**A Rank Correlation Based Detection against Distributed Reflection DoS Attacks**

**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.

**EXISTING SYSTEM:**

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. Inspecting packet content and tracking protocol status maybe helpful, but need a lot of computation which is also vulnerable to attacks. Along with more protocols being exploited to launch DRDoS, 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.

**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.

**ADVANTAGES OF PROPOSED SYSTEM:**

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.

**ALGORITHM USED:**

**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.



# SYSTEM CONFIGURATION:-

# HARDWARE REQUIREMENTS:-

# Processor - Pentium –IV

* Speed - 1.1 Ghz
* RAM - 512 MB(min)
* Hard Disk - 40 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - LCD/LED

# SOFTWARE REQUIREMENTS:-

* Operating System : LINUX
* Tool : Network Simulator-2
* Front End : OTCL (Object Oriented Tool Command Language)

**REFERENCE:**

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