A Rank Correlation Based Detection against Distributed Reflection DoS Attacks

Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin

***Abstract*—DDoS presents a serious threat to the Internet since its inception, where lots of controlled hosts flood the victim site with massive packets. Moreover, in Distributed Reflection DoS (DRDoS), attackers fool innocent servers (reflectors) into flushing packets to the victim. But most of current DRDoS detection mechanisms are associated with specific protocols and cannot be used for unknown protocols. It is found that because of being stimulated by the same attacking flow, the responsive flows from reflectors have inherent relations: the packet rate of one converged responsive flow may have linear relationships with another. Based on this observation, the Rank Correlation based Detection (RCD) algorithm is proposed. 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.**

***Index Terms*—DDoS detection, reflection DoS, Rank correlation.**

I. Introduction

DISTRIBUTED denial of service (DDoS) attack is a serious threat to the Internet, where lots of controlled hosts flood the victim site with massive packets. As a popular form of controlled hosts, botnets are still improving and ready for launching future DDoS [1]. To render it more difficult to defend, in Distributed Reflection DoS (DRDoS), 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. And the dilution of locality makes it hard to isolate attacking traffic. Local detection near single reflector may be useless because of low volume of reflected traffic [2]. Though ingress filtering is a hopeful solution, it has not been largely deployed [3].

There have been some packet-level defense methods. Filtering all incoming response packets, which is of low cost, will result in no general access to the remote server [2]. Inspecting packet content and tracking protocol status maybe helpful, but need a lot of computation which is also vulnerable to attacks [4, 5, 6]. Along with more protocols being exploited to launch DRDoS [7], countermeasures 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.

Manuscript received October 9, 2012. The associate editor coordinating the review of this letter and approving it for publication was C. Mitchell.

This work was supported in part by the National Natural Science Foundation of China (61203265); the Natural Science Foundation of Zhejiang Province (LY12F02013); the Science and Technology Planning Project of Zhejiang Province (2010C31018); the Doctor Foundation of Henan University of Technology(150126,150121); the China Henan Province Key Project (122102110106); and the Ningbo Natural Science Foundation (2012A610014).

W. Wei and F. Chen are with the College of Information Science and Engineering, Henan University of Technology, Zhengzhou, China (e-mail: weiwei_ise@haut.edu.cn).

Y. Xia is with Hangzhou Normal University, Hangzhou, China.

G. Jin is with the College of Information Science and Engineering, Ningbo University, Ningbo, China.

Digital Object Identifier 10.1109/LCOMM.2012.121912.122257

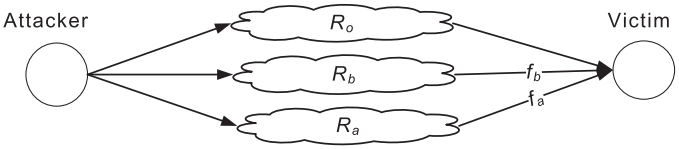

Fig. 1. Attacking scenario.

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 raises, 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 [8]. As we know, it is the first time that DRDoS is analyzed and detected using correlation.

II. System analysis

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 N_a and N_b reflectors, where the set of uninvolved reflectors are R_o, as shown in fig. 1. 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:

$$C_{a,t} \approx C_{a,t-\tau} \tag{1}$$

$$C_{b,t} \approx C_{b,t-\tau} \tag{2}$$

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 N_r, while the total number of arrived request packets are $C_{r,t-\tau}$. As bogus requests from the attacker are distributed uniformly, there are:

$$C_{a,t-\tau} \approx \frac{N_a}{N_r} C_{r,t-\tau} \tag{3}$$

$$C_{b,t-\tau} \approx \frac{N_b}{N_r} C_{r,t-\tau} \tag{4}$$

Then we have:

$$\frac{C_{a,t}}{C_{b,t}} \approx \frac{C_{a,t-\tau}}{C_{b,t-\tau}} \approx \frac{N_a}{N_b} \tag{5}$$

That is, in [*t*, *t*+*T*], for flow f_a and f_b, 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:

$$C_{a,t} + C_{b,t} \approx C_{a,t-\tau} + C_{b,t-\tau} \approx \frac{N_a + N_b}{N_r} C_{r,t-\tau} \tag{6}$$

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 present 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.

III. Algorithm

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.

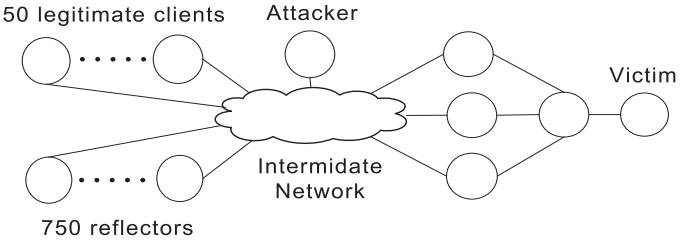

Fig. 2. Simulation topology.

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:

$$r_{X,Y} = \frac{cov(X,Y)}{\sigma_X \sigma_Y} = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma_X \sigma_Y} \tag{7}$$

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

$$r_{X,Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}} \tag{8}$$

The value range of $r_{X,Y}$ 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 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.

$$R_{a,b} = \begin{cases} 0, & \text{for } \delta_1 \le r_{a,b} \le \delta_2 \\ 1, & \text{for } r_{a,b} < \delta_1 \text{ or } r_{a,b} > \delta_2 \end{cases} \tag{9}$$

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 IV.

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 q_m. When *q* = 0.1 and *m* = 3, q_m = 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. The step of RCD is shown in Table I.

TABLE I
THE STEP OF RCD

1. Locate suspicious flows on an upstream router.
2. Sample the number of packets of suspicious flows per time unit T for a short time, get the value sequence for each flow.
3. Submit sequences to a detection center, which will divide flows into pairs and calculate coefficients for each pair according to (8).
4. Compare coefficients for suspicious flows and make decision by (9).
5. If confirmed, then discard these flows on the routers.

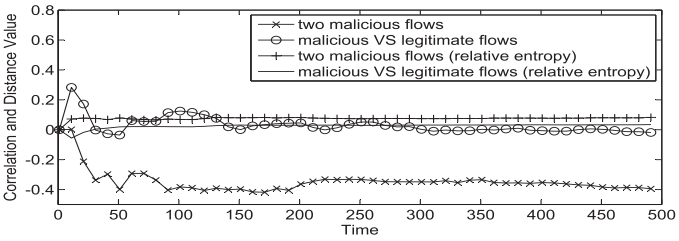

Fig. 3. Comparison of methods in scenario a.

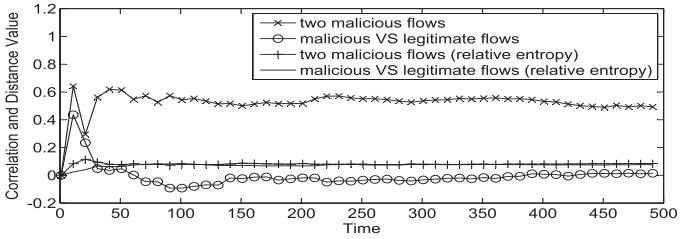

Fig. 4. Comparison of methods in scenario b.

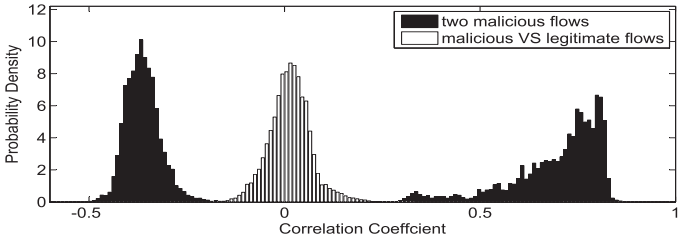

Fig. 5. Statistical comparison of RCD for both scenarios.

IV. SIMULATION

To test the effectiveness of RCD, we have conducted a number of simulations. As shown in fig. 2, we implemented a typical network including 15 routers and 800 network nodes, in the NS2 simulation system. In the network, 750 network nodes are reflectors and 50 are legitimate clients. Nodes' network latency to the victim is randomly between 10ms and 200ms, which simulates an average Internet RTT of 200ms. Legitimate requests to the victim follow a Pareto distribution.

We test two different scenarios described in section II. Fig. 3 and fig. 4 elucidate the result, in comparison with the relative entropy method in [10] which uses relative entropy between flow pairs to detect attacking flow mimicking legitimate traffic. From fig. 3 and fig. 4, it is found:

1) Even with a reasonable bulk of background traffic, there is strong correlation between two malicious flows, which is very weak between one malicious and one legitimate flows.

2) The two flow pairs can't be perfectly differentiated by relative entropy.

3) Rank correlation coefficient becomes stable after about 100 time units. When the time unit is 0.1 second, then only 10 seconds are needed to give the final alarm.

To get the thresholds, we test 200 different attacking cases. The ratio of packet rate of attacking to legitimate flows ranges from 1.0 to 10.0, to cover a broad range of low and high rate cases. Fig. 5 is the probability density of correlation coefficient in RCD, it's found that:

1) The two kinds of correlations could be clearly distinguished with a broad range of attacking packet rate.

2) To achieve low false negative and false positive, we choose the intersection point of fitted curves as thresholds. In fig. 5, the thresholds are δ_1 = -0.15 and δ_2 = 0.3 with relatively low false negative and false positive: 0.18% and 0.10%.

V. CONCLUSION

The letter concentrates on detecting DRDoS independent of specific protocols, and proposed the Rank Correlation based Detection (RCD) algorithm. Once suspicious flows found, RCD starts to calculate the rank correlation between flow pairs and give final alert according to preset thresholds. The preliminary simulations demonstrate that it could be a helpful indicator for DRDoS detection. The result could also be used to pick out and discard malicious flows. 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] 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.

[2] 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.

[3] 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.

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

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

[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.

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

[10] 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.