DDOS ATTACK DETECTION BASED ON ENSEMBLE OF NEURAL CLASSIFIER

[1]D.M.Choudhari
[1]Associate Prof, Department of Computer Science and Engineering
KLS Gogte Institute of Technology, Belgaum-59008, INDIA.
[1]dmchoudhari@git.edu

Abstract: **This paper reviews the detection of DDoS attck.The DDoS attacks could be detected using the existing machine learning techniques such as neural classifiers. These classifiers lack generalization capabilities which result in less performance leading to high false positives. This paper evaluates the performance of a comprehensive set of machine learning algorithms for selecting the base classifier using the publicly available KDD Cup dataset. Based on the outcome of the experiments, Resilient Back Propagation (RBP) was chosen as base classifier for our research. The improvement in performance of the RBP classifier is the focus of this paper. Detection accuracy and Cost per sample were the two metrics evaluated to analyze the performance of the RBPBoost classification algorithm. From the simulation results, it is evident that RBPBoost algorithm achieves high detection accuracy (99.4%) with fewer false alarms and outperforms the existing ensemble algorithms. RBPBoost algorithm outperforms the existing algorithms with maximum gain of 6.6% and minimum gain of 0.8%**

Keywords: DDoS Attack, Feed forward Neural Network, KDDCup dataset, Probabilistic Neural Network, Intrusion Detection, Machine Learning Techniques.

1. *Introduction:*

A distributed denial of service (DDoS) attack [1, 6] is a large-scale, coordinated attack on the availability of services of a victim system or network resources, launched indirectly through many compromised computers on the Internet. The first well-documented DDoS attack appears to have occurred in August 1999, when a DDoS tool called Trinoo was deployed in at least 227 systems, to flood a single University of Minnesota computer, which was knocked down for more than two days1. The first large scale DDoS attack took place on February 2001. On February 7, Yahoo! was the victim of a DDoS attack during which its Internet portal was inaccessible for three hours. On February 8, Amazon, Buy.com, CNN and eBay were all hit by DDoS attacks that caused them to either stop functioning completely or slowed them down significantly Our proposal is to make intelligent message discard Decisions based on Neural Networks to result in fewer false alarms.

The contributions of this paper include the following:

- Generic architecture of DDoS attack detection and response system for collaborative environment.
- Implementation of RBPBoost algorithm for the classification of network traffic.
- A classification accuracy of dataset

- 55.2% when training and testing of KDD data set.
- 55.5% when training and testing on the lab dataset.

2. *Related Work*

2.1. DDoS attack

DDoS attack is broadly classified into bandwidth depletion and resource depletion attack [58]. In bandwidth depletion attack, attackers flood the victim with large traffic that prevents the legitimate traffic and amplify the attack by sending messages to broadcast IP address. In resource depletion attack, attackers attempt to tie up the critical resources (memory and processor) making the victim unable to process the service. A structural approach for DDoS attack classification is proposed in [2]. The detailed analysis on DDoS attacks and available attack tools [10] show that the DDoS attack has the following characteristics:

- Source and Destination IP address and port numbers of the
- Packets are spoofed and randomly generated.
- Window size, sequence number, and packet length are fixe during the attack.
- Flags in the TCP and UDP protocols are manipulated.
- Roundtrip time is measured from the server response.
- Routing table of a host or gateway is changed.
- DNS transaction IDs (reply packet) are flooded.
- HTTP requests are flooded through port 80.

2.2. *Real time feature extraction*

Features are statistical characteristics derived from the collected dataset. Selection of real time feature set plays a vital role in online traffic classification. More number of features leads to better accuracy. But, computation of more number of features in real time causes more overhead and time consuming. 248 features are given and 1 feature is used to describe the class (normal or attack) in [4]. Computation of all the 248 features [1] took approximately two days on a dedicated System Area Network. Out of 248 features, some features such as maximum interpacket arrival time cannot be calculated until the entire flow is completed. Moreover, features based on Fast Fourier Transform values need better signal processing methods to reduce the computation time. So, less number of appropriate statistical features is to be selected for better pattern classification.

Feature extraction [3] is classified into two stages:

1. Feature Construction
2. Feature Selection.

Constructing the features is either integrated into the modeling process or into the preprocessing stage which includes standardization, normalization, etc. Feature Selection is divided into Filter methods and wrapper methods [5]. In filter methods, selection is based on distance and information measures in the feature space. In wrapper methods, selection is based on classifier accuracy. Three statistical features are used in [2]. Nine features are used in [3]. Flow based feature selection has been shown to block legitimate traffic in [3]. Flow based selection gives summary of metadata. By blocking the IP address and port, flow based selection does not permit the legitimate requests. Hence, instead of flow based solution, packet based solution has been used in this paper. Packet based solution minimizes the prevention of legal traffic as it blocks only the particular traffic based on the outcome of the analysis of the sequence number, window size, and packet length. Features are selected by classifying the IP flow into micro-flow and macro-flow [2]. Decision tree based Machine Learning (ML) algorithm combined with real time features has been proposed to be a good candidate for online traffic [6]. But, finding the smallest Decision Tree that is consistent with a set of training examples is NP-hard.

2.3 Ensemble of classifiers – motivation

Single classifier makes error on different training samples. So, by creating an ensemble of classifiers and combining their outputs, the total error can be reduced and the detection accuracy can be increased. There are two main

components in all ensemble systems [5], viz., a strategy to build an ensemble that is as diverse as possible and the combination of outputs of classifier for the accurate classification decisions

.Classifier combination is divided into two categories:

- Classifier selection, where each classifier is trained to become an expert in some local area of the total feature space.
- Classifier fusion, where all classifiers are trained over the same feature space.

3.Proposed system design:

The system is to develop an Intrusion detection system based on learning technique. Firstly known classes of intrusion like DDOS, Perl attack, Neptune attack signature is formed from standard KDD dataset. This has several string values which are not understood by the classifier. Therefore these values are converted to suitable numbers based on their properties. Database is partitioned into two parts: Training and Testing. Testing involves giving one row from the dataset as input. System classifies the row as Normal or Abnormal.

The same concept is then adopted in a real time environment to detect anomaly in internet access from college data. Router log is used to extract the features. As these features are not reclassified, we use a regression technique rather than classification to find the similarity with any data of earlier dates. Base on protocol used, we then classify the data as normal or abnormal.

The proposed system design architecture consists of the four main modules that are:

A: data collection module:
B: preprocessing.
C: Classification
D: Response

A receiver process running in promiscuous mode captures all incoming packets and stores in data storage server. The data is stored as set of traffic flows, with each instance being described by a set of features. Each instance is expressed in vector space model (A).

Preprocessing refers to the process of extracting information about packet connections from data and construction of new statistical features. The preprocessing steps are explained as follows:

1. Let ‘x’ be the input vector of dimension ‘n’, such that x = [x1, x2,x3, . . .xn]. The variables xi of the input vector is the original features.
2. Let ‘tx’ be a vector of transformed features of dimension ‘tn’

The statically characteristics features are used to find the statistical properties such as standard deviation and variance. These features quantify the behavioral characteristics of a connection in terms of number, type of various data items with respect to time. Hence, theses features are called as statistical real time features. Seven features are used as the gradients of the vector to classify the network pattern. Normalization is a process of ensuring that each attribute value in a database structure is suitable for further querying and free from certain undesirable characteristics. Hence, each variable is normalized in the range [1, 1] to eliminate the effect of scale difference. These values are used as inputs for machine learning algorithms (B).

In this module, Dataset of particular class is split into subsets. Each subset is trained with Ensemble of classifiers and results are combined by WMV [7]. TK is the total number of classifiers chosen using cross-validation. Cross-validation is a popular method of manipulating training data to subdivide the training data into ‘k’ disjoint subsets and to reconstruct training sets by leaving out some of the subsets. Results of each classification system are further combined by WPR [7]. The efficiency of classification of the classifier is significant in the decision making process. Hence, it is measured by a parameter Q-statistic. For effective decision, the Q-statistic should be zero. The training time depends on the number of times the classifier needs training which in turn depends on the mean square error between iterations reaching global minimum. The training is speeded up by removing the overlapping data and retaining only the training samples adjacent to the decision boundary. This method again consists of training and classifier is the sub stages (C). Detection system deployed

in each site maintains a hash table and updates IP address and port number (attack signature) of the suspicious blacklist nodes. When a site receives the attack signature, it checks if it exists in its hash table. If present, it means that the system is already alerted. If not, attack signature is added to the infected list. The updated attack signature is sent to all collaborating nodes, to prevent any damage that may be caused to the available services (D)

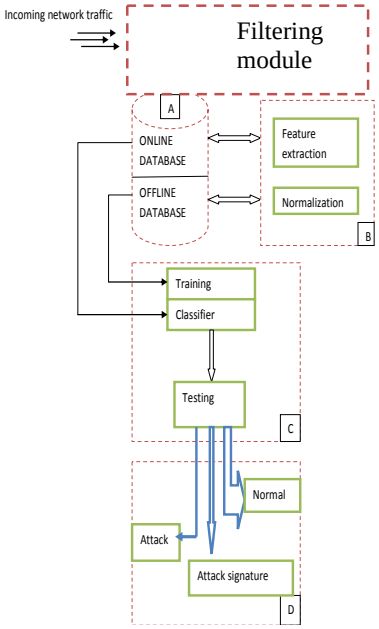

Fig 1: Architecture of ddos attack detection

4. Proposed System Algorithm:

The classification of the preprocessed data is carried out using RBPBoost algorithm. The block diagram shows that how RBPBoost algorithm uses the KDDCup99 dataset. This dataset is divided into two subset dataset and each subsets dataset is tested with this algorithm. Each subset is trained with ensemble of classifiers and results are combined by WMV [3]. TK is the total number of classifiers chosen using cross-validation. Cross-validation is a popular method of manipulating training data to subdivide the training data into 'k' disjoint subsets and to reconstruct training sets by leaving out some of the subsets. Results of each classification system are further combined by WPR [3]. The efficiency of classification of the classifier is significant in the decision making process.

The training of dataset is carried out by using feed forward neural network. But this neural network does not provide good detection accuracy. So in order to increase the detection accuracy we are used the RBP neural network

An ensemble of classifiers is trained for each individual data subset and the results are combined. A new classifier is added at each iteration. In our algorithm as given in Figure2. Two classes (Normal and DDoS attack traffic) are considered. The inputs to the algorithm are as follows:

- Training data comprised of 'n' instances with correct output labels.
- Resilient Back Propagation algorithm (RBP) as supervised base classifier.
- Number of classifier.

This dataset trained using artificial neural network and then tested with the RBP neural network to find its detection accuracy.

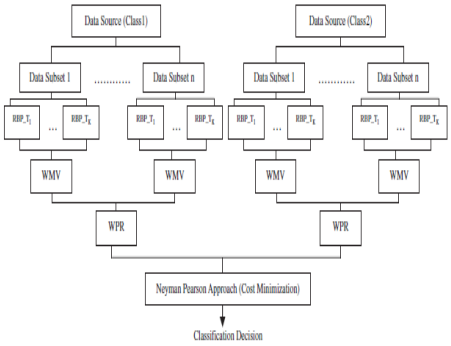

Figure 2: The Block Schematic of RBP Algorithm

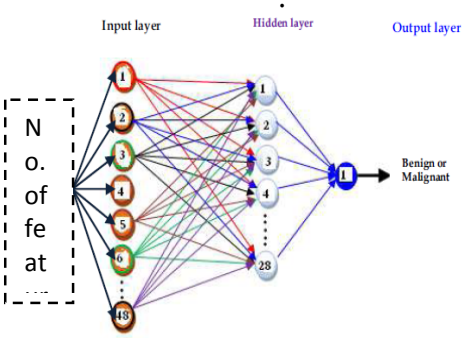

Figure 3: Proposed Architecture of RBP Neural Network

The purpose of the resilient back propagation (Rprop) training algorithm is to eliminate these harmful effects of the magnitudes of the partial derivatives. Only the sign of the derivative can determine the direction of the weight update; the magnitude of the derivative has no effect on the weight update. The size of the weight change is determined by a separate update value. The update value for each weight and bias is increased by a factor delt_inc whenever the derivative of the performance function with respect to that weight has the same sign for two successive iterations. The update value is decreased by a factor delt_dec whenever the derivative with respect to that weight changes sign from the previous iteration. If the derivative is zero, the update value remains the same. Whenever the weights are oscillating, the weight change is reduced. If the weight continues to change in the same direction for several iterations, the magnitude of the weight change increases.

First, investigate the storage format of the network. RBF networks are stored in objects with head RBFNet. The first component contains the parameters and the second component is a list of rules.
Initialize an RBF network with three inputs, two outputs, and five neurons. This is done by initializing a network with matrices of the appropriate size without any data.

Input:
- Training Data 'DS' of size 'N' with correct labels $y_i \in \Omega = \{y_1, y_2\}$
- Supervised algorithm base classifier
- No. of iterations or classifiers (y)
- Number of Classes (L)

Initialize:
- $\mu = 0.5$ // False Alarm Threshold
- $L = 2$

Training:
Do j = 1... L
1. Choose samples from class 'j' and form Data Source DS_j
2. Split DS_j into 'k' subsets (S_1, S_2,……, S_k)

Do m = 1…..k and t = 1……y
a. Train S_m by supervised algorithm and obtain hypothesis h_t
b. Compute error of h_t: $\varepsilon_t = \sum_i^n [h_t(x_i) \neq y_i]$ (4)
c. If $\varepsilon_t > \mu$, then drop hypothesis and go to step 2.a
Else add the classifier C_t to the Ensemble 'E_m'.
d. Normalized error (β_t): $\beta_t = \varepsilon_t / 1 - \varepsilon_t \quad 0 < \beta_t < 1$ (5)

End
End

Testing:
Given an unlabeled instance 'X'
A. Evaluate the ensemble 'E' of each data subset for particular class on 'X'
B. Obtain composite hypothesis for each subset by Weighted Majority Voting
C. Each subset's ensemble decision in combined by Weighted Product Rule
D. Choose the class with more weights.

Figure 4: Proposed RBP Algorithm

As like the above Algorithm here we are given some specified sample of dataset to the neural network, which takes these samples and classified into its normal and attack class.
Feed forward neural network is used to create two-layer feed-forward network of neurons. Collected data and target value are considered to configure the network's inputs and outputs to match. Configuration is the process of setting network input and output sizes and ranges, input preprocessing settings and output post processing settings, and weight initialization settings to match input and target data.
The network is trained for different values of epochs and error goal, where epoch and error goal are training parameter. Typically one epoch of training is defined as a single presentation of all input vectors to the network. The network is then updated according to the results of all those presentations. Training occurs until a maximum number of epochs occur, the performance goal is met, or any other stopping condition of the training function occurs.

Implementation is carried out using MATLAB Neural Network Toolbox for the purpose DDoS attack detection. Here we implement three separate modules which are as followings
1. The first module is according to the base paper, which finds the detection accuracy of DDoS detection attack using different types of neural network with KDDCup 99 dataset input for this one.
2. The second one is the DDOS attack like matching using our college log file.
3. The final one is just shows us that how the intrusion is happened in normal wireless artificial immune system.

5. Simulation results:

After executing the neural network we got the better detection accuracy as 55.86.this we can show below.

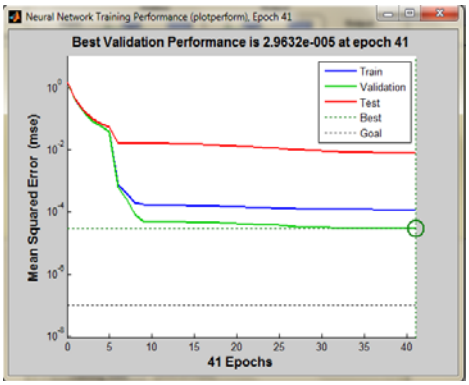

Figure 5: Performance of the neural network showing that validation is goes on optimizing the threshold.

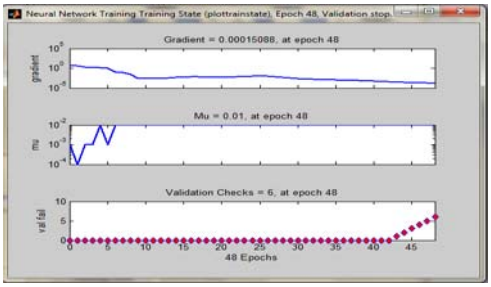

Figure 6: Training state graph showing gradient, mean deviation and validation check

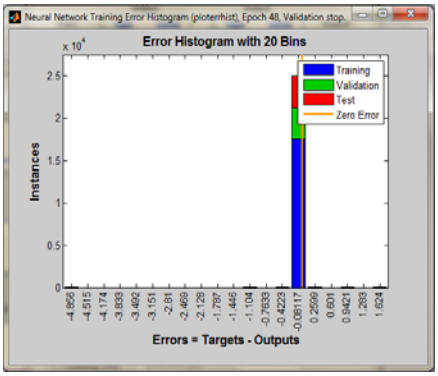

Figure 7: Error histogram of using 80 layers in the feed forward network

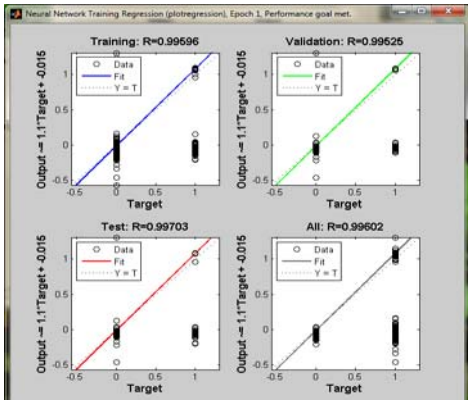

Figure 8: Regression graph showing the roc curve

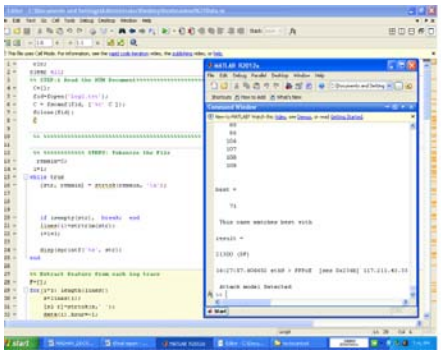

Figure 9: shows how git college data matches with its corresponding match

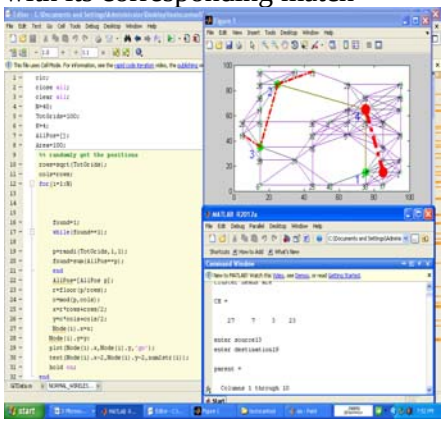

Figure 10: Shows How Intrusion Detection Is Happened In wireless AIS Network

RESULTS

Algorithm name with functions	No .of sample	Detection accuracy
Normal neural network	10000	2.88%
Best	10000	2.9623e^(-

validation		005)
Mean deviation	10000	0.01
Error rate	10000	0.08115
gradient	10000	0.00015
RBP neural network	10000	55.36%

So finally we are got the good detection accuracy. So that we are chosen RBP neural network is the base classifier.

6. Conclusion and Future Scope:

In this paper, a generic architecture for automated DDoS attack detection and response system for collaborative environment using machine learning is proposed. We have further evaluated the concept by implementing the concept in real time college data where we have used regression to suitably extract the classes from unknown pattern from college router log file. We have also defined an evolutionary technique using AIS and have applied it on simulation of Intrusion detection in mesh network where detection signature is mesh network parameters.

References:

[1] Abraham Yaar, Adrian Perrig, Dawn Song, FIT: Fast Internet Traceback, IEEEInfocomm, Mar. 2005.

[2] Alex C. Snoeren et al., Hash-Based IP Traceback, ACM Sigcomm, Aug. 2001, pp. 3–14.

[3] Alex C. Snoeren et al., Single-packet IP traceback, IEEE/ACM Transactions on Networking 10 (6) (2002) 721–734.

[4] Amey Shevtekar, Karunakar Anantharam, Nirwan Ansari, Low rate TCP denialof- service attack detection at edge routers, IEEE Communications Letters 9 (4) (2005) 363–365.

[5] Amey Shevtekar, Nirwan Ansari, A router-based technique to mitigate reduction of quality (RoQ) attacks, Computer Networks 52 (5) (2008) 957–970.

[6] Amey Shevtekar, Nirwan Ansari, Is it congestion or a DDoS attack? IEEE Communications Letters 15 (7) (2009) 546–548.

[7] Andrey Belenky, Nirwan Ansari, On IP traceback, IEEE Communications Magazine 41 (7) (2003) 142–153.

[8] Andrey Belenky, Nirwan Ansari, On deterministic packet marking, Computer Networks 51 (10) (2007) 2677–2700.

[9] Arbor Networks, Worldwide Infrastructure Security Report, Volume IV, November 2008.

[10] P. Arun Raj Kumar, S. Selvakumar, A DDoS threat in Collaborative environment "A survey on DDoS attack tools and Traceback mechanisms ", in: Proceedings of IEEE International Advance Computing Conference (IACC'09), 2009, pp.1275–
1280.