Generation of Client Puzzles through bitcoin for resolution of flooding (DDoS) attack

Venkata Sai Madhav Kaza
Department of Computer Science
Central Michigan University, USA
Email: kaza2v@cmich.edu

***Abstract*—Research Problem focuses on generation of client puzzles for resolution DDoS (Distributed Denial Of Service) attack. This attack consists of overwhelming the server with tons of requests raised by attackers. By doing so, the attackers down the website and users cannot access the servers. The proposed solution of the research ensures that users can get rid of the server break-down scenarios. The research plays around the usage of bitcoins for authentication at the server end. Bitcoin currency is used for generation of small puzzles solvable by computer and flooding attack is avoided by solving the client puzzles. By doing so, clients get debited with the bitcoin amount in their credit/debit card. But, they will be avoiding the largest network traffic attack which is even worser than spending a penny on solving the client puzzles automatically by the computer.**

I. Introduction

A. Detection of DDoS Attack

Distributed Denial Of Service attack happens to the server by overwhelming it with numerous SYN packets and SYN+ACK get more occupied at the server end. The attacker does by spoofing the Source IP address and send many SYN packets to the server. The attacker gets the advantage of getting the user not able to access the website. Thus, DDoS attack happens to suffer the clients with server breakdown scenarios. The research tackles the above scenario and UDP flood attack scenario happening in the real world dataset.

B. Generation of Client Puzzles through Bitcoin

Generation of client puzzles through bitcoins is used through multiple hash functions. The generated 2 hash functions are done by seeding the server time and some other parameters. These two hash functions are generated for solving the k value and pow(2,k) hash functions. And at the puzzle verfication time 2 hash functions are matched with the previous two values hash functions. Clients use the k value to solve the 2 hash functions from the pow(2,k) hash functions generated from a k value. Thus, Generated client puzzles are solved by computers of the clients via bitcoin currency and whichever client computer solves the puzzle get access to the server with an established connection. The research tackles he above scenario by including the bitcoin currency for generation of client puzzles in real life.

II. Related Work

Défense mechanism for mitigating the flooding attack i.e. Distributed Denial Of Service Attack. Existing work focuses on normal TCP SYN packets and flooded TCP SYN packets for identifying the flooding attack. It also focuses on Défense mechanisms for mitigating the TCP SYN attack. Proposed Défense mechanism consists of 4 types of ways in which we can counter-attack the TCP SYN attack. The four types of Défense mechanism are as follows: Detecting by using TCP flags, Detecting by using port, Detecting by ICMP Feedback and Detecting by tracing the route.

Another existing work which match with the Research Proposal is that OverDoSe technology. The technology ensures that client puzzles are generated using hash functions and seed generated by server automatically. And the handshake is done between the client and server for puzzle verification of p value as given in the OverDoSe technology article. OverDoSe ensures that targeted sites by the attacker is protected from DDoS attacks. It is intended for deployment by a single ISP who wishes to provide DDoS protection as a value-added service to its customers. Here, they run a series of DoS experiments on Emulab and validate the design of OverDoSe.

Finally, the existing work which indicates client puzzles protocols can be implemented for the resolution of DDoS attack is discussed in the article. The article suggests a three-way mechanism of deploying client puzzles as an initial screening of the legitimate and illegitimate users at the server end. Next, to make pre-computation attacks even more difficult, the hash function used to compute puzzles could be alternately changed. Lastly, to counteract the switching-load technique that attackers might use to defeat client puzzles during a DDoS attack, the server might ask clients to solve more than one puzzle during the protocol run.

III. Flaws in Related Work

A. TCP SYN Flood Attack

First part does not address the research problem by taking client puzzles generation and addresses the research problem in such a way that only TCP SYN attacks are handled properly. So, if some other network layer attack happens other than TCP, then it does not address that problem. Suppose, UDP attack is another network layer attack which is not addressed by the existing work by Part A.

B. OverDoSe Technology

Second part does address the research problem by taking client puzzles generation using hash functions. But there is

a defect in the OverDoSe technology, where the technology doesn't perfectly address the client with valid transaction of the client puzzles generation via bitcoins. Bitcoin concept is trending in the internet for today's generation and it missed that part because no one thought that bitcoin would be used for generation of client puzzles as it is not the hot topic in 2006. The OverDoSe technology is sufficient for DDoS attack at the time it has been released in 2006. Now as time flies, we need to think of more secure technology for probing the DDoS attack via client puzzle generation that is through bitcoins.

C. Client Puzzle Protocol for DDoS Attack

Third part does address the main part of client puzzle generation approach for mitigating the DDoS attack. The article makes it easy for a part of the work to be taken into consideration for resolving the flooding attack. In this proposal, I would like to make a point in generating the client puzzles through bitcoins and how effective it is for clients rather than simply generating the client puzzles for legitimate and illegitimate users. If every user, is given with the client puzzles then the success rate of solving the client puzzles will be going down. As, more people get to solve the different puzzles and puzzles solving success rate would be going down. Instead, the new approach is that only people who are in need of the server/website will pay some amount for client puzzle generation whenever there is a flooding attack possible at the server end. Then, the puzzle solving success rate would be higher as lesser number of people get to solve the puzzles effectively through their computer.

IV. Solution

A. Detection of DDoS Attack

Key Methodologies: I will use Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm. Paper cited as [**?**] indicates that we can use the proposed algorithm for real time detection of dataset for DDoS attack with efficiency rate as 98.835 percentage sapproximately. It generally uses K-Means Hybrid Feature Selection Algorithm which is semi-supervised machine learning algorithm.

Algorithm: In this algorithm, we can easily detect the attackers with a high detection rate and separate those clusters of attacker's source IP and filter them out at the server end for not allowing a valid established connection at the server end. Hence, the semi-supervised machine learning algorithm is successful in detecting the DDoS attacker's source IP and cluster them and make it hard for the source IP (attackers) to send request to server. So, the server will not accept these clustered source IP by the proposed algorithm. Hence, Défense mechanism will come into picture for not allowing the source IP of attackers which are fake. Now, comes the part in which after detection of the source IP by feature selection algorithm shown in [**?**] citation, we need to consider client puzzles for avoiding the detected source IP of the attackers.

	Puzzle	Puzzle Generation	Puzzle Solution	Puzzle Verification
Multiple-Hash	Find z1 <1,k> such that hash (z1< 1, k> | z1 <k + 1, L >) = z2	Determine k 2 hash	2^k hash	2 hash

Fig. 1. Screenshot of the Client Puzzle Verification done at server end and solved by the clients computer.

B. Generation of Client Puzzles through bitcoins

Key Methodologies: I will use algorithm proposed by citation [**?**] for generating the client puzzles for the Défense mechanism against DDoS attack. In this algorithm, there is a multiple hash function generated at the server end by taking input parameters as timestamp at which the server feels DDoS attack might happen and releases the puzzle, client ID and server secret code. Thus, a z1 is found out by hashing the values said above and hash(z1) is done to find out z2. And at last puzzle is generated for determining the k value and 2 hash functions are used. pow(2,k) hash functions are created and shown in the figure. For puzzle verification, 2 hash functions are created in such a way that puzzle generation must match the two hash functions created in the before step of puzzle solution.

Novelty in Research Idea: The novelty in research idea is that Bitcoin concept is used to authorize the puzzle generation at the initial step of client puzzle generation. In this research, I would like to use the bitcoins of clients (charged around 1 penny) for the generation of client puzzles, where it is used for avoiding DDoS attack clusters at the server end.

Algorithm: Firstly, I will detect the DDoS attackers source IP as clusters, as discussed in the algorithm section of Part 1 Solution. Next, I would like the client to authorize the money transaction at the client end which are received at server end to initialize a client puzzle. The client puzzle is then shown at the client end for solvation by computer. The puzzle is generated by taking the timestamp as one of the seed and some other parameters which can be discussed in detail in the Research Paper later in this semester. For the client to be authenticated, the client's solution is matched with the server calculated solution. If it is matched, then the client would be given access to the server and then he/she can use it. If it is not matched, client computer is given another chance to give the correct answer if and only if the source IP of the client is not in the blacklisted source IP of the DDoS attack clusters. If legitimate client is successful in giving out the answer, he will establish a connection to the server successfully. If at all, illegal users get the client puzzles, and were not able to answer the puzzles generated by the server. Then, the source IP is tracked down and clustered with DDoS attackers source IP. In

this way, whoever gets the second chance are legit clients and who cannot solve the puzzle at second time are illegal users.

V. Outcome

Outcome of the research is time in which the DDoS attack can be avoided by generating client puzzles. This time can be viewed at different datasets for DDoS attacks and multiple client puzzles given to the client's computer to solve the puzzle. The time parameter consists of detecting the attack by the algorithm (td) and puzzle solvation by client's computer (tp). The two parameters td and tp are calculated and printed out by the program at last of the results. Expected outcome of the research is the robust software algorithm which can detect the DDoS attacks with accuracy and showing us the illegitimate users. And legitimate users are charged with bitcoins. These bitcoins are used as a generation of hash function related client puzzles. And client computer has to solve the puzzle for avoiding the DDoS attack that is going to happen to the accessed server by the client.

A. Dataset used for performance evaluation

The Dataset used for network layer attack (TCP and UDP attacks) are shown in the mendeley website. Its citation is given in references for the dataset used in the research. Performance evaluation is shown by giving out time for the detection of DDoS attack (td) by the above dataset.

B. Expected Results

A robust system of current generation tools generally detects DDoS attack and client puzzles solvation combinedly takes time of 10 minutes. But I would like to use Bitcoins concept for client puzzles generation and the time is expected to be less than 10 minutes. The main goal of the research is to decrease the time from 10 minutes and showing a new angle of generation of client puzzles which is never shown in the world how cryptocurrency can be used to generate client puzzles solvable by computers.

TABLE I
Time Frame

Week	Date	Work Done
1	9/13-9/19	Training the Dataset with Machine Learning algorithm and detecting between Legitimate and Illegitimate Users
2	9/20 - 9/26	Analysing the Legitimate Users and characterisation between what type of attack is going to happen by illegitimate users at the server end
3	9/27 - 10/3	Optimal Method of recognizing the attack and characterising the TCP/UDP attack in the Dataset trained is shown as part of the Research
4	10/11 - 10/17	Puzzles generation for resolution of DDoS attack is done in a large database of puzzles created via hash functions
5	10/18 - 10/24	Client Authorization using bitcoins and give the required clients with puzzles solvable by computers
6	10/25 - 10/31	First level of analysis of the algorithm created to use the client puzzles generation through bitcoins
7	11/1 - 11/7	Optimal method of client puzzles for solvation through Computer when a DDoS trigger is created
8	11/8 - 11/14	Final Analysis and testing of the algorithm on various clients when DDoS attack is triggered
9	11/15 - 11/21	Removal of bugs after testing with several scenarios considered for Client Puzzle Generation for DDoS attack
10	11/22 - 11/28	Showcasing the final product and result of how low the parameter time is for solving the client puzzles to avoid DDoS attack to the class

Acknowledgment

I acknowledge Dr. Qi Liao for giving out the idea to use bitcoin in generating the client puzzles for resolving the DDoS attack.

References

[1] Vicky Laurens, Abdulmotaleb El Saddik and Amiya Nayak. (2006). Requirements for Client Puzzles to defeat the Denial of Service and the Distributed Denial of Service Attacks. The International Arab Journal of Information Technology, Vol 3, No. 4.

[2] Elaine Shi, Ion Stoica, David Andersen and Adrian Perrig. (2006). OverDoSe: A Generic DDoS Protection Service Using an Overlay Network.

[3] Kumarasamy, Saravanan and Gowrishankar, A.. (2012). An Active Défense Mechanism for TCP SYN flooding attacks. arXiv:1201.2103 [cs.CR]

[4] N. A. Fraser, D. J. Kelly, R. A. Raines, R. O. Baldwin and B. E. Mullins, "Using Client Puzzles to Mitigate Distributed Denial of Service Attacks in the Tor Anonymous Routing Environment," 2007 IEEE International Conference on Communications, Glasgow, 2007, pp. 1197-1202, doi: 10.1109/ICC.2007.203.

[5] Suresh M., Anitha R. (2011) Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. In: Wyld D.C., Wozniak M., Chaki N., Meghanathan N., Nagamalai D. (eds) Advances in Network Security and Applications. CNSA 2011. Communications in Computer and Information Science, vol 196. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22540-6-42.

[6] Gu, Y., Li, K., Guo, Z., and Wang, Y. (2019). Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm. IEEE Access, 7, 64351-64365.