PROACTIVE & DETECTION STRATEGY DESIGNING FOR DRDOS ATTACK

Dipika Mahire
[1] Department of Computer Engineering, G. H. Raisoni Collage of Engineering and Management, Ahmednagar. University of Pune, India

Amruta Amune
[2] Professor, Department of Computer Engineering, G. H. Raisoni Collage of Engineering and Management, Ahmednagar. University of Pune, India

***Abstract*— Nowadays in internet DRDoS has become very common and dangerous attack. The attacker launch an attack by sending spoofed request packets to victim and victim will be not able to handle such huge amount of requests and depending on the attack ,site will be crashed or offline for many days . This is most critical attack for network security world and difficult to detect is called distributed reflected denial of service (DRDOS) attack. Attacker attacks on website for some personal or commercial purpose. So, as it is common attack there are many techniques also available for detecting the attack. The detection systems are available but some of them are misuse based and some are anomaly based detection systems which are suitable for known attacks only and also designed for particular protocols only. So, it was necessary to implement the system which can detect the known and unknown attack both, which is protocol independent also. And the proposed system is more efficient and effective to detect the attack.**

***Index Terms*— DoS Attack; DRDoS Attack; Spearmans coefficient; RCD algorithm; Ada-Boost Algorithm**

I. INTRODUCTION

Nowadays, Denial of service attack has become more powerful and common attack. Denial of service attack is an attempt to make the resources unavailable to authenticated or intended users. The attacker floods the victim by sending lots of packets. So that, it's all resources and bandwidth will be used by unwanted user requests i.e. malicious requests. And because of such lots of unwanted user requests the victim will get crash or become offline for number of days or hours depends on attack and the victim also can't serve the legitimate users. There are two types of DoS attack.

1. Distributed Denial of Service attack(DDoS)
2. Distributed Reflection Denial of Service attack(DRDoS)[13]

The structure of DDoS and DRDoS attack is shown in fig.1 and fig.2 respectively.

In DDoS attack, attacker launches the attack by using vulnerable hosts called zombies. Some of them are master zombies and some are slave zombies. Attacker sends attack command to master zombies and master zombies send attack command to slave zombies. Slave zombie sends lots of request packets to victim to flood it. While in DRDoS attack, attacker launches the attack by using the reflectors in addition to zombies. Reflectors are the legitimate hosts used to launch the attack. Attacker sends attack command to master zombies and master zombies send attack command to slave zombies. Slave zombie sends lots of spoofed request packets to victim to flood it.

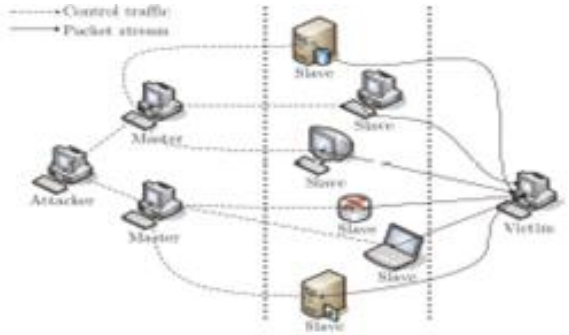

Fig.1 Structure of DDoS attack

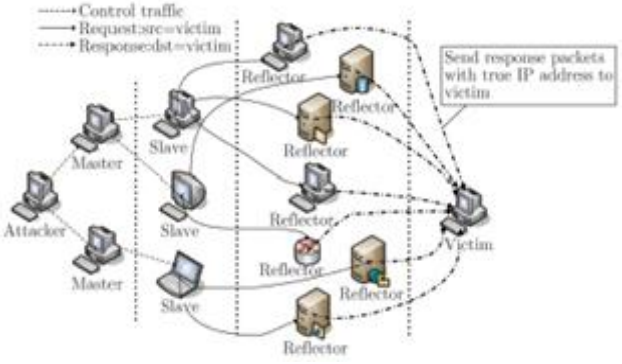

Fig.2 Structure of DRDoS attack

Manuscript received June, 2015.
***Dipika Mahire**, Computer Engg.,G.H.Raisoni, college of Engg. & Management .University of Pune, Ahmednagar, India .*
***Amruta Amune**, Computer Engg.,G.H.Raisoni, college of Engg. & Management .University of Pune, Ahmednagar, India .*

II. LITERATURE SURVEY

Sneha S. Rana, T. M. Bansod proposed the technique which uses the Hop-count filtering technique to detect the IP spoofing.and also uses the traceback[2] to get the source of attack.This technique is easy to implement but there may be significant false positives if the attacker knows the number of routers i.e., TTL value from reflector to victim.

Andrey Belenky and Nirwan Ansari has given a traceback[3] mechanism to detect the attack by using Dynamic packet Marking(DPM). The DPM(Dynamic packet marking)is easy to implement; It has low processing and no bandwidth overhead. But, the routers has more overhead of marking and it can't detect the path upto the source host.

Hongbin Luo, Yi Lin and Hongke Zhang[4] has proposed the technique in which they have separated the identifier(represents identity), locator(represents location).While in today's world the IP address consist of both identity and location into it. So, If we separate the identifier from locator it helps to prevent DDoS attack. This technique is effective enough to protect DDoS attack but,it is time consuming for legitimate users to communicate as compared to communication using IP address.

Dhruv A. Patel presented the technique in which he used HIP (Human Interaction Page) [5]which issues the graphical tests for the client, to identify whether the client is legitimate one or an attacker. It is easiest way to detect the attack and it provides more security as it uses the rate limiter but for legitimate users it is time consuming as it needs to solve the puzzles unnecessarily.

Saravanan Kumarasamy and Dr. R. Asokan presented the mechanism for defending against DDOS attack called Pushback. In which the intelligent router in ISP network identifies the attack traffic and sends pushback[6] message to the upstream routers. It is efficient technique to detect attack but routers has overhead to issue puzzles for the clients.

Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin has proposed DRDoS attack detection technique which uses the Rank correlation Based Detection algorithm[1]. It was effective and efficient algorithm to differentiate flash crowd from the attacking traffic. But, still it has some false positive and false negative rates.

III. PROPOSED SYSTEM

In proposed system, the RCD algorithm is used in conjunction to Adaboost algorithm i.e output of RCD is given as an input to Ada-Boost algorithm. It is used to minimize the false positive and false negatives of the RCD algorithm.

The system is protocol independent and not affected by network throughput. In RCD, when suspicious flow comes to a router an attack alarm raises, then upstream routers samples and calculate rank correlation of suspicious flows (i.e. Similarity between the two suspicious flows) and use the correlation value for detection of malicious flow. The correlation is has been used to detect the DDoS attack. But, here first time correlation is used to detect DRDoS attack. It can efficiently distinguish the flash crowd from attacking traffic.

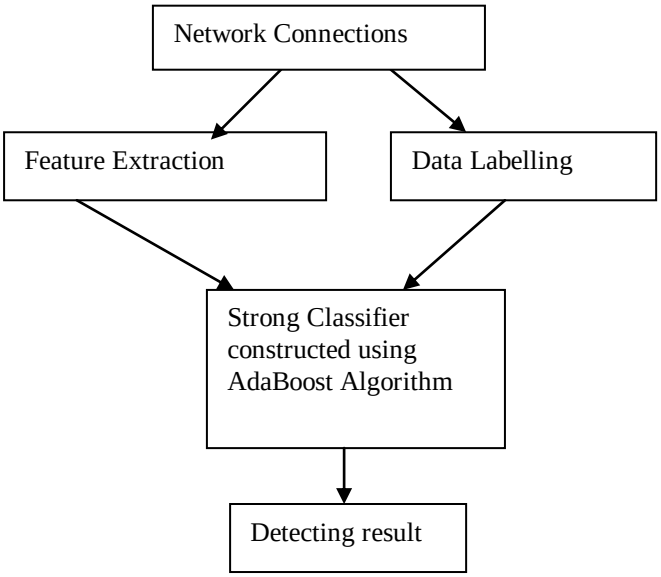

Fig. 3 Architecture of Proposed system

When the number of requests comes to the victim RCD algorithm will work. And then the output of RCD is given to the Ada-Boost algorithm. The Ada-Boost algorithm then accepts the forwarded packets from RCD. Ada-Boost algorithm Extracts the important attributes from the packets.(i.e. Feature extraction).After extracting features the packets are labeled like Attacking packet or Normal packet by using some threshold. And then by calculating the degree of threshold packet is discarded if it is malicious one.

Feature extraction :

For each request, we extract three features to detect attacking flow: "Features of TCP connection", "Content features within a connection" and "Traffic features".

Data labeling :

Here, in Data labeling the data coming from RCD is labeled based on the number of requests from particular source to particular destination within particular time limit. If number of request exceeds the threshold then it is labeled as attacking packet otherwise Normal packet.

Strong classifiers construction:

A strong classifier is constructed using our improved Adaboost algorithm. By using threshold degree of labelled data final classification is done. More detail is given in the 3.2 section**.**

RCD ALGORITHM[1]

1. Locate suspicious flows on upstream router.
2. Sample the number of packets of suspicious flows per time unit T for a short time, get value sequences for flow.
3. Submit sequences to a detection center, which will divide flows into pairs and calculate coefficient for each pair according to (1).
4. Compare coefficients for suspicious flows and make decision by (2).

5. If confirmed, then discard these flows on the routers.

In Spearman's correlation coefficient, for two random variables *X* and *Y* of ranked values, the expected values are μX and μY, and standard deviations are σX and σY. The coefficient rX,Y is their covariance normalized by the standard deviation:

$$r_{X,Y} = \frac{cov(X,Y)}{\sigma_X \sigma_Y} = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma_X \sigma_Y}$$

Where *E* is the expected value, and *cov* is the covariance which could also be represented using *E*, then it has:

$$r_{X,Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}} \quad (1)$$

The value range of rX,Y is [-1,1], closer to 1 represents stronger positive linear relationship i.e. two flows are attacking flows while closer to -1 represents stronger negative linear relationship i.e. two flows are non-attacking flows.

We could use two thresholds $\delta 1$ and $\delta 2$ to judge whether both are malicious flows or not. $Ra,b = 1$ means that both are reflection flows.

$$R_{a,b} = \begin{cases} 0, & \text{for } \delta_1 \le r_{a,b} \le \delta_2 \\ 1, & \text{for } r_{a,b} < \delta_1 \text{ or } r_{a,b} > \delta_2 \end{cases} \quad (2)$$

ADA-BOOST ALGORITHM[11]

1.Start
2.Dataset load to system.
- S={a1,a2,…..an}
- S=dataset.
- a1,a2,…an-attributes of dataset(column name)

3.Weight assign to each attribute according to their priorities.
4.Labeling to each packet by considering weight of attribute based on threshold value(for e.g threshold=10).
L={A,N}
5.Dataset will be prepared for classification with help of step 2,3.
6.Classification is done on basis of label of packet.
7.After classification degree of each label (normal and attack)gets calculated.
8.Compare the degree with threshold value.
9.Stop.

Ada-Boost algorithm is used to improve the result performance of the RCD algorithm. As it increase the performance it is called Boosting algorithm.

IV. MATHEMATICAL MODEL

Let S be the system which is used to find the DoS attack detection system presented. Here, the proposed system employs the principles of RCD and Adaboost algorithm. The proposed system quip detection system with capabilities of accurate characterization for traffic behaviours and detection of known and unknown attacks respectively.

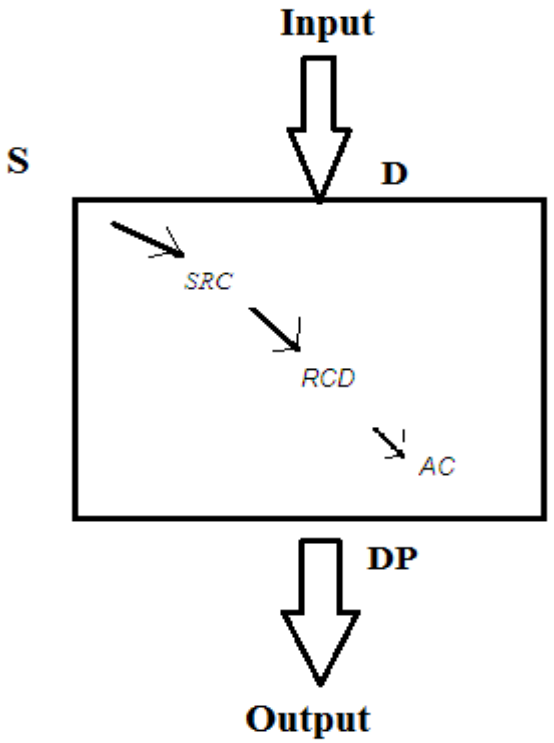

Fig. 4 Mathematical Model

As we can see in Fig.4 where,
S={D,SRC,RCD,AC ,DP}
Where,
S= System.
D= Dataset.
SRC = Spearman's Rank Correlation
RCD= Rank Correlation based Detection
AA= Adaboost Algorithm
DP= Detected packets.

1 Input:

Given an arbitrary dataset X = {x1, x2, · · · , xn}, Where xi = input traffic , $(1 \le i \le n)$ represents the ith m-dimensional traffic record.

2 Spearman's Rank Correlation[1]

In Spearman's correlation coefficient, for two random variables X and Y of ranked values, the expected values are μX and μY, and standard deviations are σX and σY. The coefficient $r_{X,Y}$ is their covariance normalized by the standard deviation.

$$r_{X,Y} = \frac{cov(X,Y)}{\sigma_X \sigma_Y} = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma_X \sigma_Y}$$

Where E is the expected value, and cov is the covariance which could also be represented using E, then it has:

$$r_{X,Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}}$$

The value range of $r_{X,Y}$ is [-1,1], closer to 1 represents stronger positive linear relationship closer to -1 represents stronger while negative linear relationship, whereas 0 means no linear relationship.

3 RCD[12]

In RCD, once an alarm appears, routers in the path will

sample flows for sufficient time. Ideally, for two pure attacking flows fa and fb, correlation coefficient $r_{a,b}$ will be close to 1. Although the Internet may not strictly satisfies the assumption due to legitimate traffic in background, the correlation between two malicious flows should be remarkably strong compared with other pairs.

Then in a DRDoS scenario, we could use two thresholds δ1 and δ2 to judge whether both are malicious flows or not. $R_{a,b}$ = 1 means that both are reflection flows.

$$R_{a,b} = \begin{cases} 0, & \text{for } \delta_1 \le r_{a,b} \le \delta_2 \\ 1, & \text{for } r_{a,b} < \delta_1 \text{ or } r_{a,b} > \delta_2 \end{cases}$$

4 Adaboost Algorithm: [11]

Adaboost is a stereotype algorithm of boosting, It extracts the features from the packets resulted from the RCD algorithm. And label the packets according to specific strategy to detect the malicious packets.

5 Output: DP (Detected Packets) :

DP={n,m}

Where,

n is normal packets and

m is the malicious packets

V. RESULTS

In proposed system the Ada-Boost algorithm is used in conjuction with the RCD algorithm.The following graph shows the difference in detection result of RCD algorithm and RCD+Ada-Boost. i.e, existing and proposed system

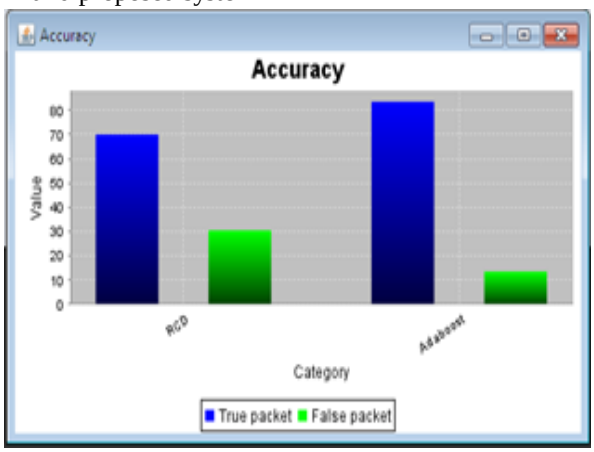

Fig 6. Comparison of Accuracy of RCD & RCD+AdaBoost.

algorithm. And it can effectively detect the attack .Proposed system will give more precise results as request packets are filtered twice.And time required to detect the malicious packets is very low.

VI. CONCLUSION

DRDoS attack is the one of the most dangerous attack as, it is difficult to detect. Although there are many techniques, algorithms available for detection of DRDoS attack. Some of them are mentioned above. But, all of them are detecting the DRDoS attack which is known and they are protocol dependent methods. So, the proposed system detects the DRDoS attack. The RCD algorithm and Ada-boost algorithm is used to detect attack.RCD algorithm is protocol independent and its computation cost is not affected by network throughput. While the Ada-Boost algorithm is the hybrid algorithm (i.e. it is combination of Misuse based and anamoly based detection).It is effective and efficient algorithm. The Ada-boost algorithm is used in conjunction with the RCD algorithm to increase the effectiveness of the system.

ACKNOWLEDGMENT

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my work successfully.

I express my gratitude towards project Prof. Amruta Amune, Bhivarabai Sawant, Department of Computer Engineering G.H.Raisoni College of Engineering & Management, Ahmednagar, who guided & encouraged me in completing the this work in scheduled time. I would like to thanks our Principal ,for allowing me to pursue my project in this institute.

REFERENCES

[1] Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin,"A Rank Correlation Based Detection against Distributed Reflection DoS Attacks",IEEE COMMUNICATIONS LETTERS VOL:17 NO:1 ,YEAR 2013.

[2] Sneha S. Rana, T. M. Bansod," -IP Spoofing Attack Detection using Route Based Information",International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 4, June 2012.

[3] Andrey Belenky and Nirwan Ansari, "IP Traceback With Deterministic Packet Marking"- IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 4, APRIL 2003.

[4] Hongbin Luo, Yi Lin, and Hongke Zhang-"Preventing DDoS Attacks by Identifier/Locator Separation", IEEE Network , November/December 2013.

[5] Dhruv A. Patel, Prof. Hasmukh Patel-**"**Detection and Mitigation of DDOS Attack against Web Server", Volume 2, Issue 2| ISSN: 2321-9939.

[6] Saravanan kumarasamy, DR. R. Asokan- Distributed Denial Of Service (DDoS) Attacks Detection Mechanism, International Journal of Computer Science, Engineering and Information Technology,Vol.1,No.5,December 2011.

[7] Xinyu Yang, Wenjing Yang, Yi Shi, Yage Gong, "The Detection and Orientation Method to DRDoS Attack Based on Fuzzy Association Rules", Journal of Communication and Computer, ISSN1548-7709, USA.

[8] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1073–1080, 2012..

[9] Wei Hu and Weiming Hu," Network-based Intrusion Detection Using Adaboost Algorithm", Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence., Sep. 2005,712-717.

[10] S. Stolfo and et al. The third international knowledge discovery and data mining tools competition [online]. Available: http://kdd.ics.uci.edu/databases/kddCup99/kddCup99.html, 2002.

[11] W. Lee and S. J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, 3(4):227–261, November 2000.

Dipika Mahire received the B.E degree 2012 Information Technology from KCEOIT,North Maharashtra University, Jalgaon, India.She is currently pursuing M.E. under Pune University ,Maharashtra,India.

Amruta Amune received the M.E degree 2012 Computer from MIT,Pune,University,Pune,India.She is working as Professor in G.H.Raisoni College of Engg. & Management,Ahmednagar,University of Pune,India.

