Intrusion Detection Using Emergent Self-organizing Maps*

Aikaterini Mitrokotsa and Christos Douligeris

Department of Informatics University of Piraeus,
80 Karaoli and Dimitriou Str. Piraeus 18534, Greece
{mitrokat, cdoulig}@unipi.gr

Abstract. In this paper, we analyze the potential of using Emergent Self-Organizing Maps (ESOMs) based on Kohonen Self –Organizing maps in order to detect intrusive behaviours. The proposed approach combines machine learning and information visualization techniques to analyze network traffic and is based on classifying "normal" versus "abnormal" traffic. The results are promising as they show the ability of eSOMs to classify normal against abnormal behaviour regarding false alarms and detection probabilities.

1 Emergent Self Organizing Maps vs KSOM

In this paper, we propose an intrusion detection approach that is based on a class of neural networks known as Kohonen's Self-Organizing Maps (KSOMs) [1]. Our approach combines information visualization and machine learning techniques and enables us with the ability to have a visual view of network activity. The proposed approach produces promising results in its ability to classify normal against abnormal behavior. Emergent SOMs (ESOMs) are based on simple KSOMs but present some advantages over them that can be exploited in order to achieve better results in the detection of intrusions.

One of the basic disadvantages of SOM maps is that their abilities are limited to a few neurons. In a Kohonen's SOM to each neuron correspond the best matches of a great number of input data. So in a way each neuron represents a cluster. On the other hand, Emergent SOMs may expand from some thousands to tens of thousands of neurons. In some cases the number of neurons may be greater than the number of input data. The cooperation of such a big number of neurons leads to structures of a higher level.

We trained Emergent Self Organized Maps with logs ([2],[3]) of network traffic and exploited the main advantage of Emergent SOMs the large number of neurons. In order to visualize these structures the U-Matrix method is used. This method permits us to achieve a good visualization of the network traffic and observe the existence of possible intrusions.

Each log of network traffic is represented by a vector with some fixed attributes. Each vector has a unique spatial position in the U-Matrix [3] and the distance between

* This work was partially supported by the GSRT under a PENED grant.

G. Antoniou et al. (Eds.): SETN 2006, LNAI 3955, pp. 559 – 562, 2006.

two points is the dissimilarity of two network traffic logs. The U-Matrix of the trained dataset is divided into valleys that represent clusters of normal or attack data and hills that represent borders between clusters. Depending on the position of the best match of an input data point that characterizes a connection this point may belong to a valley (cluster (normal or attack behaviour)) or this data point may not be classified if its best match belongs to a hill (boundary). The map that is created after the training of the Emergent SOM, represents the network traffic. Thus, an input data point may be classified depending on the position of its best match. In order to achieve meaningful distance calculations the means and the variances of the features should be comparable. We have normalized the data with mean zero and variance one.

Mukkamala et al. [4] identified the most significant features from the KDD-99 dataset using two ranking methods for the SVMs (Support Vector Machines) and ANNs (Artificial Neural Networks). We have performed binary classification using the important features of each type of attacks and multi-class classification combining the most important features for the 4 types of attacks (DoS, probe, R2L, U2R) (13 features) and the most important features of each type of attack and normal data (18 features). We have to note here for features, whose values are alphanumeric, we map each instance of alphanumeric value to sequential integer values.

2 Experimental Results

According to the proposed approach ESOMs are trained to learn the normal behavior and attack patterns and then deviations from normal behavior are flagged as attacks. It is demonstrated that ESOMs are capable of making highly accurate attack/normal classifications. For the evaluation we have used the Databionics ESOM tools [5].

We performed various evaluation experiments. Table 1 presents the datasets that were used in order to train and test our approach. All the datasets are part of the available 10% KDD dataset [6] of various sizes that include normal data and DoS, Probe, R2L and U2R attacks. We performed binary classification (i.e. normal/attack) to classify each class of attacks (DoS, Probe, R2L, U2R) against normal traffic.

The ESOM of a trained dataset containing normal traffic and DoS attacks is depicted in figure 1. As it can be clearly seen the training data set has been divided into two classes that are very well distinguished, normal data class (dark color) and DoS data class (light color). In figure 2 the testing dataset for the corresponding training dataset is depicted. In order to evaluate the efficiency of the proposed approach we use two measures, i.e. the detection rate and the false alarm rate:

$$\text{Detection rate} = \frac{TP}{TP + FN}, \text{ False alarm rate} = \frac{FP}{TN + FP},$$

where TP is the number of true positives (attack logs classified as attacks), TN the number of true negatives (normal logs classified as normal), FP the number of false positives (normal logs classified as attacks) and FN the number of false negatives (attack logs classified as normal). The most effective approach should reduce as much as possible the *False alarm rate* and at the same time increase the *Detection rate*.

Table 1. Datasets used for evaluation

Dataset	Attacks		Normal
Dataset 1	3732 DoS		5065 normal
Dataset 2	3737 DoS		5064 normal
Dataset 3	2052 probe		3905 normal
Dataset 4	2055 probe		3503 normal
Dataset 5	562 R2L		1001 normal
Dataset 6	564 R2L		1001 normal
Dataset 7	3732 DoS 562 R2L 6372 Total attacks	2052 probe	10072 normal
Dataset 8	3737 DoS 564 R2L 6383 Total attacks	2055 Probe 27 U2R	9669 normal

Table 2. Evaluation Results

Experiment	Number of Features	Training Dataset	Testing Dataset	Detection Rate	False Alarm
Experiment 1	11	Dataset 1	Dataset 2	93,55%	0,21%
Experiment 2	7	Dataset 3	Dataset 4	91,33%	0,25%
Experiment 3	5	Dataset 5	Dataset 6	95,92%	2,6%
Experiment 4	13	Dataset 7	Dataset 8	93% DoS 96,29% U2R 98,97% probe 92,3% R2L 96,29% U2R 95,17% Total	6,39%
Experiment 5	18	Dataset 7	Dataset 8	99,49% DoS 99,75% probe 99,46% R2L 100% R2L 99,59% total	3.4%

Thus experiments have been performed with 50x82 neurons and 20 training epochs. The Gaussian function was used as a kernel neighborhood function and weight initialization method and the Euclidean as a distance function. The initial and final learning rate, were 0.5 and 0.1 respectively and the initial and final value for radius were 24 and 1 respectively. Moreover in order to avoid topology errors caused by border effects we have used boundless toroid grids.

As it can be seen from the table 2 where the evaluation results are presented the detection rate ranges from 91,33% to 95,92% for binary classification (experiments 1,2,3) and the corresponding false alarms from 0,21% to 2,6%. The highest detection

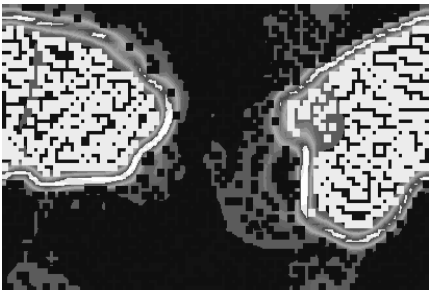

Fig. 1. U-Matrix of the training dataset

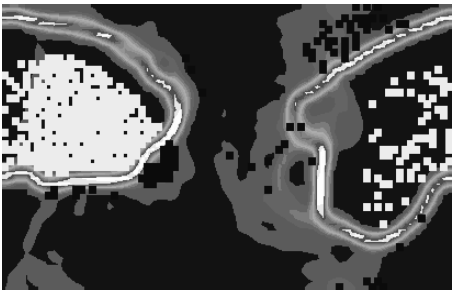

Fig. 2. U-Matrix of the testing dataset

rate and lower false alarm is achieved for DoS attacks while the R2L attacks present lower detection rate and false alarm equal to 2,6%. The ESOM approach presents good results with extremely low false alarms when only one attack is included in the training and testing dataset. When datasets include more than one attack the results are more promising, using 18 features that derive from the combination of important features of each type of attack and normal traffic.

By exploiting the visualization of network traffic our approach detects attacks by classifying malicious and normal actions. The proposed approach produces efficient results for randomly selected datasets. We should note that even though we employed small datasets of the 10% KDD dataset, the results are extremely promising.

References

1. S. Haykin, "Neural Networks: A comprehensive Foundation", Prentice- Hall, USA, 2nd edit.
2. A. Ultsch, "Data Mining and Knowledge Discovery with Emergent SOFMs for Multivariate Time Series", In Kohonen Maps, (1999), pp. 33-46.
3. A. Ultsch, "Maps for Visualization of High-Dimensional Data Spaces", Proc. WSOM, Kyushu, Japan, (2003), pp. 225-230.
4. S. Mukkamala, A.H. Sung, "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques", International Journal of Digital Evidence,2003(1)4.
5. Databionic ESOM Tools, http://databionic- esom.sourceforge.net/devel.html.
6. The Third International Knowledge Discovery and Data Mining Tools Competition, May 2002. http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html