International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 09-Apr-2015,ISSN_NO: 2320-7248

Detection and Elimination of Distributed Reflection DoS (DR-DOS) Attack Using Rank Correlation Detection (RCD) Algorithm

Shewale Chetan S.[1], Patil Chetan M.[2], Pawar Sushil S.[3], Jadhav Shirish S.[4] Seema Shabadi.[5]

Student, Computer Engineering , JSPM's Rajarshi Shahu College of Engineering, india[1].
Student, Computer Engineering , JSPM's Rajarshi Shahu College of Engineering, india[2].
Student, Computer Engineering , JSPM's Rajarshi Shahu College of Engineering, india[3].
Student, Computer Engineering , JSPM's Rajarshi Shahu College of Engineering, india[4].
Professor, Computer Engineering , JSPM's Rajarshi Shahu College of Engineering, india[5].

Abstract— *DDoS represent Denial of service in Distributed system and presents a serious threat into the Internet, when it incepts. In Distributed Reflection DoS (DRDoS), attackers may try to make fool innocent servers while flushing massive packets to victim. But most of current DRDoS detection mechanisms are available which contain own protocol and doesn't work on other than specific protocol. In DDoS attcks it is found that because of attacking flow and normal flow from server have relation between different packets. While taking this consideration, the Rank Correlation Detection algorithm is comes under the picture. RCD is most efficient algorithm to finding a difference between massive packets and normal packets. It finds the rank of each packets and if it is found as massive then, it discard from the router. RCD can find the difference between reflection flows from legal clients. It is most efficient as well as effectively algorithm for DRDoS, it is used as a indicator in DRDoS.*

Keywords— **Rank Correlation, RCD, Distributed Reflection, DoS, Denial of Service.**

1. INTRODUCTION

Distributed Denial of Service (DDoS) attack is a threat into the Internet, in which lots of controlled hosts deluge the victim site with massive packets. It is more difficult to protect, in Distributed Reflection DoS ,in which attackers spoof requests to many Internet servers which will send responses back to the victim. Therefore, a lot of connectionless request-response based protocols could be exploited, because of this dilution of locality makes it hard to isolate attacking traffic. Local detection near single reflector will be useless because of low volume of repelled traffic. Though ingress filtering is a hopeful solution, it has not been largely deployed .There have been some packet-level defense methods, which filter all incoming response packets, which is of low cost, and the result will be no access to the server. While Inspecting packet content and tracking protocol the status maybe helpful, but as per our need a lot of computation which is also prone to attacks, along with more protocols being fully used to launch DRDoS. The counter measures must consider a list of possible protocols with each one treated specifically, and the list needs to be

updated in time. So we urgently expect some protocol independent methods to help detecting most kinds of DRDoS. We investigate the basic traffic pattern introduced near the victim under DRDoS, and propose a general detection method i.e. the Rank Correlation based Detection (RCD). RCD is protocol independent and its computation cost is not affected by network throughput. In RCD, once an attack alarm raises, upstream routers will sample and test rank correlation of suspicious flows and use the correlation value for further detection.

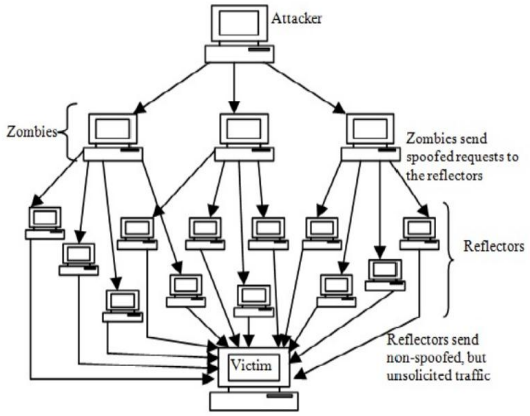

Fig 1. Attacking Mechanism

Correlation has been successfully used in DDoS detection, e.g., correlation coefficient has been successfully employed to discriminate DDoS attacks from flash crowds.

2. LITERATURE SURVEY

Now a days people using internet are increased from last decade due to increase in number of users. The reason for sudden growth of internet is users unable to communicate directly with the clients so they decided to communicate over the internet. For E.g. MNC has situated in many countries but headquarters are able to provide work information through mail or any other services in this case other users can access the information and make changes in it[1]. The attacks present in internet are Dos, DDos, DRDos, worm hole attack etc. so the communication should be strictly safe for transmission of information users are also needed for this safety[3]. Due to Serious threat the controlled node which are flood over the destination and the packets are unable to reach the clients.

There are many ways to detect for these attacks:

1) Locate the detection in single server technique can be done but the failure is not suitable for heavy traffic and path were the collision is more.

2) Tracing packets with protocol can be used but it requires more number of complex calculations with lot of time needed for this method but this method not suitable for vulnerable attacks.

The above method cannot be used now because the nodes needs more security and these cannot provide very high level security for data. For more security communication we need to have the linear relationship between source and destination [1]. In these condition we are implementing Rank Correlation Coefficient in each nodes in through each path of the router, when the communication established the request signal from the source and destination should be calculated the rank value and the response from the destination signal i.e. (Acknowledge signal) has the rank value in these condition the both flows can matched with each other and packets discard or transmitted on basis on rank valve are as follows:

1. If both the valves are matches means it establish the communication (but the valve can slightly vary anyone it should be point variation only be allowed).

2. If both the valve are mismatches means the destination node able to understand that the attacker are trying to access the data, now totally the communication are terminated.

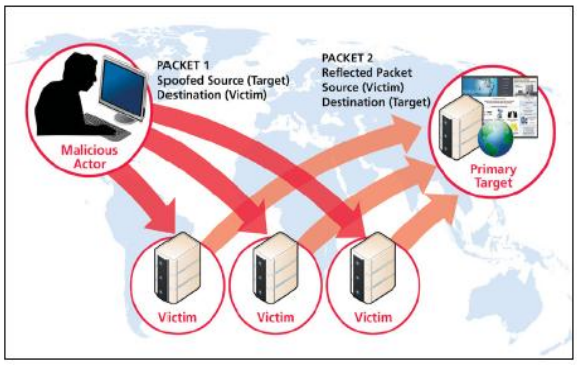

Fig 2. Attacker and victims in the system

2. SYSTEM FEATURES

1. User Module: In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. Rank Correlation based detection (RCD): DoS attack traffic behaves differently from the Legal network traffic, and the behavior of network traffic is reflected by its statistical properties. To well describe these statistical properties, we present a novel Rank correlation based detection (RCD) approach in this section. This RCD approach employs triangle area for extracting the correlative information between the features within an observed data object.

3. Detection Mechanisms: In this module, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack.

Otherwise, it is labeled as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed Rank correlation based detection approach to analyze legitimate network traffic.

4. Computational complexity And Time Cost Analysis: While in this module we conduct an analysis on the computational complexity and the time cost of our proposed Rank correlation based detection system. On one hand, as discussed in, triangle areas of all possible combinations of any two distinct features in a traffic record need to be computed when processing our proposed RCD. This is the former technique which extracts the geometrical correlations which are hidden in individual pairs of two distinct features within each network traffic record, and it offers more accurate characterization for network traffic behaviours. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

3. MATHEMATICAL CONCEPTS

In view of limited space, we mainly focus on two typical scenarios involving one attacker and multiple reflectors:

a) One attacker spoofs requests to reflectors randomly with uniform distribution, at a constant rate, e.g., the outgoing bandwidth.

b) One attacker spoofs requests to reflectors randomly with uniform distribution, at a low but variable rate.

We define all packets to the victim through one router as a flow. The packet count of suspicious flows is sampled per time unit T when an alarm appears. Set the start of a time span as t, then for two suspicious flows f_a and f_b, their respective set of source reflectors are R_a and R_b in time span [t, t+T], with Na and N_b reflectors, where the set of uninvolved reflectors are R_o,.Here source reflectors of one flow is all the reflectors which will contribute packets to the flow if received bogus request packets. For the impact of network latency, the packets arrived at the victim in flow f_a and f_b should be generated a little earlier at R_a and R_b. With average latency τ, if T is far greater than τ, the count of arrived packets at victim in time span [t, t+T] (say, C_a,t and C_b,t) could be approximated by the count of generated packets in reflectors in [t-τ, t+T-τ] (say, C_a,t$-\tau$ and C_b,t$-\tau$), shown as follow:

$$C_a,t \approx C_a,t-\tau \quad (1)$$

$$C_b,t \approx C_b,t-\tau \quad (2)$$

The generated packets in reflectors are the immediate result of arrived packets from the attacker. For most scenarios, one arrived packet generates N (usually 1) packets, e.g., only one packet will be produced for each arrived request packet from attacker. So in [t-τ, t+T-τ], the arrived request packets at reflectors are also C_a,t$-\tau$ and C_b,t$-\tau$, and the total number of reflectors (including ones not in set R_a and R_b) involved in the attack is Nr, while the total number of arrived request packets are Cr,t$-\tau$. As bogus requests from the attacker are distributed uniformly, there are:

$$C_a,t\text{-}r \approx N_a/N_r * C_{r,t}\text{-}T \quad (3)$$

$$C_b,t\text{-}r \approx N_b/N_r * C_{r,t}\text{-}T \quad (4)$$

Then we have:

$$C_a,t/\ C_b,t \approx C_{a,\ t\text{-}T}/\ C_{b,\ ,t\text{-}T} \approx N_a/N_b \quad (5)$$

That is, in [t, t+T], for flow fa and fb, the ratio of the packet count is close to the size of their reflector set. If R_a and R_b don't change significantly between adjacent time units, N_a/N_b could approximate a constant for a short period of time. Consequently, the packet arriving rates for f_a and f_b is proportional. On top of that, if the attacker sends bogus request at the full speed, $C_r,t-\tau$ is approximately the outgoing bandwidth of the attacker, then:

$$C_a,t + C_b,t \approx C_a,t\text{-}r + C_b,t\text{-}r \approx N_a + N_b/\ N_r * C_{r,\ t\text{-}r} \quad (6)$$

So, summation of packet arriving rates for f_a and f_b approximate a constant. In above two typical scenarios, the count of arrived packets per time unit for f_a to f_b presents a linear relationship, which could be accurately expressed by correlation coefficient. For the situation with two or more attackers, the above conclusion holds as long as attackers share the same set of reflectors, which is reasonable as an attacker may not utilize all reflectors, and the master attacker needs to add more slaver attackers to generate massive traffic.

4. ALGORITHMS

A. Spearman's Rank Correlation

The well-known Pearson's correlation coefficient is suitable for describing the linear relationship [9]. However, due to the background traffic and delay, the linearity may not be obvious. And Pearson's correlation is sensitive to outliers introduced by traffic bursts. Through experimental comparisons, Spearman's rank correlation coefficient (Spearman's rho) is more suitable for detection, where a raw value is converted to a ranked value and then Pearson's correlation is applied. For a given value, its ranked value is the average of its position(s) in the ascending order of all values.

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:

$$rX,Y = \mathrm{cov}(X, Y) / \sigma X \sigma Y = E((X - \mu X)(Y - \mu Y)) / \sigma X \sigma Y \quad (7)$$

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

$$rX,Y = E(XY) - E(X)E(Y) / \text{sqrt}\,(E(X2) - E2(X)E(Y2) - E2(Y)) \quad (8)$$

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

B.Rank Correlation Detection

In RCD, once an alarm appears, routers in the path will sample flows for sufficient time. Ideally, for two pure attacking flows f_a and f_b, 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 δ_1 and δ_2 to judge whether both are malicious flows or not. $R_a,b = 1$ means that both are reflection flows.

$$Ra,b = \begin{cases} 0, \text{ for } \delta 1 \leq ra,b \leq \delta 2 \\ 1, \text{ for } ra,b < \delta 1 \text{ or } ra,b > \delta 2 \end{cases} \quad (9)$$

5. FUTURE SCOPE

1) Other correlation-like measurement and the comparison of their effectiveness.
2) Extensive experiment against real DRDoS in the Internet.
3) Using RCD in more sophisticated scenarios.
4) What the attackers can do to escape detection and the counter measures.

6. CONCLUSION

We detect the DRDoS independent of specific protocols, and proposed the Rank Correlation based Detection (RCD) algorithm. Once massive packets or suspicious flow are found, then Rank correlation technique are used to differentiate between the massive packets and normal packets, also if suspicious flows found, RCD starts to calculate the rank correlation between flow pairs and give final alert according to preset thresholds. If confirmed that flow are not authenticated, then discard these flows from the routers.

7. 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, January 2013.

[2] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He‡,Priyadarsi Nanda and Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," IEEE Transactions on Parallel and Distributed Systems VOL:25 NO:2 Year 2014

[3] L. Zhang, S. Yu, D. Wu, P. Watters, "A survey on latest botnet attack and defense," in Proc. 2011 IEEE Conf. on Trust, Security and Privacy in Computing and Communications, pp. 53–60.

[4] V. Paxson, "An analysis of using reflectors for distributed denial-ofservice attacks," ACM Computer Commun. Rev., vol. 31, no. 3, pp. 38–47,2001.

[5] P. Ferguson and D. Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing."

[6] "Stateful Inspection Technology (the industry standard for enterprise class network security solutions)." Available: http://www.checkpoint.com/products/downloads/StatefulInspection.pdf.

[7] G. V. Rooij, "Real stateful TCP packet filtering in IP filter," in Proc. 2001 USENIX Security Symposium.

[8] T. Hiroshi, O. Kohei, and Y. Atsunori, "Detecting DRDoS attacks by asimple response packet confirmation mechanism," Computer Commun., vol. 31, no. 14, pp. 3299–3306, 2008.

[9] 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.

[10] G. E. P. Box, G. M. Jenkins, and G. C. Reinsel, Time Series Analysis: Forecasting and Control, 3rd edition. Prentice Hall, 1994.

[11] S. Yu, W. Zhou, and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," IEEE Commun. Lett., vol. 12, no. 4, pp. 319–321, 2008.