MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

DDOS WALL: AN INTERNET SERVICE PROVIDER PROTECTOR

Maharudra V. Phalke, Atul D. Khude,Ganesh T. Bodkhe, Sudam A. Chole
Information Technology, PVPIT Bhavdhan
Pune,India
maharudra90@gmail.com, atul.khude12@gmail.com,
gs.ganeshbodkhe@gmail.com, sudamchole@gmail.com

Abstract: *Distributed denial-of-service (DDoS) attacks remaina major security problem, the mitigation of which is very hard especiallywhen it comes to highly distributed botnet-based attacks.The early discovery of these attacks, although challenging, is necessaryto protect end-users as well as the expensive network infrastructure resources. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of DDOS Wall. The core of DDOS Wall is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of DDOS Wall using extensive simulations and a real dataset is presented, showing DDOS Wall effectiveness and low overhead, as well as its support for incremental deployment in real networks.*

Keywords: *Collaboration, detection, distributed denial- of-service (DDos), flooding, network security.*

1. INTRODUCTION

Distributed denial-of-service (DDoS) attacks still constitute a major concern even though many works have tried to address this issue in the past. As they evolved from relatively humble megabit beginnings in 2000, the largest DDoS attacks have now grown a hundredfold to break the 100 Gb/s, for which the majority of ISPs today lack an appropriate infrastructure to mitigate them. Most recent works aim at countering DDoS attacks by fighting the underlying [1] vector, which is usually the use of botnets. A botnet is a large network of compromised machines (bots) controlled by one entity (the master). The master can launch synchronized attacks, such as DDoS, by sending orders to the bots via a Command & Control channel. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself, which raises important ethical issues, or to first detect botnet-related malicious activities (attacks, infections, etc.), which may delay the mitigation. To avoid these issues, we focuses on the detection of DDoS attacks and per se not their underlying vectors. Although no distributed denial-of-service attacks usually exploit a vulnerability by sending few carefully forged packets to disrupt a

service, DDoS attacks are mainly used for flooding a particular victim with massive traffic.. In fact, the popularity of these attacks is due to their high effectiveness against any kind of service since there is no need to identify and exploit any particular service-specific flaw in the victim. Hence, we focuses exclusively on flooding DDoS attacks .A single IPS or IDS can hardly detect such DDoS attacks, unless they are located very close to the victim. However, even in that latter case ,the IDS/IPS may crash because it needs to deal with an overwhelming volume of packets (some flooding attacks reach 10–100 Gb/s). In addition, allowing such huge traffic to transit through the Internet and only detect/block it at the host IDS/IPS may severely strain Internet resources. We implement DDos Wall, a new collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level.

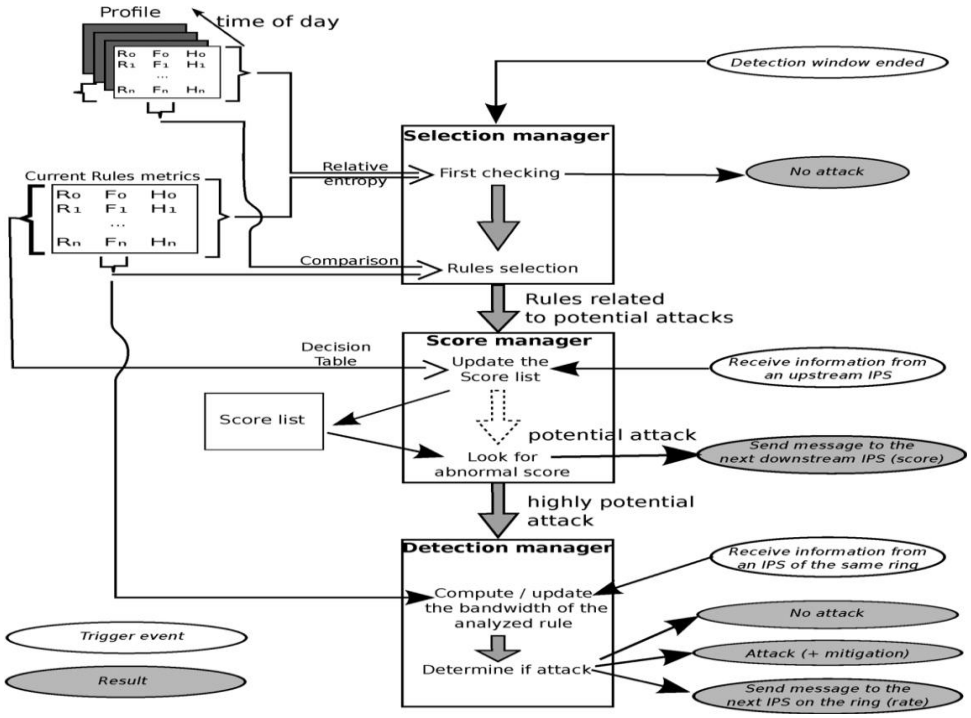


Fig.1: System Architecture [1]

DDos Wall relies on a distributed architecture composed of multiple IPSs forming overlay networks of protection rings around subscribed customers. DDos Wall is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging belief scores on potential attacks. The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high. In this way, the threat is measured based on the overall traffic bandwidth directed to the customer compared to the maximum bandwidth it supports. In addition to detecting flooding DDoS attacks, DDos Wall also helps in detecting other flooding scenarios, such as flash crowds, and for botnet-based DDoS attacks.

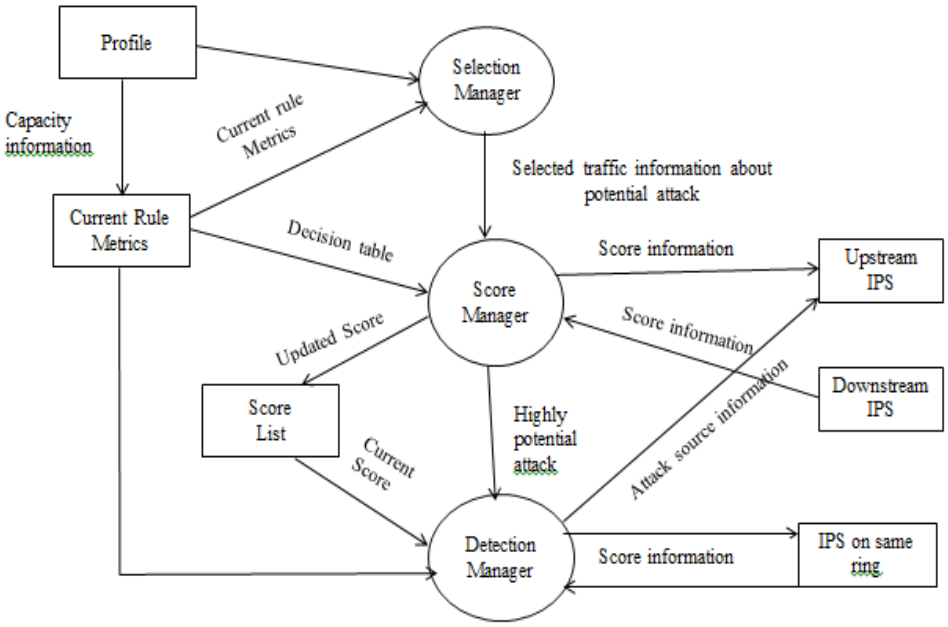


Fig.2: Data Flow for DDoS Wall

2. PROPOSED WORK

2.1 Formalization of the Problem

'DDoS Wall :A System for the detection and mitigation of flooding DDoS attacks' is a system for the early detection of flooding DDoS attacks. There is not such system exist which can detect source of flooding DDoS attack and block that source, hence we aim to develop such system which detect and mitigate DDoS attack.

2.2 Methodologies

2.2.1 Determining Potential of Attacks:

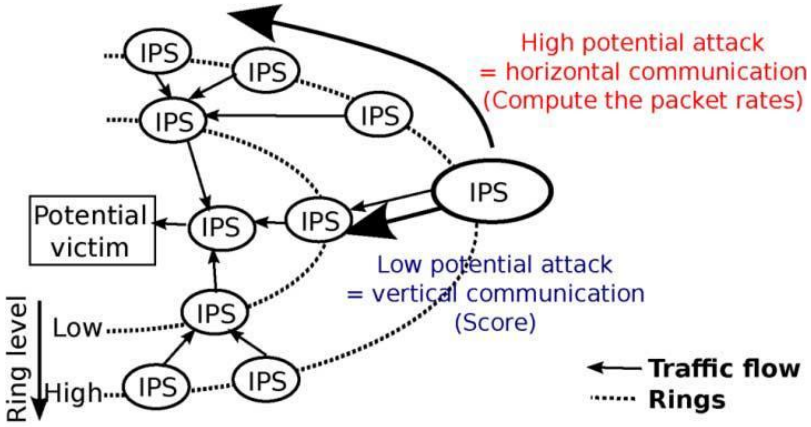


Fig.3: Horizontal and vertical communication in DDos Wall.

A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer (Fig.3). Using a threshold, a quite low score is marked as a *low potential attack* and is communicated to the downstream IPS that will use to compute its own score. A quite

high score on the other hand is marked as *high potential attack* and triggers ring-level (horizontal) communication (Fig.3) in order to confirm or dismiss the attack based on the computation of the *actual packet rate* crossing the ring surpasses the known, or evaluated, customer capacity.

2.2.2 Subscription Protocol:

The DDos Wall corresponds to an IP sub network or a single IP address. *DDos Wall* is an added value service to which customers subscribe using the protocol depicted in Fig.4. The protocol uses a trusted server of the ISP that issues tokens.

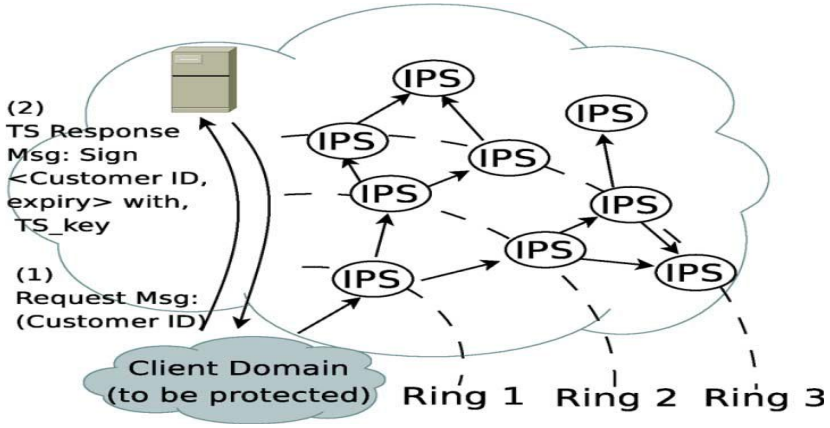


Fig.4: DDos Wall subscription protocol.

2.2.3 Multiple Customers:

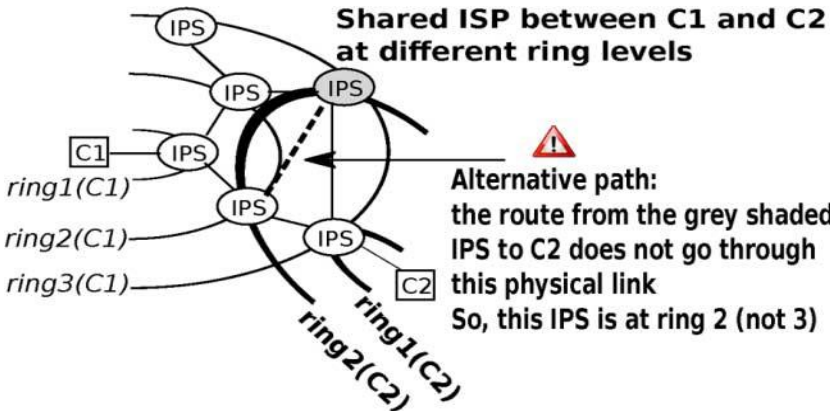


Fig.5: DDos Wall with two customers: C1 and C2.

IPS may act at different levels with respect the customers it protects as depicted in Fig.3.3. Although most of the figures in this paper represent overlay networks with a single route, from an ISP to a customer, this figure highlights that alternative paths are possible.

2.3. **System Module**

2.3.1 Server Information Module:

This module used to gather server IP address and port number.
Using this address and port number, the following modules perform based on this module.

2.3.2 DOS Attacker Module:

This module depicts how to detect the denial of service problem during data transmission. For example we check our examination results through our college website, there are so many students check their results at a time, for that time the server become slow, and busy. The same student checks their results again and again, that time that student will consider as anonymous user and the page will denial. Here we implement two types of scanning.
We can scan offline by using IP address and port number which is already store in server module. Then we browse and select the file name. Then the client sends that file name. if the client sends that file again and again then that IP consider as anonymous IP.

2.3.3 Detection Module: (Trigger Ring)

This module shows the IPSs rule simulator. In IPSs rule simulator it will create virtual protection ring. Consider the number of clients connect to one ring with separate IP address and specific ring range. The clients can easily access data form one to another with in that ring. The traffic problem will reduce, and processing time is increased. If suppose one client in another ring wants to share data to that ring , the process will denial and the another ring of client is considered as anonymous user. So the IPSs rule will protect the DOS problem.

2.4 ALGORITHMS

2.4.1 Check rule Algorithm:

For each selected rate, the collaboration manager computes the corresponding packet rate using rule frequencies and the overall bandwidth consumed during the last detection window. If the rate is higher than the rule capacity, an alert is raised. Otherwise, the computed rate is sent to the next IPS on the ring. When an IPS receives a request to calculate the aggregate packet rate for a given rule, it first checks if it was the initiator. In this case, it deduces that the request has already made the round of the ring, and hence there is no potential attack. Otherwise, it calculates the new rate by adding in its own rate and checking if the maximum capacity is reached, in which case an alert is raised. Otherwise, the investigation is delegated to the next horizontal IPS on the ring.

2.4.2 Mitigation Algorithm:

When an attack is detected, IPSs rule rings form protection shields around the victim. In order to block the attack as close as possible to its source(s), the IPS that detects the attack informs its upper-ring IPSs (upstream IPSs), which in turn apply the vertical communication process and enforce the protection at their ring level (mitigation algorithm). To extend the mitigation, the IPS that detects the attack informs also its peer IPSs on the same ring to block traffic related to the corresponding rule. This is done by forwarding the information in the same manner as done by the collaboration manager in check rule algorithm. Only traffic from suspected sources (i.e., triggered some rule) is blocked. This process entails the potential blocking of benign addresses. However, this is a temporary cost that is difficult to avoid if a flooding attack is to be stopped.

4. RESULTS AND ANALYSIS

4.1. Port Number Selection

In this form we select port number for communication. This port number is use for pairing between client and server.

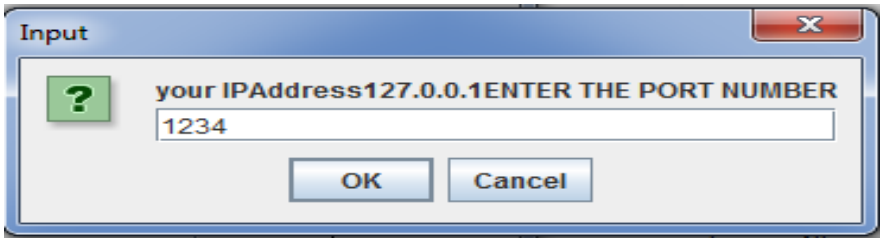


Fig.6: Port no selection

4.2. Attacker window

This is the attacker side GUI.Attacker may try to attack using bulk file or sending single file multiple times.

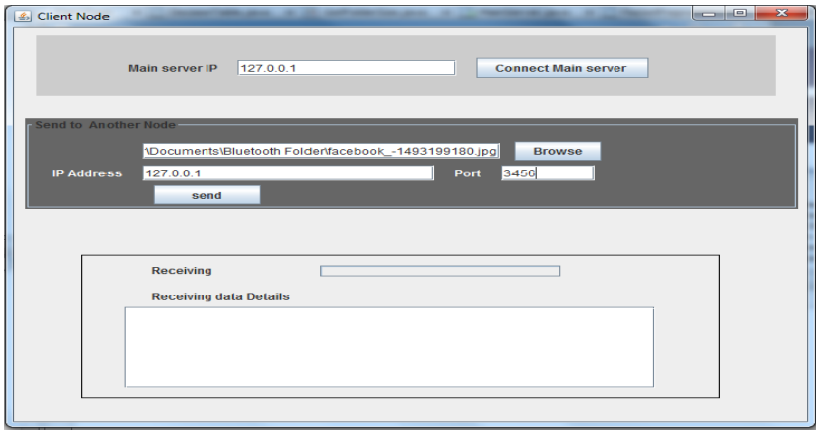


Fig.7: Attacker Window which attacks by sending repeated data

4.3. Client to be protected

This window represents the Client machine which has to be protected from attack.

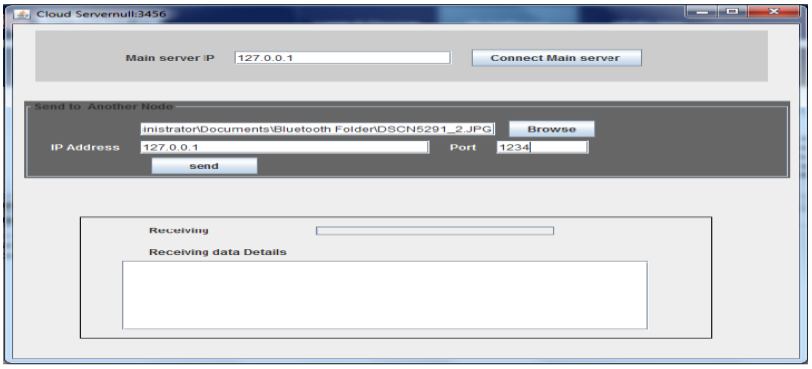


Fig.8: Client side window

4.4. Monitoring server

This is the monitoring server which works as a middleman between client and server.

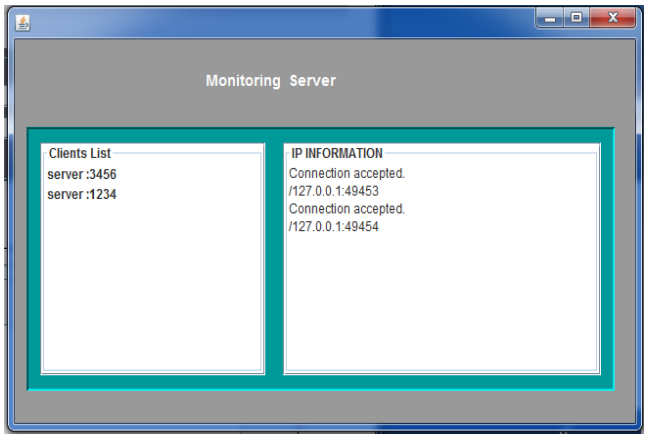


Fig.9: Monitoring server window which display monitoring information

4.5. DDos Wall Administrator

This window represents administrator's machine who can set or establish virtual rings.

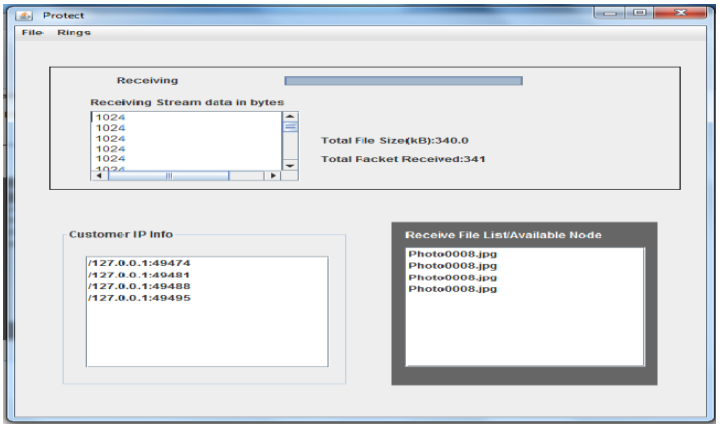


Fig.10: DDos Wall administrator

4.6. Attack Detection and mitigation

This window shows the message to attacker that his attempt is misbehavior and monitoring server drop those packets.

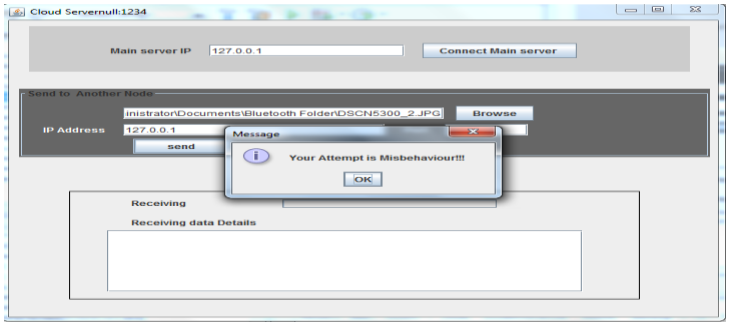
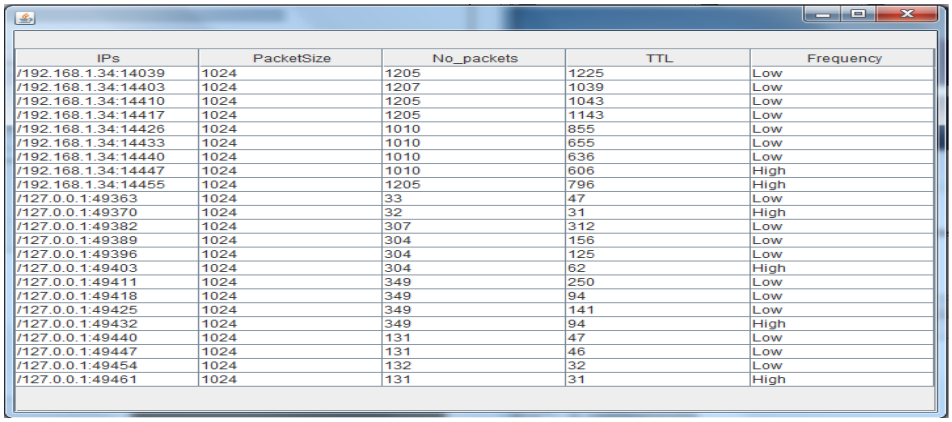


Fig.11: Attack detection and mitigation window

4.7. Packet Processor

Packet processor processes incoming packets. This table shows summery data about incoming packets retrieved by packet processor.



IPs	PacketSize	No_packets	TTL	Frequency
/192.168.1.34:14039	1024	1205	1225	Low
/192.168.1.34:14403	1024	1207	1039	Low
/192.168.1.34:14410	1024	1205	1043	Low
/192.168.1.34:14417	1024	1205	1143	Low
/192.168.1.34:14426	1024	1010	855	Low
/192.168.1.34:14433	1024	1010	655	Low
/192.168.1.34:14440	1024	1010	636	Low
/192.168.1.34:14447	1024	1010	606	High
/192.168.1.34:14455	1024	1205	796	High
/127.0.0.1:49363	1024	33	47	Low
/127.0.0.1:49370	1024	32	31	High
/127.0.0.1:49382	1024	307	312	Low
/127.0.0.1:49389	1024	304	156	Low
/127.0.0.1:49396	1024	304	125	Low
/127.0.0.1:49403	1024	304	62	High
/127.0.0.1:49411	1024	349	250	Low
/127.0.0.1:49418	1024	349	94	Low
/127.0.0.1:49425	1024	349	141	Low
/127.0.0.1:49432	1024	349	94	High
/127.0.0.1:49440	1024	131	47	Low
/127.0.0.1:49447	1024	131	46	Low
/127.0.0.1:49454	1024	132	32	Low
/127.0.0.1:49461	1024	131	31	High

Fig.12: Packet Processor window

4.8. Selection Manager

This is Selection Manager Window keeps the track of entropy, frequency and attacks conclusion for further purpose.

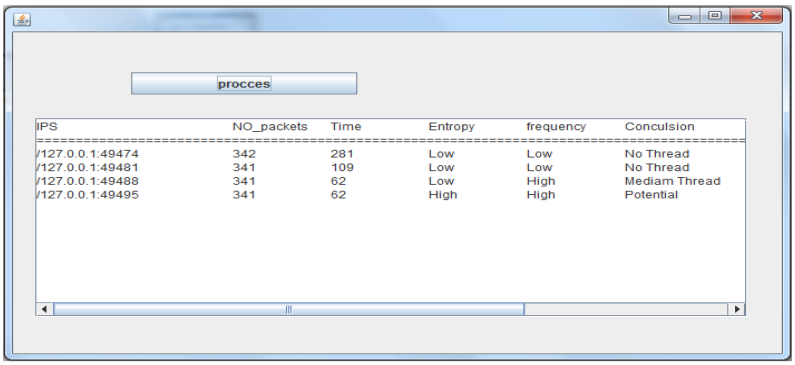


Fig.13: Selection Manager Window

4.9. Score manager

This is Score Manager Window keeps count of score for further use.

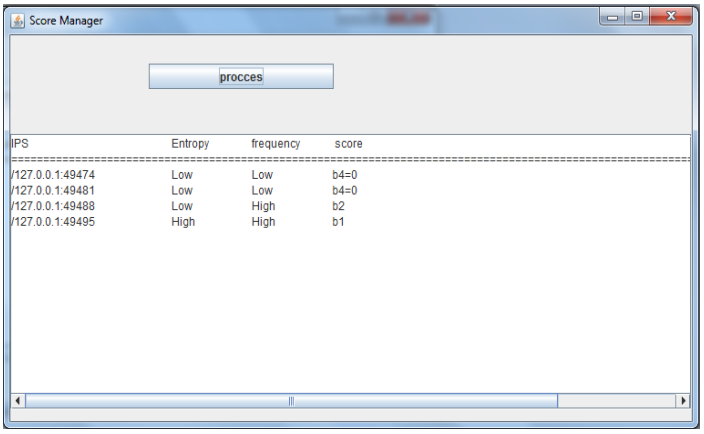


Fig.14: Score Manager Window

4.10. Decision Table

This is decision table which keeps count of entropy and frequency. Depending Upon this entropy and frequency conclusion about threat level is taken and further action is taken.

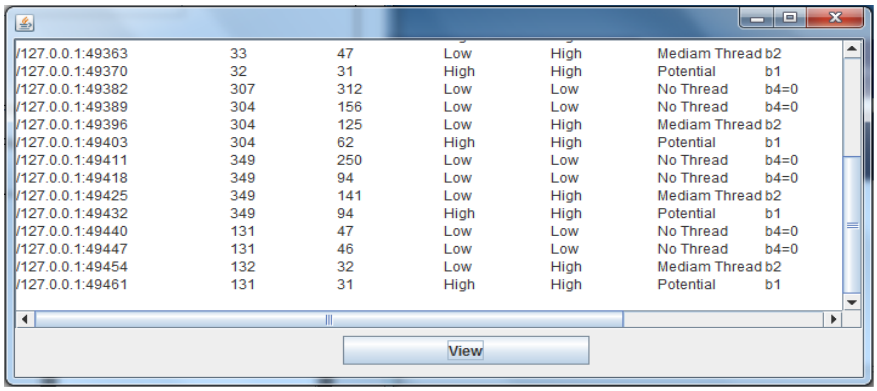


Fig.15: Decision table representations

4.11. Database Client Status Table

This is client status table which keeps records like client ID, send IP, send port, file name, receive IP, count of files etc.

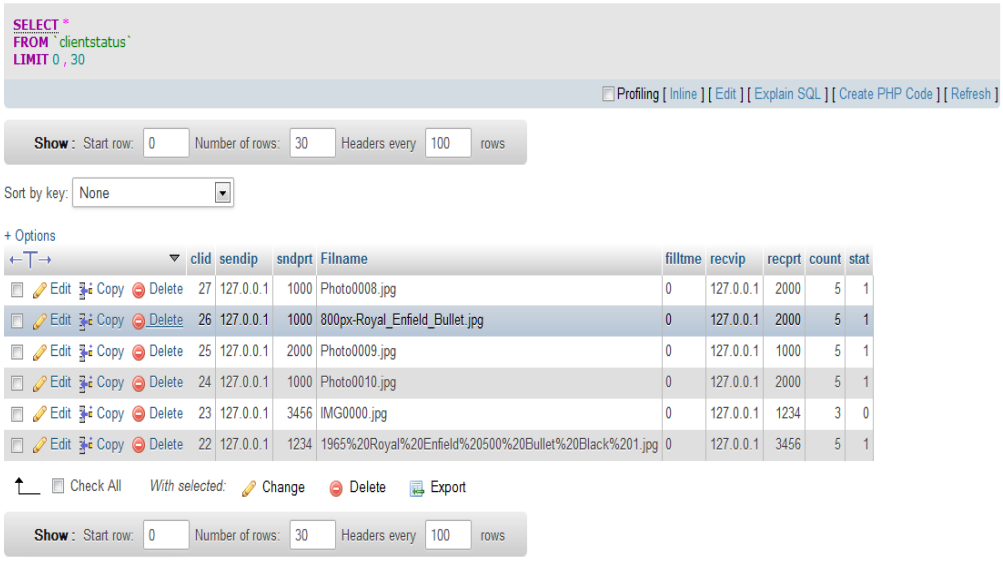


Fig.16: Client Status Table

5. CONCLUSION

This project proposed DDos Wall, a scalable solution for the early detection of flooding DDoS attacks. Belief scores are shared within a ring-based overlay network of IPSs. It is performed as close to attack sources as possible, providing a protection to subscribed customers and saving valuable network resources. Experiments showed good performance and robustness of DDos Wall and highlighted good practices for its configuration. Also, the

analysis of DDos Wall demonstrated its light computational as well as communication overhead. Being offered as an added value service to customers, the accounting for DDos Wall is therefore facilitated, which represents a good incentive for its deployment by ISPs.

6. FUTURE SCOPE

IPSs rule is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging belief scores on potential attacks. The IPSs form virtual protection rings around the host they protect. Being offered as an added value service to customers, the accounting for IPSs rule is therefore facilitated, which represents a good incentive for its deployment by ISPs. As a future work, we plan to extend IPSs rule to support different IPS rule structures.

REFERENCES

[1]. H. Wang, D. Zhang, and K. Shin -"Change-point monitoring for the detectio of DDoS attcks," IEEE Trans. Depend. Secure Compute, vol. 1, no. 4, pp. 193–208, Oct.–Dec. 2004.

[2]. T. M. Gil and M. Poletto -"Multops: A data-structure for bandwidth attack detection," in Proc. 10th USENIX Security Symp., 2001, pp. 23–38.

[3]. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker "Controlling high bandwidth aggregates in the network,"Comput. Commun. Rev., vol. 32, no. 3, pp. 62–73, 2002.

[4]. T. Peng, C. Leckie, and K. Ramamohanarao -"Detecting distributed denial of service attacks by sharing distributed beliefs," in Proc. 8Th ACISP, Wollongong, Australia, Jul. 2003, pp. 214–225.:

[5]. G. Badishi, A. Herzberg, and I. Keidar, "Keeping denial-of-service attackers in the dark," IEEE Trans. Depend. Secure Comput., vol. 4, no.3, pp. 191–204, Jul.– Sep. 2007.