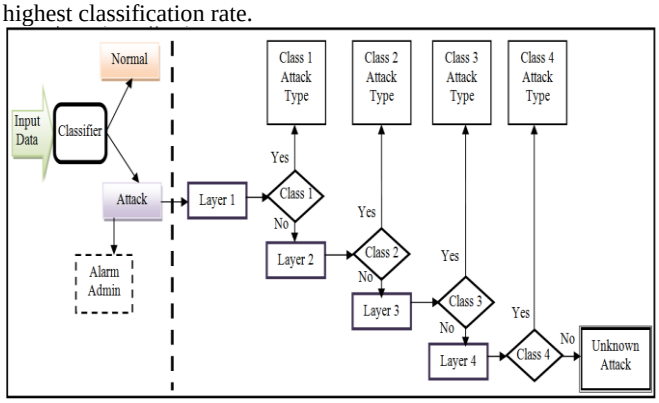

Fig 4: Adaptive Enhanced Layered-Model Approach System

Actually each combination was performed by 4 experiments. For example in the experiment number 1, after 1st stage classifier, the attacks connection start with DOS attack type classifier as class 1 attack type, then Probe attack type classifier as class 2 attack type, then U2R attack type classifier as class 3 attack type, then R2L attack type classifier as class 4 attack type, finally the connection classified as unknown attack. This means 94 experiments for the 24 model that were performed as shown in figure 4.
In this step, the model is enhanced by not specifying the layer class type so it will be more flexible and adaptive in any environment.
The experimental results showed that the proposed model with different order of training classes enhances the accuracy specially of U2R and R2L.
Also experimental results showed that the adaptive model takes less training computations because each layer act as a filters that classifies the attacks of each layer category which eliminate the need of further processing at subsequent layers.
Also the model is flexible to any combination of classes desired to be implemented. The experimental results shows the best combination sequence R2L, DOS, U2R, and Probe which get the highest classification rate for all attacks categories. All the procedures can be summarized in following algorithm.

Algorithm:

Step 1: *Each input record will be detected if either*

normal or attack in the first stage.

Step 2: *If the input record is identified as an attack, it will be pass through the second stage, and the administrator will be alarmed with the suspicious record.*

Step 3: *Separately perform Gain Ratio Feature selection for each layer (DOS, Probe, U2R, and R2L).*

Step 4: *Train each layer with three machine learning techniques (C5, MLP, and Naïve Bayes).*

Step 5: *In each Layer, the attack records are tested; if it is categorized correctly then its attack class/type will be identified.*

Step 6: *if the attack record pass to the next layer then it couldn't be classified in previous layer.*

Step 7: *Records that couldn't be classified in any layer then it will be classified as unknown attack and will be relabeled by the 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 by notifying the network administrator. If the attack record was not detected at any layer, then it will be detected as unknown until it relabeled by the admin.

5 COMPARATIVE STUDY

Intrusion detection is the process of trying to find out activities that violate security policy when they are taking place in computer networks and systems. Since its invention, intrusion detection has been one of the key elements in achieving information security. It acts as the second-line defense which supplements the access controls [1].

When the controls failed, the intrusion detection systems should be able to detect it real-time and warn the security officers to take prompt and appropriate actions. The main challenges how to detect malicious activities and correct classification of large amount of network traffics [9]. All possible cases can be shown as follow:

1- Normal classified as attach.
2- Attack classified as attack with wrong types.
3- Attack classified as attack with right types.
4- Attack classified as normal.

The first two cases the erroneous not harmful to the computer network, but the last two cases represent the serious problem for the computer system.

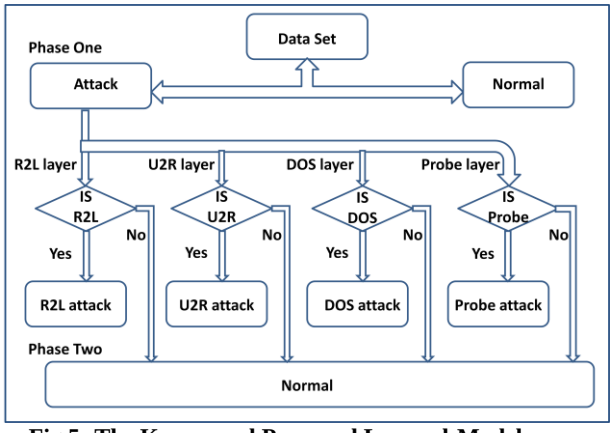

Fig 5: The Kumaravel Proposed Layered-Model

The kumaravel model [10],[11], show that if first layer detect a malicious activity then transfer it to the second layer for classify this malicious activity as proper type by passing through R2L classifier layer, U2R classifier layer, DOS classifier layer, finally Probe classifier layer.

In case the model not recognizes the malicious activity to suitable (correct) type, it re-classified it as normal activity, which is a time-bomb as shown in figure 5.

Our model solve this problem by re-classify the attack activity which not classified to one of four attacks types as general attack and the administrator can take a general action to stop this malicious activity.

6 CONCLUSION

In this work an Adaptive Enhanced Layered-Model for Intrusion Detection system was represented and experiments show very high detection classification rate, this results obtained through three steps each one solve and enhance a problem. Also a comparative with the kumaravel model [10],[11], which criticized previous intermediate model with his work but our final model show the superiority of our proposed model.

7 REFERENCE

[1] Sneha Kumari1, Maneesh Shrivastava, "A Study Paper on IDS Attack Classification Using Various Data Mining Techniques": International Journal of Advanced Computer Research, Vol. 2 No. 3, Sep., 2012.

[2] Naelah Okasha, Sherif M. Badr, Prof. A. Hegazy, "Towards Ontology-Based adaptive multilevel Model For Intrusion Detection and Prevention System (AMIDPS), ECS, Vol. 34, No. 5, Sep., 2010. http://net2.shams.edu.eg/ecs/

[3] Heba Ezzat Ibrahim, Sherif M. Badr , M. Shaheen, "Adaptive Layered Approach using Machine Learning Techniques with Gain ratio for Intrusion Detection systems", IJCA, Vol. 56, No. 7, Oct. 2012. http://www.ijcaonline.org/archives/volume56/number7/8901-2928

[4] Heba Ezzat Ibrahim, Sherif M. Badr , M. Shaheen, "Phases vs. Levels using Decision Trees for Intrusion Detection Systems", IJCSIS, Vol. 10, No. 8, Aug 2012. http://sites.google.com/site/ijcsis/

[5] Sherif M. Badr, "Implementation of Intelligent Multi-Layer Intrusion Detection Systems (IMLIDS)", IJCA, Jan. 2013. http://www.ijcaonline.org/archives/volume61/number4/9918-4526

[6] Sherif M. Badr, "Adaptive Layered Approach using C5.0 Decision Tree for Intrusion Detection Systems (ALIDS), IJCA, Mar. 2013. http://www.ijcaonline.org/archives/volume66/number22/11247-5956

[7] Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri, "Layered Approach Using Conditional Random Fields for Intrusion Detection", IEEE Transactions on dependable and secure Computing, vol. 5, no. 4, October-December 2008.

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

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

[10] A.Kumaravel, M.Niraisha, "Comparison of two Multi-Classification Approaches for Detecting Network Attacks", IJAIR Vol. 2, Issue 5, may 2013.

[11] A. Kumaravel, M. Niraisha, "Multi-Classification Approach for Detecting Network Attacks,"International Conference on Information and communication Technologies (ICT 2013), ICT545,4, Apr. 2013.