International Journal of Engineering Technology, Management and Applied Sciences

IJETMAS

www.ijetmas.com December 2017, Volume 5, Issue 12, ISSN 2349-4476

Resource Availability Characteristics and Node Selection in Cooperatively Shared Computing Platforms

S.Mohanapriya,
Assistant Professor, Department Computer Science,
Nadar Saraswathi College Arts and Science,Theni

ABSTRACT

The resource availability characteristics of large-scale, cooperatively pooled, and shared computing platforms. We model the probabilistic behavior of a system comprising a failure detector and a monitored crash-recovery target. We extend failure detectors to take account of failure recovery in the target system. This involves extending QoS measures to include the recovery detection speed and proportion of failures detected. Mostly failure detectors focus on providing fast and accurate detection of all failure events. In this research mass, an algorithm which act as a failure detector, detects the failure and recover it. When the servers get crashed the services are redirected to other active server based on minimum number of users and maximum amount of bandwidth.

Keywords: Quality of Service (QoS), Maximum Availability Server Selection Policy(Mass),Mean Time to Failure(MTTF).

INTRODUCTION

Fault-tolerance in session control systems is achieved by introducing redundancy, e.g., through reliable server pooling or clustering. Namely session control servers are multiplied in server sets. Session control is a time-critical application. Performance of session control is quantified by transaction control time. Transaction control time is defined as the mean time between the moment of request sending and the moment of final response receipt at the transaction initiator including possible multiple fail over's to different servers. One important challenge in such replicated session control systems is how to enhance performance reduce transaction control time. The SSPs are crucial in reducing transaction control time.

Reducing transaction control time enhances performance. Server selection policies (SSP) are crucial in achieving this goal. The maximum availability (MA) SSP is proposed to improve session control performance in scenarios with server and communication failures RMA aims at maximizing the probability of successful transaction with the current transmission, the minimizing the average number of attempted servers until success. MA is applicable in a broad range of IP-based systems and services, and it is independent of the fault-tolerant platform. A simple protocol extension is proposed in order to integrate MA into the RSerPool fault-tolerant architecture.

MASS ALGORITHM

By MASS an algorithm, once when the server get crashed the services are re-directed to the active sever based on the least number of users, suppose when the server holds equal number of users then based on maximum amount of bandwidth the serves services are re-directed.

CUSTOMER TRANSACTION

First the client sends the request to the server, the server process the clients request by retrieving the data from the remote data base and sends the response to the client.

www.ijetmas.com December 2017, Volume 5, Issue 12, ISSN 2349-4476

DETECTION OF CRASHED SERVER

The services are provided to client by the server from the data base. The clients requests are processed by the server and the responses are sending to the client.

RE-DIRECTION OF FAILED SERVICES

.To overcome this problem the crashed services are redirected according to the server has maximum amount of bandwidth .Depending upon the amount of bandwidth the services are re-directed.

MUTENESS FAILURE

Muteness failures are malicious failures in which a process stops sending messages but might continue to send other messages.

TIMING FAILURE

Timing failure occurs when a service response lies outside the specified time interval. Example if the service-hosting machine or network is overloaded or some other resources on which the service depends are overloaded then the service response might be delayed and a timing failure might occur.

OMISSION FAILURE

. If the service can throw a fail to send or fail to receive message exception or send this information to the failure detector then the failure is regarded as an omission failure D. **RESPONSE FAILURE**

To detect value failure voting algorithms can be adopted if multiple service replications are deployed. To detect state transition failure, the service design specification should be available to check whether a service has deviated from its estimated state or not.

PARTIAL FAILURE

Reliability can be clear as the probability that the system will run correctly in a specified operating environment up until time t (t>0).

MAXIMUM AVAILABILITY SERVER SELECTION POLICY

Distributing SIP transactions among replicated servers is an increasingly significant issue. In particular, a SIP transaction consists of a single request, any intermediate provisional response, and a final response. The transaction definition is thus given as

SIP Transaction = (Request => (Provisional Responses) => Final Response).

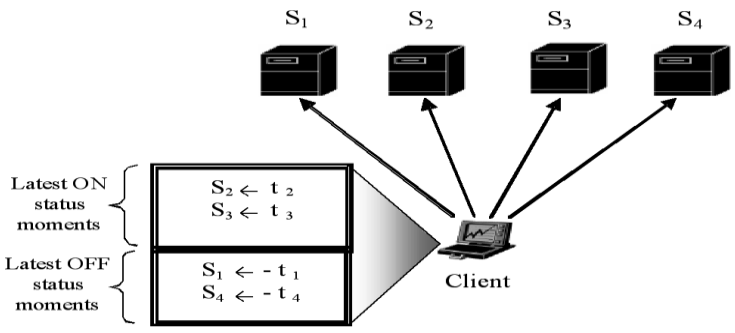

Fig: 1 Status Moment Sever

IJETMAS

www.ijetmas.com December 2017, Volume 5, Issue 12, ISSN 2349-4476

MA ALGORITHM

The MA SSP makes use of the assumption that the server whose last known up time is closest to the actual time, is most likely to be up at the actual time. The MA algorithm aims at maximizing the probability of successful transaction with the current transmission. The client is provided the so called server up status (SUS) vector and server down status (SDS) vector. The SUS and SDS vectors are denoted by u and d, respectively, and are defined as follows:

$$\mathbf{u} = [u_1(t_n), u_2(t_n), \ldots, u_N(t_n)]$$
$$\mathbf{d} = [d_1(t_n), d_2(t_n), \ldots, d_N(t_n)]$$

It should be noted that the inequality always holds because a server cannot be in ON and OFF state at the same time.

$$u_i(t_n) \neq d_i(t_n)(\forall i = 1, \ldots, N)$$

Let the vector f_n represent the servers, which failed while starting or completing the transaction in any of the first (n – 1) attempts

$$\mathbf{f_n} = \left[f_1^{(n)}, f_2^{(n)}, \ldots, f_N^{(n)}\right]$$

Where $f^{(n)}_j = 1$ if the transaction failed with the server j in one of the first (n-1) attempts, and to $f^{(n)}_j = 0$ if the transaction was not sent to the server in any of the first attempts.

OVERVIEW SERVER-BASED DYNAMIC SERVER SELECTION

Server replication is a common technique that has been used to provide scalable distributed service over the Internet.

RANDOM SERVER SELECTION ALGORITHMS

Our server-based approach to the problem of server selection has the following salient features. First, it is client-transparent. We define two major performance metrics used in our server selection algorithms: server loads and fast paths, which indicate the status of servers and different network paths from servers to clients.

```
1. if (a client X is a regular client)
2.  if (server load is light) and (the path from S to X is not slow)
3.    accept the request
4.  else
5.    if (all other servers are heavily loaded)
6.      accept the request
7.    else
8.      randomly redirect the request to R other than S
9. else
10. if (server load is light) or (all other servers are heavily loaded)
11.   accept the request and generate metrics about the client
12. else
13.   redirect to a light-loaded server
```

Fig 2: Random Server Selection Algorithms

Performance Metrics

IJETMAS

www.ijetmas.com December 2017, Volume 5, Issue 12, ISSN 2349-4476

SERVER LOAD: For given server S, its load, denoted by LS, is defined as the ratio of Ttotalto Rmax. Rmaxis the maximum response delay that a typical client can accept for a request of average size, such as 10 Kbytes. LS is called light if LS ≤ 80%; otherwise, it is called heavily loaded.

FAST PATH: As shown in Figure 3.4.1.1, if the transferring delay of a reply from a server S to a client X is k times longer than the transferring delay from another server R to X plus the cost of redirecting the request from S to R, the path from S to X is called slow, and the path from R to X is called fast. Here, k is an experimental parameter, such as 2 or 4. Both transferring delays are estimated through the RTTs of the paths which are obtained through the passive measurement on servers.

BEST GUESS REDIRECTION SERVER SELECTION ALGORITHMS

The second algorithm examines all servers and selects the best one as R based on the current metrics on S. Because the current metrics on server S may not be accurate due to the delay of metrics exchange among servers the second method is called Best-guess Redirection (BR).

```
1. if (a client X is a regular client)
2.  if (server load is light) and (the path from S to X is not slow)
3.    accept the request
4.  else
5.    computing equivalent classes
6.    if (no better server)
7.      accept the request
8.    else
9.      redirect the request to the ''best'' server R
10. else
11. if (server load is light) or (all other servers are heavily loaded)
12.   accept the request and generate metrics about the client
13. else
14.   redirect to a light-loaded server
```

Fig 3: Best Guess Redirection Server Selection Algorithm

RESULT AND DISCUSSION

MASS is a simple extension of round robin. It assigns a certain weight to each server. The weight indicates the servers processing capacity. This SSP may also be dynamic if it can evaluate individual server's capacities and their loads occasionally. The main problem addressed in this system is maximizing the probability of successful transaction with the current transmission, thereby minimizing the average number of attempted servers until success.The server selection policy in solves the problem by exploiting the dynamically obtained information on the last server access moments and the corresponding activity status of servers in a server set. The user can work without any disturbance when one server fails doing its work the other server will replace it and perform the same task.

CONCLUSION

The system more users can access a server at a time if the server gets busy the user will be responded by the availability server. This system is most useful in cases of frequent interaction between the client and the same server set (e.g., in messaging sessions utilizing SIP servers) as the status for a given server set stored in the client is in that case always maintained up-to-date. The maximum availability Server Selection Policy is proposed to improve session control performance in scenarios with server and communication failures. Suppose if available server having same user means we find out highest bandwidth server. The redirected server starts service user lost session page.

www.ijetmas.com December 2017, Volume 5, Issue 12, ISSN 2349-4476

REFERENCES

[1]. "Gateway discovery algorithm based on multiple QoS path parameters between mobile node and gateway node",Bouk, S.H. ; Sasase, Iwao ; Ahmed, S.H. ; Javaid, N. Communications and Networks, Journal of Volume:14 , Issue:4 Digital ObjectIdentifier:10.1109/jcn.2012.6292250 Publication Year: 2012.

[2]. "A Domain-Based Data Distribution Strategy for FaultTolerance",FeiLuo ; Jianjun Yi Service Sciences (ICSS), 2013 International Conference on Digital ObjectIdentifier: 10.1109/ICSS.2013.46 Publication Year: 2013.

[3]. "A Novel Cross-Layer Architecture for Wireless Protocol Stacks",XiongweiRen ; Jianqiang Zhang Multimedia Technology (ICMT), 2010 International Conference on Digital Object Identifier: 10.1109/ICMULT.2010.5632152 Publication Year: 2010.

[4]."The Process Conducting and Member Audit in the Distributed Enterprise Modeling", CaiZhiming ; Yin JunAsia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE Digital Object Identifier: 10.1109/APSCC.2008.219 Publication Year: 2008.

[5]."Energy efficient head node selection algorithm in wireless sensor networks",Wanming Chen ; Meng, M.Q.-H. ; Shuai Li ; Tao Mei ;Huawei Liang ; Yangming Li Robotics and Biomimetics, 2007. ROBIO 2007. IEEE International Conference on Digital Object Identifier: 10.1109/ROBIO.2007.4522363 Publication Year: 2008.

[6]."Distributed Node Selection for Sequential Estimation over Noisy Communication Channels",Wimalajeewa, T. ; Jayaweera, S.K. Wireless Communications, IEEE Transactions on Volume: 9 , Issue: 7 Digital Object Identifier: 10.1109/TWC.2010.07.090967 Publication Year: 2010.