Journal of Computer Science 7 (9): 1426-1431, 2011
ISSN 1549-3636


# Novel Mechanism Control Algorithm for Wired Network

[1]V.B. Kirubanand and [2]S. Palaniammal
[1]Computer Application Department, SKCET College, Coimbatore-8,
[2]Science and Humanities Department, VLBJCET College, Coimbatore-42, India

**Abstract: Problem statement:** A critical issue in wireless network where the data can hack by the person and we add a novel encryption mechanism to protect the data transfer from client to server and vice versa. **Approach:** We present a queuing model of a client and server that uses for bulk arrival service. The arrival of data requests is assumed to Markov Poisson Distributed Process (MPDP) and the events are considered in the server for process sharing. We obtained the parameter of service rate, arrival rate, expected waiting time and expected busy period. We also derive the expression for the data value of threshold. **Results:** The total number of packets request processed, there was no time limit to arrivals, while compared to m/m/1 model. Our model m/m (1,b)/1 was more efficient to find response and request time in between client and server. **Conclusions:** Our proposed simulation model validated through Java programming.

**Key words:** Client server, queuing petri nets, novel encryption, bulk service rule, Markov Poisson Distributed Process (MPDP), encryption technique, wired device, data transaction, vice versa, file server

## INTRODUCTION

Client-Server System are becoming increasingly common in the world today as users move to networks of distributed, interacting computer through internet. This process of work demands new Novel encryption mechanism to protect the data transfer from client to server and vice versa. The more complex solvers in parameters like inter arrival and service time, expected waiting time and expected busy period.

An analytical model was presented Nan *et al.* (2008) to analyze the system performance in terms of distribution data time capacity and data services delay while data transaction in between client and server. This facilitates the integration of both hardware and software aspects of the system behavior in the improved model.

The user gets much benefit in Sharing Data Packets through Wired Device (SWITCH) in intranet access to find the performance modeling in between the client and server using markov models of bulk service rule.
In, some of the models are congested in the data packets in arrival as well as service period. The model like m/m/1 found a services description can predict server performance quite well.

In our model is a very simple model like M/M/(1,b)/1 using queuing models, in bulk arrival of data requests, will predict the inter arrival and inter service in between server and client. In this model, the performance is quite possible to work in all aspects.
In addition to that, here we can add security features while transmitting the data in between client and server. A novel encryption mechanism will be used to protect the data from hackers while transaction the data from client to server and vice versa.

In this study we have derived a model of the File server which includes a processor sharing node to one system to another. The inter arrival and service process in between server and clients is assumed with the help of MPDP. The MMPP are commonly used to represent busy arrival traffic to communication system (Performance modeling), but we use MPDP to find the average arrival rate and service rate. Both are considered in the distribution data process. The average arrival rate and service rule is assumed to the mean value.

**Performance modeling:** The average service time and the maximum number of jobs are parameters that can be determined through minimum likelihood estimation. After completing the Markovian Poisson distribution process we had found the root of specification in between the expected waiting time and busy period. By simulating the system, we are able to obtain the server and client performance measures such as request and response time in the wired device (SWITCH) probability. We prefer the validation environments

**Corresponding Author:** V.B. Kirubanand, Computer Application Department, SKCET College, Coimbatore-8

provided in a server and client connected through via SWITCH. The solution shown in the model can predict the performance measures in both lighter data packet and overloaded data packets.

**Client server model:** Wireless data transition device, it allows a higher data rates over larger distances, efficient use of bandwidth and avoids interference almost at minimum.

We model the File server and clients using markovian model in bulk service rule of M/M (1,b)/1. M/M(1,b)/1 clients get much benefit when compared to M/M/1/ Queueing model, while using M/M/(1,b)/1 bulk service rule, client request are to taken bulk service rule, client requests are taken to server for service in a bulk(more than one), not one by one. A waiting time in queue is abridged and clients don't need to wait for long in a queue to get services. Similarly a model of an M/M/1 bulk queue with service rate dependent on the batch size is developed (Nan *et al*., 2008).

**Queueing petrinets:** We use the Queueing petrinets tools in between client and server, while transaction the data packet, it will deposit in PLACE (graphical tool) after the packets are release one by one (Ghoul *et al*., 2007). So, there is no traffic arrival and service on data transaction in between client and server, vice versa.

The tokens, when fired into place, by any of its input transition, are inserted into the queue of clients. The tokens of packets in the queue are all deposit for output transition to the server. After completion of its service, a token of packet is immediately moved to the wired device to the server, from depository place.

**Encryption technique: Cryptography:** In cryptography the structure of the message is scrambled to make it meaningless and intelligible unless the decryption key is available. I make no attempt to disguise or hide the encoded message (Zollner *et al*., 1998). Basically, cryptography offers the ability of transmitting information between client and server in the way that prevents from third party hacking. Cryptography can also provide authentication for verifying the identity of someone or something Figs. 2 and 3:

P: Plain Text K: Key C: Cipher Text
E: Encryption Function D: Decryption function

**Steganography:** In contrast, Steganography does not alter the structure of the secret message, but hides it inside a cover-image so that it cannot be seen (Amin *et al*., 2003). A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an invisible message created with Steganography methods will not (Provos and Honeyman, 2001).

Cryptography hides the content of the secret message from malicious people, whereas Steganography even conceals the existence of the message (Amin *et al*., 2003).

**Proposed novel encryption scheme:** In this study, we discussed a novel encryption mechanism which deals a message is transformed into a binary image which cannot be identified as a cipher text or steno object. This scheme is very much useful for transmitting a confidential data from client and server and vice versa. It is very much useful for authentication purpose also.

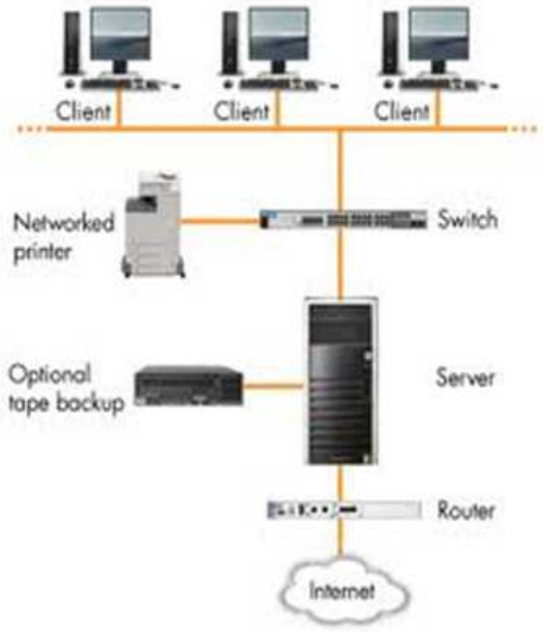


Fig. 1: Client server model connected with 'N' number of clients with server through wired transition SWITCH device, person encrypted to customer with key

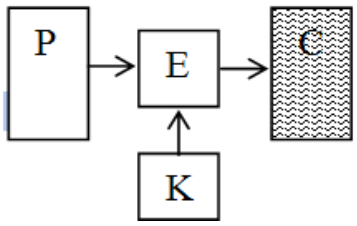


Fig. 2: Encryption model (customer decrypted to person with key)

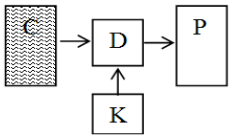


Fig. 3: Decryption model (image hidden using insteganography

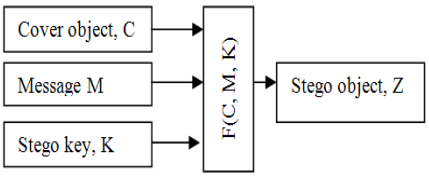


Fig. 4: Basic steganography model (message encrypted in cipher image

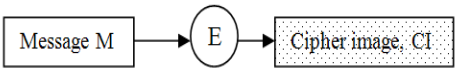


Fig. 5: Encryption model (message M image encrypted into cipher image CI)

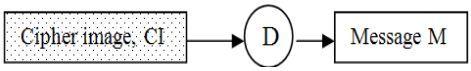


Fig. 6: Decryption model (cipher image CI decrypted into message M)

```
Algorithm
                Computing plot cipher image
int[] compute_Cipher(String str){
    int i=0;
    int plotdata[strlen(str)];
    while(i<strlen(str)){
        int a = str[i] – 33;
        plotdata[i]= 47 – a;
        i++;
     }
     return(plotdata);
```

Fig. 7: Novel encryption block diagram

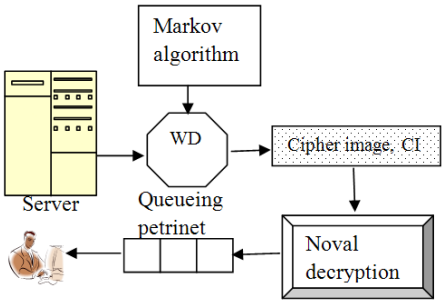


Fig. 8: Novel decryption block diagram

In Fig. 5, for the encryption function E with an input of message M we get the cipher image CI. In this encryption function we don't need key to produce the cipher image.

In Fig. 6, the decryption function D with cipher image CI as input without the knowledge of key we recover the message M.

In Figs. 7 and 8 shows the novel encryption and decryption block diagram. In Fig. 7, the user request will queued with help of the Petri net and it is encrypted into cipher image forwarded through wireless devices with the help of markov algorithm to the server. The server automatically decrypted cipher image to a proper request from the client. Why we introduce this encryption model between client and server, while during the transfer of a request from client to server no one should not be hack the request.

In Fig. 8, The server automatically encrypt the reply to the request by the user, with the help of the markov algorithm through wired device forward to novel decryption function can recover the reply from the server and this reply will be forwarded by the queuing Petri net. The reply also in secure because of encrypt in nature.

The novel encryption scheme is very useful when we transmit the information from client to server and vice versa. In between anybody crack or hack the file information, they don't understand the message, because it is available in the cipher image like an ECG diagram. The image is stored in the format of JPEG which is the most commonly used format on the internet and mail attachments because of its compressed by default nature.

In this algorithm, we don't need a key like cryptography and Steganography, without a key this algorithm works. There is no need to send the key to the receiver or any others who receives the message. From this we save a time on sending the key through another separate channel. Overall this will improve the security of the data. So we achieve the confidentiality, authenticity, integrity and non-repudiation.

The service can handle at the most 'N' request at a time. A request will be blocked if the number 'N' has been reached (Dilley *et al*., 1998). The $\lambda$ is the rate of completed request and response $\mu$ i.e average response of time 'T' probability are performance measures which will be provided in the simulation using java programming.

## RESULTS

We proceed with the following parameters for consider in mean value, root of specification, average of request and average of response time.

Table 1: Comparison between cryptography, steganography and novel encryption, The results were provided in the Novel encryption, compare with cryptography and steganography in the following table

| Cryptography | Steganography | Novel Encryption |
|---|---|---|
| Known message passing | Unknown message passing | Unknown message passing |
| Common technology | Little known technology | Novel technology |
| Key required | Key Required | Key not required |
| Most algorithms known to government departments | Technology still being developed | |
| for certain formats | Technology is no where used | |
| Strong algorithms are currently resistant brute force attack | Once detected message is known | Detection is impossible |
| High expensive computing power required for cracking | Small expensive computing power | |
| Required for cracking | Not possible for cracking | |
| Technology increase reduces strength | Technology increase reduces strength | No technology is available |
| Only Text formats are available | many carrier formats | Image Carrier is used here |

Table 2: Network parameter specification (Calculation details)

| Mean arrival rate per node | 100 Packets/sec |
|---|---|
| Mean service time | 3 Sec |
| Number of nodes | 1-100 |
| Threshold number of packets | 1-20 |
| Root of specification | Lies between 0 and 1 |

Table 3: Comparison statement value for M/M/1 and M/M(1,b)/1 queueing model . has been done with help of bulk service rule. The queueing model of M/M/1 and M/M(1,b)/1 consider with 100mbps bandwidth.(Performance in between Two Models) through SWITCH transition device

| Queueing model | M/M/1 | M/M(1,b)/1 |
|---|---|---|
| Wired device | SWITCH | SWITCH |
| Request | 0.07452 sec | 0.07452 sec |
| Response | 0.36801 sec | 036801 sec |
| Root of specification | 0.20249 | 0.16907 |
| Expected waiting time E(T) | 0.65751sec | 0.53501 sec |
| Expected busy period E(B) | 3.40725 sec | 3.27021 sec |

Table 4: Novel encryption from character to plot (results)

| | Forward (embedding) | | |
|---|---|---|---|
| Char | ASCII | Substitute | Plot |
| K | 75 | 42 | 5 |
| i | 105 | 72 | -25 |
| r | 114 | 81 | -34 |
| u | 117 | 84 | -37 |
| b | 98 | 65 | -18 |
| a | 97 | 64 | -17 |
| n | 110 | 77 | -30 |
| a | 97 | 64 | -17 |
| n | 110 | 77 | -30 |
| d | 100 | 67 | -20 |
| O | 79 | 46 | 1 |
| P | 80 | 47 | 0 |

Table 5: Novel decryption from plot to character results

| | Reverse (extraction) | | |
|---|---|---|---|
| Plot | Substitute | ASCII | Char |
| 5 | 42 | 75 | K |
| -25 | 72 | 105 | i |
| -34 | 81 | 114 | r |
| -37 | 84 | 117 | u |
| -18 | 65 | 98 | b |
| -17 | 64 | 97 | a |
| -30 | 77 | 110 | n |
| -17 | 64 | 97 | a |
| -30 | 77 | 110 | n |
| -20 | 67 | 100 | d |
| 1 | 46 | 79 | O |
| 0 | 47 | 80 | P |

**MPDP Parameter:** We calculate using $\lambda/\mu$, to find the average response and request time.

**Root of specification:** The threshold value of Root of specification lies between 0and 1

**Inter arrival time:** It is the time taken between client and server (i.e., request)

**Inter service time:** It is the time taken between server and client (i.e., response)

Table 2 Simulation results are obtained for various scenarios by varying the number of nodes and threshold number of packets per node in a network data transaction. Simulation results clearly show that there exists trade-offs between the server and data service. And also the results show that the average of number of packets.

In the Table 4 and 5 shows the conversion of plain text into cipher plot values and vice versa. We have to plot a pixel corresponding to a cipher plot value in an image.

The parameters are given below for experimental results.

**Probability that the server is idle:**

$$p_{0,0} = \frac{(1-r)}{1-r+(\lambda/\mu)} = \frac{(1-r)^2}{(1-r)^2 + r(1-r^b)}$$

Probability that the server is busy and n units in the system:

$$p_{1,n} = \frac{(1-r)(1-r^b)}{(1-r)^2 + (1-r^b)} r^{n+1}, n = 0,1,2,..$$

Waiting time density:

$$v(t) = \frac{\lambda p_{0,0}}{((1-r))}[+(1-r^b)\exp\{-\mu + (1-r^b)t\}]$$

Expected waiting time density:

$$E(T) = \frac{r}{\mu[(1-r^b) + r(1-r)]}$$

Expected busy period:

$$E(B) = \frac{1}{\mu(1-r)}$$

From the above formulas we are calculating the Performance of Client-Server model:
Expected waiting time density:

$$E(T) = \frac{r}{\mu[(1-r^b) + r(1-r)]}$$

Expected busy period:

$$E(B) = \frac{1}{\mu(1-r)}$$

From the above algorithm we are calculating the data packets values in between client and server vice-versa. These equations are all considered in the markov algorithm.

**Markov algorithm:** A Markov algorithm is a string rewriting system that uses, grammar like rules to operate on strings of symbols. Markov algorithm have been shown to turing complete, which means that they are suitable as a general model of computation and can represent any mathematical expression from its simple notation (Nan *et al*., 2008).

**Performance measures:** We consider the validation measurements used single server computer and multi client computer which are connected through 100mbps. The server is Intel® core Duo Processor, 2.0 GHZ, 2MB L2 cache memory, 1GB DDR2 RAM, 160GB Serial ATA 7200RPM Hard Disk.

The computer representing the client is a processor of 2.99GHZ, RAM-1GB. Both server and client computers were connected through windows XP and windows server 2003 operating system. We use different hardware configuration in between client and server. Maximum users access the data from server to client.

We proceed with the following performance measures to the average of request and response time, root of specification and inter arrival and service time, expected waiting time and busy period. The request time is the time difference in response time. i.e., the data request to server and the server response data to the client. The average response and request time is calculated using Markov Poisson Distribution Process (MPDP). After measuring the request and response time it is forwarded to the root of specification. This will be provided to the expected waiting time and busy period. Similarly, with the measures of root of specification, we can include these values to the waiting time and busy periods measurements.

The model of M/M/1 and M/M (1, b)/1 are client and server through wired device (performance).The results of the performance modeling is done in the java program. A TCP/IP connection is timed out at the client computer (request) when it will take a long time to the server to return (acknowledge) (Bause *et al*., 1994)

The number of systems ‘N’ is the model; we use the some parameters that were found (Heffes, 1978). Where a similar model was used with MPDP arrivals instead of MMPP arrivals. The same parameter, where it is not new parameter has been obtained in the models. This model will be a correct solution measure. We can use this parameter for future devices

**Simulation model:** We considered performance modeling in wired device like SWITCH data transition. we perform the simulation for data transaction in between client and server.

Simulation results are obtained for various scenarios by varying the number of nodes and threshold number of packets per node in a network data transaction. Simulation results clearly show that there exists trade-offs between the server and data service (Zollner *et al*., 1998). And also the results show that the average of number of packets.

## DISCUSSION

In this experiment we measure the performance modeling using bulk service rule by simulation with java program. The values are measured in the client and server with different configurations and also operating system. The value with corresponding measurement shows the average response and request time. Irrespective of number of request each configurations are having constant threshold for root of specification value measured in request and response time rate in M/M/(1,b)/1 model. The request time and response time is calculated in different configuration using M/M/(1,b)/1. This way of finding the value is given result when compared to M/M/1 model.

## CONCLUSION

In this study, we have proposed a new Novel Encryption scheme, which achieve a strong encryption mechanism to protect the data while transfer from client to server and vice versa. We have obtained the client and server performance valid such as average of request and response time and also the expected waiting time and busy period. It has been found the value in comparison of M/M/1 and M/M (1, b)/1. Finally, we have found in M/M (1, b)/1 is a better implementation for better performance to fit in the server and client.

## REFERENCES

Amin, M.M, M.S. Salleh, M.R.K. Ibrahim and M.Z.I. Shamsuddin, 2003. Information hiding using steganography. Proceeding of the 4th National Conference on Telecommunication Technology, Jan. 14-15, IEEE Xplore Press, Shah Alam, Malaysia, pp: 21-25. DOI: 10.1109/NCTT.2003.1188294

Bause, F., 1993. QN+PN=QPN Combining Queuing Networks and Petri Nets. University Dortmund.

Bause, F., P. Buchholz and P. Kemper, 1994. Hierarchically combined queueing petri nets. Proceeding of the 11th International Conference on Analysis and Optimization of Systems, Discrete Event Systems, Sophie-Antipolis France, pp: 176-182. DOI: 10.1007/BFb0033546

Cao, J., M. Anderson, C. Nyberg and M. Kihl, 2003. server performance modeling using an M/G/1/K*PS Queue. Proceedings of the 10th International Conference on Telecommunications, Feb. 23-Mar. 1, IEEE Xplore Press, Papeete, Tahiti, pp: 1501-1506. DOI: 10.1109/ICTEL.2003.1191656

Dilley, J., R. Friedrich, T. Jin and J.Rolia, 1998. Web server performance measurement and modeling techniques. Perform. Evaluat., 33: 5-26. DOI: 10.1016/S0166-5316(98)00008-X

Ghoul, R.H., A. Benjelloul, S. Kechida and H. Tebbikh, 2007. A scheduling algorithm based on petri nets and simulated annealing. Am. J. Applied Sci., 4: 269-273.

Heffes, H., 1978. A class of data traffic processes-covariance function charaterizationn and related queuing results. Bell Syst. Technical J., 59: 897-929.

Nan, F., Y. Wang and X. Ma, 2008. Application of multiscale hidden markov modeling wavelet coefficients to fMRI activation detection. J. Math. Statist., 4: 255-263.

Provos, N. and P. Honeyman, 2001. Detecting Steganography Content on the Internet. University of Michigan.

Widell, N., 2002. Performance of distributed information systems. Lund University.

Zollner, J., H. Federrath and H. Klimant, A. Pfitzmann and R. Piotraschke *et al*., 1998. Modeling the security of steaganography systems. Proceedings of the 2nd Workshop on Information Hiding, Springer-Verlag, Portland, pp: 345-355.