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:

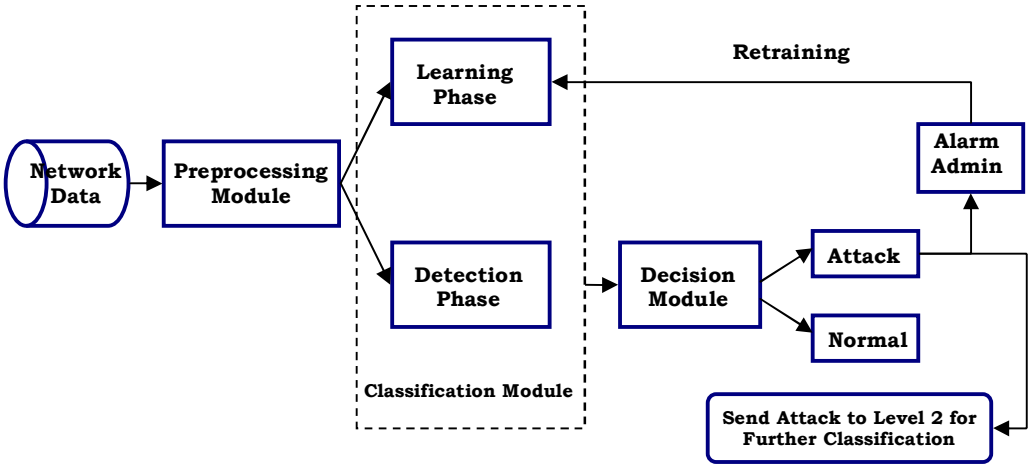

Figure 1. System architecture

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