ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Virtual Protection Ring to Detect the Flooding DDOS Attacks

Pradnya S. Date[1], Monika D. Bachhav[2], Tejashree A. Deshpande[3], Vaishali A. Malode[4]

B.E. Students, Dept. of Computer Engineering, PVG COE, Nashik, Maharashtra, India[1, 2, 3, 4]

Abstract: There are many types of attacks from that distributed denial of service (DDoS) is major security problem because this attack try to make system, machine or network resource unavailable to user. The flood of incoming messages to target system that attempt to make machine shut down and this way services get unavailable. This paper provides solution to problem of DDoS in the network. This service provides virtual rings of set of intrusion prevention system (IPS) around the user's system. For implementation of this service requires real datasets of DDoS attack that can be create or it is easily available. Also require two main algorithm that is detection and mitigation algorithm.

KEYWORDS: Distributed denial of service (DDoS), intrusion prevention system (IPS), network security.

I.INTRODUCTION

This Target of a DDoS attack may vary, it generally consists of efforts to solve the problem of interrupt or suspend services of a user connected to the Internet. DDoS attack performs by two or more persons or bots. The DDoS attacker mainly tries to target different sites or server like bank server, any organization server [1] [2]. DDoS attack becomes more serious problem to internet because it causes financial loss [3]. That's why this system is use to mitigate DDoS flooding based attacks. This system work as antivirus which scan the files, removable tools also it generates the pop-up window if attack get detected. This system, provide virtual ring of multiple IPS around the user or victim. If there is use of single IPS to protect system then that IPS may get crash because of whole burden on that single IPS [4] [8]. So to avoid this kind of problem this system provides the virtual ring of multiple IPS around user.

II.RELETED WORK

Here the necessary thing for designing this system datasets. We have to maintain datasets (profile) i.e. it should update time to time. Also we have to study about different parameter of the header of the file. Headers of file send by another system are compare with already stored datasets if both are match then block those packets far from user. If not then send that file to the user. Headers are either TCP or UDP. We have to study each parameter of these headers.

III.ARCHITECTURE

Fig.1 [5] consists of architecture of Virtual Protection Ring. It consists of three managers that are selection manager, score manager, detection manager. For developing this system needs, profile that is dataset of different DDoS flooding attacks [6]. Datasets are same as antivirus library. In that every incoming file matches with antivirus library. If match get found then there is virus detected by antivirus. Basically antivirus library consist of file extensions of affected viruses. Similar like this datasets (rule) consist of symptom of DDoS flooding attacks. There is also current rule metrics which is incoming file to the victim. Here selection manager matches dataset with current rule metrics. If match get found then there will be attack and that rule forward to the score manager. Otherwise there is no attack. Score manager is for to checking the potentiality of attack. It assigns score based on calculating frequency and entropy. Here threshold value is use, if it is low score then there is low potential attack and in Fig. 2 communication done vertically means upstream IPS communicate vertically to the downstream IPS. And high score is mark as high potential attack then it sends to its next IPS means horizontal communication takes place between IPS. That high potential attack can confirm or dismiss that is based on user capacity. High potential attack sends to detection manager determine attack and mitigate attack using algorithms. If there is no attack then simply that file sends to user.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

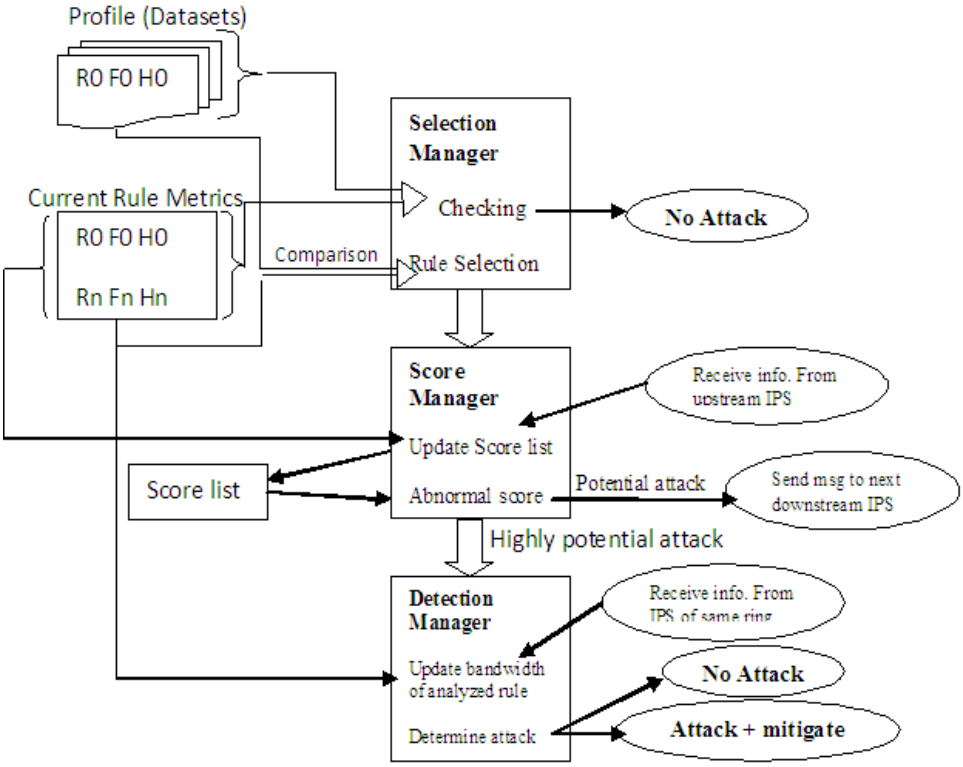

Fig 1. Architecture of Virtual Protection Ring

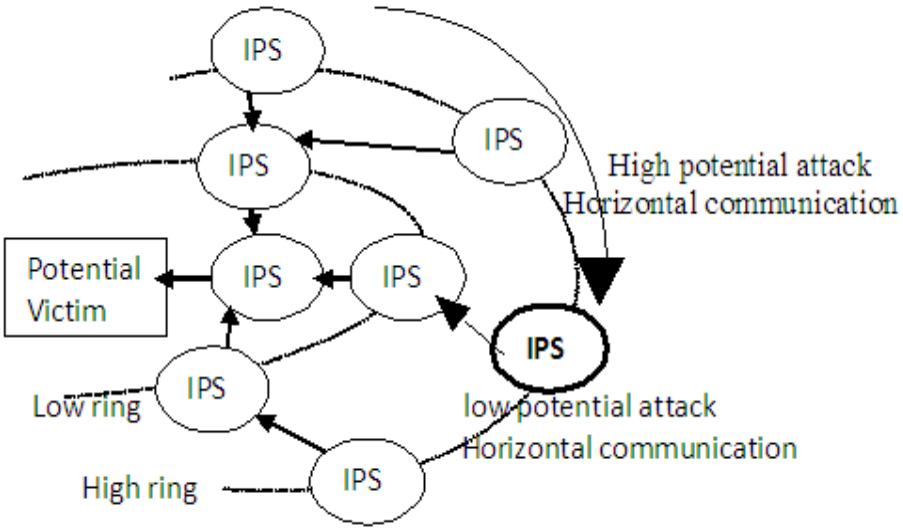

Fig 2. Horizontal & Vertical Communication between IPS

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

For calculating the frequency and entropy, consider following things that are as follows

Here metrics consist of set of rule i.e. R= {r_i | i Є [0, n]}.

1] ***Frequency*:** proportion of packets

$$f_i = \frac{F_{JJJJJJJ\,i}}{\sum_{j=0}^{n} Fj}$$

Where Fi is number of packet matched by rules.

2]***Entropy*:** it is used to measures the uniformity of distribution of frequency, If frequencies are equal then entropy is maximum.and if is not equal then it is low entropy [5].The Firecol system is composed of five components: Packet Processor, Metrics Manager, Selection Manager, Score Manager, and Collaboration Manager.

- **Packet Processor:** The packet processor watch the traffic and updates metrics i.e. (frequencies) whenever a rule is matched.
- **Metrics Manager:** The metrics manager calculates entropies and relative entropies.
- **Selection Manager:** Here we check the k (f, f')<=ω
  Where f is the current frequency of packet, f' is stored frequency of packet ω is maximum admitted deviation.
  k (f, f') is relative entropy .
  k (f, f')<= ω there is no attack in file but if
  k (f, f')>ω then this is abnormal situation and have to mitigate that attack in file.
- **Score manager:** The main aim of the score manager to assign score based on frequency and entropy , there are four conditions to assign score these are as follows :

1) **High entropy High rule frequency:** If entropy and frequency is high then it is consider as high potential attack.

2) **Low entropy High rule frequency:** If there is low entropy and high frequency then that attack consider as medium threat attack.

3) **High entropy Low rule frequency:** If there is high entropy and low frequency then this is consider as a potential attack.

4) **Low entropy Low rule frequency:** If there is low entropy and frequency then there is no attack [7].

- ***Collaboration manager*:** It is used to conforming potentiality of the attack according to user's capacity.

IV.ALGORITHMS

Algorithm 1: checkRule (IPS_id,i,rate$_i$,cap$_i$)

```
1: if b_i^ (IPS_id=! null)then
2:     if IPS_id==myID then
3:         b_i=false;
4:         return
5:     else
6:         rate_i ←rate_i +F_i
7:         if rate_i>cap_i then
8:             b_i=false;
9:             raise DDOS alert;
10:            return
11:        else
12:            nextIPS.checkRule (IPS_id, i, rate, cap_i)
13:        end if
14:    end if
```

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

15: else
16: b_i=true;
17: nextIPS.checkRule (myID, i,0,cap_i)
18: end if

For the given rule r_i collaboration manager calculates the packet rate for this purpose it uses rule frequencies and bandwidth use during last detection window. If the packet rate is higher than the capacity cap_i then alert message is generated [9]. When any IPS within the ring receives request then it calculate the packet rate foe that rule. Firstly it checks if this request is initiator. If this request is not initiator then the ring of IPS is already made but if this request is initiator then it calculate $rate_i$ this rate is compare with cap_i .If maximum capacity is reached then alert is raised otherwise this process is done for next horizontal IPS on the ring .
b_i is Boolean value. Initially b_i is set to true and after computation b_i is reset and rate to zero. Rate computation is done on the basis of pps that is packet per second and bps that is byte per second.

Algorithm2: mitigate (r_i, firstRing)

1: for all ips ϵ upstreamIPss do
2: ips.mitigate (r_i, False)
3: end for
4: for all a ϵ getAddr (r_i) do
5: block_IPS (a)
6: end for
7: if firstRing=True then
8: nextIPS.mitigate (r_i, True)
9: end if
10: setCautiousMode (r_i)

System detects and blocks an attack as far as possible from the victim. Hence for doing this process for all the IPS in the upstream rings which allows the vertical communication process. When an attack gets detected then forms protection rings around the victim.

V.CONCLUSION

Thus this system provides virtual protection ring to detect flooding DDoS attack, which is for the early detection of flooding DDoS attacks It will detect attack as close to the sources as possible and as far as possible from user, providing a protection ring around user or victim and it will helps for saving valuable network resources. It also provides a solution to problem which associated with single IPS system. It also helps to detect attack very effectively as well as efficiently like antivirus.

REFERENCES

[1] J. L. Berral, N. Poggi, J. Alonso, R. Gavaldà,, J. Torres, and M.Parashar, "Adaptive distributed mechanism against flooding network attacks based on machine learning", in *Proc. ACM Workshop Artif Intell. Security*, 2008, pp. 43–50.

[2] Y. You, M. Zulkernine, and A. Haque, "A distributed defense framework for flooding-based DDoS attacks," in *Proc. 3rd ARES*,Mar. 2008,pp. 245–252.

[3] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: A statistics-based packet filtering scheme against distributed denial-ofservice attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 3, no. 2,pp. 141–155, Apr.–Jun. 2006.

[4] J. Françcois, A. El Atawy, E. Al Shaer, and R. Boutaba, "A collaborative approach for proactive detection of distributed denial of service attacks," in *Proc. IEEE MonAM*, Toulouse, France, 2007, vol. 11.

[5] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *Comput. Surv.*, vol. 39, Apr. 2007, Article 3.

[6] G. Koutepas, F. Stamatelopoulos, and B. Maglaris, "Distributed management architecture for cooperative detection and reaction to DDoS attacks," *J. Netw. Syst. Manage.*, vol. 12, pp. 73–94, Mar. 2004.

[7] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "Packet Score: A statistics-based packet filtering scheme against distributed denial-of service attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 3, no. 2,pp. 141–155, Apr.–Jun. 2006.

[8] H. Farhat, "Protecting TCP services from denial of service attacks," in Proc. ACM SIGCOMM LSAD, 2006, pp. 155–160.

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