INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

Advanced Computer Network Project

REPORT ON

Detection of DDoS using RDF-SVM

Submitted To-:
Dr. P Sateesh Kumar
Asst. Prof.
Computer Science & Engg

Submitted By-:
Himanshu Gupta (18535012)
Rishabh Mamgain (18535023)
Shubham Bhatia (18535024)
Tushar Rangari (18535028)
Vishal Arora (18535029)

Contents

1 Problem Statement:-

DDoS attack detection using RDF-SVM. Previously DDoS attacks were easily misled by flash crowd traffic but new method can detect DDOS attack using RDF-SVM algorithm. This algorithm is made to exploit random forest which uses important feature and SVM to rescreen it which will prevent from removing features taken mistakenly. At last is obtained with optimal features which will high detection rate and recall rate. We have used KDD99 dataset to train and test which distinguish between DDoS attack traffic and normal traffic which is flash crowd. RDF-SVM algorithm has much higher detection rate as compared to CART, neural network, logistic regression and ADABOOST.

2 Brief of the protocol:-

Denial of Service (DoS) forces the victim to receive false traffic which makes him fail to receive legal requests, resulting in providing no services to legitimate users. DDoS attacks have generally two important factors, i.e., resource consumption and bandwidth consumption. Bandwidth and resource are consumed by the control of botnets to generate many forged packets. DoS attacks are implemented by hackers on one or more than one targets and exhaust victim's resources, making the victim incapable of providing normal network services.

As the technology is developing day by day, DDoS attacks have been increasing year by year, making difficult to perform commercial operations, and disturbing people's normal life. Statistics have shown that there were repeated attacks on DNS root servers by DDoS resulting in large number of paralyzed servers. GitHub also encountered large traffic from DDoS attacks.

Tracing back for fake source IP DDoS becomes difficult. Moreover, detection can be easily misled by flash crowd traffic which is quite similar to the DDoS attacks.

A new method is proposed to detect DDoS attacks which is based on RDF-SVM, i.e., random forest-support vector machines. Random forest is used to calculate variable importance, whereas SVM algorithm is used to rescreen features. This algorithm will obtain a subset with higher detection rate.

Following are some of the innovations:-

1. Rescreening and preventing from deletion of features which contribute to DDoS detection.
2. Attacks are suppressed before reaching target host.
3. Differentiate between flash crowd traffic and DDoS traffic.
4. Detection of both unknown and known attacks.

3 Methods of implementation:-

3.1 Random forest:-

This algorithm is an integrated machine learning which uses random sampling technique and node splitting technique to construct multiple decision trees randomly and gain final classification result by voting. Random forests are an ensemble learning technique for classification, regression as well as other tasks that use decision trees.

This algorithm uses several classification models $\{ (X, \theta_k) | k = 1,2 \dots \dots \}$ of decision tree. $\{\theta_k\}$ is assumed to be independent and identically distributed random variable and k is number of decision trees. Following are some important highlights of this algorithm.

a. N samples are selected randomly and then they are put back after the selection. This is done in order to train the decision tree.
b. There are M attributes to each sample, when we split the decision tree node is split. Then m attributes are selected (m << M) and the information gain strategy is used to select an attribute as spit attribute of the node.
c. Each node in step 2 is split, until it can't be splitted further.
d. Build decision trees without pruning
e. Then the vote on the variable X_i is collected from decision trees, then the highest votes is set as label for classification.

Entropy tells about the disorder-ness. Information Entropy

$$\text{Entropy}(x) = \sum_{i=1}^{c} -P_i \log_2 P_i \qquad (1)$$

X is a random variable of finite random discrete variable, P_i is the ratio of the random variable and the dataset C. The expectation of feature Y for x is:

$$\text{Entropy}_Y(x) = \sum_{J=1}^{N} \frac{|x_i|}{|x|} \text{Entropy}_Y(x) \qquad (2)$$

The rise in information entropy leads to the rise in uncertainty of training samples. Information gain is as follows:

$$\text{Gain}(x, Y) = \text{Entropy}(x) - \text{Entropy}_Y(x) \qquad (3)$$

Entropy is used as information gain. Feature is directly related to the information gain. Thus feature makes contributions to the detection rate.

3.2 SVM Algorithm:-

The SVM algorithm is a 2 step classification algorithm and it performs good in generalization and handling with imbalanced dataset.

For the training set

D = $\{(x_1, y_1), (x_2, y_2), \ldots\ldots (x_n, y_n)\}, y_i \epsilon \{-1,1\}$,

the basic step is to find a hyper-plane. We can represent the hyper plane by the linear equation

$$\omega^T x + b = 0 \qquad (4)$$

ω is normal vector set, b is displacement. The distance r of any point x of sample space to hyper-plane (ω, b) is expressed as follows:

$$r = \frac{|\omega^T x + b|}{||\omega||} \qquad (5)$$

We assume that the samples are trained correctly by the hyper-plane. For$(x_i, y_i) \epsilon\ D$, then

$y_i = +1$, so $\omega^T x + b > 0$. If $y_i = -1$, then $\omega^T x + b < 0$.

Then we obtain the most suitable variables ω and b, thus the optimize SVM problem is as follows

$$\max_{\omega, b} \frac{2}{||\omega||} \qquad (6)$$

$$\text{s.t. } y_i(\omega^T x_i + b) \geq 1,\ i = 1,2, \ldots\ldots, m \qquad (7)$$

For dual hyper-plane problem the optimum solution Q(a) is :

$$Q(a) = \sum_{i=1}^{n} a_i - \frac{1}{2}\sum_{i,j=1}^{n} a_i a_j y_i y_j (x_i \cdot x_j) \qquad (8)$$

Finally optimal classification function f(x) is

$$f(x) = sgn\{\sum_{svm} a_i^{\cdot} y_i\ (x_i \cdot x) - b^{\cdot}\} \qquad (9)$$

3.3 Proposed RDF – SVM algorithm

The F(xi) function define as

$$F(x_i) = \begin{cases} 1, & x_i\ is\ positive\ feature \\ -1, & x_i\ is\ negative\ feature \end{cases} \qquad (10)$$

We obtain 2 values. $P_j^{(1)}$ denotes the training and prediction with deletion and $p_j^{(2)}$ denotes prediction without deletion. The value sum_P denotes the difference

$$\text{sum\_P} = P_j^{(1)} - P_j^{(2)} \qquad (11)$$

Then main difference is found for n samples by the equation

$$\text{Mean\_sumpre\_diff} = (\sum_j (P_j^{(1)} - P_j^{(2)})) / n, j = 1,2,\ldots \qquad (12)$$

If Mean_sumpre_diff > t, then $X_i \epsilon C$,the feature will be retained. Otherwise, X_i ! ϵC, then it will be removed.

3.4 Proposed Algorithm

Algorithm 1 RDF-SVM algorithm

Input: $\{x_i | i = 1,2,3 \ldots\ldots, N\}, S_{train}, S_{test}$
Output: Optimal feature subset C
Steps:
initial $\omega \leftarrow \phi$, sum_P $\leftarrow$ 0, Mean_sumpre_diff $\leftarrow$ 0
for each x_i do
    $\omega_{X_i} \leftarrow$ Randomforest(x_i);
end for
    W $\leftarrow$ Sort(ω_{x_i});
for each $\omega_{x_i} \in W$ do
    if $\omega_{x_i} > \alpha$ then
        A_index $\leftarrow x_i$;
    else
        B_index $\leftarrow x_i$;
    end for
end for
for each $X_i \in$ B index do
  for $j \in (1, n)$ do
    $P_j^{(1)} = SVM(y_i, x_i, \text{y\_train}, \text{X\_test})$;
    $P_j^{(2)} = SVM(y_i, A_{X_i}, \text{y\_train}, \text{A\_ X\_test})$;
    $sum\_P = sum\_P + P_j^{(1)} - P_j^{(2)}$;
    j++;
  end for
    Mean_sumpre_diff = sum_P / n;
  if Mean_sumpre_diff > t then
    A_index $\leftarrow x_i$;
  else
    remove(x_i);
end for
return A_index;

4 Results Achieved:

Analysis on KDD99 dataset
We have the KDD99 dataset and it consists of 42 features and these features belong to normal and attacked dataset. We further have 2 sets

1. KDD Test+ set which contains 39 kinds of attacks which is 17 kinds more than KDD Train+.
2. KDD Train+ set which contains 22 kinds of attacks.

42 features are:

“duration","protocol_type","service","flag","src_bytes","dst_bytes","land","wrong_fragment","urgent","hot","num_failed_logins","logged_in","num_compromised","root_shell","su_attempted","num_root",num_file_creations","num_shells","num_access_files","num_outbound_cmds","is_host_login","is_guest_login","count","srv_count","serror_rate","srv_serror_rate","rerror_rate","srv_rerror_rate","same_srv_rate","diff_srv_rate","srv_diff_host_rate","dst_host_count","dst_host_srv_count","dst_host_same_srv_rate","dst_host_diff_srv_rate","dst_host_same_src_port_rate","dst_host_srv_diff_host_rate","dst_host_serror_rate","dst_host_srv_serror_rate","dst_host_rerror_rate","dst_host_srv_rerror_rate","label"]

. Then we have applied RDF_SVM algorithm on the test data to find the best features (src_bytes, dst_bytes, logged_in, duration, protocol_type, and num_file_creations) out of these which can detect DDOS attack.

The RDF-SVM algorithm prevents from removing the feature subset from which classification is promoted. We can detect unknown and known attacks, differentiate real ip attacks from random ip attacks and flash crowd more effectively as compared to other methods.

After applying Random Forest Algorithm, the detected features out of all 42 are with their importance values

Detected Feature	**Importance value**
Duration	0.013450231133692056
src_bytes	0.5563474527516045
dst_bytes	0.32320092844470516
logged_in	0.03535644214871085
Hot	0.010177058552346224
num_access_files	0.0009165270390737588
srv_count	0.05868177970868924
is_guest_login	0.001869580221178301

We took all those features whose importance value is greater than a (0.20). A_index contains

Detected Feature	Importance Value
src_bytes	0.5563474527516045
dst_bytes	0.32320092844470516

On applying SVM classifier on the remaining features we captured one more feature which got missed out in Random forest classification.

Detected Feature	Importance Value
src_bytes	0.5563474527516045
dst_bytes	0.32320092844470516
logged_in	0.03535644214871085

5 Remarks on result:

We have Random Forest on data set KDD99 with the importance set threshold value 0.22 and SVM on remaining features with the threshold value of 0.000000000005. Using these features we have tried to differentiate between DDoS attack and flash crowd traffic.

6 References:

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8089926