**DDoS Attacks Analysis Based on RDF-SVM**

**Yasaswi Kolasani**

**ID: 001533428**

**ABSTRACT:**

DDoS attacks bring huge threaten to network, how to effectively detect DDoS is a hot topic of information security. Currently, there are some methods designed to detect DDoS attacks, but the detection rate of them is low. Moreover, DDoS detection is easily misled by flash crowd traffic. A new method to detect DDoS attacks based on RDF-SVM algorithm is proposed. By considering the importance of feature selection in DDoS attacks detection, the RDF-SVM algorithm is designed to exploit random forest to compute the feature importance and SVM to rescreen the features, which will prevent from removing features mistakenly. Finally, an optimal feature subset is obtained, which will reach a higher detection rate and recall rate. Two kinds of datasets are used to train and test. Compared with the CART, Neural Network, Logistic Regression, AdaBoost, and SVM method, RDF-SVM algorithm has a higher detection rate and recall rate.

**INTRODUCTION:**

DoS stands for Denial of Service. Which is making the service unavailable over the network by increasing the network traffic load. Hackers use a network of systems like botnets to perform the DoS attack which is called the Distributed Denial of service (DDoS). With the development of network technology, these types of attacks are increasing year by year, severely disrupting the commercial operation, network environment and people`s normal life. There are several methods to detect DDoS attacks but they are not able to detect attacks effectively. The reason for this is that the detection is easily misled by flash crowd traffic which is the traffic that came from the normal people who are trying to access the service in huge numbers. For example, an E-commerce website gets more load with traffic on the day of offers during festivals. The methods used for the detection of DDoS attacks may mislead this huge traffic with the flash crowd. There are some restrictions on finding previous works DDoS attacks with low detection rates and high false-positive rates.

DDoS flooding attacks have been further studied, is classified into two categories based on the protocol level that is targeted: (1) Network/transport-level DDoS flooding attacks: such attacks are mostly launched using Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Domain Name System(DNS) protocol packets. (2) Application-level DDoS flooding attacks: such attacks are focused on disrupting legitimate user services by exhausting the server resources, e.g., sockets, central processing unit (CPU), memory, disk/database bandwidth, and input/output (I/O) bandwidth. Application-layer DDoS attacks are usually more subtle than volume attacks because they use less bandwidth and are very similar to secure traffic. The biggest challenge in fighting DDoS attacks is to detect them early and contain them as close as possible to the source of the attack. The implementation of a comprehensive solution taking these features into account has not yet been implemented.

**PROPOSED APPROACH:**

A Method RDF-SVM based attack detection and detection method that combines random forest and SVM. This approach uses a random forest to calculate feature importance and reselects features using an Support Vector Machine SVM algorithm. Finally, obtain an optimal subset of features with a higher detection rate. It is just rescreening the features and prevent from deleting the features, which contribute to DDoS detection and distinguish between DDoS traffic and flash crowd. It uses KDD99 Dataset which contains 42 features of 39 kinds of attacks.

**PLANNED TIMELINE:**

I will work on the random decision forest for 2 weeks to compute the importance values of the features, prioritize them and get the features of high importance values based on the threshold value. Then I will work on the Support Vector Machine for 2 weeks to rescreen the features by considering previously deleted features.

**ANTICIPATED RESULTS:**

precision rate and recall rate of the RDF-SVM algorithm are the anticipated results and compare the results with results of different algorithms like, Adaboost, Logistic Regression, SVM. The effectiveness of the model is assessed with the cross validation to mitigate the overfitting.

**REFERENCES:**

[1] Chenguang Wang , Jing Zheng ,Xiaoyong Li, “Research on DDoS Attacks Detection Based

on RDF-SVM”, Beijing Jiaotong University, 2017