A Rank Correlation Based Detection against Distributed Reflection DoS Attacks

Preeti Goyal¹, Sangeeta Phogat² and Deepak Goyal³

¹M. Tech. (CSE), Vaish College of Engg., Rohtak, Haryana (India)  
preeti.15.92@gmail.com

²Assistant Professor, Vaish College of Engg., Rohtak, Haryana (India)  
sangeeta.phogat@gmail.com

³Associate Professor, Vaish College of Engg., Rohtak Haryana (India)  
deepakgoyal.vce@gmail.com

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 usable indicator for DRDoS.

Keywords: DDoS detection, reflection DoS, Rank correlation.

I. Introduction
Now a day’s 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. 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.

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 calculation with lot of time needed for this method but this method not suitable for vulnerable attacks.

The above method cannot be implemented now a days due to nodes need to be more security these cannot provide very high level security for data. For more security communication we need to have the linear relationship between source and destination. 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 valve and the response from the destination signal i.e. (Acknowledge signal) has the rank valve 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

II. Attacks on Protocols
DDOS: Distributed Denial-Of-Service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend
services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (See botnet) DoS (Denial of Service) attacks are sent by one person or system. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Zombie: Zombies have been used extensively to send e-mail spam; as of 2005, an estimated 50–80% of all spam worldwide was sent by zombie computers. This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth. This spam also greatly furthers the spread of Trojan horses, as Trojans are not self-replicating. They rely on the movement of e-mails or spam to grow, whereas worms can spread by other means. For similar reasons zombies are also used to commit click fraud against sites displaying pay per click advertising. Others can host phishing or money mule recruiting websites. Zombies can be used to conduct distributed denial-of-service attacks, a term which refers to the orchestrated flooding of target websites by large numbers of computers at once. The large number of Internet users making simultaneous requests of a website's server are intended to result in crashing and the prevention of legitimate users from accessing the site. Distributed degradation-of-service is the moderated and periodical flooding of websites, done with the intent of slowing down rather than crashing a victim site.

DRDOS: Distributed Reflector Denial of Service is like Denial of service attacks in which it has servers and multipoint communication between source and destination. And also has more number of communication also be present. This attack is more severe than the other kinds of attacks as it could be able to damage the data and fool the servers. The way for the prevention of the kind of attacks can be made the lot of victim node to be floods.

III. 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.

IV. 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 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 satisfy the assumption due to legitimate traffic in background, the correlation between two malicious flows should be remarkably strong compared with other pairs.

B. Steps 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 .
4. Compare coefficients for suspicious flows and make decision by .
5. If confirmed, then discard these flows on the routers.
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


