DPM: Defence Prevention Mechanism for Flooding based DDoS Attack

Rajan Patel[1], Nipa Patani[2]

[1]rgpce21@gmail.com, Dept. of Computer Engineering, Sankalchand Patel College of Engineering-384315
[2], GTPL Hathway Ltd, Ahmedabad

Abstract— *Flooding attack threatens among all the flavours of DDoS (Distributed Denial of Service) causing deadliest impact in network. The ability of DDoS attack doesn't need to have much computational efforts to target the destination servers and networks. Developing a mechanism against unidentified attacks on application and transport layer is a desired goal of intrusion detection and/or intrusion prevention system research. This paper presents discussion on several vulnerabilities that explicitly attempts to disrupt legitimate users access to services at application and transport layer of TCP/IP. In this paper, we explore various DDoS attacks and their attempts to combat it. We proposed a DPM (DDoS Prevention Mechanism) approach from existing taxonomies for the detection and analysis of synchronous and non-synchronous traffic flow with the observation of network continuously. Furthermore, DPM uses traffic source authentication of legitimate and malicious traffic using challenge-response mechanism. At last we evaluate accuracy of our proposed algorithm in terms of defending number of incoming malicious request. We overcome the issue of detecting malicious request in asynchronous flow.*

Keywords— DDoS flooding attack, DPM, IP filtering, Network Security

1. Introduction

In the world of Internet, computer network plays major role and Distributed Denial of service, or better known DDoS attack is to recruit the army of bots which turned into a noteworthy danger to current systems. In order to turn a computer into bot, attackers develop specialized malware, which they spread as many vulnerable computers as possible. Malware can spread via compromised websites, email attachments, or through an organization's network as depicted in figure 1.

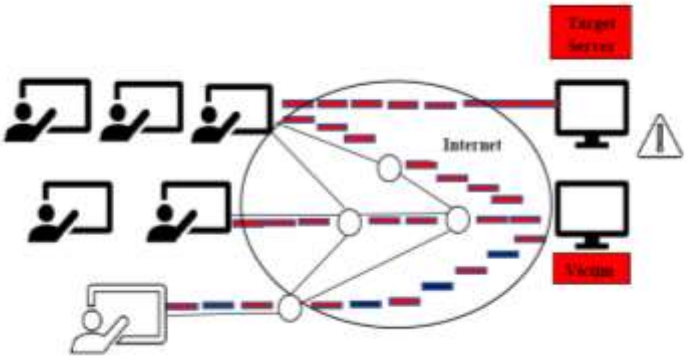

Fig. 1. Operation of a DDoS attack

Many users, tricked into such malware, will unintentionally turn their computer into bot and provide access point for attackers to their computer. Once a computer turns into a bot, it connects to attacker's command and control servers and begins to accept orders from the centralized machines. It includes directions for launching an attack from the bot's malware to a particular target using selected attack methods (HTTP, GET, Flood). An army of bots is named botnet and usually consist of thousands of bots. Anytime the botnet owner wants to launch an attack they send messages to their botnet command and control server with instructions to perform an attack on particular target. Any infected machines in the botnet will comply by launching a coordinated, well timed distributed attack known as a DDoS attack. Launching a large-scale DDoS attack is not difficult task to carry out. What does it need to create its own Botnet? Various pay-for-hire DDoS service are available. Anyone using such a service can launch a powerful DDoS attack on a target of their choice for anywhere from $5 to

$200 per hour depending on attack size and duration [1]. The motivation behind DDoS attacks can be financially driven, hacktivism, or even just for fun. No one, however, should doubt the potential cost of a successful attack. The business impact of a DDoS attack is substantial and can involve financial losses, reputational damage, customer agitation, and legal repercussions.

In this paper, provides the driven solution, mechanism and techniques which helps to prevent DDoS attack that is DPM: Defense prevention Mechanism for flooding attack. The later section of paper covers history work in defence mechanism of DDoS based flooding attack with their identified vulnerabilities. Section three describes the algorithm description for designing defense prevention mechanism for the DDoS based attacks. Section four and five discusses contribution of this paper and shows the effectiveness of proposed prevention mechanism for DDoS attack with an existing monitoring mechanism, that by improving existing well-performing detection mechanisms over them. Finally, concluded in the last section of our work for securing the DDoS attack.

2. DDoS based Flooding Attack

Flow Count is recognizing property which demonstrates the seriousness of the flooding attack. The flow count is figured for every association at a specific time interval. DDoS attack is described when the contrast between fast entropy of flow count at every interval and mean value of entropy in that time interval is more prominent than the threshold value. This shows the effectiveness in terms of computational time in comparison to conventional entropy.

In real Internet traffic, packets can be in synchronous long flow or low rated non-synchronous flow. It is assumed that normal traffic flows are short-lived and non-synchronous [2]. Such a traffic behaviour can trade off a host or system with DDoS attacks by direct attacks or reflectors attacks using bots. There is a lack of detection mechanism for Low-rate Denial of Service (LDoS). The proposed Multisampling Sampling Averaging Based on Missing Sampling takes network traffic as a signal based on a small signal model for10 ms within 30s. The results generated compared with threshold for identifying the LDoS attack [3]. There are several Information theory-based metrics in the detection of distributed DoS attacks [4]. To overcome the deficiency of early detection and high accuracy, a victim end based mechanism is constructed with a low false positive ratio within a short interval. In [5], they increased the order of information difference measures in detecting both low-rate and high-rate DDoS attack.

For DDoS flooding attacks, consuming bandwidth or resources are the main methods to make service unavailable. The larger the number of synchronous flow in a time interval the stronger traffic is synchronized. The suggested algorithm [2] records the address pair of source and destination address in time slots and performing several intersecting operations in consecutive time slots and record it for enough times. If it exceeds the threshold it is labelled with alarm and further it is detected by using HCF (Hop Count Filter) for mapping number of hops from a source to destination.

Another approach for preserving quality of service of the legitimate traffic they have proposed Traceback-based Defense against DDoS Flooding attack that detects attack at source end. TF (Traffic Flow), DFM (Deterministic Packet Marking) IP (Internet Protocol) based traceback algorithm at a victim end modules are established in a network that efficiently drops the attack packets at the source end [6].
Attack packets are generated generally by tools that are installed in a bot for flooding the link or a network. This shows that flow similarity among DDoS flooding attack is much higher than among random flash crowds.

Table 1. Comparison between DDoS attack and flash crowd

Parameter	**DDoS Attack**	**Flash crowd**
Network	Congested	Congested
Server Resources	Overloaded	Overloaded
Traffic Source	Illegitimate	Genuine
Traffic Flow	Sync, Async	Sync, Async
Degree of Automation	Automatic, Semi-automatic	Manual
Response to Traffic Control	Unresponsive	Responsive
Prediction	Unpredictable	Predictable

3. DPM: DDoS Prevention Mechanism

In our previous proposed prevention mechanism [7] that is DPM, source IP address and destination address is paired for monitoring the intermediate packets. The destination capacity is confined according to the utility of server. Moreover, the factors like packet type is considered for the defense method to trigger an interrupt whenever, malicious packets are encountered. Firstly, categorizing repeated IP address pair and next level prevention mechanism for IP authentication is applied. Figure 2 shows the design working for challenge response module for the suspicious IP address pair, to genuine users are differentiated and allowing further to serve their request. Figure 3 shows the initialization of monitoring the network based on frequency of packet and capacity of server.

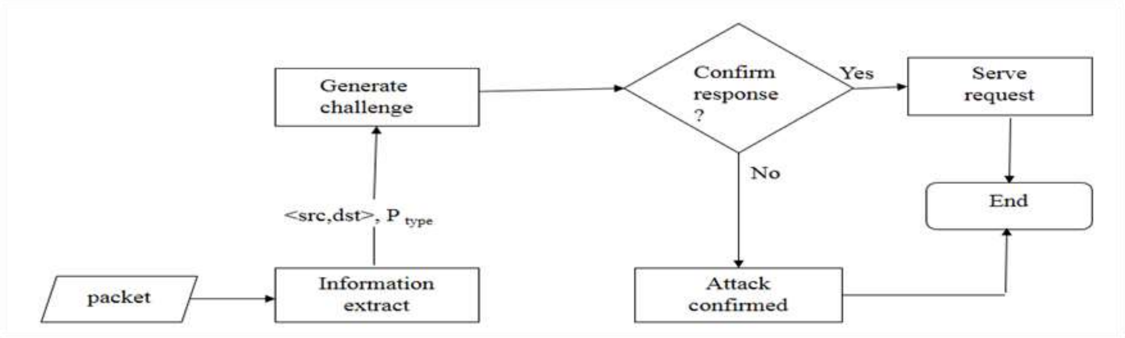

Fig 2. Procedure of DDoS module

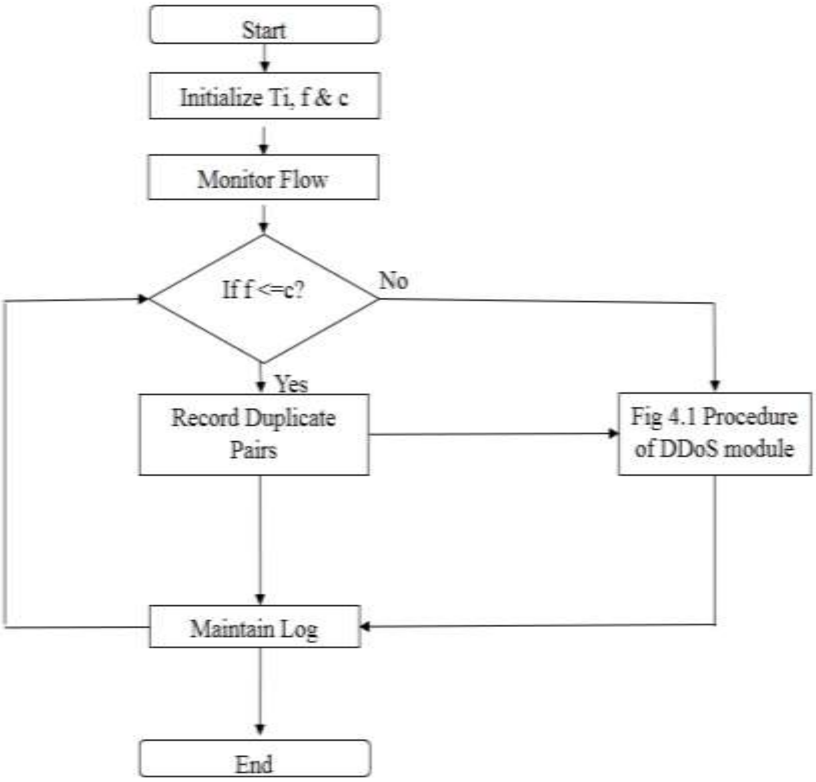

Fig 3. Procedure for DDoS prevention module

The procedure of our algorithm is showed as follows.

```
Proposed Algorithm
Step1:   Initialize observation slot Ti, frequency of packet f, destination capacity c.
Step2    Monitor flow of arrival of request and serve till destination capacity c.
         If c is full
         For every duplicate pairs <src,dest> in Ti , packet type.
         T*( i )=T1+T2 ∩ T2+T3  ∩ T3+T4  ∩ …. ∩ Tn-1  ∩ Tn
Step 3   If frequency of packet/traffic > c. (for a given time-slot, T=30s) then go to 4 else go to step
         6.
Step4    Send reply back using challenge response approach
         Generate $C_{ch}$ for <src,dest>
Step5    Serve only the responses and drop other packets.
Step6    Observe traffic flow in next consecutive time slot $T_i$
```

The proposed DPM mechanism method based on following two objectives. (i) Flow count is considered for detection of malicious packet. (ii) Genuine user request is focused to be served first. In our algorithm, we firstly stated the capacity of destination server. For every incoming packet in a defined time slot is monitored, we record all the address pair and serve till the destination capacity is not reached. If it exceeds a destination capacity server, we will ack back the recorded duplicate pairs stored in observation table. Then after it is organized in terms of confidence level for further filtering techniques of IP request on destination server. In addition, the traffic flow is observed in last two consecutive time slots for the analysis of incoming packets thoroughly in the network.

4. Experimental Setup

There are three categories of network condition consisting of the situation when the evaluation is carried out for legitimate traffic and under attack as shown in table 2. This segment assesses the validation of our proposed method using various simulation scenarios with and without using topology generator. We used network simulation tool for the traffic generation and the parameters like total number of attacker as well as genuine nodes, number of routers, various traffic agents, simulation time etc as shown in table 3.

Table 2. Examination scenario

	Scenario	
1	Normal	Low access High access
2	Attacking	Flooding
3	Random	Legitimate user and attack

Table 3. Simulation parameters

Total Number of Nodes	8
Attacker Node	2
No. of Destination	1
No. of routers	3
Simulation Time	30 sec
Traffic agent	TCP, UDP
No. of wifi nodes	4

5. Evaluation of DPM

In the detection of DDoS flooding attack, we concern more about where the malicious traffic comes from and it is of less concern about destination hop. So, we only need source address and destination address to identify a flow. Table 4 described the traffic generation rate from source after fixed interval of time by constant amount. In table 5 legitimate traffic and attack traffic flows traffic are generated through UDP and TCP flows in network simulator. In existing work, the data set for the comparison of traffic flow is considered. It is shown in table 6 the incoming rate of packets in different data set after fixed interval.

Table 4 Experiment 1: Flow statistics

1s	30s	60s	90s	120s
1500	1800	2600	2856	3900
1265	1231	985	847	525

Table 5. Experiment 2: Flow Statistics

1s	30s	60s	90s	120s
900	1465	855	5630	6000
547	698	1020	567	365

Table 6. Flow statistics of existing work

	1s	30s	60s	90s	120s
DA	90595	68529	54800	50158	46706
EC	244094	37585	28925	25702	21880

To make our defense mechanism effective, we need to select the optimal time slot to measure the proportion of incoming traffic rate. Figure 4 shows the simulation evaluation from the values of table 4. As shown in figure 4 with increasing in time from 1 sec to 30 sec number of packets are increasing at a normal speed. As soon as simulation reaches to 90 sec there is a sudden increase in a network as a result of burst of request in tome slot of 60 sec to 90 sec. There is an exponential increase in the mixed traffic of a network.

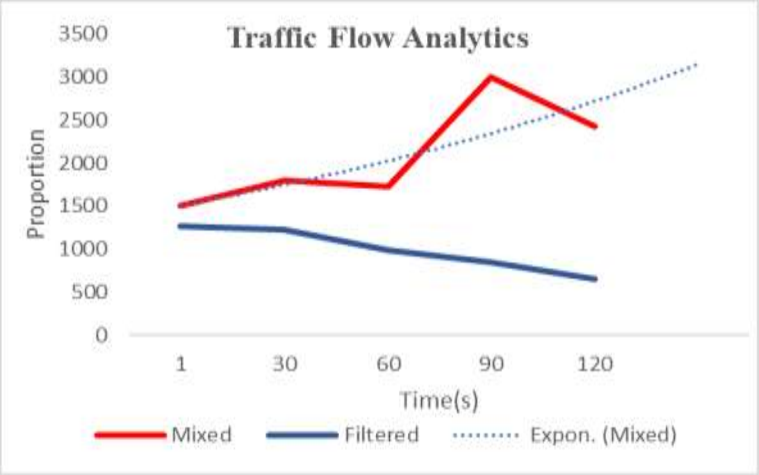

Fig. 4. Exp-1 evaluation

To measure accuracy of experiment, the time slot from 1 sec to 30 sec is close to genuine traffic. As shown in figure 5, there is an intersection of mixed as well as filtered traffic. Here it is difficult to detect the incoming traffic for IP filtration. This shows the linear growth of filtered incoming packets for filtered packets in an experiment.

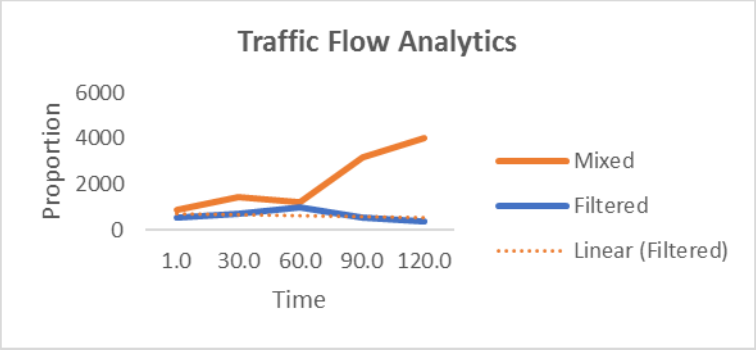

Fig. 5. Exp-2 evaluation

As shown in figure 6, the evaluation of our proposed work with comparison to existing work is shown. We analysed that from our DPM approach number of incoming packets are filtered better than HCF approach. By intersecting in consecutive time slot, it gives more accuracy in counting and identifying malicious IP request. In figure 6, filtered traffic (blue line) is closer to the capacity of server that serve the purpose of feeding all the genuine request. Our proposed algorithm accuracy is based on the number of filtered request with respect to proportion of time slot.

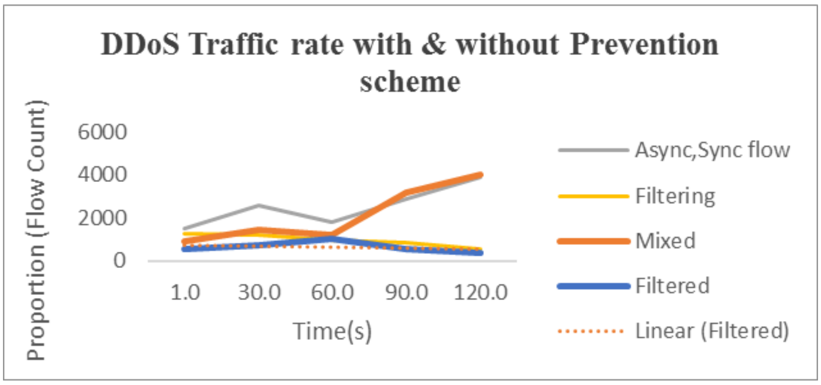

Fig. 6. Proportion of synchronize and asynchronies flow for incoming traffic

6. Conclusion

In this paper, we simulated constant bit rate traffic for the amount of time and differentiate between attack flow and normal flow. We have marked the duplicate IP source and destination address pair for the time period in synchronous as well as asynchronous traffic flow. Furthermore, the challenge response mechanism for the authenticity is implemented. It gives high accuracy in detecting mixed traffic. We also detect flash crowd and DDoS attack traffic in a proportion of time. In future we will focus more on optimizing our technique.

References

1. Qijun Gu, Peng Liu, Denial of Service Attacks, A Report, pp.1-28. https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf
2. Li, Chenxi, Jiahai Yang, Ziyu Wang, Fuliang Li, and Yang Yang, "A Lightweight DDoS Flooding Attack Detection Algorithm Based on Synchronous Long Flows", In IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2015.
3. Zhi-Jun, Wu, Zhang Hai-Tao, Wang Ming-Hua, and Pei Bao-Song, "MSABMS-based Approach of Detecting LDoS Attack." Computers and Security, Vol. 31, no. 4, pp. 402-417, 2012.
4. Bhandari, Abhinav, A. L. Sangal, and Krishan Kumar, "Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks", International Journal of Computer Network and Information Security, Vol. 7, no. 8, 2015.
5. Bhuyan, Monowar H., D. K. Bhattacharyya, and Jugal K. Kalita, "An Empirical Evaluation of Information Metrics for Low-rate and High-rate DDoS Attack Detection", Pattern Recognition Letters, Vol. 51, pp. 1-7, 2015.
6. Foroushani, Vahid Aghaei, and A. Nur Zincir-Heywood. "TDFA: Traceback-based Defense Against DDoS Flooding Attacks," 28th International Conference on Advanced Information Networking and Applications, IEEE, pp. 597-604. 2014.
7. Patani, Nipa, and Rajan Patel, "A Mechanism for Prevention of Flooding based DDoS Attack", International Journal of Computational Intelligence Research, Vol 13, Issue 1 pp. 101-111, 2017.