Heuristic Approach to Enrich Servers Performance

Sanket Lalge[#1], Sonali Bhondve[#2], Sucheta Jeurkar[#3], Prasenjeet Paratwagh[#4]

[#]*Computer Department, University Of Pune*
AISSMS's IOIT, Kennedy Road, Shivajinagar, Pune-411001, Maharashtra, India.

[1]lalgesanket@gmail.com, [2]sonalibhondve.55@gmail.com
[3]such.jeurkar@gmail.com, [4]prasenjeetparatwagh@gmail.com

Abstract— **Load Balancing and DOS attack detection are two most essential factors for optimizing the performance of system over the internet. Load balancing refers to distributing incoming client requests across web servers in a server farm. We suggest a method by considering image processing application by computing load value depending upon current and last tasks being processed and exchange load value using central node among the processing servers. Central node selects the least loaded server among farm of servers to process the request and also the central node is capable of detecting DOS attack over system by blocking the connection of robot clients to server based on K-Means algorithm to improve performance of system.**

***Keywords*— load value, central node, DOS attack detection, robot client, load balancing.**

I. INTRODUCTION

With the rapid development of the Internet and the increase in the number of users over internet, one server node may be accessed by a lot of users simultaneously. This situation has result in heavy demands on the sever node, because the single server cannot control its load from user requests in time. So the cluster computer has been already proposed. The key question of a cluster computer is the load balancing. Load balancing is responsible for allocating user requests to the server nodes to prevent the emergence of the situation that some server nodes are loaded heavily while others are loaded lightly. There are two main approaches in dynamic load balancing, global load balancing and local load balancing, categorized by the level of knowledge utilized in the load balancing process. In the local method, each local server performs load balancing with its own neighboring servers based on their load information. In the global method, a central server/process determines how each local server should perform the load balancing using the load information of all servers and then instructs each local server to carry out the suggested load balancing with its neighboring servers [4].

Also if we performed load balancing, the detection of robot clients over internet becomes necessary [2]. The robot clients send multiple requests in a span of time to reduce the speed of response to normal user clients by servers. This can be viewed as robot clients performing DOS attack on system by sending multiple requests and not allowing normal users to get desired response from server.

In this paper, we propose Heuristic Approach to Enrich Server Performance in which the central node or server is analyzing the load on group of processing servers and performing load balancing among the processing servers as well as it is analyzing the incoming client requests whether they are from normal user client or from robot client. If it found the incoming request is from robot client then instead of forwarding the request to processing server, the service to robot client is stopped.

The rest of paper is organized as follows: Section II presents the Literature Survey. Section III describes Algorithms; Section IV describes system design and implementation. And at last, Section V concludes this paper.

II. LITERATURE SURVEY

A. Load Balancing Algorithms

Load balancing algorithm directly influences the effect of balancing the server workloads. Its main task is to decide how to choose the next server and transfer a new connection request to it. We know that load balancing algorithm is divided into static algorithm and dynamic algorithm [1]. The static algorithm doesn't refer to server states so they can be implemented easily and also it takes less time. The common static algorithms are Random Algorithm, Round-Robin Scheduling Algorithm, and Weighted Round-Robin Scheduling Algorithm etc. In a random Scheduling, from the group of servers, the requests are assigned to any server which is picked randomly. In this situation, from group of servers one or two servers will be assigned large number of requests and the other servers will remain idle. But, on average, due to the random selection each server gets its share of the load. It is

simple to implement, but it can lead to overloading of one server while under-utilization of others.

Dynamic load balancing system mainly includes two processes: monitoring the load states of servers and assigning the request to the servers [1]. The state supervision, which depends on the load information of each server in the cluster monitored and collected by the central node server or balancer and according to this information the load balancing among the processing servers is performed by central server or balancer.

B. DOS Attack in System

An effort to make one or more system or network resources unavailable for legal users is called as denial of service attack (DOS attack). The intentions for performing DOS attack may be different for different situations, it generally consist of attempt to temporarily or permanently suspend the service of normal user which is connected to internet. The attackers generally targets the sites which has maximum users or the sites which are making more profits such as banks, credit card, payment gateways or root name servers. Most known common method of attack is that making large number of communication requests to server, so that the load on server will increase and it will become impossible for server to handle normal user request. As there is a load on server, the response to normal user will be given slowly or not given at all. Such attacks usually lead to a server overload [5]. So we can say that DOS attacks are performed to force target server to get reset or block the communication media between normal users and the server which is under attack so that they cannot communicate efficiently with each other.

Following factors tell that system is under denial of service attack:

- Network speed or performance slows down.
- Particular website is unavailable.
- Not able to access any web site.
- There is drastic increase in number of spam emails.
- Wired or wireless internet connection disconnected.

There are many different ways to perform DOS attack. Following are some basic types of attack:

1. The computational resources such as bandwidth, disk space, processor time are consumed in large amount.
2. Interruption in system or network configuration information, such as information of routing.
3. Interruption in state information, such as resetting of TCP sessions even if we do not want to reset the session.
4. Interruption in physical network components.
5. Block the communication media between normal users and the server which is under attack so that they cannot communicate efficiently with each other [5].

III. ALGORITHM DESCRIPTION

A. Load Balancing Algorithm

As we are using Image processing servers, Load balancing algorithm performs the dynamic load balancing among the processing servers by analysing the current executing tasks that are being processed by each server. Steps of algorithm are as follows:

1. Initialize S_LOAD=0.
2. IDLE_SRVER_IP=0.
3. Accept Image.
4. IDLE_SRVER_IP = IP of server which is currently not executing any task.
5. if(IDLE_SERVER_IP != 0)
6. Assign task to server with IP = IDLE_SERVER_IP and go to step 10.
7. For each i^{th} server calculate LAST_TASK_TIME.
8. Compare LAST_TASK_TIME of each server i.
9. Assign processing task to server with least value of LAST_TASK_TIME.
10. Update task data i.e. S_LOAD[i].
11. Repeat 3.

Where, S_LOAD[ ] represents array storing current load on each processing server. IDLE_SERVER_IP stores the IP address of server which is currently not executing any task. LAST_TASK_TIME represents time of last task accepted by the server.

B. DOS Attack Detection Algorithm

The client request is analysed to check whether the request is from robot client or from normal user client. If the request is from robot client then it is not forwarded to processing servers which will improve the processing time of servers by not providing service to robot client. The detection of robot client can be performed using K-Means clustering algorithm which can be stated as follows:

1. Place K points into the space represented by the objects that are being clustered. These points represent initial group centroid.
2. Assign each object to the group that has the closest centroid.
3. When all objects have been assigned, recalculate the positions of the K centroids.
4. Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.

K-Means clustering is a method of cluster analysis which aims to partition *n* observations into *k* clusters in which each observation belongs to the cluster with the nearest mean.

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2$$

Where, $\left\| x_i^{(j)} - c_j \right\|^2$ is a distance measure between a data point $x_i^{(j)}$ and the cluster centre c_j, is an indicator of the distance of the *n* data points from their respective cluster centers.

Using K-Means clustering algorithm two clusters, one for Normal User Clients and another for Robot Clients will be created on the basis of last request time. If new request belongs to Normal User Clients cluster then it will be processed normally and response is given back to user. If it belongs to Robot Clients cluster then the service to that client is blocked.

IV. SYSTEM ARCHITECTURE

The system consists of group of processing servers and one central server as shown in Fig 1. The clients are sending images to add effects to images such as gray scale, blur, red filter, blue filter etc. to the central server. Then the central server checks that whether request is from normal user or from robot using DOS attack detection algorithm.

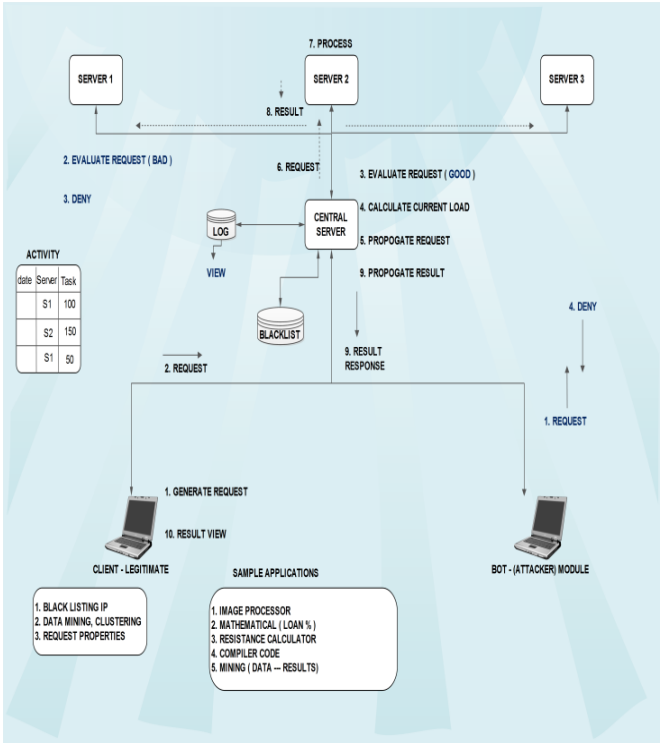

Fig 1 System Architecture

If the request is from robot user then service to robot user is blocked by central server. If the request is from normal user then according to load balancing algorithm the request is forwarded to one of processing servers. The processing server performs image processing operations on image that is sent by client and sends the processed image as response to client.

V. CONCLUSION

In this paper we proposed heuristic approach to enrich server performance which is performing load balancing among the processing servers dynamically along with DOS attack detection. It satisfies the aim of improving performance by not wasting time to process request from robot client as well as client requests are transferred to each processing server so as only one server don't get overloaded.

REFERENCES

[1] Gowtham Kanagaraj, Naveen Shanmugasundaram And Sathish Prakash. W ,"Adaptive Load Balancing Algorithm Using Service Queue",2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April 28-29, 2012.

[2] Andoena Balla, Athena Stassopoulou, Marios D. Dikaiakos, "Real-time Web Crawler Detection", 2011 18th International Conference on Telecommunications.

[3] Nadya El MOUSSAID , Ahmed TOUMANARI, **"** Intrusion Detection Based On Clustering Algorithm",International Journal of Electronics and Computer Science Engineering.

[4] Y. Deng and R.W.H. Lau, "Heat diffusion Based Dynamic Load Balancing for Distributed Virtual environments," Proc. 17th ACM Symp. Virtual Reality Software and Technology (VRST '10), pp. 203-210, 2010.