# Anomaly based Mitigation of Volumetric DDoS Attack Using Client Puzzle as Proof-of-Work

Prachi Gulihar
National Institute of Technology,
Kurukshetra, India
prachigulihar2@gmail.com

B.B. Gupta
National Institute of Technology,
Kurukshetra, India
brij.gupta@gmail.com

***Abstract*— Increasing use of Internet has made its users vulnerable to various types of attacks like Distributed Denial of Service (DDoS) attack which makes the resources unavailable to the benign user. Many mechanisms exist against DDoS attack for its detection, prevention, response and mitigation, one such technique is using client puzzles. It is a mitigation technique which has main motive to prevent the attackers from flooding the Internet Service Provider (ISP) network by checking the incoming packets for the sending rights in the form of client puzzle solution. This paper presents a combination of anomaly and volume based approach to safeguard the victim network from DDoS attack by checking the sender for sending rights which are granted against a challenge puzzle generated by client puzzle module and diverting the attack traffic to dynamic provisioning module when the flooding traffic is becoming cumbersome to be handled by the victim. This defense technique is an on-demand mechanism which is activated on the basis of volume of traffic being flooded towards the victim. Network simulator 2 (NS2) is used to simulate the proposed approach. The proposed approach limits various cons of existing approaches like it reduces the collateral damage by distinguishing packets having Proof of Work (PoW)The simulation results depict high malicious packet drop rate and less benign packet drop rate.**

***Keywords*— *cryptographic client puzzle, flooding distributed denial of service attack, DDoS mitigation***

## I. INTRODUCTION

With an increase in the number of cyber attacks and significant rise in DDoS attack has made it evident to detect and trace the activities of attacker for mitigation. The largest DDoS attack was reported in 2014 [1]. It was of size 400 Gbps. With the growth in size of DDoS attacks, their sophistication levels have also increased. A statistics [1] of different kinds of DDoS attacks show that the instances of volumetric DDoS attack instances are maximum standing at 65%. A majority of these volumetric attacks are UDP and ICMP floods. State-exhaustion attacks take place somewhat more often than application-layer attacks.

Figure 1 shows the DDoS attack vectors which were exploited in 2017 for performing volumetric DDoS attack. A jump of 69 percent was recorded from August 2017 to December 2017 peaking in September 2017. The Mirai malware which came into existence in August 2016 continued to create problems in 2017 also generating attacks of 104 Gbps [2]. In April 2017, telnet vulnerabilities of the devices were exploited by Brickerbot for a period of four days causing permanent denial of service [3]. With an immense boost in the

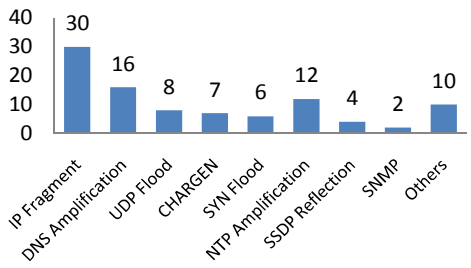


Fig. 1. DDoS attack vectors frequency [2]

sophisticated cyber crimes, relying on conventional defense mechanisms is not enough. Multiple lines of defense will be a comprehensive solution. Hence, keeping a constant track of client's authority to send traffic to any server by checking for Proof-of-Work (PoW) is used for improving network security.

DDoS attack is one of the most widespread attacks that need to be handled to secure the network. The problems the proposed model addresses are [4]:

*Lineal Deployment:* Any defense mechanism must ensure that it is reasonable and affordable to be deployed by the individual party wanting protection for its server machine.

*On-Demand DDoS Mitigation:* The mitigation strategy should come under action only when the attack is happening, it should not remain active under normal circumstances. This will lower the maintenance costs.

*Network-layer DDoS Defense:* The DDoS mitigation techniques must be able to segregate the network-level traffic as timely drop the malicious packets based on anomaly detection.

*Non-distinguishable DDoS Defense:* Non-filterable traffic is the one which cannot be filtered from the legitimate traffic. Proof-of-Work (PoW) scheme helps in prioritizing the connection requests hence reducing the collateral damage done to the legitimate traffic.

*Instant Deployability:* One important goal in designing any kind of scheme is that it should be easily deployed on the existing infrastructure without any major modifications. The PoW ensures easy deployment.

The proposed approach addresses some of the existing issues of the DDoS defense schemes. It combats DDoS attack by mitigating the attack traffic and allowing selective access to

978-1-5386-2440-1/18/$31.00 ©2018 IEEE

the services offered by the server. It works in two different modules based on the value assigned to the volume metric by the traffic checker module for the incoming packets. The next section presents the related work. Section 3 explains the proposed approach to protect the ISP network. Results and Discussions are covered in section 4. Section 5 concludes the paper and discusses the scope of future work.

## II. Related Work

DDoS defense mechanisms include four techniques namely prevention, detection, response and mitigation. Many methods are already proposed to fight against DDoS attack but no guaranteed defense mechanism exists till now. A number of solutions have been proposed to combat DDoS attack using cryptographic puzzles in its defense mechanism. Some of the prominent mechanisms proposed till 2017 are discussed below.

Saravanan et al. [5], have used a combination of dual techniques- pushback and client puzzles. They have dealt with the DDoS defense challenge as the problem of congestion control. The routers are trained to selectively drop the packets which exhibit malicious traits. The same mechanism is pushed upwards to the upstream routers. To allow the traffic from any client to reach the server, the suspected client has to solve the challenge puzzle. It has the advantages of both pushback scheme and client puzzle scheme.

Wu et al. [6], have addressed a major drawback of any puzzle mechanism which is GPU inflation attack .It is the ability to inflate the power of the attacking machine which will then be able to perform computationally expensive operations at a quicker rate. This is done by making use of additional software and Graphic Processing Unit (GPU). To prevent the attackers from inflating their ability to solve puzzles, a new kind of software puzzle is introduced. In software puzzle, the puzzle algorithms are not generated before-hand. Only when a client request arrives the algorithm is revealed which makes it impossible for the client to develop a computable implementation which solves the puzzle in advance. The translation of Central Processing Unit (CPU) based puzzle to its GPU based equivalent challenge is a time consuming task. The results of security analysis of software puzzle shows that real-time reproduction is delayed.

Boyd et al. [7], authors have given the concept of fair client puzzles. These puzzles make use of the blockchain network of the bitcoin cryptocurrency and the solution of these puzzles is not affected by the amount of computational resources the attacker client machine posseses. The computational effort required to solve the challenge puzzle is widely distributed because it is solved by the mining process of bitcoins. These fair client puzzles behave as proof-of-work which curbs overuse of limited resources. All other works have focused on difficulty level and cost-effectiveness of challenge puzzle but this is the only work which has taken into account the fairness aspect as well. The major drawback of this scheme is real-time delays in generation of bitcoin blocks.

Fallah et al. [8], distributed attack defense mechanism has been designed using the formal approach of game theory. This work is focused on solving the flooding type of DDoS attack by following a set of puzzle-based mechanisms which are optimal and effective. An optimum defense strategy is designed based on the Nash equilibrium concept. The mechanism designed is independent of the number of attack traffic generation sources.

Brent et al. in [9], have explored the technique of cryptographic puzzles which are outsourced. They have proposed an external service called bastion which distributes the constructed puzzles. This way the puzzle distribution point can never be compromised by the attackers. The waiting time of the clients wanting to access the service is reduced because these puzzles are solved offline.

Table 1 Comparison between different DDoS mitigation approaches using Client puzzles

| Approach | Advantages | Limitations |
|---|---|---|
| Router based Pushback with Client Puzzles [8] | • Puzzle work load is transferred to the upstream path routers which decreases work load of processing on the path routers. | • It is not effective in performing rate-limiting defense on the malicious traffic inside the aggregate.<br>• Fails to mitigate the attack traffic which is distributed within the inbound links in a uniform manner. |
| Software Puzzle [6] | • Attackers cannot inflate their puzzle-solving capabilities using GPU.<br>• Can be easily integrated with the data puzzle schemes existing on the server side because it is made upon a data puzzle.<br>• Easily deployed. | • Generation of puzzle at the server side makes it a time consuming process as the victim server only has to put in time for construction of the puzzle.<br>• No provision for construction of the software puzzle at the client-side. |
| Bitcoin Blockchain [4] | • Fair client puzzles are computed independent of power of client machine's computing resources.<br>• Client cannot save the puzzles to respond afterwards at a later stage with an overwhelming count of correct puzzle solutions at a single point of time. | • Blocks in a bitcoin blockchain are generated approximately every ten minutes which is makes it impractical for client puzzle applications. |
| Game Theory with Nash equilibrium [9] | • Applicable in defending both distributed and single-source attacks. | • Does not support larger payoffs to be feasible in the game. |
| Outsourced puzzles [5] | • Robust puzzle distribution mechanism.<br>• Offline computation of puzzles | • One server is able to compute tokens associated with other servers resulting in diffusion of trust across other participants. |
| Standard Model Client Puzzles [7] | • Less number of modular multiplication operations for puzzle generation by defending server.<br>• Faster cumulative verification time. | • Slower puzzle generation time.<br>• Slower solution verification time as compared to hash based puzzles. |

Lakshmi et al. [10], discussed a set of number theoretic cryptographic puzzles which are secure in the standard model. A comparative analysis of various puzzle generation and verification algorithms is presented. The discrete logarithm concept is used to generate the client puzzle. A variant of interval discrete logarithm (IDL) problem is also discussed on which the security of the proposed DL puzzle is based. Table 1 presents a comparative analysis of the various approaches that lead to the formulation of our proposed approach as presented in the next section.

## III. Proposed Approach

In this section, we illustrate the various components of the proposed approach to protect the ISP network from DDoS attack. Figure 2 describes the proposed approach of an ISP network that combines the different defense mechanisms proposed. Following sub-sections elaborates the working of each module, The multi-level defense approach using congestion level control and anomaly based techniques can be explained by the following four steps which are executed in a consecutive manner of execution.

*Detection of DDOS attack:* This is carried out on the basis of traffic level measurements. When the volume of the incoming traffic reaches the threshold, taken as 300 in this simulation, the model detects that the DDoS attack has begun.

*Challenging the attacking sources*: In this step of the algorithm the clients which are sending the requests are challenged to solve a puzzle using their computing resources. Only the legitimate clients will be in the real need to get the access to the server's services so it solving the puzzle will indicate its interest and urgency levels. On solving the challenge correctly, it gains a rights and capability to send data to the server.

*Suppression of malicious packets:* This is the step in which the incoming packets are dropped based on anomaly. The legitimate packets will have the capabilities they have gained by solving the challenge problem. Not having these capabilities is defined as an anomaly and those packets are then blocked from going to the victim machine.

*Diverting the traffic flood:* This is the last step which comes into action when the traffic level reaches its peak load. In this the traffic is diverted to the cooperative nodes in the network which are in best position to handle the excess traffic. These cooperative nodes can be free caches and unused storage devices in the network.

As shown in figure 2, the architecture of defense scheme comprise of three modules which does the filtering of incoming packets destined to the ISP server on the basis of modules described below.

*A. Traffic Level Checker Module:* This module finds out the volume of the traffic which is directed towards the victim server. Each packet has to pass through this module before reaching the victim node. This behaves as a front-end protection and depending on the volumes recorded either puzzle generation module is called or the traffic is diverted to dynamic provisioning module denoted by DPM in the algorithm.

*B. Puzzle Generation Module:* When the volume of traffic crosses the normal traffic level this module comes into action. It gives capability to the client by using the following sub-modules to complete challenge handshake authentication protocol.

1) *Core Selector:* This is used to select two numbers from any random number oracle which will be used to generate the challenge puzzles.

2) *Challenge Generator:* The puzzle generated by this module varies in its difficulty level depending on the random numbers selected. Challenges can be of many kinds, here the puzzle is the selected random number encrypted by client's IP.

3) *Puzzle Obfuscator:* This ensures that the generated puzzle is secured by causing delay in reverse engineering due to code protection.

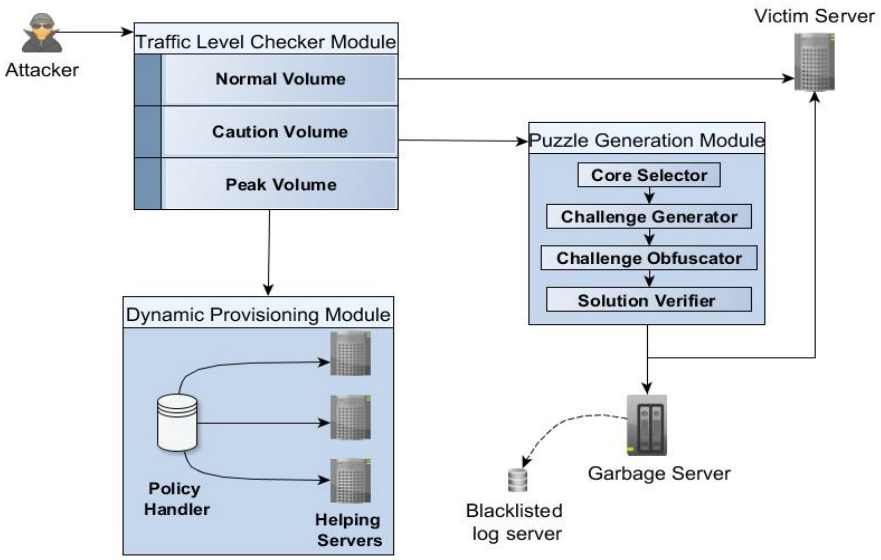


Fig. 2. Architecture of defense scheme

4) *Verifier:* Its function is to match whether the solution S returned by the client node matches the correct solution or not.

*C. Garbage Server:* The clients which have failed in solving the challenge sent to them but are still sending the traffic to the victim server are diverted to the garbage. It handles the request that is marked as illegitimate by the algorithm proposed. It will set a time window and store all the information about that packet in the blacklisted log server. This traffic is further used to blacklist such clients by mark suspicious IP address in a log server. This record is regularly updated as the traffic arrives at this server

*D. Dynamic Provisioning Module:* When the traffic volume at the traffic checker module exceeds the peak volume then this traffic flood is diverted to DPM. It behaves as a broker and matchmaker matching the availability of the servers where traffic can be diverted. It comprises of the following.

1) *Policy Handler:* It is a kind of yellow page directory which maintains a record of the available helping servers and their terms and conditions to cooperate.

2) *Helping Servers*: These are the nodes in the network which are ready to share their free resources like free ISP caches against monetary payment.

The Algorithm I as shown in Figure 3 is applied on the packets in the incoming traffic. The incoming traffic grows over a transition period of ($t_x$, $t_y$) where the volume of traffic rises from normal in the time range (0, $t_x$), cautious from range ($t_x$, $t_y$) and reaches the peak volume at $t_y$. The threshold volumes at $t_x$ and $t_y$ are taken as 200 and 300 in the simulation on NS2. If the volume at any instant the algorithm is above the threshold volume then the incoming traffic is diverted to Dynamic Provisioning module and if the volume lies above the suspicious traffic volume the client puzzle module is executed and the traffic from the senders not having PoW are sent to the garbage server. And if the traffic level is below the suspicious level then the requests that are found to be legitimate are directly sent to the ISP server.

## IV. Results And Discussions

For evaluation of the performance of proposed approach, we did its simulation in Network Simulator 2 (NS2). It is done to calculate the anticipated mitigation rate of the proposed

**Algorithm 1**

```
Time range (tx, ty) is the transition period of ddos attack.
Input: Incoming traffic Xin
Start
Vin = null; //set initial volume metric as null
Fetch (Xin[t], Vin[t]);
If (Vin[t] < V[tx ])        //no defense
        {
                Forward_ISP (Xin[t])
        }
ElseIf (V[tx] < Vin[t] < V[ty])                 //client puzzle P
        {
                S : Generate(P);
                S -> C : Send(P);
                C : S=Solve(P);
                C->S : Send(S);
                                If (S==Solution[P])
                                                {
                                                Forward_ISP (Xin[t]);
                                                }
                                Else
                                                {
                                                Forward_Garbage(Xin[t]);
                                                }
        }
Else                                                    //dynamic provisioning
        {
                Forward_DPM(Xin[t]);
        }
Forward_ISP (Xin[t]){
                Handle (Xin[t]);
                }
Forward_DPM(Xin[t]){
                Send(Xin[t]) -> PolicyHandler;
                Forward(Xin[t]) -> HelpingServers;    //diversion
                }
Forward_Garbage(Xin[t]){
                Discard(Xin[t]);
                SourceIP(Xin[t]) -> logServer;      //blacklisting
                }
End
```

Fig. 3. Defense Algorithm

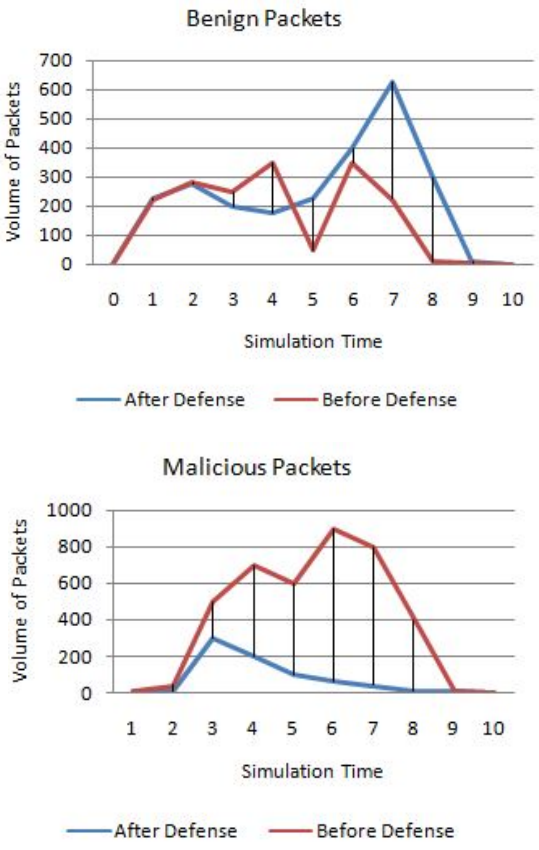


Fig. 4. Volume of Packets vs Simulation Time

framework under two conditions. Firstly, when the defense mechanism. In the simulation a heterogeneous network comprising of different types of traffic is taken, and defense is done under three attack load condition of the network traffic.Proposed framework is tested under varied client loads taking varied number of generated packets to calculate the drop rate of benign and malicious packets. Simulation of the model is tested under the two types of DDoS attack: TCP packet flood and under UDP packet flood, in both the cases similar performance is observed. In DPM module simulation, minimum charge policy in kept in policy handler. Other complex trade policies can also be kept for complex exchanges. The attacker will not invest its resources in solving puzzles to flood the victim. The same can be explained by the results shown in Figure 4, it depicts the drop rate of two kinds of packets- benign packets and malicious packets. There is a peak rise in the volume of the benign packets as the checking of PoW begins. The volume of legitimate traffic accessing the server increases and similarly as can be observed in the second graph, the volume of malicious packets was at peak when the PoW was not being checked. After the checking began the malicious packet flow drops nearly to zero.

## V. Conclusion And Future Work

The DDoS attacks are evolving with time and the attackers are creating new ways to exhaust the resources. To improve the security of Internet, collateral approaches are required besides first line of defense. This paper presents a method to authenticate the clients and permit only the authoritative clients to gain access to the services offered by the server using client puzzles as Proof-of-Work (PoW). It actively puts an eye on client's intentions and logs the malicious addresses it in log files to block their ability to access the server in future. This proposed approach to shield the ISP network provides a defense mechanism along with detection and mitigation against DDoS attack. Activation of different modules depending on the incoming packet volume tracked by traffic checker module reduces the collateral damage done to the legitimate traffic under normal load conditions.

This volume based activation of defense scheme ensures the design goal of on-demand mitigation. The client puzzle module permits access to only those clients which spend some of their computing resources. Use of dynamic provisioning module increases the efficiency as the packets with high probability of being part of DDoS attack are directly diverted. Taking into account multiple network parameters in defense strategy will lead to handle all the suspicious requests efficiently, our proposed approach has high rate of detection of malicious traffic with less false positives. This proposed model can be lineally deployed with the existing infrastructure. Considering a wider perspective, the research problem of helping servers allowing others to use their machine in DDoS defense for money is an interesting part to investigate in future.

## References

[1] https://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/ [Last access on 21/03/2018].

[2] https://www.akamai.com/us/en/about/news/press/2017-press/akamai-releases-third-quarter-2017-state-of-the-internet-security-report.jsp [Last access on 21/03/2018].

[3] Britton T., Liu-Johnston I., Cugnière I., Gupta S., Rodriguez D., Barbier J., & Tricaud, S. Analysis of 24 Hours Internet Attacks.

[4] Khor, S. H.. "Deployable Mechanisms for Distributed Denial-of-Service (DDoS) Attack Mitigation" , 2010.

[5] Kumarasamy, Saravanan, and R. Asokan. "Distributed Denial of Service (DDoS) Attacks Detection Mechanism." *arXiv preprint arXiv:1201.2007* , 2012.

[6] Wu, Yongdong, et al. "Software puzzle: A countermeasure to resource-inflated denial-of-service attacks." *IEEE Transactions on Information forensics and security* 10.1, 2015: 168-177.

[7] Boyd, Colin, and Christopher Carr. "Fair client puzzles from the bitcoin blockchain." *Australasian Conference on Information Security and Privacy*. Springer, Cham, 2016.

[8] Fallah, Mehran. "A puzzle-based defense strategy against flooding attacks using game theory." *IEEE transactions on dependable and secure computing* 7.1 , 2010: 5-19.

[9] Waters, Brent, et al. "New client puzzle outsourcing techniques for DoS resistance." *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 2004.

[10] Kuppusamy, Lakshmi, et al. "Practical client puzzles in the standard model." *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*. ACM, 2012.