International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 11 (November 2014) www.ijirae.com

Denial-of-Service Attack Detection

Mangesh D. Salunke* Prof. Ruhi Kabra
G.H.Raisoni CEM, SPPU, Ahmednagar *HOD, G.H.Raisoni CEM , SPPU ,Ahmednagar*

Abstract: ***A DoS (Denial of Service) attack as name indicates is simply an attempt by an attacker to exhaust the resources available to a network, application or service so that authorize users cannot gain access. The Denial of Service (DOS) attacks are one of the most widely spread problems faced by most of the Internet Service Providers (ISP's) today. Denial-of-Service (DoS) attacks cause serious impact on the computer network systems. Therefore, effective detection of DoS attacks is essential to the protection of network and resources. Detection System is built by using layered frame work approach for an effective attack detection system The proposed system will create own data set by analyzing the incoming packets in real time system, by comparing with previous existing system that uses Knowledge Discovery & Data Mining(KDD) 1999 dataset, and classify the DoS Attack such as SYN Flood, Ping Flood, UDP Flood.***

Keywords: Computer & Network Security; DoS Attack; IDS; Layered framework, K-means clustering, Naive Bayes

I. INTRODUCTION

Denial-of-Service (DoS) Attack is an attack that deny or prevents the access of network, system or resources to its authorize user. Although the motivation and targets of DoS attack are vary, it is generally consist of efforts to suspend the service of the authorize user .One common method to perform DoS attack, where attacker sends the packet in flooded way based on system response time. That is an attacker can calculate packet sending time by using retransmission timeout of that system, so that when the system is ready for retransmission of packet after timeout period it is flooded again new request to process. Because of this the target system is busy with processing that flooded request, the authorize user can wait for processing its request. In most cases DoS attack involves Spoofed IP addresses and intended as authorized user, so that location of attacker cannot easily identify and also prevent that packet from packet filtering. Typical aims of DoS attack are, by sending large traffic volume consuming the bandwidth, Consume limited available resources by sending specific type of packets, Crash or overload the network by flooding packets.

A. Types of DoS attack

1) TCP SYN Flood: In this type of attack, attacker first spoof the IP address by using one of the methods of IP spoofing. After that attacker sends the flood SYN packets with that spoofed IP address .Each of these packets are handling by connection request and sending back TCP-SYN ACK packets, waiting for packet in response from that spoofed IP address. As the response is never come back, because of spoofed IP address, the other authorize user does not get the access to the server as server is waiting for response of spoofed address.

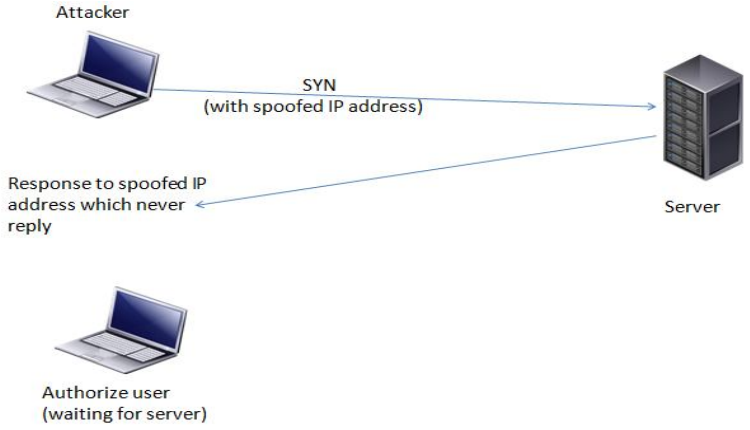

Fig. 1 SYN FLOOD Attack

2)PING Flood: This is simple type of DoS attack .In Ping flood attacker sends a continuous series of ICMP Echo request ping packets to target host on network, to which the target host replies with ICMP reply packets that is ICMP Echo reply. Because of this continuous Request and Reply packets the network become slow and authorize user can have reduce speed network or some time become disconnected.

3) UDP Flood: Similar to Ping Flood it is also one of the simple type of DoS attack.UDP flooding occur when attacker send UDP packet containing the IP packets to target system with purpose of slowing down the target network. so that target system can no longer handle authorize connections. After UDP threshold reaches the server then rejects other request of UDP packets.

B. DoS Countermeasures

1) Attack prevention system: DoS prevention technique is use before the attack happens. This enables the authorize user to reduce attack attempts without denying the services by providing backup services available on demand. This technique can be preferred approach to DoS attack but may be impractical with all types of flooding attacks.

2) Detection system: DoS detection system is used during attack. This enables to detect attack as it begins and respond immediately by minimizing the impact of attack. Detection system involves detection of suspicious pattern or suspicious behavior of that packet.

DoS detection system can be divided into two types such as signature based detection and anomaly based detection. Anomaly based detection is based on traffic deviation from normal and signature based detection are mostly of packets and protocols attacks based on some pattern.

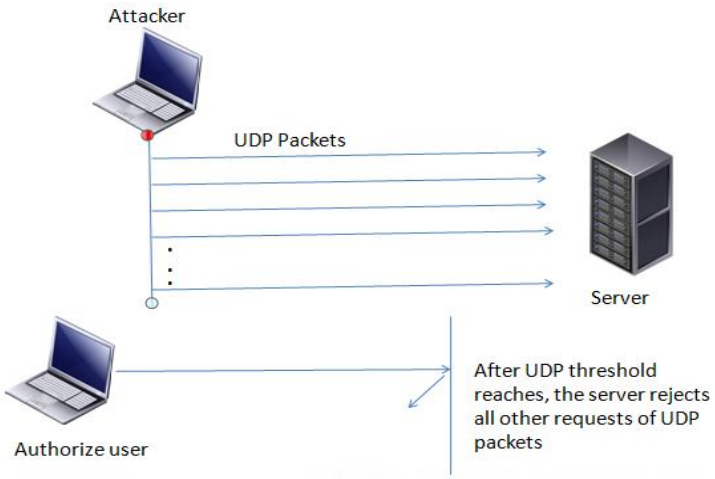

Fig. 2 UDP FLOOD Attack

II. LITERATURE SURVEY

1. Gang Wang, et al. discussed in [4] The author propose approach FC-ANN, based on Fuzzy clustering using ANN algorithm. They divide the architecture into three parts, Fuzzy Clustering Module, ANN module, Fuzzy Aggregation Module and works on KDD database. The result of the system shows that fuzzy clustering with ANN gets the average accuracy 96.71%, greater than BPNN for attacks other than flooding attack. But needs to improve the performance in the flooding type of attack.

2. S.Chavan et al. proposed in [5], in that they use artificial neural network (ANN) and fuzzy Inference systems (FIS) together for the IDS. In that they create new neurons by using ANN algorithm and also uses Fuzzy rules by using algorithm that use snort to build there IDS so the result of the system is depend upon the performance of the Snort tool. EFuNN took few seconds to train the IDS models, ANN took few minutes to converge. Except U2R, the developed fuzzy inference system could detect with high accuracy. The performance was degraded when used all the 41 variables, which also illustrates the importance of input variable selection. Also the experiment results also reveal the importance of input variable reduction. By having less than 40% of the original number of input variables.

3.Mitrokotsa et al. proposed in [6] In which they propose an approach by using emerging SOM for detection of DoS attack based on traffic classification such as normal and abnormal. The approach focusing on the detection of DoS attacks in KDD99 data. Although their work showed very high accuracy (between 98.3% to 99.81%) and a low false alarm rate (between 2.9% to 0.1%), the training procedure suffered from a high computational overhead, especially when the size of the training set was over 10,000.

4. A.M. Chandrasekhar et al. proposed in [7],In that they proposed a concept of IDS by using K-means and two classification algorithms that is fuzzy neural network and SVM classifiers. The proposed technique has four major steps: first one is to use K-means algorithm to generate different training subsets. And then neuro-fuzzy models are trained by using that training subsets. After that classification using Support Vector Machine(SVM). The result shows that the overall performance of their system performs very well and achieved 98.94% accuracy in case of DOS intrusion.

5. M. S. Abadeh et al. in [8], in that they tried to improve fuzzy rules by using local search operators to search their neighborhood the iterative learning approach. Classification rates of the three approaches are better than the winning entry at the Normal, DoS and Probe classes they achieved 84.7% and 92.4%.

6. G.H. Kayacik et al. proposed in [9], In that they propose an approach for IDS that is based on a hierarchy of KSOMs. They try to define how far an intrusion detection approach using a sequence of hierarchical SOMs using only 6 features from the 41 features of KDD dataset. This clustering algorithm significantly reduced the dimensions seen by neurons in SOMs from the second layer. When comparing their results with best supervised learning solutions, their methods have shown a similar detection rate but a higher FP rate. The major reason, in their perspective, is the availability of suitable boosting algorithms for unsupervised learning.

7. C. Jirapummin, N. et al. in [10], in that they propose system based on SOM and Resilient Propagation Neural Network (RPROP) in order to achieve ID combined with visualization and classification on normal traffic and intrusions. In experiments, they perform both quantitative and qualitative analysis. From IDS simulation results achieves more than 90% detection rate and less than 5% false alarm rate in three selected attack programs.

8. Zheng Zhang et al. in [11],they describes CIDS (Correlation Intrusion Detection System), a novel approach in the detection of DoS attacks that utilizes the change in cross-correlation between selected features. As the DOS attack evolves the cross-correlations rise thus revealing the attack.

CIDS relies on changes in correlation magnitude upon shifting from normal to attack conditions, thus it is an anomaly type intrusion detection system (IDS). However it is characterized by several advantages over anomaly IDS, primarily due to the fact that it greatly reduces and/or eliminates the need to maintain normal reference profiles.

9. Allen, W.H., et al. in [12], they present a new technique for detecting the possible presence of certain Denial-of-Service attacks in network traffic. The effectiveness of the technique is demonstrated in experiments against 23 attacks in three different traffic backgrounds. Even though some attacks persist for only 2-4 seconds, results show detection rates up to 84%. Results also show that (for these data) the technique can be tuned to eliminate false alarms. These results are especially favorable given the technique's objective of detecting new (previously unseen) attacks without a template of the background traffic.

III. PROPOSED SYSTEM

DoS attacks are a threat to the Internet. They decrease the service quality of Internet services, therefore it is important to apply countermeasures against Denial of Service attacks or even to only analyze them, and the first crucial step is to detect such attacks. So, develop an effective DoS attack detection system for protecting the network and resources of user from the attacker.

The basic terminology that can be use to build the system

A. *Clustering*

Clustering is the classification of similar objects into different groups, or more precisely, the partitioning of a data into subsets (clusters), so that the data in each subset (ideally) share some common trait-often proximity according to some defined distance measure.

1) K-means clustering: The K-means clustering is a classical clustering algorithm. After an initial random assignment of example to K clusters, the centers of clusters are computed and the examples are assigned to the clusters with the closest centers. The process is repeated until the cluster centers do not significantly change. Once the cluster assignment is fixed, the mean distance of an example to cluster centers is used as the score. Using the K-means clustering algorithm, different clusters were specified and generated for each output class.[13]

The general steps for the K-means algorithm were the following

- Number of clusters (K) are choose
- Centroids Initialization
- Each pattern Assigned to the cluster with closest centroid
- Means of each cluster is calculate to be its new centroid
- Repeat step 3 until stopping criteria is met
- The best clustering solution was chosen after repeating this procedure 10 times.

2) Improved k-Mean Clustering: Another variation of K-mean clustering algorithm is improved K-Mean. The modified K-means algorithm that is Improved k-means algorithm which does not require number of clusters (K) as input. In this algorithm initially two clusters are created by choosing two initial Centroids which are farthest apart in the data set, so that in the initial step itself we can create two clusters with the data members, which are the most dissimilar ones.

Input: D: The set of n tuples with attributes Al,A2, . . . , Am where m = no. of attributes. All attributes are numeric

Output: Suitable number of clusters with n tuples distributed properly [14]

B. Classification algorithm

There are various data mining classification algorithms are available for classification of data sets from database, such as Bayesian Classifiers, Decision Trees, Neural Networks, k-nearest neighbour classifiers, Support Vector Machines, etc.

1) *Naive Bayes Classifier:* A naive Bayes classifier is a simple classifier in which a probability of given data set is found onto the given query. Naive Bayes is the basis for many machine-learning and data mining methods. The algorithm is used to create models with predictive capabilities. It provides new ways of exploring and understanding data.
2) *Artificial Neural Networks:* Also known as Back propagation algorithm is nothing but training algorithm. Training is provided to algorithm for network or how the network should work. When training is done it will give you required output for provided input based on training data.

C Architecture of proposed system

The architecture of proposed system is divided into two modules, Training set generation and Real time layered IDS. Architecture of proposed system provides layered approach for real time detection system. First the incoming packet is going through Training set generation for creating the dynamic set for packet classification by using TCP/IP features. Then all the incoming traffic is going through this layered approach and classify as normal packet or malicious packet. The proposed architecture uses the various TCP/IP features to classify the packets.

1) *Training set generation:* The system uses dynamic database for classification of incoming packets. It is nothing but a creation of database for future use .All incoming packets are goes through each level of training set generation and create dynamic data set and mark incoming packet as" OK packet" or "Attack". packet sniffer scans the incoming packet by using WinPCap library function used for windows platform to capture packet and network analysis.
2) Packet analyzer analyze the packet and detects its type, protocol used, etc. by using JPCap library function for capturing and sending network packets from java application, that is it simply decodes the packet data. Packet signature extract the

signature from packet data, after feature extraction from packet the packet is labeled as ok or attack packet. And that information is stored into the database.

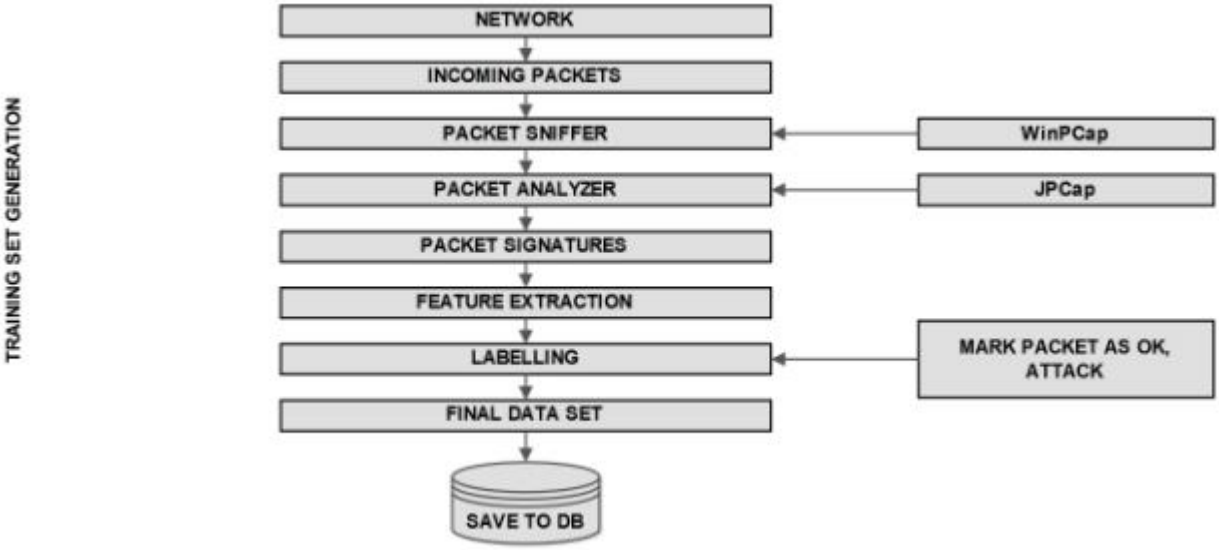

Fig. 3 Training set generation

2) Real Time layered IDS: All incoming packets must go through this layered architecture for real time detection system. In this layered approach packet goes through series of phases such as analyzer, signature, and feature selection and so on. The incoming packets are first analyzed and pass to Signature module where the actual pattern of packet is extracted. e.g. If a single command is issued multiple of times on server that may be one of the signature type for DoS attack. For classification of packet first some particular feature of packet are selected and then data set have been loaded from dynamic database, after that transformation is done on that data and by applying K-means clustering and Naive Bayes algorithm for data mining and classification algorithms on packet is done by using current selected features. The result of algorithm is either the packet is Normal or Attack is detected. And can be classify attack as SYN FLOOD, PING FLOOD, UDP FLOOD.

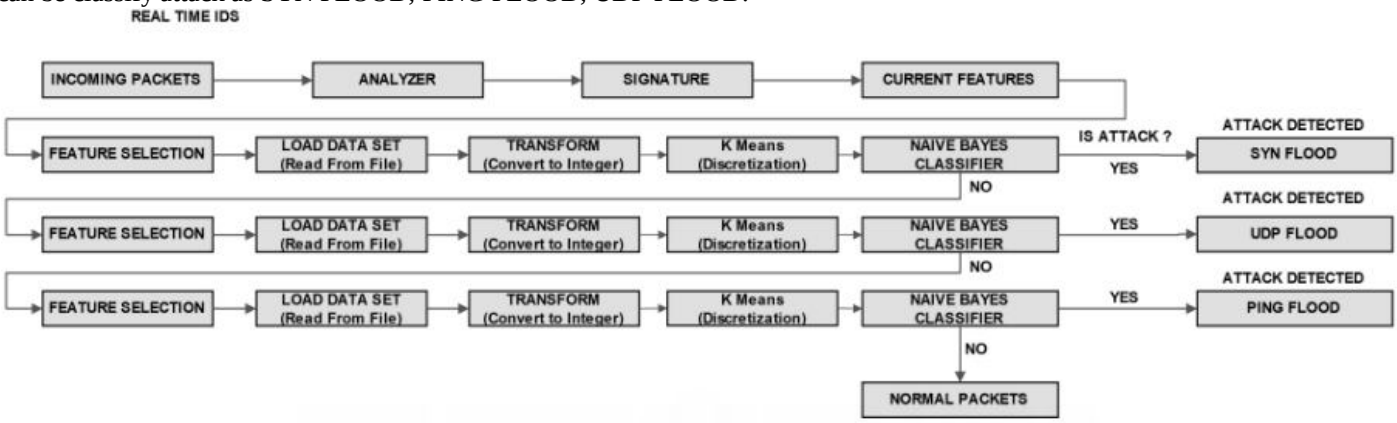

Fig. 4 Real Time IDS-Layered approach

IV. CONCLUSION

Now a days, DoS attack are real threats to Computer Security, therefore detection of such attacks and to protect computer network and increase the security in computer networks there is need to build a detection system. Also it is observed that one method is not sufficient for classification of packets so there is need to combine more than one methods of classification, to improve the packet classification for detecting the normal packet from malicious packet.

ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to my Project Guide Prof. Ruhi Kabra for her valuable suggestions and expert guidance throughout my course of study and timely help given to me in the completion of my project report.

I express my gratitude to Dr.V.B.Chowdhary, Principal, G.H.R.C.E.O.M, and Prof. Ruhi Kabra HOD Department of Computer engineering for their kind help and co-operation.

REFERENCES

[1] Nidhi Srivastav,Rama Krishna Challa,*"Novel Intrusion Detection System integrating Layered Framework with Neural Network"*, 2013 3rd IEEE International Advance Computing Conference (IACC).
[2] J. Mirkovic and P. Reiher,"*A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39-53, 2004.
[3] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai,"*Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10*.
[4] Gang Wang, Jian Ma ,Lihua Huang and Jinxing Hao, In the "*A new approach to Intrusion Detection using ANN and fuzzy clustering*", in the Elsevier 2010
[5] S.Chavan, K.Shah, S.Sanyal, S.Mukherjee, A.Abraham, and N.Dave, In the "*Adaptive neuro-fuzzy Intrusion detection systems*, in ITCC-Vol. 1of 2004
[6] Mitrokotsa, A. Douligeris, in the "*Detecting denial of service attacks using emergent self-organizing maps", in "Signal Processing and Information Technology*", 2005. Proceedings of the Fifth IEEE International Symposium
[7] A.M. Chandrasekhar, K. Raghuveer, in the "*Intrusion detection technique by using K-means, fuzzy neural network and SVM classifiers*", In ICCCI, 2013
[8] M. S. Abadeh and J.'Habibi, In the, " *Computer intrusion detection using an iterative fuzzy rule learning approach*", In IEEE International Conference on Fuzzy Systems, IEEE Press
[9] G.H. Kayacik, A.N. Zincir-Heywood, M.I. Heywood,in the "*On the capability of SOM based intrusion detection systems", IEEE IJCNN*, Portland, USA
[10] C. Jirapummin, N. Wattanapongsakorn, P. Kanhamanon,In the"*Hybrid Neural Networks for Intrusion Detection System*", ITC – CSCC, Thailand
[11] Zheng Zhang , Manikopoulos C.N.,*"Detecting denial-of-service attacks through feature cross-correlation* Published in:Advances in Wired and Wireless Communication, 2004 IEEE"
[12] Allen, W.H., Marin, G.A. ,*The LoSS Technique for Detecting New Denial of Service Attacks*, Published in: SoutheastCon, 2004. Proceedings. IEEE
[13] M. Jianliang , S. Haikun, B. Ling, "*The Application on Intrusion Detection Based on K-means Cluster Algorithm*" , in International Forum on Information , Technology and Applications ,Vol.1,I EEE ,2009
[14] Anupama chadha, Suresh kumar, "*An Improved K-means clustering algorithm :A step forward for removal of dependency on K*",at 2014 International Conference on reliability,optimization and information tech-ICROIT 2014,INDIA

