Earnest Access of Divulging and Aversion of DDOS Attack

A.R. Sathyabama
Assistant Professor
Department of IT
Velammal Engineering College

C.M. Nalayini
Assistant Professor
Department of IT
Velammal Engineering College

S. Priyadharshini
Assistant Professor
Department of IT
Velammal Engineering college

ABSTRACT
In recent days, technology has reached new heights. In the same way malicious programs has also touched the level of sky and the above. Secret information are nowadays stored and managed through high secure sites. However, critical problems like hacking happens due to DDOS(Distributed Denial of Service Attacks) resulting in crashing of website for certain period of time and hacking of sensitive information thereby affecting the services issued. Such problems can be sorted by the scope of MASTDP (Multiple Authenticated Scoring Technique for denial and prevention of DDOS attacks). In this technique, internet protocol address and physical address of the users are entered and stored in the history and scores will be allotted for each and every entry. Similarly, horizontal and vertical communication scoring are given for every entry based on the vulnerability of the user (using scores). At-last, by association rule, users with peak scores are denied entry from the network or site.

Keywords
Association rule; DDOS attacks; MASTDP; IP tracer; Scoring technique

1. INTRODUCTION
DDOS attacks are the most hazardous which spoils the webpage services and cracks the information from them. These type of attacks are specifically divided into UDP flood, ICMP (PING) flood, SYN flood, Ping of death, slowlouis, NTP amplication, HTTP flood etc., DDOS attacks can be of shorter duration but the attack volume may of very large packet per second. These attacks are usually politically or criminally motivated having capacity to target various application websites, mail servers and VoIPs. To overcome DDOS attacks, we are using a new approach – MASTDP of DDOS attacks. This approach is an effective approach where users are given a scoring and placed in a VH network. The users itself become as intrusion prevention system. VH based communication takes place based upon the rules and scores are allotted, and if the scores exceeds a threshold limit, access is denied for the user.

2. ALGORITHM FOR MASTDP OF DDOS ATTACKS
Initially, process has started and IP and physical address are noted.[22] Score is denoted by the term (i) Entry of users are denoted by (A) If A is greater than number of times entered (n), then access is denied. Else, it is going to VH based network[17]. Where VH based network arrange the users based on their previously allotted scores. After arranging in VH based networks each and every user acts as IPS (Intrusion Prevention System). So communication takes place whenever any vulnerable activity is detected. If threat is high, then vertical communication will take place and a high score is added to score lead 2. If threat is low, then horizontal communication will take place and a small score is added to score lead 2.[7]

Algorithm:-

1. Start the process
2. Track and score (i) the ip address and physical address for each entry of the users (A).
3. If A > n (n= number of times the users entered), access is denied
4. Else go to VH based network
5. If H path is noted, i is minimum else i is maximum
6. Compare A(i) with VH(i)
   - $S = \frac{\sigma A(i)*VH(i)}{n}$
7. If S is maximum, access is denied
8. Else i is recorded.

3. MASTDP OF DDOS ARCHITECTURE
The users who are accessing the URL, are noted by the entry checker and a score is allotted by score lead 1. At the end of this process, user having obtained scores equal to or greater than 1.0 is denied further access[12]. Upon gaining access, the IP and physical address are tracked by IP tracker tool[6]. The physical address verifier scrutinizes the physical address and updates the score further. Then VH based network is formed by means of checking the scores given by score lead 1[16]. Now, by following the rules, scores are given by score lead 2. After obtaining scores from both the them, association rule is used to obtain an effective final score.[9] If the resultant score is higher than the threshold, access is denied. If not the scores updated in the score list database[18].(Depicted in Fig. 1).

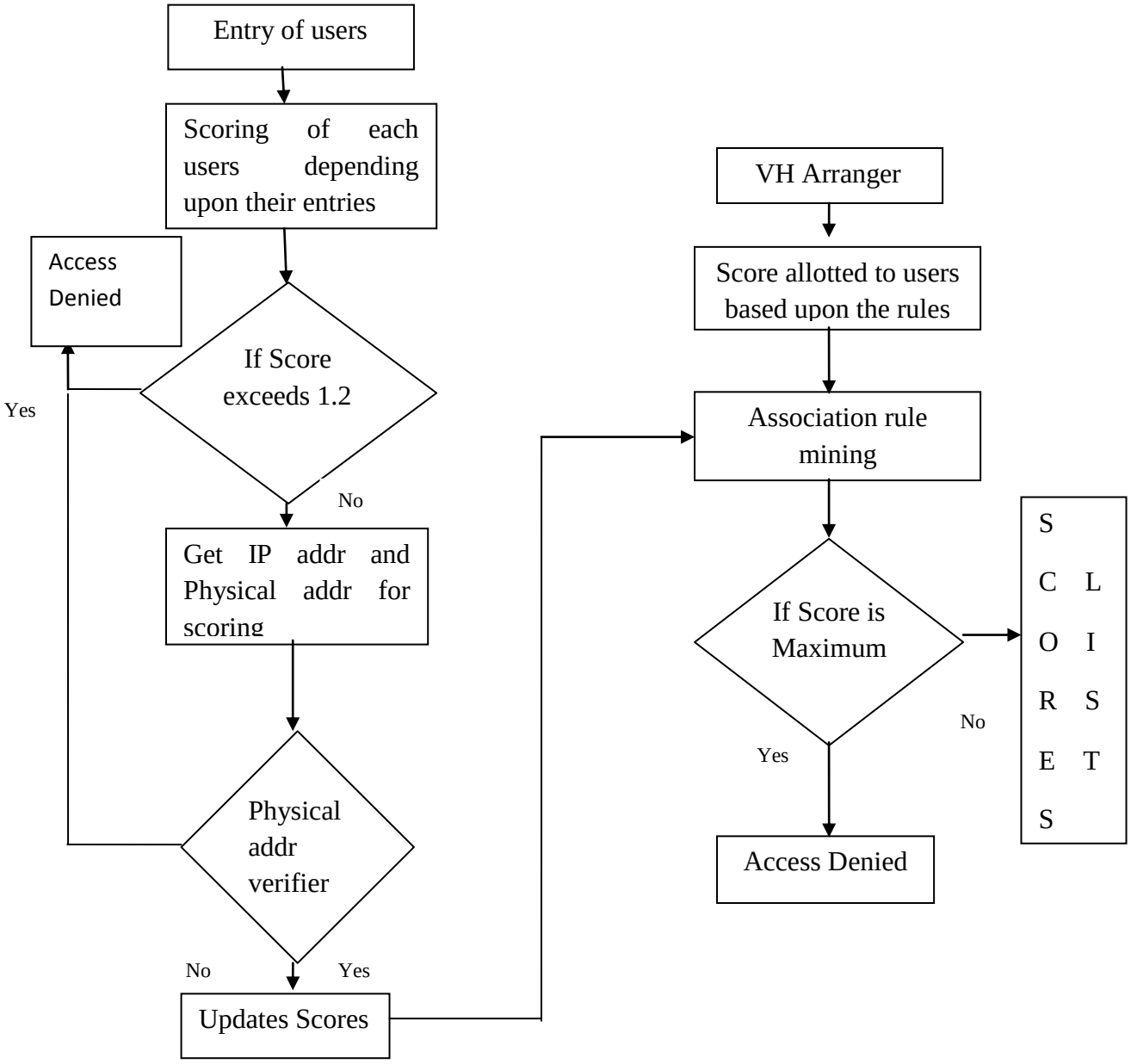

Figure 1 Mastdp of DDOS Architecture

4. MODULES DESCRIPTION

4.1 Entry checker

It checks the entry of the users. It scores the IP address and physical address by using IP tracker tool. Updates database consistently.

4.2 Score lead 1

Score are allotted based upon their entries. Scores starts from 0 to 1. It increases 0.2 for each entry.[14] When it reaches 1.2, then automatically access is denied for the user. If the score is between 0 and 1, it is sent to VH arranger. (Depicted in Fig. 2)

4.3 VH arranger

Based upon the scores given by score lead 1, VH network is formed[11]. If score is high, it is placed in H based networks. If score is low, it is placed in V based networks.[1][2]

4.4 Score lead 2

Depending on the following rules, scores are allotted by score lead 2.

Whenever information measure is high and rate is high then the score allotted is four. Whenever information measure is low and rate is high then score allotted is three.[20] Whenever information measure is high and rate is low then score allotted is two.[10] Whenever information measure is low and rate is low then there is no threat and the score allotted is one. (Depicted as table in Table 1 and as graph in Fig. 4)[4]

Table 1 Rule for Score lead 2

Case	Information measure	Rate	Score
1	High	High	4
2	Low	High	3
3	High	Low	2
4	Low	Low	1

4.5 Association rule minder

After obtaining the scores from score lead 1 and score lead 2, association rule derives the effective scores are obtained. Consider A(i) as entry scores and VH(i) as VH network scores.[8][19]

Then,

$$S = \frac{\sigma A(i) * VH(i)}{n}$$

where, n is number of users

Scores are updated finally in the score list.

4.6 Hustle Vincible

Based on the score of association rule minder, access is denied if the score is high[21] and the score is updated if the score is low. (Depicted in Fig 5)[5][13]

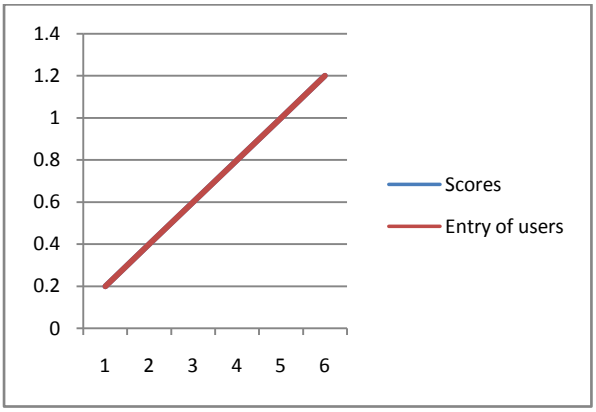

Figure 2 Results of Score lead 1

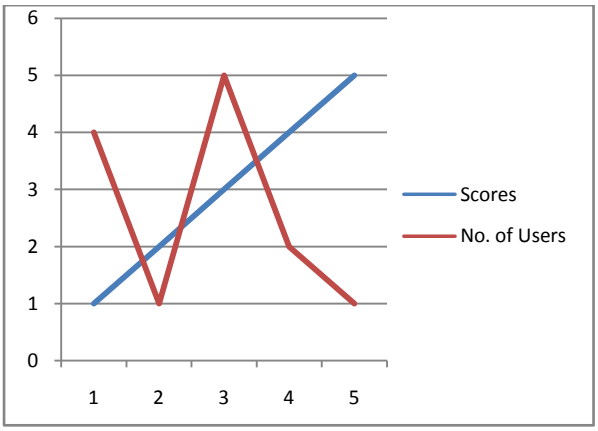

Figure 3 Results of VH Communication

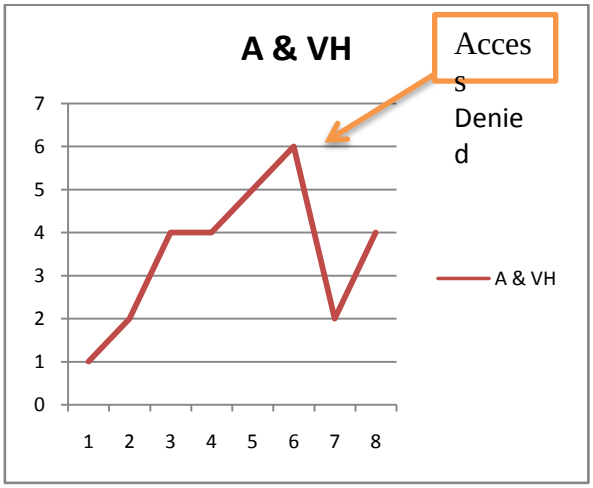

Figure 4 Association rule minder

5. CONCLUSION

MASTDP of DDOS attacks is the best and effective technology and approach to overcome highly dangerous DDOS attacks. Scores are allotted to users at various stages via entry score and VH based communication scores. These scores are combined by association rule to give accurate results. Fig. 1 depicts the scores allotted by the entry of users. Fig. 3 shows the VH based communication. In this scores are allotted based on the critical and minor communications respectively. Fig. 5 is the association rule where both the scores attained in Fig. 1 and Fig. 3 are combined and an accurate score is assigned is for each user. Thus the overall technique offers multiple authentication of each and every user thereby making MASTDP of DDOS attacks a very effective tool to avoid hazardous DDOS attacks and provides safer platform against vulnerably affected web portals. The future enhancement of MASTDP of DDOS attacks can be done using better scoring technique than used in this technology.

6. ACKNOWDGEMENT

Our Sincere Thanks to Professors, Lectures of IT Department and our family members who continuously supported to publish paper.

7. REFERENCES

[1] A. Networks, Arbor, Lexington, MA, “Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm,” “Worldwide ISP security report,” Tech. Rep., 2010.

[2] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, in Proc. USENIX LEET, 2008, Article no. 9.

[3] 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.

[4] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, “Locating Internet routing instabilities,” Comput. Commun. Rev., vol. 34, no. 4, pp. 205–218, 2004.

[5] A. Basu and J. Riecke, “Stability issues in OSPF routing,” in Proc. ACM SIGCOMM , 2001, pp. 225–236.

[6] T. Peng, C. Leckie, and K. Ramamohanarao, “Protection from distributed denial of service attacks using history-

based IP filtering," in Proc. IEEE ICC, May 2003, vol. 1, pp. 482–486.

[7] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," Comput. Netw., vol. 34, no. 4, pp. 579–595, 2000.

[8] J. A. Barnett, "Computational methods for a mathematical theory of evidence," in Proc. 7th Int. Joint Conf. Artif. Intell., 1981, pp. 868–875.

[9] R. N. Smith and S. Bhattacharya, "A protocol and simulation for distributed communicating firewalls," in Proc. COMPSAC, 1999, pp. 74–79.

[10] 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.

[11] K. Deeter, K. Singh, S. Wilson, L. Filipozzi, and S. T. Vuong, "APHIDS: A mobile agent-based programmable hybrid intrusion detection system," in Proc. MATA, 2004, pp. 244–253.

[12] 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.

[13] 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.

[14] D. Nashat, X. Jiang, and S. Horiguchi, "Router based detection for lowrate agents of ddos attack," in Proc. HSPR, May 2008, pp. 177–182.

[15] H. Wang, D. Zhang, and K. Shin, "Change-point monitoring for the detection of DoS attacks," IEEE Trans. Depend. Secure Comput., vol. 1, no. 4, pp. 193–208, Oct.–Dec. 2004.

[16] P. Verkaik, O. Spatscheck, J. Van der Merwe, and A. C. Snoeren, "Primed: Community-of-interest-based DDoS mitigation," in Proc. ACM SIGCOMM LSAD, 2006, pp. 147–154.

[17] 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.

[18] A. El-Atawy, E. Al-Shaer, T. Tran, and R. Boutaba, "Adaptive early packet filtering for defending firewalls against DoS attacks ," in Proc. IEEE INFOCOM, Apr. 2009, pp. 2437–2445.

[19] A. El-Atawy, T. Samak, E. Al-Shaer, and H. Li, "Using online traffic statistical matching for optimizing packet filtering performance," in Proc. IEEE INFOCOM, May 2007, pp. 866–874.

[20] D. Das, U. Sharma, and D. K. Bhattacharyya, "Detection of HTTP flooding attacks in multiple scenarios," in Proc. ACM Int. Conf. Commun., Comput. Security, 2011, pp. 517–522.

[21] A. Sardana, R. Joshi, and T. hoon Kim, "Deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate DDoS attacks in ISP domain," in Proc. ISA, Apr. 2008, pp. 270–275.

[22] V.Priyadharshini, Dr.K. Kuppusamy," Prevention of DDOS Attacks using New Cracking algorithm" in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.