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 mining programs are sent to IP addresses which are detected as DDOS traffic and bitcoins generated are reverted to the account of the server. And, Client puzzles go to the IP addresses which are detected as Benign traffic and clients need to solve the human solvable puzzles to access the website. So, whoever solves the client puzzles can access the website. Thus, the research plays a vital role in designing client puzzles which are not solvable by DDOS bots and only solvable by humans who are legitimate clients.**

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 as cited in paper [3]. 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 as cited in paper [1], [4]. 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.

TABLE I
Confusion Matrix Results

Confusion Matrix	Predicted DDOS	Predicted Benign
Labelled DDOS	1662237	414181
Labelled Benign	223556	1912448

II. Literature Overview of Research on DDOS

A. Detection of DDOS Attack

The detection of DDOS attacks can be explained in the paper cited as [5]–[10]. In the article cited, it is mentioned that DDOS attacks happen now and then. And different papers mention the evaluation metrics and best Machine Learning Algorithm for detecting the DDOS attacks have been given in the papers. The research mainly focuses on the paper cited in [7]. The paper mainly focuses on how differently we can use the different known Machine Learning Algorithms for evaluating a particular traffic to DDOS and Bengin Dataset based on the training of the dataset. In the research, we split the train and test data into 70-30 ratio. Here, 70 percent will be training dataset and 30 percent will be testing dataset. And accuracy obtained for the test dataset is around 85 percent with False Negative as 5.3 percent and False Positive as 9.8 percent.

B. Client Puzzles for Benign Traffic

The Client Puzzles section mainly focuses on decreasing the False Positive Source IP's. The False positives are the main cause of DDOS attackers who get detected as Benign samples. So, inorder to attack these samples, we give client puzzles as cited in the papers [1], [4], [11]–[14]. The client puzzles generated for the False Positive Samples are looking after the samples which attacker try to get the access to the website. If the attacker get access to the website, then the research is wasted. So, the research primarily focuses on stopping the attackers with the client puzzles as we give human solvable puzzles to the source IP's predicted as benign traffic.

C. Bitcoin Mining Program for DDOS Traffic

The Bitcoin Mining Program is send to the traffic for False Negative Source IP's. The False Negatives are the main cause of Genuine people who get detected as DDOS dataset unkowningly by the Machine Learning Algorithm used in the research. So, inorder to benefit the server in the form of

bitcoins, we give bitcoin mining program to users of genuine people and ask them to run the program as cited in the papers [15], [16]. The bitcoin mining program generates bitcoins to the server and we get benfited with the bticoins generated by linking generated bitcoins to a server account where he can redeem those bitcoins automatically by clicking on redeem option.

III. 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 as cited in paper [3]. 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 as cited in paper [2]. 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 [1], [4]. 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.

IV. 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.

V. Literature of Dataset

The citation [7], [17] gives the link for DDOS dataset and how the dataset is been generated for required DDOS dataset from the Canadian website where 85 attributes are mentioned in the article. The attributes which are considered mainly in the link provided are Flowid, Timestamp, Fwd Seg Size MIn, Src IP, Dst IP, Flow IAT Min, Src port, Tot Fwd Pkts, Init Bwd Win Bytes. I acknowledge Devendra for giving out the blanaced dataset of the DDOS dataset which has 50-50 of Benign samples and DDOS samples respectively. The dataset is then analysed for further research on how to use Naive Bayes Machine Learning Algorithm.

VI. Solution

A. Detection of DDoS Attack

Key Methodologies: I will use Naive Bayes Machine Learning Algorithm for the detection of DDOS Traffic from the total dataset. Paper cited as [7] indicates that we can use the proposed algorithm for real time detection of dataset for DDoS attack with efficiency rate as 85 percentage approximately. It generally uses Bernoulli's Naive Bayes Library for modeling the data and predicting the values of the type of dataset whether it is good or bad based on feature extraction done in Naive Bayes Algorithm.

Algorithm 1 Naive Bayes Machine Learning Algorithm

procedure SHORTREPEAT(Dataset)
    read csv file from the path
    preprocess columns to float type
    Splitting the dataset into train and test data
    Detection Time is evaluated using Bernoulli NB
    Evaluation Metrics and ROC curve is shown
end procedure

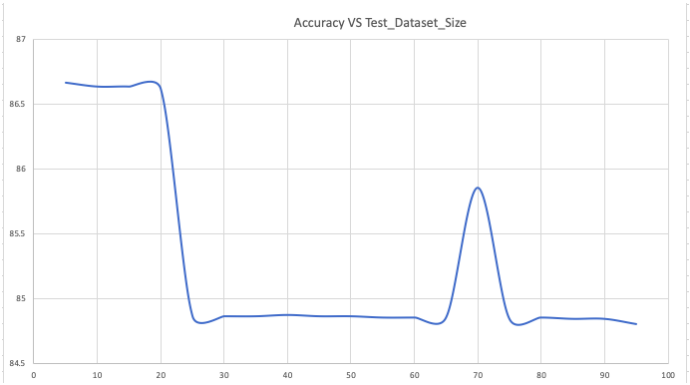

Fig. 1. Screenshot of the accuracy versus test data size taken in terms of percentage of total dataset size.

B. Algorithm for Detection

Algorithm: In this algorithm, we can detect the DDoS traffic with 85 percent accuracy on average and algorithm is shown in Naive Bayes Machine Learning Algorithm. The algorithm uses preprocessing of the data and converting every non-float data type to float data type by fitting the values using Label Encoder in scikit-learn.preprocessing library. The algorithm proposed by [7] is modified according to the accuracy said in the paper and achieved 85 percent accuracy on average. Please see figure Screenshot of accuracy versus test data size taken in terms of percentage of total dataset size for variation of accuracies with the increase of data from 5 percent to 95 percent of the total dataset. Please see figure Screenshot of ROC curve of NB Machine Learning Algorithm for keen observation of characteristics of False Positive Rates vs True Positives Rate in the ROC curve.

C. Generation of Client Puzzles and bitcoins

Key Methodologies: I will use algorithm proposed by citation [1] 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

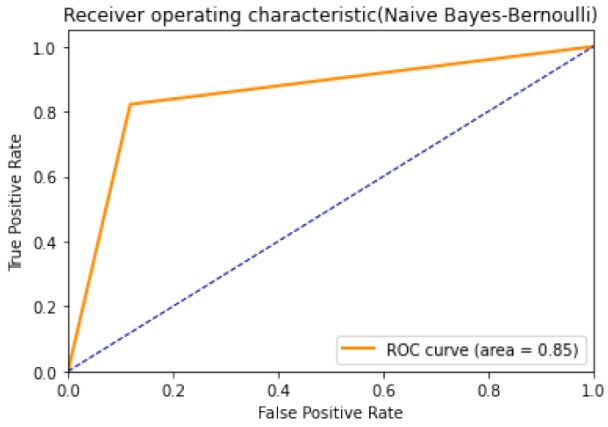

Fig. 2. Screenshot of ROC curve of NB Machine Learning Algorithm.

the two hash functions created in the before step of puzzle solution.

Algorithm 2 Client Puzzle and Bitcoin generation alogrithm

procedure SHORTREPEAT(Puzzles and Bitcoins)
    PuzzleSolved = 0
    for every Label **do**
        $length \leftarrow ipArrayLength$
        for $i \leftarrow 0$ to $length - 1$ **do**
            if Label[i] = 'Benign' **then**
                $ClientIP \leftarrow Puzzle$
                while PuzzleSolved = 0 **do**
                    Wait until puzzle is solved
                    PuzzleSolved = 1
                end while
                if PuzzleSolved =1 **then**
                    Access to Website
                end if
            end if
            if Label[i] = 'DDOS' **then**
                $AttackIP \leftarrow BitcoinMiningProgram$
                Makes attackers to generate bitcoins for the server
            end if
        end for
    end for
end procedure

Novelty in Research Idea: The novelty in the research is that bitcoin mining programs are never used on attackers to generate bitcoins. In this research, I would like to use bitcoins generated by attack IP samples to store in the server account of bitcoins. Thus, the novelty in research comes into play how to generate bitcoins from the attackers not letting them know that they have been running the bitcoin mining programs on the bots.

	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. 3. Screenshot of Client Puzzles cited in references of Vicky Laurens.

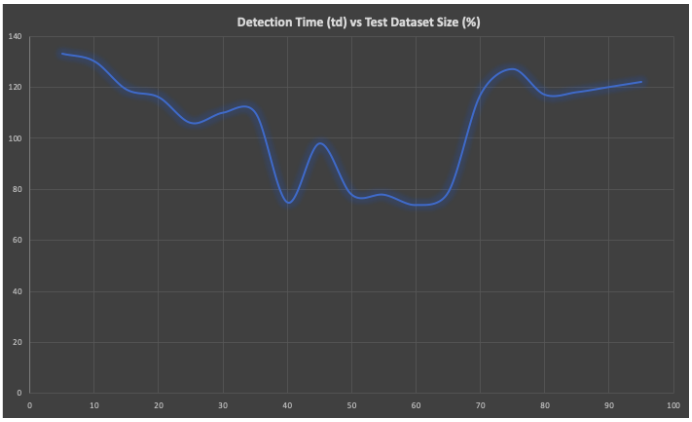

Fig. 4. Screenshot of the detection time versus test data size taken in terms of percentage of total dataset size.

D. Algorithm for Client Puzzles and Bitcoin generation

Algorithm: Firstly, there are four types of IP based on the testing dataset and predicted dataset of the label column. They are as True Positive , False Negative , False Positive and True Negative. True Positive means a labelled DDOS sample is also predicted as DDOS Traffic by the ML algortihm. False Negative means a labelled DDOS sample is predicted as Benign Traffic by the ML algorithm. False Positive means a labelled Benign Sample is predicted as DDOS traffic by the ML algorithm. True Negative means a labelled Benign Sample is predicted as Benign Traffic by the ML Algorithm.

Here, Supervised ML algortihm is used where we have labelled dataset with us from the starting. So, we can easily eliminate True Positive and True Negative samples as they are the correct predictions done at the USER end. Now, comes the main role of the second part of the research where False Negative which are costly than False Positives are stopped by simple approach. False negatives says that Benign traffic as predicted by the ML algorithm and we can just give human solvable computer puzzles like GOOGLE CAPTCHA for the server to know that bad traffic is not touched with the access to website. False positives says that DDOS traffic as predicted by the ML algorithm and we can give bticoin mining program like redirecting them to cgminer programs in the server and let the good clients run those programs for the benefit of the server. And, after one cent is depostied by the good clients bitcoin mining program, the server gives access to the website.

VII. 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 (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 of greater than 90 percent and showing us the illegitimate users. And client IP's has to solve the puzzle for avoiding the DDoS attack that is going to happen to the accessed server by the client. And attacker gets into the loop of the bitcoin mining program where he gets stuck in generating bticoins to the server and cannot access the website atlast.

A. Dataset used for performance evaluation

The Dataset used for network layer attack (TCP and UDP attacks) are shown in the [17]. 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 stopping the DDOS attack by predicting the samples with more accuracy. Eventhough the accuracy of the ML algorithm is less than 90 percent in the initial stage of the research and as further research the DDOS traffic cannot get access to the website as they are stuck at generating bitcoins to the server.

Acknowledgment

I acknowledge Dr. Qi Liao for giving out the idea to use bitcoin mining program for attackers and client puzzles for clients to mitigate 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]

TABLE II
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

[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.

[7] M Devendra Prasad, Prasanta Babu V, C Amarnath, "Machine Learning DDoS Detection Using Stochastic Gradient Boosting", International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.157-166, 2019.

[8] Balkanli, E., Alves, J., and Zincir-Heywood, A. N. (2014, December). Supervised learning to detect DDoS attacks. In 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS) (pp. 1-8). IEEE.

[9] Idhammad, M., Afdel, K., and Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. Applied Intelligence, 48(10), 3193-3208.

[10] Kim, M. (2019). Supervised learning-based DDoS attacks detection: Tuning hyperparameters. ETRI Journal, 41(5), 560-573.

[11] Wang, X., and Reiter, M. K. (2004, October). Mitigating bandwidth-exhaustion attacks using congestion puzzles. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 257-267).

[12] Wang, X., and Reiter, M. K. (2003, May). Defending against denial-of-service attacks with puzzle auctions. In 2003 Symposium on Security and Privacy, 2003. (pp. 78-92). IEEE.

[13] Chen, L., Morrissey, P., Smart, N. P., and Warinschi, B. (2009, December). Security notions and generic constructions for client puzzles. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 505-523). Springer, Berlin, Heidelberg.

[14] Suriadi, S., Stebila, D., Clark, A., and Liu, H. (2011, July). Defending web services against denial of service attacks using client puzzles. In 2011 IEEE International Conference on Web Services (pp. 25-32). IEEE.

[15] Haghighat, A. T., and Shajari, M. (2019). Block withholding game among bitcoin mining pools. Future Generation Computer Systems, 97, 482-491.

[16] Wu, S., Chen, Y., Li, M., Luo, X., Liu, Z., and Liu, L. (2020). Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools. IEEE/ACM Transactions on Networking, 28(2), 874-887.

[17] Dataset URL: https://www.kaggle.com/devendra416/ddos-datasets