International Journal of Computer

(IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

Simulation of Rank Correlation Based Detection Mechanism for Distributed Denial of Services Attacks

G. Rama Rao[a], Avinash Konduri[b], Prof. T. Venkat Narayana Rao[c*]

Asst. Professor, Department of C.S.E, Christu Jyothi Institute of Technology and Science

Asst. Professor, Department of C.S.E, Christu Jyothi Institute of Technology and Science

Professor, CSE, Sreenidhi Institute of Science and Technology [SNIST], Hyderabad, TS, INDIA

[c]Email: tvnrbobby@yahoo.com

Abstract

Since the dawn of the Internet, DDoS exhibits a serious threat to the Internet, in which large number of controlled hosts floods the scapegoat or victim site with enormous packets. Furthermore, in Distributed Reflection DoS (DRDoS), invaders bluff or cheat innocent servers into flushing packets to the victim. However, most of current DRDoS detection mechanisms are associated with specific protocols and cannot be used for mysterious or unrecognized protocols. It is learnt that the stimulation by the same attacking flow, the responsive flows from reflectors may have inherent relations: the packet rate of one converged responsive flow may have linear relationships with another. Based on this investigation, the Rank Correlation based Detection (RCD) algorithm is proposed. The primary simulations denote that RCD can differentiate reflection flows from authorized and authenticated ones effectively and efficiently thus, can be utilized as a useable indicator for DRDoS. The paper presents a study of latest botnet attacks and proposes an appropriate guard method for DDoS attacks.

Keywords: Denial of Services; Distributed Reflection DoS (DRDoS); Rank Correlation based Detection; Distributed Denial of Services (DDoS).

----

* Corresponding author.

E-mail address: tvnrbobby@yahoo.com.

1. Introduction

A Botnet is a group that comprise of computers, remotely administered by hackers to commence various attacks on network, such as DDoS attack and information phishing. Botnet has emerged as a famous and dynamic tool behind many cyber attacks. Fluxing techniques usage have been started to avoid detection by the owners of some botnets, such as storm worm, torpig and conflicker recently. Therefore, the understanding of their fluxing tricks is vital to win over as a defense mechanism from botnet attacks. Motivated by this, this paper surveys the latest botnet attacks and defenses. First introduction of the principles of fast fluxing (FF) and domain fluxing (DF) is given and explanation of how these techniques were employed by botnet owners to fly under the radar. Additionally, the state-of-art investigation is done for research on fluxing detection. Comparison and evaluation of fluxing detection techniques is done in terms of multiple criterions. Finally, the future directions on fighting against botnet based attacks are discussed. Attackers can render distributed denial-of-service attacks more difficult to defend against by, bouncing their flooding traffic off of *reflectors*; that is, by spoofing requests from the victim to a large set of Internet servers that will in-turn send their combined responses to the victim. Due to this locality dilution in the flooding stream it complicates the victim's competence both to isolate the attack traffic in order to block it. It further, used to trace back techniques to discover the source of streams of packets with spoofed source addresses, for instance ITRACE, probabilistic packet marking and SPIE. Numbers of possible safeguard methods are discussed against reflector attacks, finding such cases to be most impractical one in some cases, and then evaluate the degree to which different forms of reflector traffic will have characteristic signatures that the victim can use to analyze and figure/ filter out the traffic attack. Upon investigations, it is specified that three kinds of reflectors pose particularly significant threats: DNS and Gnutella servers and TCP-based servers (particularly Web servers) running on TCP implementations that suffer from expected initial sequence numbers. In this paper the authors propose a simple but robust scheme to discover denial of service attacks (including distributed denial of service attacks) by monitoring the increase of new IP addresses [7,6].

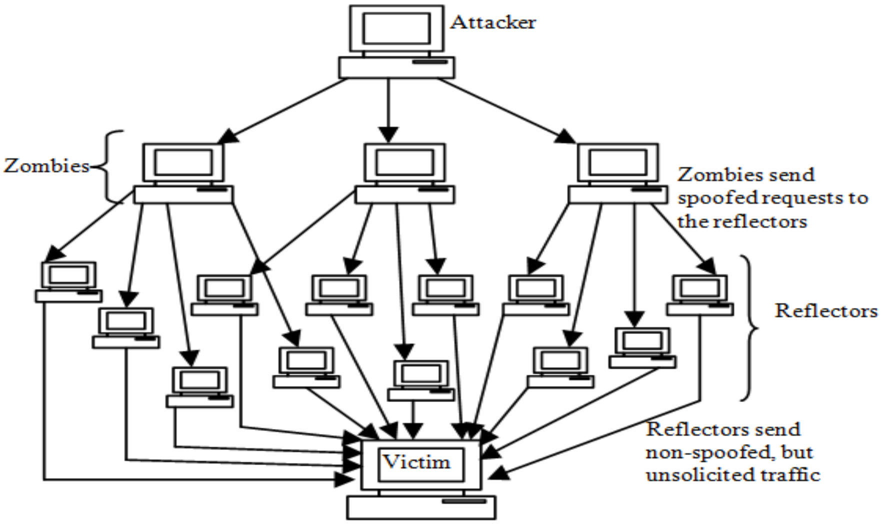

Attacker
Zombies
Zombies send spoofed requests to the reflectors
Reflectors
Victim
Reflectors send non-spoofed, but unsolicited traffic

Fig 1:System Architecture

Unlike earlier proposals for bandwidth attack detection schemes which are based on monitoring the traffic volume, the proposed mechanism is very effective for highly distributed denial of service attacks. The proposed strategy utilizes an inherent feature of DDoS attacks, which makes it difficult for the attacker to counter this detection scheme by changing their attack signature. The proposed mechanism uses a sequential nonparametric change point detection strategy to enhance the detection accuracy without the need for a detailed model of normal and attack traffic. The paper explains the high detection accuracy on a range of different network packet traces can be achieved.

From Fig. 1, the system architecture depics that an attacker with n-number of clients and victim person. If any of the zombies client fail to execute the particular file it would be not able to understand from where the exact data has been transmitted. To verify this, Zombies spoofing requests are mplemented so that the attacker will not be able to access the data easily [5].

2. Implementation

There have been some packet-level defense methods. Filtering of all incoming response packets, which is of low cost, would result in no common access to the remote server. Packet assessment and protocol tracking status may be helpful but requires heavy computation which may be susceptible to attacks. Along with more protocols being exploited to launch DRDoS, counter measures must consider a list of possible protocols with each one treated specifically, and the list needs to be updated time to time. So some protocol independent methods can be expected to help in detecting most types of DRDoS. The basic traffic pattern introduced near the victim under DRDoS is investigated and a general detection method is proposed.

The proposed method is the Rank Correlation based Detection (RCD). RCD is protocol independent and its computation cost is not affected by network throughput. In RCD mechanism, when an attack alarm rises, upstream routers have to sample and test the rank correlation of suspicious flows and use the correlation value for further detection [1].

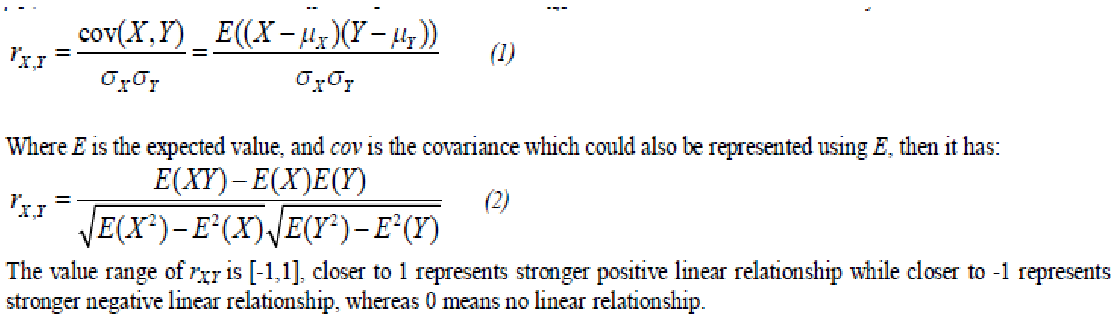
The correlation has been successfully used in DDoS detection, i.e. the correlation coefficient has been successfully implemented to differentiate DDoS attacks from flash crowds. It is the first time that DRDoS is analyzed and detected using correlation strategy. The preliminary simulations indicate that RCD can differentiate reflection flows from acknowledged ones efficiently and effectively, thus can be used as a useable index for DRDoS.

A. Shared Monitoring of Network

The basic idea is to set up a monitor or supervisory body at each node in the network to produce pertinent information about the network state and to share them among all the nodes. A watchdog or monitor can be considered as a case of the ghostly network packet sniffer. It arrests the traffic and displays the meticulous information on it. For each packet that is captured, the watchdog or monitor displays a inclusive view of packet headers, payload and add some general statistics information such as the timestamp, frame number and frame length in the size represented in bytes. Information is stored in the form of list of events. Events are the single transmitted packet or the times in which the channel is inactive, which can be inferred from the timestamp of the packets and the packet transmission times. The grouping of different list of events results in enhanced understanding of the status of the network, particularly in distinguishing the jamming attacks and channel failures, where the packets are sent by one peer and the other peer never receives the packets. When both the channels fails, then the jamming attack build the FCS check of the packet fail, thus the packet which is in transit will be incorrectly received and dropped, that increments the “dropped frames” counter in the device driver at the receiver. The difference among the two cases is the quantity of incorrectly received frames at the receiver. Assume if the receiving station is under jamming network, and the packets which pass through the jamming area get jumbled. The display located at the sender’s side will see the number of frames sent on the channel and the monitor at the receiver end won’t observe the receipt of data properly, and continue to grow erroneous received frames counter.

B. Correlation Coefficient

The responses from the reflectors are found to have intrinsic relations: linear relation, as they are motivated by same attacking flow. The Rank Correlation based Detection algorithm [1] is based on this observation. The Pearson’s correlation coefficient suits linear relationship, based on its sensitivity to outliers caused by traffic burst, the linearity may not be apparent. The Spearman’s rank correlation coefficient (rho) is more appropriate for the detection. Whereas a raw value is converted to a ranked value and then Pearson’s correlation is applied. In Spearman’s correlation coefficient, for two random variables X and Y of ranked values, the predictable values are µX and µY , and standard deviations are σX and σY . The coefficient rX, Y are the covariance normalized by the standard deviation:



$$r_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X\sigma_Y} = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma_X\sigma_Y} \qquad (1)$$

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

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

The value range of r_{XY} 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.

C. Rank Correlation Based Detection Algorithm

This algorithm, assumes that the packets pass through one router to reach the sufferer. The packet flow is sampled per unit time T. As shown in Fig.2 i.e. two suspicious flows *fa* and *fb*, their respective set of source reflectors are *Ra* and *Rb*, where the set of common reflectors are *Ro* when a suspicious flow is alerted. In this algorithm, once alert surface then the routers in the path will sample the flows for sufficient time.

D. Matching Algorithm

The fundamental algorithm to match two lists of events is as follows: Initially start from the first list and for every event (packet or channel idle) try to find a matching event on the second list that is, given a packet we look for it on the second list. As we don’t have cheaters into play for now, what we find is that for every packet on the first list we find it on the second one if the network is working fine, else we would find a channel idle event if some problem persist (i.e. jamming or malfunctioning). Ub continuation to the above example, we would have transmitted packets on the first event list and channel idle, along with a high number of dropped packets on the second one.

We can locate unmatched events on the second list at the end (for example if the first node was jammed), so we shall merge the two lists and perform rank correlation algorithm yet again. Since all nodes take part in the detection process, we would extend it in order to match the multiple lists. The idea is to amalgamate one list at a time with the outcome of the previous merge. In other words, we merge lists 1, 2 and then we match the result with list 3, until we processed every list. In this way we attain an aggregated list of all events which happened in the network in a given time frame. We have to note that a node might not overhear the traffic of each other node base on range. We supposed that each node has appropriate information to tender, but this is not for eternity true. The key characteristic here is that the monitoring system is considered to be distributed.

A single station alone may not tell if it is subjected to an attack or just a momentary network failure, and support among all nodes is required for the nodes to recognize what is going on. The event lists are shared amid all nodes in the network [2].

E. Multicast DRDOS Attack on Neighboring Nodes

When the DRDOS attack is detected, the address of the DRDOS attack path is sent to the whole network by multicasting. The neighbor nodes receive the IP address of the DRDOS attack path and store it in the event lists to foil future attacks from that node in the network. The multicasting of the DRDOS attack address is done by source as shown in figure 2.

F. Sending Data to the Destination

The data sending process is done by splitting the selected text file into packets for transmission. The data send process is invoked after the source discovers a DRDOS attack free path. In the case of jamming/network malfunction, the source waits till the network is reinstated, and starts the training process to find the DRDOS attack and if any detected, then selects a path free from DRDOS attack. The source sends the data directly to the target through the ‘safe’ path. Destination receives the data in the form of packets and checks for abnormalities if any, to detect any loss of data in the data owing DRDOS attack [3].

3. Spearman’s Rank Correlation

The well-known Pearson’s correlation coefficient is suitable to narrate the linear relationship. Due to the background traffic and delay, the linearity may not be apparent. The Pearson’s correlation is responsive to outliers introduced by traffic bursts. Through experimental comparisons, Spearman’s rank correlation coefficient (Spearman’s rho) is more appropriate 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 [8,4].

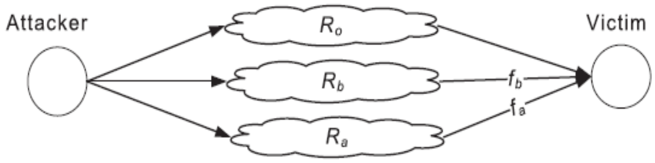


Fig. 1. Attacking scenario.

Fig 2: Attacking Scenario

This would give the information regarding how the data has been used for implemeted using Spearman's Rank Correlation coefficient computations.

r=1-$\left(\frac{6\Sigma d^2}{n(n^2-1)}\right)$

d= difference between the two numbers in each pair of ranks

a=number pairs of data

Interpretation of results (it can vary from -1 to +1)

Close to -1 – Negative Correlation

Close to 0 – No linear Correlation

Close to +1 – Positive Correlation

Example:

Table 1. Results of Implementation

Data 1	Data 2	Rank 1	Rank 2	d	d^2
6	2	2	1	1	1
9	9	1	3	2	4
7	3	3	2	1	1

Rank 1 : Rank data 1 from lowest to highest

Rank 2 : Rank data 2 from lowest to highest

D=difference between rank 1 and rank 2

$$r = 1 - \left(\frac{6\sum d^2}{n(n^2-1)}\right)$$

$$r = 1 - \left(\frac{6X6}{3(3^2-1)}\right)$$

$$r = 1 - \left(\frac{36}{3(9-1)}\right)$$

$$r = 1 - \left(\frac{36}{3X8}\right)$$

$$r = 1 - \frac{36}{24}$$

1-1.5 i.e. = 0.5

4. Conclusion

DRDoS attacks are a growing rampantly and are causing problems in networking systems. Every best mechanism existed so far has its own merits and demerits. The issue is addressed in this paper that proposes a suitable solution that focus on detecting DRDOS independent of specific protocols using the Rank Correlation based Detection algorithm. We have suggested some methods to reduce the disadvantages of DRDoS by identifying the path causing the attack and avoiding the path to send or receive packets for a specified time period. There are many future scope issues works to be addressed which include:

1) Extension of experiment against real DRDoS in the Internet.

2) The efficient algorithms for more complicated network scenario with multiple routers.

3) Evolving tracing methods to find the attacker for avoidance of the attack rather than detection later.

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] Lei Zhang, Shui Yu, Di Wu and Paul Watters “A Survey on Latest Botnet Attack and Defense”, 2011 – International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[3] Vern Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, Computer Communication Review 31(3), July 2001.

[4] “Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring”, Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, In Proceedings of the Third International IFIP-TC6 Networking Conference(2002).

[5] Yonghui Li, Yulong Wang, Fangchun Yang, Sen Su , “Traceback DRDoS Attacks”, Journal of Information & Computational Science 8: 1 (2011) 94–111

[6] 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.

[7] T. Vogt, “Application-level reflection attacks.” Available: http://www.lemuria.org/security/application-drdos.html.

[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.