ISSN:0975-9646

A Model for Detection of Application Layer Denial of Service Attacks using Group Testing Theory

Shazia Shafi, Sanjay Jamwal

Department of Computer Science,
Baba Ghulam Shah Badshah University,
Rajouri, J&K, India

***Abstract*— Computer network technology is a very important technology for most of the applications. So security for these applications is most important. As network security is a great requirement in the growing networks, there is a lack of security techniques that can be implemented easily. Everyday a number of attacks are launched. There are different categories of attacks. Some of them are used to gain personnel information and some are used to interfere with the intended function of the system. Some attacks are used to consume all the resources of the system uselessly. Among different categories of security attacks, Denial of Service Attack is considered as the most dangerous type of attack. Denial of Service Attacks are increasing exponentially in the today's world of internet. These attacks are one of the critical issues in the network security. These are consuming the bandwidth and all the services of the target computer. In Denial of Service Attacks, Application Layer Denial of Service Attacks are more harmful as these attacks are harder to get detected. Many methods have been proposed so as to detect and mitigate Application Layer Denial of Service Attacks. In this Paper, we propose a security model for the detection of Application Layer Denial of Service Attacks. Here we have used the Group Testing for proposing the model for Detection of Application Layer Denial of Service Attacks.**

***Keywords*— Denial of Service Attack,Passive Attacks.Active Attacks, Masquerade, CAPTCHA ,Group testing.**

I. INTRODUCTION

With the increase in the network of the internet there is an exponential increase in the number of the attacks. So there is a great need of the security of the network [1]. With the advent of internet today's world is becoming more connected, so large number of personnel, organisational, military and government information is being transmitted over the internet. Therefore there is a great importance of network security as the most important information can be easily acquired through the internet.

A. *Network Security attacks:*

Security attacks may be defined as any attempt that endangers the security of the data owned by any organization. These attacks are divided into many categories. Some of the attacks are used to gain personnel information or system knowledge. Other attacks are used to interfere with the intended function of the system. Some attacks are used to consume all the resources of the system uselessly. Security attacks are classified as active and passive attacks.An active attack is that type of attack in which the attacker tries to alter the resources of the system or affects the operations of the system. A passive attack is that type of attack in which the attacker tries to make use of the data from the system but does not affect the resources of the system [2].

1) Passive attacks: Passive attacks monitor the traffic and transmission of the data. The aim of the attacker is to gain knowledge of data that is being transferred. There are two types of the passive attacks: "Release of message content" and "Traffic analysis".

2) Active attacks: Active attacks are that type of attacks that involve the alteration of the data or involve the forming of the false data stream. Active attacks are divided into four types: Masquerade, Replay, Modification of the messages and Denial

Denial of service attacks actually inhibits or prevents the normal use of communication facilities. It can disrupt the whole network either by overloading the network with the message so that the performance of the network gets degraded or by disabling the network. It can either have a particular target or it can degrade the whole network.of service attacks.

II. PROBLEM DEFINITION

Denial of service attacks have become a serious threat in the internet security. In these attacks, the attacker in a short span of time sends a large data to the server which does not make the service available to the legitimate users. These attacks are done easily but are harder to get detected. Previously a large amount of work has been done on the detection of application Denial of Service attacks but all the methods are having some limitations that prevent the complete detection of this attack. Previously the work done

on detection of Application Denial of Service Attacks was based on the DDOS shield and CAPTCHA-based but these methods need the session validation that becomes an overhead for each session. The previous work done on detection of application denial of service attacks was effective to some extent. This leads to selecting an effective model for detection of application denial of service attacks. So to propose a new solution for detecting the attack is the main aim of this paper.

III. Group Testing Theory

In detection of application denial of service attacks the main problem in identifying the attackers is in how to group together the clients on each server so that when a server is attacked, we can easily identify the attacker without analysing each request. So here we use group testing theory for the detection of application denial of service attacks with high efficiency and accuracy. In group testing technique attackers can be detected based on the performance of the attacked resources and there is no need to track each request. We have proposed a model, which will be used for the detection of application denial of service attacks using the group testing theory.

IV. Analysis of DOS Attacks and Group Testing Theory

A. *Analysis of DOS Detection Techniques:*

In [3], the author has proposed the CAPTCHA test against Application Layer Denial of Service Attacks. This technique is human solvable and can eliminate zombie machines, but the technique also eliminates the service requested from legitimate automated client and also brings an additional operation at the client end, that may delay the customer from receiving services. Also in [2] the author used the inter-arrival time distribution. These methods study the behaviour of the traffic and filter out the malicious packets but need to check each session which increases the overhead of the system. DWARD defence technique [4] is also used for detection and defence against Denial of Service Attacks. This technique is used at source end and detects all the outgoing malicious traffic, but in this technique there is a large overhead employed at router which decreases the performance of network. In [5] the author has made use of a victim-and technique that observes the time-to-live value of all the incoming packets, but this technique is valid only for static IP address only. Also a technique known as SYN cookie [3] was proposed that stored the SYN/ACK packet authentication information. But this technique also needs a large amount of values to be calculated so there is a large use of resources and computation power. In [6] the author has made an attempt to distinguish between DOS attacks and flash crowd by making the use of hybrid probability metric. This also became an overhead as it needs to calculate the differences between the traffic rates, access dynamics and source IP address distribution for examining the abnormalities in the traffic. In [7], the author has proposed a fundamental model for the detection of illegitimate users. In this model the author has made use of group testing and the aim of this model is to offer a universal defence to all the type of attacks. The author has made various algorithms and after the analysis of these algorithms it shows that these algorithms identify all the illegitimate users in short detection time.

On the basis of the previous work done on Denial of Service Attacks there is a need of an improved system that overcomes these drawbacks. On that basis we have come on a conclusion that it would be much better to test the clients in a group instead of testing them one by one, as it can easily identify the attacker and save much time. But the issue was how to group the clients and plot them to different servers for finding illegitimate traffic. This issue is same to that of the group testing theory that detects the infected items out of a large pool by performing a few numbers of tests only. So we have proposed to apply group testing to detect Application Layer Denial of Service Attacks.

B. *Classic Group Testing Model:*

The group testing model is represented by a matrix Mhxm in which groups are represented by h and items are represented by m. M [u,v]=1 only if the uth group comprises vth item, and else, M [u,v]=0. Here column vector v which is h-dimensional represents results of the test for u groups, in which 0 indicates the negative result and 1 indicates the positive result.

$$M=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 1\end{bmatrix} \text{----------}> V=\begin{bmatrix}1\\ 1\\ 0\end{bmatrix}$$

Group testing is of two types. Sequential method and non-adaptive method [8]. Sequential method which is also known as the adaptive method, it uses the result outcomes of the former tests so as to find the group for following test as several rounds are performed so as to complete the test. In the non-adaptive group testing mechanism the multiple tests are performed in parallel using the d-disjunct matrix [8]. This test is completed in one round only. In the adaptive group testing if the result comes out to be negative at the end of the round then it is identified as negative and if the result comes out as positive then there is the need of further testing. In the detection model we make an assumption that I represent the virtual servers, m represents the clients, and d represents the clients that are attacker. Assume the matrix Mhxm, in which columns represent clients and rows represent virtual servers. Here M[u,v]=1 if the request from v are sent to virtual server u. the test result V [u]= 1, only when virtual server u has received the infected requests from one or more attackers, otherwise when V [u] = 0, the number of clients that are allotted to the server are legitimate ones. The number of d attackers can be calculated from the V vector in addition to M matrix.

V. PROPOSED MODEL

The defence system that is proposed needs to combine many virtual servers in every backend server, then plot those servers to groups that are tested in the group testing, and then allocate clients in the groups by dispensing their request for service to diverse virtual servers. After observing few of the parameters periodically for the usage of the resource in each server and then making their comparison with some threshold values , the virtual server are analysed to be safe or under the attack using the decoding algorithm of group testing of the attackers are identified. The main objective of the model is to enable an accurate detection of Application Layer Denial of Service Attacks. Besides detection of Application Layer Denial of Service Attacks, it can also be used on other layers.

A. *Detection System*

In this model, every pool for testing is plotted with the virtual servers in backend server. Here we use two parameters as input which are B that represents the maximum number of servers and X that represents the maximum number if clients.

Here we assume a matrix M and let $Xu = \sum_{v=1}^{m} M[u, v]$ is weight for uth group, h total groups. This, model actually identifies the d malicious clients in least time possible by using the Mhxm matrix and performing the group testing where Xu <= X for the given value of X and h <= B for a given server Number B.

TABLE I

REPRESENTATIONS OF NOTATIONS USED IN USED IN MODEL

Notations	Descriptions
m	Total number of users
B	Total number of servers
d	maximum attack number
X	Virtual Servers in Parallel handling maximum number of users.
P	Testing round time.
Q	Total servers for testing
Z	total suspected users
J	Total servers under attack
D	Total number of users connected to negative servers
F	Total number machines not being tested.

B. *Overview of the System*

The process of the detection of the attack consists of many rounds of testing.

- First of all matrix M is generated and updated for the testing.
- After that clients are being allotted to the virtual server on the basis of matrix M. It is that backend server which plots each client to a column of the matrix M, then distributes the token of the queue which is encrypted to that. There are tokens in queue that represent 1 if M [u,v]=1. On the arrival of the requests at the physical server these are validated so as to identify the malicious IDs. This method prevents the attacker from accessing the virtual server and also ensures that the requests from the clients are distributed evenly.
- After that the servers are analysed for their periodic use of the service resources. The total requests that are incoming and the time of response of the virtual servers are all noted so as to compare them with the threshold value. Accordingly, the virtual server is accompanied with the negative / positive results.
- At last there is the decoding of the results and identification of the malicious IDs. By using the model all the attackers are identified in the several rounds of testing.

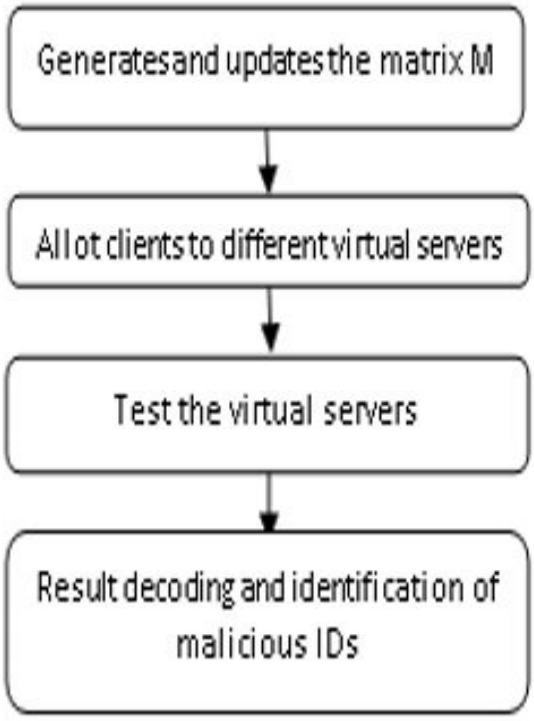

Fig. 1 Overview of the proposed system

C. *Flow chart of Proposed Security Model*

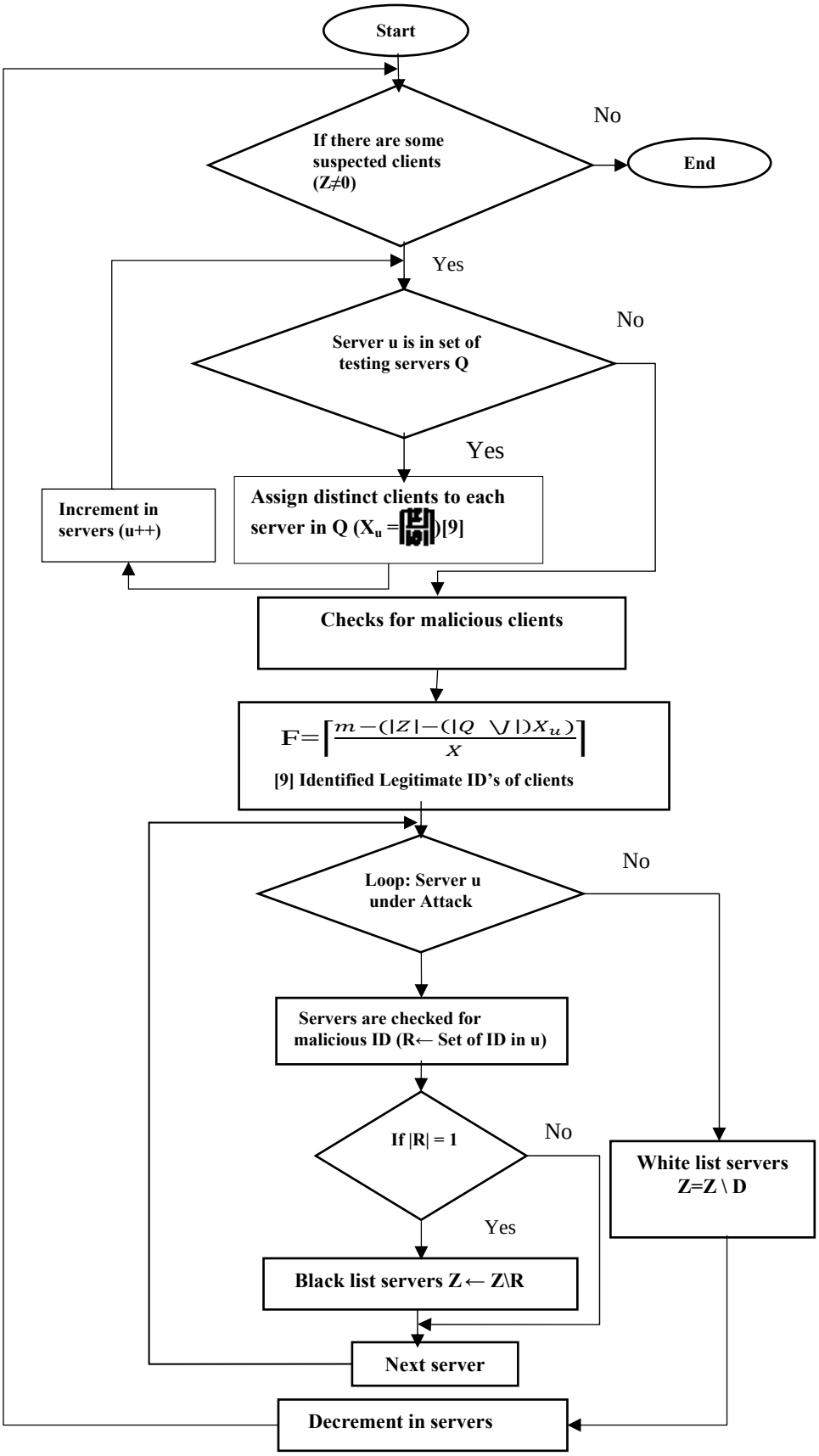

Fig. 2 Proposed Security Model

VI. CONCLUSION

In the last two decades there has been a tremendous increase in the rate of the attacks on the internet. One of the greatest contributor to this rate is the Denial of Service Attacks. Denial of Service Attacks have dominated the world of internet. These attacks make the service unavailable to the legitimate user. In this paper we have studied the existing techniques to detect and mitigate the Denial of Service Attacks. We studied the limitations of all the methods. The model proposed in this paper is to detect the Application Layer Denial of Service Attacks. We use group testing in this model so as to detect the attacks. The Application Layer Denial of Service Attacks exploit the flaws in the design or implementation of the application so as to deny access to the target services. The attackers also control a large number of compromised hosts to launch a Denial of Service Attack. So by using the group testing we test the clients in a group so that there is no overhead of testing each client. By using the group testing a lot of time is saved and we are able to detect the malicious items in a short span of time. In this mechanism we drop the clients that are malicious, in a blacklist so that they are not able to send the data to the servers. The items that are not malicious are allowed to go through without further testing them.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *international journal of innovative research in science and engineering*", vol.31, no.9, pp.24-28, Sep 1998.

[2] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks," *IEEE/ACM Transactions On Networking*, vol. 17, no. 1, pp. 26-39, February 2009.

[3] H. Beitollahi and G. Deconinck, "Analysing Well- Known Countermeasures against Distributed Denial of Service Attacks" In Computer Communications, Elsevier, Vol. 35, issue 11, pp. 1312-1332, 2012.

[4] J. Mirkovic and P. Reiher, "D-WARD: A Source-end Defence against flooding denial of Service Attacks", *In IEEE Transactions on Dependable and Secure Computing*, Vol. 2, pp.216-232, 2005.

[5] H. Wang, C. Jin, and K. G. Shin, "Defense against Spoofed IP Traffic using Hop-Count Filtering", *ACM Transactions on Networking*. Vol. 15, pp. 40 – 53, 2007.

[6] K. Li, W. Zhou, P. Li, J. Hai, and J. Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics," *In Proc. of 3rd Intl' Conference On Network and System Security (NSS '09), IEEE*, pp. 9- 17, October 2009.

[7] M. T. Thai, Y. Xuan, I. Shin, and T. Znati, "On Detection of Malicious Users Using Group Testing Techniques," *in Proceedings of ICDCS*, 2008.

[8] D. Z. Du and F. K. Hwang, "Pooling Designs: Group Testing in Molecular Biology", *World Scientific, Singapore*, 2006.

[9] M. T. Thai, "Group Testing Theory in Network Security", *Springer*, Chapter 2, 2012.