Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.85 – 92

RESEARCH ARTICLE

Detection of Distributed Reflection DoS by using Rank Correlation

Preeti Goyal[1], Sangeeta Malik[2]

[1]M.Tech (CSE), Vaish College of Engineering, MDU, Haryana (India)

Preeti.15.92@gmail.com

[2]Assistant Professor, Vaish College of Engineering, MDU, Haryana (India)

Sangeeta.phogat@gmail.com

Abstract: Information technology has widened itself over the last two decades and has become the axis of today's global development, but this development also faces many problems among which DoS is one of the big problem. DoS presents a great threat to internet as an attacker sends a lots of requests to the victim, Such that the victim will not be able to entertain the legitimate user and the next stage of this problem is Distributed Reflection DoS in which many attacker sends the request to a server which sends these request with multiple reflection to the victim because of so many request the victim face the severe problem. There are many protocol based Algorithm to detect this problem but they are not efficient and have high cost. Here we have introduced an algorithm i.e. Rank Correlation Detection Algorithm which will detect the malicious node among the legitimate nodes so that node can be removed from the path of transfer of the data packs.

Keywords: DRDoS, Spearman's Rho, Rank Correlation

I. Introduction

Denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks pose a grave danger to Internet operation. They are, in essence, resource overloading attacks. The goal of the attacker is to tie up a chosen key resource at the victim, usually by sending a high volume of seemingly legitimate traffic requesting some service from the victim. The overconsumption of the resource

leads to degradation or denial of the victim's service to its legitimate clients. In the absence of effective defense mechanisms, the denial-of-service effect lasts for the entire duration of the attack (i.e., as long as key resources are being tied with malicious traffic), and vanishes quickly once the attack is aborted. Since machine resources are usually shared among many applications, the DoS effect inflicts significant damage — not only on client transactions with the victim, but on the victim's total operation. The victim experiences a significant slowdown in all applications sharing the targeted resource, and frequently also connectivity disruption. Both DoS and DDoS attacks are seemingly simple in design and operate without requiring any special skill or resource for their perpetration. The attack tools can be obtained easily online and the attack goal (resource exhaustion) is attained whenever a sufficiently large amount of malicious traffic is generated. The targeted resource dictates the type and contents of attack packets, e.g. exhaustion of CPU resources requires computation-intensive packets such as CGI or authentication requests, while network resources can be exhausted by any high-volume traffic.

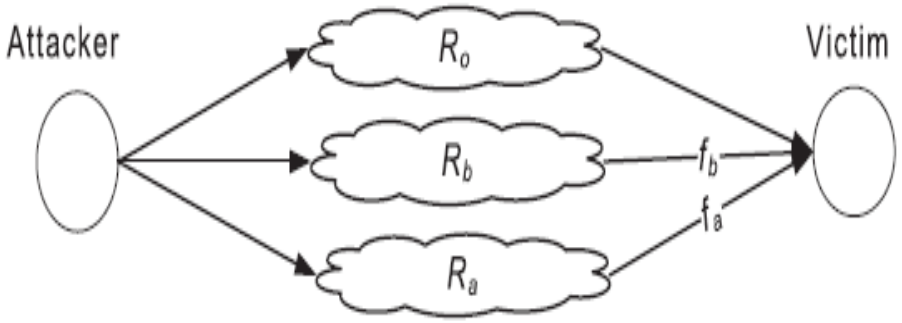


Fig. 1. Attacking scenario.

The main difference between DoS and DDoS attacks is in scale — DoS attacks use one attack machine (to generate malicious traffic) while DDoS attacks use large numbers of attack machines. The scale difference also invokes differences in operation modes. The large number of attack machines allows DDoS perpetrators a certain recklessness — they frequently trade sophistication for brute force, using simple attack strategies and packet contents to overload victim resources. However, the simplicity in both attack types arises from convenience, not necessity. The lack of effective defense mechanisms, even for simple attacks, offers no motivation for perpetrators to design more sophisticated ones. Once defenses successfully counter one attack class (e.g., like ingress filtering [FS00] has countered random IP source spoofing), attackers quickly deploy slight modifications in their attacks to bypass defensive actions.

There are many attack variations and many dimensions in which attacks can still evolve while preserving the ability to inflict damage on the victim. This feature makes it very challenging to design successful defenses. Due to attack variety, defense systems must maintain a volume of statistical data in order to detect attacks and sieve legitimate from attack traffic. This incurs high operation costs. On the other hand, attackers can easily bypass or trick defenses with slight modifications to their attacks. Any such modifications require added complexity in defense mechanisms (in order to handle the new attack class), thus skyrocketing the cost.

II. Proposed System

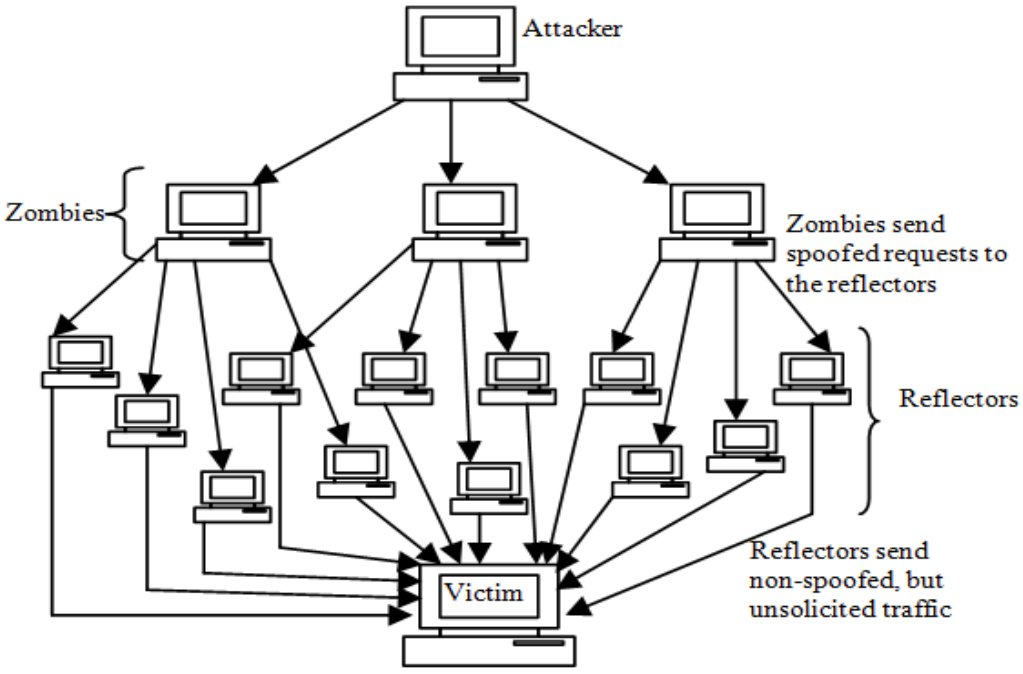
We investigate the basic traffic pattern introduced near the victim under DRDoS, and propose a general detection method: the Rank Correlation based Detection (RCD). RCD is protocol independent and its computation cost is not affected by network throughput. In RCD, once an attack alarm rises, upstream routers will sample and test rank correlation of suspicious flows and use the correlation value for further detection. Correlation has been successfully used in DDoS detection, e.g., correlation coefficient has been successfully employed to discriminate DDoS attacks from flash crowds. As we know, it is the first time that DRDoS is analyzed and detected using correlation.

The preliminary simulations indicate that RCD can differentiate reflection flows from legitimate ones efficiently and effectively, thus can be used as a useable indicator for DRDoS.

III. Algorithm

A. Spearman's Rank Correlation:

The well-known Pearson's correlation coefficient is suitable for describing the linear relationship. 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 μ_x and μ_y, and standard deviations are σ_x and σ_y . The coefficient $r_{x,y}$ is their covariance normalized by the standard deviation:

$r_{x,y} = \text{cov}(X, Y) / \sigma X \sigma Y$

$= E((X - \mu X)(Y - \mu Y)) / \sigma X \sigma Y$

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

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

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. Algorithm

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 ra,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. Ra,b = 1 means that both are reflection flows.

$$R_{a,b} = \begin{cases} 0, & \text{for } \delta 1 \le r_{a,b} \le \delta 2 \\ 1, & \text{for } r_{a,b} < \delta 1 \text{ or } r_{a,b} > \delta 2 \end{cases}$$

It is difficult to determine thresholds once for all, and it should suit various network scenarios and different detection contexts. For given scenarios, a feasible method is to derive thresholds statistically from different attacking cases. The thresholds for our simulations will be given in section V.

Suppose the false negative rate is q, we can decrease q further by using multiple flow pairs, e.g., we have m flow pairs, then q will be decreased towards qm. When q = 0.1 and m = 3, qm = 0.1% which is low enough.

Furthermore, the value of correlation coefficient indicates the percentage of malicious packets in two flows and could help throttling. And the computation cost of RCD is not affected by the network throughput because of only taking packet count into consideration.

IV. Methodology

Input: No. of Nodes

Output: Detection of Malicious Node

Step 1. Locate suspicious flows on an upstream router.

Step 2. Sample the number of packets of suspicious flows per time unit T for a short time, get the value sequence for each flow.

Step 3. Submit sequences to a detection center, which will divide flows into pairs and calculate coefficients for each pair .

Step 4. Compare coefficients for suspicious flows and make decision.

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

V. Result

Here in Fig Source node is sending Data packets to the Receiver node 15 and 30 through the optimized path calculated by using ranks

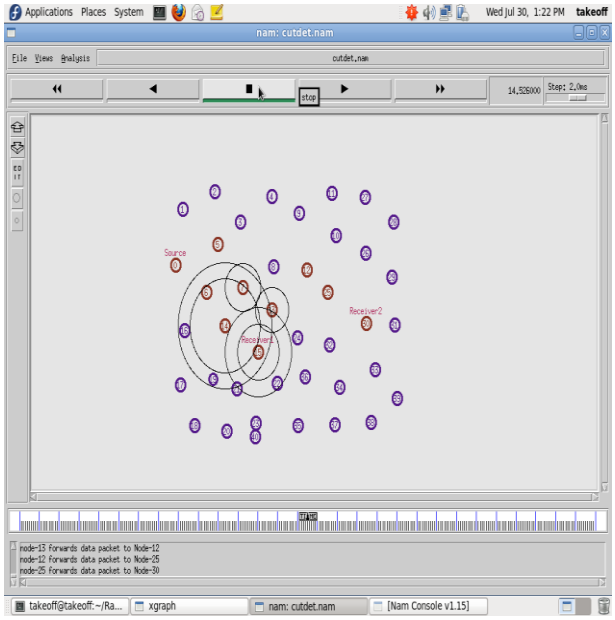
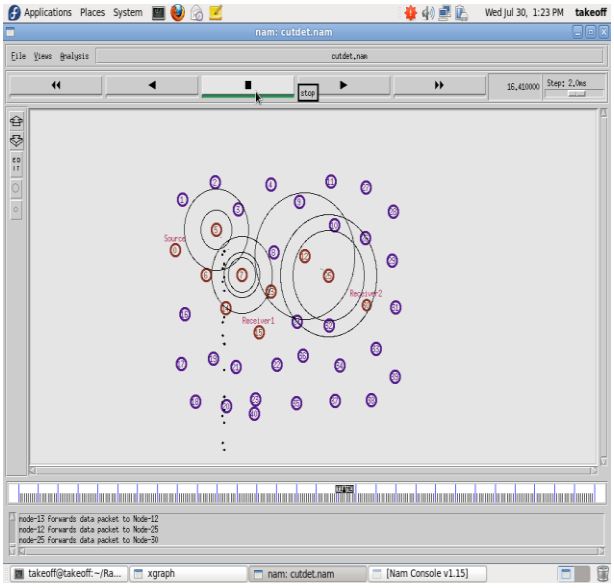


Fig. 3 Source node sending data packets to the receiver node

Here in Fig. 4 node 5 is dropping data packets which happen due to the presence of a malicious node in the network. So, now the nodes will search for that malicious node. Such that the new path can be searched for sending data packets to the receiver



Here in Fig.5 Malicious node is detected by using the algorithm proposed in this paper. In this network node 7 is detected as the malicious node. So, the source node have searched the another path to send data packets to the receiver node 2.

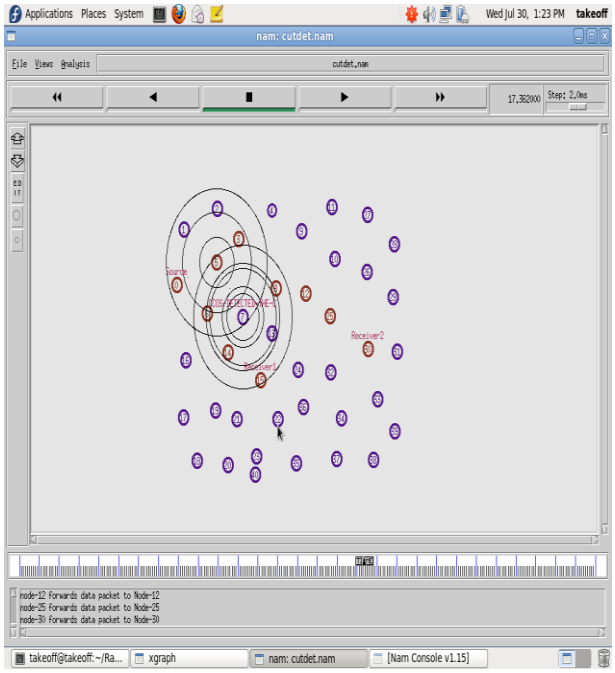


Fig.5 Malicious Node is detected

Here in Fig 6 it shows the Packet Delivery Ratio i.e. The ratio of the no. of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

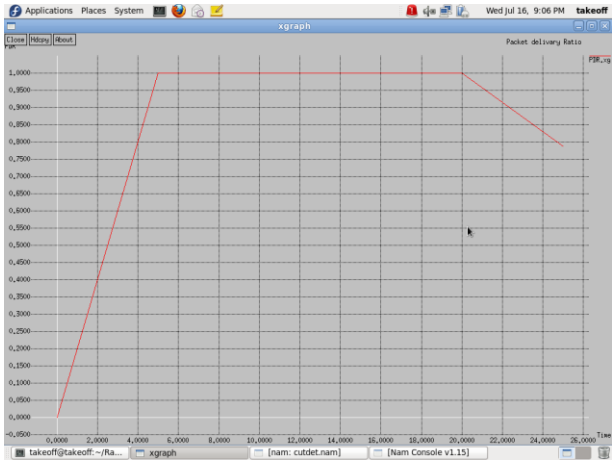


Fig.6 Graph showing packet delivery ratio

Here in Fig. 7, it is a Throughput graph i.e. the total no of packets delivered over the total simulation time.

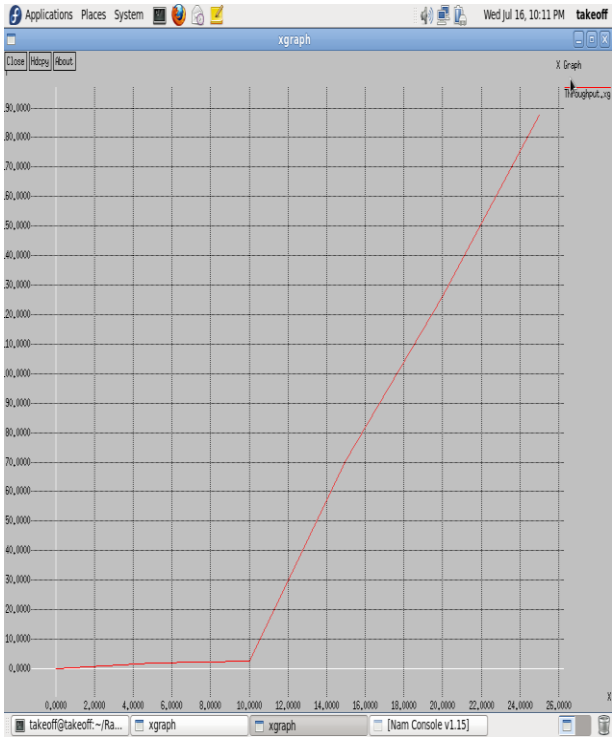


Fig. 7 Graph showing Throughput

VI. Conclusion and Future Scope

This letter concentrates on solving this problem. We investigate the basic traffic pattern introduced near the victim under DRDoS, and propose a general detection method: 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 rises, upstream routers will sample and test rank correlation of suspicious flows and use the correlation value for further detection. Correlation has been successfully used in DDoS detection, e.g., correlation coefficient has been successfully employed to discriminate DDoS attacks from flash crowds. As we know, it is the first time that DRDoS is analyzed and detected using correlation.

There are a lot of interesting works in the future, including:
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 countermeasures.

References

[1] CERT Coordination Center. Trends in Denial of Service Attack Technology, October 2001. http://www.cert.org/archive/pdf/DoStrends.pdf
[2] V. Paxson. "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks." ACM SIGCOMM Computer Communications Review, 31(3), July 2001.
[3] J. Nagle. "Congestion Control in IP/TCP." RFC 896, January 1984
[4] S. Floyd. "Congestion Control Principles." RFC 2914, September 2000.
[5] wei wei, Feng Chen,Yingie xia,and Guang jin on "A Rank correlation based detection in DRdos attacks " in 2013 IEEE communication letters vol 17.

[6] 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.
[7] V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks," ACM Computer Commun. Rev., vol. 31, no. 3, pp. 38–47, 2001.
[8] P. Ferguson and D. Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing." Available: http://www.ietf.orgrfc/rfc2827.txt.
[9] "Stateful Inspection Technology (the industry standard for enterprise class network security solutions)." Available: http://www.checkpoint.Com/products/downloads/StatefulInspection.pdf.
[10] G. V. Rooij, "Real stateful TCP packet filtering in IP filter," in Proc. 2001 USENIX Security Symposium.
[11] T. Hiroshi, O. Kohei, and Y. Atsunori, "Detecting DRDoS attacks by a simple response packet confirmation mechanism," Computer Commun., vol. 31, no. 14, pp. 3299–3306, 2008.
[12] 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.
[13] V. Paxson, "An analysis of using reflectors for distributed denial-ofservice attacks," ACM Computer Commun. Rev., vol. 31, no. 3, pp. 38–47,2001.
[14]P. Ferguson and D. Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing." Available: http://www.ietf.org/rfc/rfc2827.txt.
[15] "Stateful Inspection Technology (the industry standard for enterprise class network security solutions)." Available: http://www.checkpoint. com/products/downloads/StatefulInspection.pdf.
[16]G. V. Rooij, "Real stateful TCP packet filtering in IP filter," in Proc. 2001 USENIX Security Symposium
[17]T. Hiroshi, O. Kohei, and Y. Atsunori, "Detecting DRDoS attacks by a simple response packet confirmation mechanism," Computer Commun., vol. 31, no. 14, pp. 3299–3306, 2008.
[18]T. Vogt, "Application-level reflection attacks." Available: http://www.lemuria.org/security/application-drdos.html.
[19]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.
[20]G. E. P. Box, G. M. Jenkins, and G. C. Reinsel, Time Series Analysis: Forecasting and Control, 3rd edition. Prentice Hall, 1994.
[21]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.

