Novel Network Intrusion Detection System using Hybrid Neural Network (Hopfield and Kohonen SOM with Conscience Function)

Wesam K. AL-Rashdan
AL-Balqa'a Applied University, Irbid College, Jordan

Reyadh Naoum
Arab Academy for Financial and Banking Sciences, IT College, Jordan

Wafa' S. Al_Sharafat
Al Al-Bayt University, IT College, Jordan

Mu'taz Kh. Al-Khazaaleh
AL-Balqa'a Applied University, Irbid College, Jordan

Summary
Intrusion detection technology is an effective approach to dealing with the problems of network security. In this paper, it presents an intrusion detection model based on hybrid neural network and SVM. The key idea is to aim at taking advantage of classification abilities of neural network for unknown attacks and the expert-based system for the known attacks. We employ data from the third international knowledge discovery and data mining tools competition (KDDcup'99) to train and test the feasibility of our proposed neural network component. According to the results of our experiment, our model achieves 97.2 percent detection rate for DOS and Probing intrusions, and less than 0.04 percent false alarm rate. Expert system can detect R2L and U2R intrusions more accurately than neural network. Therefore, Hybrid model will improve the performance to detect intrusions.

Key words:
Novel Network, IDS, SOM, Hybrid Neural Network

1. Introduction

This paper describes an integrated neural network and SVM for intrusion detection Model. Our Model consists of three phases: Phase-1 clustering and Selecting, we use some classification and clustering methods such as K-Medoid. Phase-2 Training, we build the Hybrid NN system to generate a new set for each type of attacks. We use Hopfield network to detect known intrusions, and Kohonen SOM to detect Unknown intrusions and then create new vectors similar to original ones. This will expand number of vectors that will be used by SVM in Phase-3 learning and detecting phase. Therefore, our integrated model improves the performance to detect most intrusions. Our experiment results demonstrate efficiency and accuracy of the detector.

2. An integrated IDS model

With the combination of the misuse detection and anomaly detection, can IDS have an effective detection on the known attack and the capabilities of monitoring the unknown attacks. To improve the identification rate of the IDS and put it into use, an intrusion detection model based on integrated neural network and expert system has been designed. The model consists of the following three important Phases: phase-1 Clustering and Samples Selection, Phase-2 Training phase, phase-3 Learning and Testing.

The engine of classifier match the decoded data based on each protocol fields to the rules in the attack signature database. If the result of match is true, the detective engine will alarm. This module belongs to misuse detection. Meanwhile, the decoded data also feed to the Data Formatting Module which can make data numerical so as to be dealt with Artificial Neural Network (ANN) component [1][2]. The ANN component executes anomaly detection with its output

processed by the engine of intrusion detection. As the host-based intrusion detection method, the statistical analysis module can compare statistical data about the characteristics on security of the host and system logs with those expected features under the normal situation. The statistical analysis module will carry on measurement at regular time. If the data exceed the predicted threshold, the engine will alarm. In the following part the classifier, ANN, SVM will be introduced as shown in figure 1.

2.1 Clustering and Samples Selection Phase

The model captures the data from training dataset which exists in the environment unit.

1. The Codification Unit coding data into appropriate format.
2. The Features Extraction Unit, extracting data into data vector of 41 to 42 feature.
3. The Clustering Unit clusters the input dataset by two steps as follows:

   a-Clustering the Dataset into 16-Cluster according to the number of the different features

Manuscript received November 5, 2010
Manuscript revised November 20, 2010

which works to determine the main Clusters according to the intrusions intrusion type (Normal, DoS, Prob., R2L, U2R) using K-Means and K-Medoid algorithms, to choose the algorithm with best results.

b-The Sample Selection Unit, selects The representative set of vectors for each class, i.e. the significant vectors.

2.2 Training Phase (ANN Unit)

The work flow can be ordered as follows:

4. The Sample Selection Unit selects The representative set of vectors for each class, i.e. the significant vectors.
5. The Novel Hybrid Neural Network Model of supervised with unsupervised NN algorithms (Hopfield and Kohonen SOM with Conscience Function) acts as a training machine, to generate new representative set of vectors for each class[1].

Hopfield NN and Kohonen's SOM with Conscience function will work as follows; Using Hopfield NN as a classifier only for patterns that have been labeled as attacks to determine the type of attack (DoS, Prob., R2L, U2R) and Using Kohonen's SOM with Conscience function as a classifier only for patterns that haven't been labeled to determine the type of attack (DoS, Prob., R2L, U2R). This work executes in the following manner :

Extract Data Pattern features then Check whether that data pattern is labeled or not. If the data pattern labeled then check whether its normal or abnormal. If the data pattern labeled as normal then let it pass through the system. If the data pattern labeled as abnormal then send it to the Hopfield NN unit in Hybrid NN model. If the data pattern is not labeled then send it to the Kohonen's SOM with Conscience function unit in Hybrid NN model.

The output of the HNNMLM model will be combined to the output of phase-1 and this will expand the set of intrusions vectors that we can compare with in phase-3. This will help us in detecting more new attacks.

2.3 Learning and Testing Unit

The work flow can be ordered as Following:

1. comparing new vectors from testing data with a grouped set of vectors which is formed from the union of main clusters vectors and the vectors the have been generated by Hybrid Neural Network Model.
2. Identifying Attack type according to the main attacks types. The Support Vector machine (SVM) method [4][5] for features ranking will be used as testing unit in order to build a new IDS as a try to maximize the Detection Rate (DR),and/or to minimize the False Positive Rate (FPR) and to minimize the testing time.

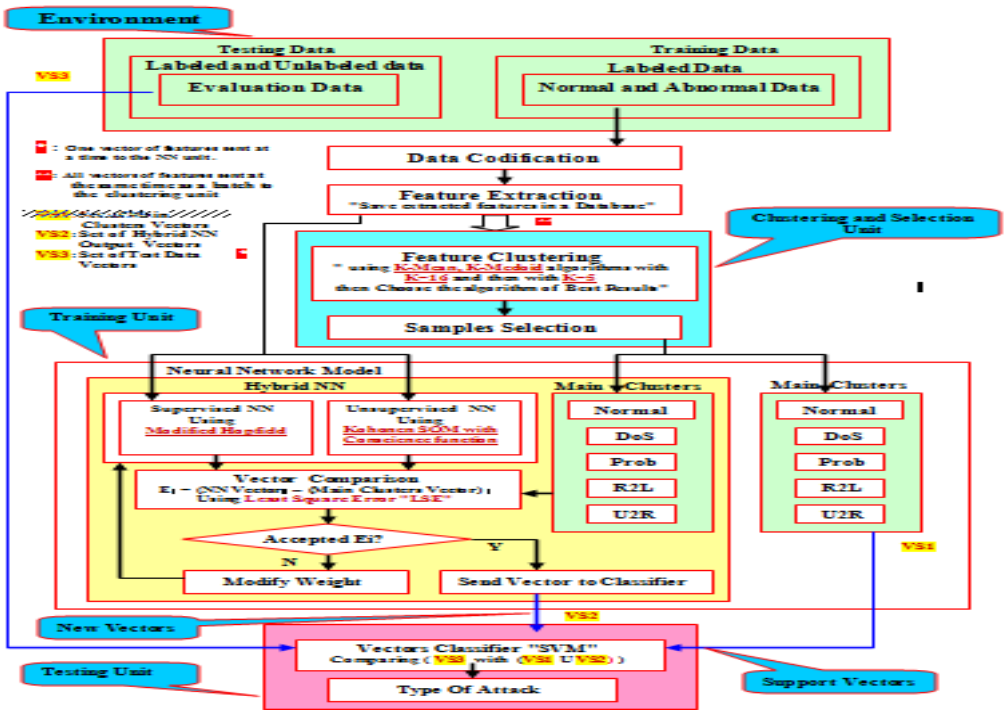

Figure 1. Novel Hybrid NN Machine Learning Model

3. Experiments and Results

To illuminate the performance of the model, we employ data from the third international knowledge discovery and data mining tools competition (KDDcup'99)[3] to train and test the feasibility of our proposed model. In the KDD dataset, the training set contains 494021 samples and the test set contains 311029 samples. Nearly 80% of samples are DoS attacks. Samples of normal connection are about 20%. Other types of attack samples, including U2R (0.011%), R2L (0.228%) and Probe (0.831%), are really rare. It is important to note that the test data is not from the same probability distribution as the training data. It includes 17 specific attack types those are not in the training set. This makes the dataset more realistic. We select normal dataset, Neptune attack, Portsweep attack, satan attack, buffer_overflow and guess_passwd datasets to train and test our IDS prototype. The complete description of features is found in [3]. The normal and 5 attack categories are numbered as follows:1-normal, 2-neptune ,3-satan, 4-portsweep,5-buffer_overflow,6-guess_passwd. Network intrusion detection is a two-class classification problem. Its effectiveness can be defined as the ability to make correct class predictions of samples. For each single prediction, there are four different outcomes (known as the confusion matrix for the two-class case shown in Table 1).

The true-positives and true-negatives are correct classifications. A false-positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. Although this type of error may not be completely eliminated, a good system should minimize its occurrence to provide useful information to the users. A false-negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior. In other words, malicious activity is not detected and alerted. It is a more serious error. Notably, in a real world system, the effect of incorrectly detecting abnormal
network behavior (false-negative) is different from that of incorrectly predicting normal classification outcome (false-positive). These two kinds of errors will generally have different costs; likewise the two types of correct classification will have different benefits.

Table 1. Confusion Matrix [6]

Predicted / Actual	**Negative**	**Positive**
Actual	**a**	**b**
Negative	**c**	**d**
Precision rate (PR)	**= d / (b + d)**	
Recall rate (RR)	**= d / (c + d)**	
False-Positive rate (FBR)	**= b / (a + b)**	
False Negative rate (FNR)	**= c / (c + d)**	

We get 3000 train data patterns from 10% training set and 10000 test data patterns from Test set which has attack patterns that are not present in the training data. Therefore Problem is more realistic. The training of the neural networks was conducted using back propagation algorithm using scaled conjugate Kohonen network structure for IDS gradient decent for learning. The network was set to train until the desired mean square error of 0.001 was met or 1500 epochs was reached. During the training process, the performance of Hopfield and Kohonen network is 0.00157434 at 1500 epochs. We put 10000 data into the TESTSET for Kohonen network. The classified results, the false positive and detect rate are obtained as the follows:

The test result indicates that in total 99.6% of the actual "normal" examples were recognized correctly. For DOS and Probing intrusion (2-neptune,3-satan,4-portsweep) ,we can obtain the average detect rate of 96.6% and the false positive rate of 0.049%. Because all buffer_overflow and guess_passwd attacks fail to be classified by Kohonen network, we only obtain the average detect rate of 64.9% and the false positive rate is 26.7% for all the five kinds of attacks. However, these two kinds of attacks can be accurately detected by rule-based detector. Hopfield can detect the R2L and U2R intrusions more accurately than neural network. Thus, taking advantage of the performance of each module for various attacks, the model improves the detection rate for all intrusions.

All the experimental results are summarized in Table 2.

Our experiment show that the training time of our model 1s 1450 seconds. However the training time for BPN is 21746 seconds.

Table 2. The experimental result in confusion matrix

Predicted / Actual		Prob.	DoS	U2R	R2L
Prob.	ours	2540	91	509	8
	BPN	2515	181	0	0
Dos	ours	560	227050	156	0
	BPN	25	222153	0	0
U2R	ours	20	0	78	8
	BPN	0	0	0	0
R2L	ours	20	470	150	6660
	BPN	4	2	0	0

PR	ours	76.2%	99.1%	9.5%	76.5%
	BPN	91.1%	99.6%	00.0%	00.0%
RR	ours	61.0%	98.8%	36.4%	41.5%
	BPN	60.3%	96.7%	00.0%	00.0%
FPR	ours	24.7%	01.2%	91.0%	24.6%
	BPN	8.96%	0.42%	00.0%	00.0%
FNR	ours	37.6%	02.3%	65.3%	59.1%
	BPN	39.6%	03.4%	100.0 %	100.0 %

4. Conclusion

In this paper a new model is introduced for learning intrusion detection in networks. We develop an integrated hybrid neural network and SVM model for intrusion detection. Firstly, we build the hybrid NN to improve the detection rate for known and unknown attacks. Hopfield network works on detecting known attacks, Kohonen network works on detecting unknown intrusions. Experiment show that our model could gain effective with better classification, better detection rate, and less training and learning time. Therefore, our model improves the performance to detect all intrusions. Our experiment results demonstrate efficiency and accuracy of the detector. Specially, the neural network could provide significant benefits to intrusion detection through data reduction, classification, clustering the unlabeled system log data, and the each process of identifying intruders.

References

[1] A.Bivens, C.Palagiri, R.Smith, B.Szymanski, “Network-Based Intrusion Detection Using Neural Networks”, 2002

[2] J Cannady, “Artificial Neural Networks for Misuse Detection”, National Information Systems Security Conference (NISSC’98), Arlington. VA., Oct.1998, pp. 443-456.

[3] S.J. Stolfo, et al. “KDD cup 1999 dataset”. UCI KDD repository. http://kdd.ics.uci.edu, 1999

[4] V. N. Vapnik, Statistical learning theory. Adaptive and learning systems for signal processing, communications, and control, New York: Wiley, 1998.

[5] S. Kaplantzis, “Classification techniques for network intrusion detection,” 4th year thesis project, Monash University, 2004.

[6] R. Kohavi, F. Provost, "Glossary of Terms," Machine Learning, vol. 30, no. 2-3, 1998, pp. 271-274.