IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Comparative Study of Algorithms used for traffic Engineering during DDOS Attacks

Sufiyan Khalid Shaikh
Student, Master of Computer Applications
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

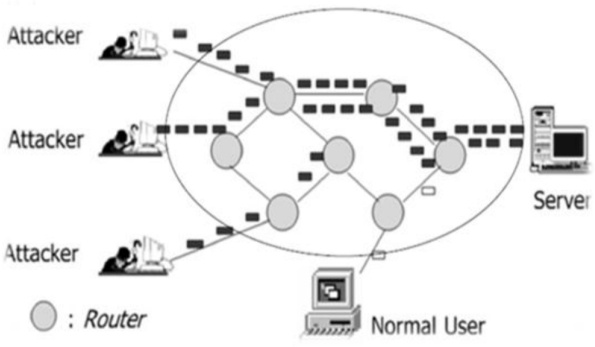
Abstract: *This paper proposes a study of distributed denial-of service attacks and a study of the defence mechanism that strive to counter these attacks. The attack illustrate do using both known and potential attack mechanisms along with this classification we discuss important feature.So each attack category that in turn define the challenge involved in combating these threats. Distributed Denial of Service (DDOS) attacks Have become a large problem for users of computer Systems connected to the Internet. In this paper we will se comparisons of various algorithms used for traffic engineering during DDos attack.*

Keywords: DDOS, Threats, Traffic Engineering, Algorithm

I. INTRODUCTION

Distributed denial-of-service attacks (DDOS) pose an immense threat to the Internet, and consequently many defence mechanisms have been proposed to combat them. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. The DDOS field is evolving quickly, and it is becoming increasingly hard to grasp a global view of the problem. DDOS means there are more than one object which is DOS attacker (either automated tools or human) . A DDOS attacker can greatly reduce the quality of a target internet service or even can completely break the network connectivity of a server generally to achieve resource overloading, a DDOS attacker will first compromise a large number of hosts and subsequently instruct this compromised host to attack the service by exhausting a target resource. A Distributed Denial of Service (DDoS) attack is a distributed, coordinated attack on the availability of services of a host server (application server, storage, database Server, or DNS server) or network resource, launched indirectly through many compromised systems called botnets on the Internet. Multiple compromised systems are used to attack a single target. Since a DDoS attack is launched from multiple sources, it is often more difficult to detect and block than a DoS attack. Nowadays Internet Services become crucially important. Therefore, degradation of service quality or total denial of service can be critical. Denial of Service (DoS) attack goals to stop legitimate users from accessing network or system resources. Attacks driven from more than one node / sources in an Internet traffic it is recognized as a Distributed Denial of service (DDoS) as illustrated in Fig.1.[1]

To blast-off a DDoS attack there are mostly two methods. The first method is taking advantage of design defects of the network. Attackers send some mimicry packets to the target server to confuse an application running on target. The second method adopts flooding traffic that either exhausts bandwidth or resource of the server. The chief targets of attack launcher are routers, links, firewalls, victim's computer and network infrastructure, victim OS, current communications and victim's application



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

There are two main challenging features of DDoS. One is DDoS packet manages to seem as genuine packets which are not able to clarify without any influence is puzzling. Second is nearly impossible to find out the source path of an intruder due to the spoofed IP address. Due to these two main weaknesses, the network systems have often become the targets of various attacks which are transmitted illegally gain approach to useful resources. DDoS may arise due to extreme need of trustworthy users for specific resource such as flash crowd and make the server overloaded. DDoS are acute concerns for companies that have been integrating their technology to public network, allowing multiple parties or users to access data. As stated by the research and educational communities there is a noteworthy growth in frequency and size of targeted network by the year 2015 is 20 percent of service provider repeatedly report attack over 50Gpbs. The percentage of suspects sighted application-layer attacks endures to rise, up to 93 percent this year, from 90 percent last year and 86 percent in 2013.Mostobserved DDoS attacks are still comparatively small with 84 percent of observed events less than 1 Gbps in size. There is a proportion 760 Mbps attacks this year. In the world of internet, it is not considered as a large amount but it will surely degrade the business and other related firms severely in their functions. In the statistics of ATLAS data on attack duration there is an increase of about 1% from the previous two years which lasted for less than one hour. The average attack duration in 2015 was 58 minutes, which is relatively consistent with previous results.[1]

II. RELATED WORK

2.1 Proposed Algorithm

The proposed work is focused on traffic flow analysis of both usual and malicious traffic. In initial stage, aim of the proposed algorithm is serve the entire incoming traffic request including both genuine requests as well as illegitimate request within time-slots. As shown in Fig.2, time-slot (T) 210s is divided into 30s for the observation of all incoming packets and after that it will record in observation table 2. This table describes the flow of packets along with the source and destination information and categorize according to its type in time-slots group (TGn). If server capacity (c) < frequency of packet (f), then observation TG1, TG2 ,.. TGn in time-slots and record it. Else from observation table find out the frequently repeated IP address for sending the challenge through CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart).[1]

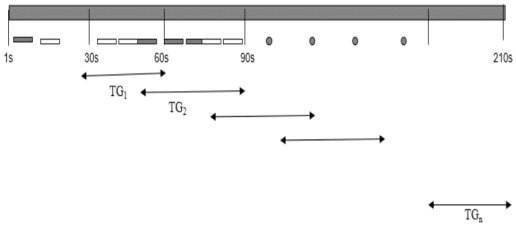


Fig.2 Traffic flow

Table: Observation Table

Time-slot Group	Address Pair	Packet Type
TG_1	<src,dest>, <src,dest>…<src,dest>	ICMP, Ping, IPv4 packet, TCP,UDP etc.
TG_2	<src,dest>, <src,dest>…<src,dest>	
TG_3	<src,dest>, <src,dest>…<src,dest>	
.	.	
TG_n	.	

The proposed algorithm explains the process of traffic analysis with respect to server capacity (c) and types of packets in pre-defined time-slots (T) with arrival frequency of packets (f). In the algorithm, first initialize the capacity (c) of destination server for every incoming packet within predefined time-slot (T) is monitor and record the information such as address pair (source address, destination address), packet type, source and destination port address etc. This process is continuing till the serving capacity of detonation server. If it exceeds the c then the algorithm determined the repeated IP address from recorded information during step 2. After that, step 4 execute for sending the challenge using CAPTCHA.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

All the CAPTCHA responses are served considering it as a genuine. Discard the traffic for those IP which doesn't get ack. This observation keep alive in next consecutive time-slot

Proposed Algorithm

Step1: Initialize observation slot T, frequency of packet f, destination capacity c.
Step2: Monitor flow of arrival of request and serve till destination capacity c and record duplicate pairs <src,dest>, packet type.
Step3: 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 CAPTCHA
Step 5: Serve only the CAPTCHA responses and drop other packets.
Step6: Observe traffic flow in next consecutive time-slots T.[1]

DDOS Attack detection algorithm based on Hybrid Traffic Prediction Model

A) The Block Diagram of DADA-HTPM

The DADA-HTPM includes two main parts: the hybrid traffic prediction model and the DDoS attack detection algorithm. The block diagram of DADA-HTPM is shown in Fig. 1.[6]

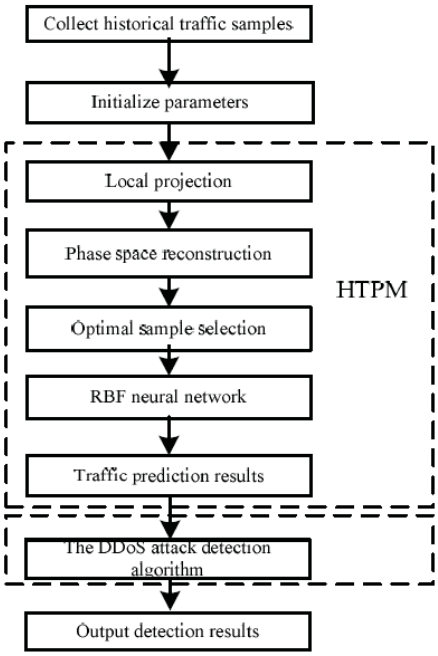


Fig.1 The block diagram of DADA-HTPM algorithm

As can be seen from Fig. 1, the DADA-HTPM algorithm includes two main parts: HTPM and the DDoS attack detection algorithm. The historical traffic samples are collected and the parameters are initialized first. Then the traffic is predicted by HTPM. Local projection and phase space reconstruction are used to restore the chaos of original traffic. Optimal space selection is introduced to select the suitable traffic samples which improves the prediction performance and reduces the complexity. The RBF neural network is introduced to predict the future traffic based on the selected samples. After HTPM, the traffic prediction results are used to detect the DDoS attack based on the DDoS attack detection algorithm. At last, we output the detection results

A hybrid traffic prediction model is proposed. The detailed steps are as follows:

Step 1: Make local projection and denoise the collected historical samples to eliminate the influence of high dimensional noise.

Step 2: Reconstruct the phase space.

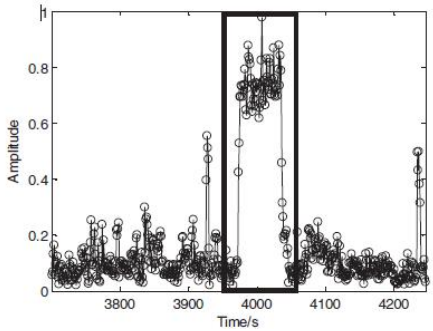
Step 3: Select the most relevant samples according to the optimal sample selection algorithm.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Step 4: RBF neural network is used for sample training and traffic prediction.
Step 5: Output the prediction results.[6]

B) The Hybrid Traffic Prediction Model
Input: the historical traffic samples
Output:"DDoS attack"
1. for t=1:M
2. predict the traffic value s(t+1) based on historical traffic
samples and calculate the average value ave_s(t) ;
3. if s(t+1)>α·ave_s(t)
4. save s(t+1) into set G
5. for b=1:q
6. if s(t+1+b)>α·ave_s(t)
7. save s(t+1+b) into set G
8. calculate the variance of G and get var(G) ;
9. if var(G)<β
10. continue
11. else
12. break
13. end if
14. else
15. break
16. end if
17. end for
18. return "DDoS attack"
19. t=t+1+b;
20. else
21. t=t+1;
22. end if
23. end for
[6]

C) The DDoS Attack Detection Algorithm
When DDoS attack occurs, the network traffic increases and tends to steady which is shown as "high platform". An example of DDoS attack is shown in Fig. 1.[6]



According to above traffic characteristics of DDoS attack, we propose the DDoS attack detection algorithm and the traffic characteristics of DDoS attack is shown as "high platform", in which the traffic suddenly increases and tends to steady. We use the threshold α to judge the increasing of traffic and the threshold β to judge the stability after traffic increasing. If s(t+1)>α·ave_s(t), we begin to judge if the next b values from s(t+1) to s(t+1+b) are all larger than s(t) and if their

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

values are approximate equal based on the variance. If they are all larger than s(t) and they are approximate equal, we will output "DDoS attack".

Matching Pursuit Algorithm

MP is a sparse signal representation method that pretends linear approximations of signals, by iteratively projecting them over a set of atoms selected from the dictionary. The dictionary of the MP algorithm can be a predened structured dictionary built from a mathematical model. Also, the dictionary can be generated directly from sample data. Structured predened dictionaries consist of atoms formed from expansions of a single basis, such as Wavelet or Fourier. On the other hand, generating the dictionary from sample data often leads to better representation and can yield better results in many practical applications.[5]

To achieve a sparse representation of a given signal y 2 Rn using an over-complete dictionary D 2 RnxK , we define the representation of y D Dx or y _ Dx subject to k y-Dx kp_ _ for some small number _. The sparsest representation is the solution to either :

$\min||x||0$ subject to $y=Dx$ (1)

or $\min_x|| x ||0$ subject to $||y-Dx|| \leq e$ (2)

where $||.||_0$ is the L_0 norm of a vector.

The MP algorithm decomposes any vector y 2 H in a Hilbert space over a redundant dictionary D D 1;_2 : : : ;_K _ H, where _i 2 H is an atom in the dictionary, i is the index of the atom, and x 2 RK contains the representation coefficients of y.

In the first step, to achieve the best sparse decomposition of signal y, we have to find atom that has the highest inner product with the signal y. First residual r is equal to the entire signal r0 D y. In order to minimize the energy of residual r1, the algorithm starts with finding α_0 that gives a maximum projection of y

$\alpha_0 = \arg\max (y,\alpha_i)$ (3)

The residual is updated by subtracting α_0 times its magnitude of projection c0 from y:

$y1=y-c_0\ \alpha_0$ (4)

where c0 D hy;_0i is called coefficient of _0 This process continues iteratively by projecting ri on dictionary atoms and updating ri+1. After m iterations y can be written as:

$$y= \sum_{i=0}^{m-1} c_i\ \alpha_i - r_m \quad (5)$$

The residual can be written as:

$R_m=y-Dx$ (6)[5]

Alarm Generation

For every time window in the test dataset, a characteristic feature vector is obtained using the feature generation module. These feature vectors are decomposed by the MP algorithm using the dictionaries obtained from the dictionary generation module. The abnormality indicator value is calculated from the resulting residual vectors as follows:

Algorithm 1 AMP Alarm Generation Pseudo-Code[5]

Input: Dictionary generated from training dataset D, characteristic feature vectors Y D fy1; y2; : : : ; yk g, maximum number of iterations M, threshold _ , maximum number of time windows k.

Output: Alarm

Initialization; i ← 1

Repeat: Find

$R_M= y_i-\sum^{M-1}_{i=0} c_i\alpha_i$

Using D and MP algorithm.

Alarm generation

if $\psi \leq$ $alarm_i= 0$ else $alarm_i= 1$

Until: i = k [5]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

III. CONCLUSION

In this paper, a DDoS attack detection algorithm based on HTPM is proposed which includes the HTPM and DDoS attack detection algorithm. In HTPM, local projection, phase space reconstruction and optimal sample selection algorithm are used to restore the chaos of network traffic and select suitable network traffic samples. Then, the training of network traffic samples and the accurate prediction of future traffic are realized based on RBF neural network technology. In this study, we propose the AMP method for DDoS detection that uses the MP algorithm. We also introduce the characteristic feature vector generated from a combination of multiple one-dimensional traffic attributes. Furthermore, in this study, adaptation to the traffic data to the MP algorithm is provided by creating dictionaries from the training dataset. Because there is no recent study that uses the MP algorithm in the detection of DDoS attacks, the proposed methodology is compared with the MPMP and Wavelet methods. It is precisely a necessity to remove the burden of illegal packets due to DDoS attacks in a network/Internet. This paper makes remark on several vulnerabilities that explicitly attempts to interrupt legitimate user access to services at application and transport layer of TCP/IP. Hence, it is necessity to reduce the DDoS attack from synchronous and non-synchronous traffic flow. The proposed work is able to observe some suspicious or spoofed IP addresses using recorded information for both synchronous and non-synchronous traffic flow during time-slot. Furthermore, it marked address pairs that are authenticated by challenge response mechanism i.e. CAPTCHA while other packets are dropped. In extension to this paper, the proposed work will be simulated the results with dataset and tools in future.

After studying all the algorithms used for traffic engineering during DDOS we came to know That the HTPM(Hybrid Traffic Prediction Model) is best among all the algorithms shown in this paper.

REFERENCES

[1]. A Mechanism for Prevention of Flooding based DDoS Attack Nipa Patani1 and Rajan Patel2 Sankalchand Patel College of Engineering, Visnagar-384315, India.

[2]. Saranya, R., S. Senthamarai Kannan, and N. Prathap: A Survey For Restricting The DDOS Traffic Flooding And Worm Attacks In Internet.In:2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Pp. 251-256, IEEE (2015)

[3]. Q1State of the Internet / Security Report, https://content.akamai.com/PG6292-SOTI-Security (2016)

[4]. Bhandari, Abhinav, A. L. Sangal, and Krishan Kumar: Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks. In: International Journal of Computer Network and Information Security 7, no. 8 (2015)

[5]. DERYA ERHAN , (Member, IEEE), AND EMIN ANARIM Electrical and Electronics Engineering Department, Bo§aziçi University, 34342 Istanbul, Turkey Corresponding author: Derya Erhan (derya.erhan@boun.edu.tr) This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) through the Cloud-Based Privileged Access Management Systems Project under Project 117R030.

[6]. Yuze SU Information and Navigation College Air Force Engineering University Xi'an, China Xiangru MENG Information and Navigation College Air Force Engineering University Xi'an, China Qingwei MENG Information and Navigation College Air Force Engineering University Xi'an, China Xiaoyang HAN Information and Navigation College Air Force Engineering University Xi'an, China DDoS Attack Detection Algorithm Based on Hybrid Traffic Prediction Model

[7]. A. Sanmorino, R. Gustriansyah, "An alternative solution to handle DDoS attacks," J. Theor. Appl. Informat. Technol., vol. 96, pp. 657- 667, March 2018.

[8]. J. Zheng, Q. Li, G. Gui, J. Cao, K. David, Y. Yau and J. Wu, "Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis," IEEE T. Inf. Foren. Sec., vol. 13, pp. 1838-1853, July 2018.

[9]. P. O. Tiago, S. B. Jamil and S. S. Alexsandro, "Computer network traffic prediction: a comparison between traditional and deep learning neural networks," Int. J. Big Data Intel., vol. 3, pp. 28-37, January 2016.

[10]. Z. Tang, T. Peng and W. Wang, "A local least square support vector machine prediction algorithm of small scale network traffic based on correlation analysis," Acta Electronica Sinica., vol. 63, pp. 130504, July 2014.

[11]. B. Yang, "Small-time scale network traffic prediction based on complex-valued neural network," Mat. Sci.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Eng. R., vol. 224, pp. 012044, July 2017.

[12]. J. Li, X. Liu and Z. Han, "Research on the ARMA-based traffic prediction algorithm for wireless sensor network," J. Elec. Informat. Technol., vol. 29, pp. 1224-1227, May 2007.

[13]. D. Zhou, S. Chen and S.Dong, "Network traffic prediction based on ARIMA model," Int. J. Comput. Sci. Issu., vol. 6, pp. 106-111, June 2012.