CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

Estimation of the performance of the network devices in both wired and wireless network in terms of various parameters using Markovian Model with bulk service M/M(1,b)/1, and the usage of Queuing Petri Net are the major contribution of this research work. This chapter summarizes literature survey of all the related works of basic network and interface devices, Markovian model, queuing network, job scheduling algorithms, queuing petri net, and network security which has been developed by referring all these existing works. Based on this the overall objective of this research work is to develop a Multi Mechanism Client Server which is suggested to use in various network applications for wired and wireless data transfer.

2.2 BASIC NETWORK AND INTERFACE DEVICES

Computer networking devices are units that mediate data in a computer network. Computer networking devices are also called network equipment or Intermediate Systems (IS). (Bailey 1954) obtained the mean queue-length and the distributions of the length of busy period when at least one channel is busy and both channels being busy.

Predictive performance models are used increasingly throughout the phases of the software engineering lifecycle of distributed systems. However, as systems grow in size and complexity, building models that accurately capture the different aspects of their behavior becomes a more and more challenging task. The
challenge stems from the limited model expressiveness on one hand and the limited scalability of model analysis techniques on the other. Samuel Kounev et al (2006) presented a novel methodology for modeling and performance analysis of distributed systems.

In the client/server model for distributed on-line requests processing, the concept of a server class that consists of multiple identical servers is often provided for the fast response time, high fault-tolerance, or continuous availability. Jin Hyun Son and Myoung Ho Kim (2002) discussed that there is no concrete formulation that provides the optimal number of servers of a server class in distributed client/server systems. The number of servers has been usually chosen only by heuristic methods or statistics after monitoring system behavior for some period of time. In this method based on queuing theory that determines the optimal number of servers in a server class for a general distributed client/server model that encompasses the state-of-the-art on-line transaction processing environment described in the literature.

Network Management Systems have played a very important role in information systems. Management is very important and essential in any fields. There are many managements such as configuration management, fault management, performance management, security management, accounting management etc. Among them, configuration, fault and security management are more important than others, because these are essential and useful in any fields. May paing zaw and Su myat marlar soe (2008) analysed that configuration management is to monitor and maintain the whole system or LAN. Fault management is to detect and troubleshoot the system and security management is to control the whole system.
The first attempt for functional requirement in Client Server performance modeling was presented by (Joseph Martinka 1995). (Stamatelopoulos 1995) implemented the manager architecture for hierarchical management based on a DBMS core module, aiming to minimize the network traffic overhead and the system response time. Gohain and Borthakur (1979) have solved bulk service model using difference equation technique. (Chobrolu 2005) investigated the performance of two feature selection algorithms involving Bayesian networks (BN), Classification and Regression Trees (CART) and an ensemble of BN and CART. Empirical results indicate that significant input feature selection is important to design an IDS that is lightweight, efficient and effective for real world detection systems. It also proposed hybrid architecture for combining different feature selection algorithms for real world intrusion detection.

2.3 MARKOVIAN MODEL

(Kendall 1951) has designed a very convenient and universally accepted notation to donate a queuing system. It consist of a five part descriptor A/B/C/X/Y where A and B inter-arrival time and service time distribution respectively, C is the number of parallel servers, X is the system capacity and Y is the queue discipline. In practice, the queuing system is represented by A/B/C with the understanding that the system capacity is infinite and FIFO queue discipline is followed, in case they are not specified. A single server Markovian queuing system with general bulk service rule is represented by the notation M/M (a,b)/1

Markovian Queuing Model

Queuing model with exponential inter-arrival times and exponential service times are called Markovian queuing models. Markovian queuing models are usually solved by
(i) Difference – Differential equation method, using Rouche’s Theorem and generating functions and
(ii) Neut’s matrix – geometric algorithm

The first method is discussed by Gross and Harris (1979) and (Saaty 1961). Gohain and Borthakur (1979), Neuts (1967) developed the matrix geometric algorithm approach for studying the steady state queuing models.

Batch service queuing system with batch sizes (a,b) without server's vacation has been analyzed by many authors. The significant contributors to this field are Chaudhry et al (1987) Chaudhry et. al. (1999 a). Medhi and Borthakur (1972). Batch service queuing system with single and multiple vacation for a=1 are studied by some authors Lee et al (1997).

2.4 QUEUING NETWORK


Kounev and Buchmann (2003) studied the real-world application and demonstrated the benefits, in terms of modeling power and expressiveness, that QPN models provide over conventional modeling paradigms such as Queuing Networks and Petri Nets. QPNs facilitate the integration of both hardware and software aspects of system behavior in the same model. In addition to hardware contention and scheduling strategies using QPNs, one can easily model simultaneous resource possession, synchronization, blocking and contention for software resources.
It has been observed in recent years that in many applications service time demands are highly variable. Without foreknowledge of exact service times of individual jobs, processor sharing is an effective theoretical strategy for handling such demands. Steve Thompson et al (2009) investigated that the processor sharing must be implemented by time-slicing with a round-robin discipline. It investigates how round-robin performs with the consideration of job switching overhead. By analyzing time-slicing with overhead, it derive the effective utilization parameter, and give a good approximation regarding the lower bound of time-slice under a given system load and overhead.

2.5 QUEUING PETRI NETWORK

Queuing Petri Nets (PQPNs) combine the results of product form for Stochastic Petri Nets with the well-known BCMP results in one modeling formalism and include them as special cases. Bause and Buchholz (1994) establishes an exact aggregation approach, based on the product form, which extends Norton's theorem for aggregation in multi-class product form Queuing Networks.

Lee et al (1997) shows that in some queuing systems server unavailability is sometimes beneficial both to the system owner and to the customers. Proth and Lorraine Metz (1997) discussed in detail the modeling and the evaluation of discrete event systems. The first part concerns with cyclic manufacturing systems. The model of such a system is an event graph which encapsulates both the physical and the decision making system models. The approach aims at maximising the productivity while minimising the Work-In-Process (WIP) in both the deterministic and the stochastic cases.
The second concerns address acyclic manufacturing systems. The Petri net model of such a system is different from the Petri net model of a cyclic system in the sense that only the physical part of the system and the related constraints are modeled using Petri nets. It shows that such a model perfectly fits with a hierarchical management of manufacturing system.

Petri nets are, by definition, discrete event systems. David et al (2001) defined subsequently continuous Petri nets. Both models can be combined to produce what are known as hybrid Petri nets. These continuous and hybrid nets are used to model hybrid systems whether or not time is taken into account.

(Luis Alejandro Cortés 2001) has developed a software tool, called SimPRES, that allows PRES+ models to be simulated. It has a graphical interface that lets the designer construct, modify, and simulate systems represented in PRES+. Such a tool is of great help for the designer because it allows visualizing the model of the system under design and running it, so that an animation of the dynamic behavior of the net is possible. SimPRES supports full graphical editing of the model of the system and provides methods to store/recover the net in/from a file.

(Samual Kounev 2005) implemented queuing petri nets as a modeling paradigm in realistic scenarios in e-business applications in terms of modeling power and expressiveness that QPN models provide over conventional modeling paradigms such as Queuing Networks and Petri Nets.

Queuing Petri nets are a powerful formalism that can be exploited for modeling distributed systems and analyzing their performance and scalability. Samuel Kounev and Christofer Dutz (2006) by combining the modeling power and expressiveness of queuing networks and stochastic Petri nets, queuing Petri nets
provide number of advantages. QPME (Queuing Petri net Modeling Environment), a tool that supports the modeling and analysis of systems using queuing Petri nets. QPME provides an Eclipse-based editor for designing queuing Petri net models and a powerful simulation engine for analyzing the models. After presenting the tool, it discusses the ongoing work on the QPME project and the planned future enhancements of the tool.

(Gabor Imre 2006) developed a methodology for performance metrics of a queuing model system. The results of this work included the number of clients and values of the tuning parameters which have a considerable impact on the performance metrics.

(Samuel Kounev 2006) Studied a realistic distributed component-based system, which shows how queuing Petri net models can be exploited as a powerful performance prediction tool in the software engineering process. A detailed system model is built in a step-by-step fashion, validated, and then used to evaluate the system performance and scalability.

2.6 NETWORK SECURITY

As the server is usually the central location for critical data, adequate physical security and operational security measures need to be taken to insure the safety of the data. Although there are a large number of tools available to perform security and control functions on mainframe systems, there are significantly less tools available that are designed specifically for client/server systems. Carl Stephen Guynes et al (1996) tools are developed, for the end-user computing evolution to provide computing power at the workplace, and resulted in end-user demand for access to corporate data with little regard for the security.
Carl Stephen Guynes et. al. (1996 a) examines the problems associated with enforcing stated DBMS access controls, and how the data administration team can work with top management to ensure that the current database security strategy is consistent with the goals of the organization. Although early security techniques utilized an approach of simply limiting access to corporate data, today's demands for data availability have created a new subset of related security issues.

Ramaraj and Karthikeyan (2006) implemented a mechanism which focuses on single trusted authority using public key cryptography RSA in Eap and also included AES rijndael stream cypher algorithm instead of RC4 for MPPE. Thomas Chardin and Raphaël Marinier (2009) used the Improved Cellular Message Encryption Algorithm (CMEA-I) which is an improved version of the Telecommunication Industry Association’s Cellular Message Encryption Algorithm (CMEA). They present a chosen-plaintext attack of CMEA-I which requires less than 850 plaintexts in its adaptive version. This demonstrates that the improvements made over CMEA are ineffective to attacks and confirms that the security of CMEA.

Thien and Lin (2003) discussed the modulus operation. The method outperforms the simple LSB substitution method given the same range of data digits in the embedded data. The method achieves good image vision quality without the need for post processing. The method is almost as simple as the LSB method in both coding and decoding.

Tanako et al (2000) developed the transformation which is achieved in the frequency domain and the concept of fourier filtering method is used. An input image is transformed into a fractal image, which can be used in computer graphics (CG) application. One of the main advantages of this scheme is the amount of data
to be hidden is equal to that of the host signal while it is in general limited in the conventional data hiding scheme.

Sunil Gaddam and Manohar Lal (2010) developed cryptographic techniques applied for data Encryption or Decryption with the aid of cancellable biometric features. Conventional techniques depend on biometric features like face, fingerprint, hand geometry, iris, signature, keystroke, voice and the like for the extraction of key information.

(Simmons 1984) describes how the dilemma can be solved through parameter substitution in digital signature algorithms. In signature algorithms like ElGamal and DSA exist parameters which have to be set with random. It is shown that how one can make usage of these parameters to send a message subliminally. Because the algorithm's signature creation procedure is unchanged, the signature remains verifiable and indistinguishable from a normal signature. Therefore it is hard to detect if the subliminal channel is used. Santosh Ghosh et al (2011) discussed the development of Identity Based Encryption (IBE) that is ideally used in identity aware devices. The security of such devices using pairing algorithms against side-channel and fault attack has not been studied extensively. It examines the security of existing countermeasures and shows their weaknesses against fault attacks. Subsequently, it proposes a new countermeasure that prevents such kind of attacks.

Ross et al (1998) described the related disciplines of cryptography and track security and presented a terminology outline of a number of approaches that many of them developed to hide encrypted copyright marks or serial numbers in digital audio or video. It presented a number of attacks, some new, on such information
hiding schemes. This leads to a discussion of the formidable obstacles that lie in the way of a general theory of information hiding systems.

Qiang Tang and Dongyao Ji (2010) described the notion of Verifiable Attribute-Based Encryption (VABE) and given two constructs of key-policy VABE. One is with a single authority, and the other is with multi authorities. Especially, in multi-authority case, if the key does not pass the check, the user only needs to ask the particular authority to resend its own part, without need to go to all the authorities; second, if the keys pass the verification but the user still does not rightly decrypt out the message.

The main obstacle of the data hiding in audio is to develop a system which has the quality to include a big amount of data and without affecting the quality of sound. (Osamah Abdulgader Al-rababah 2005) proposed a novel information-hiding method to hide more information into audios media file (MP3). The bits of information will be hidden between frames (BF) in MP3 file.

Nan Wu and Min-Shiang Hwang (2007) described the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists large variety of Steganography techniques, some are more complex than others and all of them have respective strong and weak points.

The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Mohammed Ali Bani Younes and Aman Jantan (2008) implemented the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and
entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image.

Mobasseri and Berger (2005) developed the algorithm which exploits the inefficiency of the code-space of popular compression standards by recognizing that not all code words appear in the bit stream. By mapping the code words to the outside of the used code-space, it can embed the watermark into the stream as forced bit errors. The decoder recognizes such code words, recovers the watermark from them, and restores the media to its original state.

Min Wu and Bede Liu (2004) it proposed a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates "flippable" pixels to enforce specific block-based relationship in order to embed a significant amount of data without causing noticeable artifacts. Shuffling is applied before embedding to equalize the uneven embedding capacity from region to region.

Most Steganography detection tools rely on signatures that describe particular Steganography programs. Signature-based classifiers offer strong detection capabilities against known threats, but they suffer from an inability to detect previously-unseen forms of Steganography. Mcbride et al (2005) proposed Novel Steganography detection that requires an anomaly based classifier. It presents analysis and discussions on robustness and security issues.

Marvel et al (1999) described the method of digital Steganography, entitled spread spectrum image Steganography (SSIS). This system hides and recovers a message of substantial length within digital image while maintaining the original image size and dynamic range. The hidden message can be recovered using
appropriate keys without any knowledge of the original image. A message embedded by this method can be in the form of text, image, or any other digital signal.

(Maged Hamada Ibrahim 2009) discussed the deniable encryption which is an important notion that allows user (a sender and /or a receiver) to escape a coercion attempted by a coercive adversary, such an adversary approaches the user after transmission, forcing to reveal all the random inputs used during encryption or decryption. Since traditional encryption schemes commit the user for random input, the user is forced to reveal the true values of all the random inputs which are verifiable by using the intercepted cipher text. Lou and Liu (2002) proposed the method to enhance security and the quality of image in spite of high capacity of concealed information. Lin and Tsai (2004) a method is proposed a method to protect a secret image by applying (t, n) threshold scheme.

Lee and Chen.L.H. (2000) proposed an image steganographic model that is based on variable-sized LSB insertion to maximize the embedding capacity while maintaining the image fidelity. Krishna and Vinaya Babu (2010) proposed the model which involves an identified value which is used as nonce (IV), considered a non linear set of values which are used as key and different timings as time stamp rounds which are very important parameters in symmetric data encryption schemes.

Katzenbeisser and Peticolas (2002) described the security of a steganographic communication between two principles lies in the inability of an eavesdropper to distinguish cover-objects from stego-objects, that is objects which contain secret messages.
Johnson and Jajodia (1998) discovered and rendered useless covert messages a new art form known as steganalysis. It provided an overview of some characteristics in information hiding methods that direct the steganalyst to the existence of a hidden message and identify where to look for hidden information.

Jicang et al (2009) proposed the image steganalysis. According to two types of universal blind detection and specific steganalysis, a united-judgment method based on weight and threshold, and also a method based on segment. Hrytskiv et al (1998) proposed image encryption and for steganography to increase the security level of the encoded image and to make it less visible. Finally, two keys are needed to decrypt the image. The efficiency of the proposed approach is demonstrated by the computer modeling.

The definition and several constructions of public-key stegosystems have been introduced by von Ahn and Hopper (2004). (Fitzmann 1996) described a legitimate communication among the prisoners is called cover text, and a message with embedded hidden information is called stego text. Naor and Shamir (1995) discussed cover text distributions that do not admit perfectly secure stego systems.


(Andrew 2007) proposed steganalysis methods for extension of least – significant bit (LSB) overwriting to both of the two lowest bit planes in digital images and there are two distinct embedding paradigms. The author investigated how detectors for standard LSB replacement that can be adapted to such embedding
and how the methods of “structural steg analysis”, which gives the most sensitive detectors for standard LSB replacement, may be extended and applied to make more sensitive purpose – built detectors for two bit plane steganography. Ross and Fabian (1998) discussed a number of possible approaches to a theory of the subject that public key Steganography may sometimes be possible in the presence of an active warden. Mohammed Ali Bani Younes and Aman Jantan (2008) used the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. (Tartakovsky 2006) discussed nonparametric method that can be effectively applied to detect a wide variety of attacks such as denial-of-service attacks, worm-based attacks, port-scanning, and man-in-the-middle attacks. In addition, the proposed detection algorithms are based on the change-point detection theory.

Ross et al (1998) discussed the theoretical considerations lead to ideas of practical value, such as the use of parity checks to amplify covertness and provide public key steganography. (Andrew 2007) proposed the most sensitive detectors for standard LSB replacement that may be extended and applied to make more sensitive purpose-built detectors for two bit plane steganography. Mohammad Ali Bani Younes and Aman Jantan (2008) discussed the experimental results that shows the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion.

(Christian Cachin 1998) described that the goal of Steganography is to hide the presence of a message and to create a covert channel, that can be seen as the complement of cryptography. (Uma Devi 2006) described the stegospace and cover space can be any of the digital media like images, audio, video etc. The advantage of steganography over cryptography alone is that messages do not attract attention
to themselves, to messengers, or to recipients. Steganography and Cryptography are both intended to protect information from unwanted parties and both are excellent means to accomplish this but neither technology alone is perfect and both can be broken.

Nan-I Wu and Min-Shiang Hwang (2007) described that the steganography is a collection of crypto-graphic techniques that provide protection to the secret message by offering it the appearance of an image. Bin Li et al (2011) discussed a survey on steganography and steganalysis for digital images, mainly covering the fundamental concepts, the progress of steganographic methods for images in spatial representation and in JPEG format, and the development of the corresponding steganalytic schemes.

Rajaram Ramasamy et al (2009) implemented encryption/decryption involving the ASCII value of the characters constituting the message, and then subjecting it to the knapsack algorithm. Thomas Chardin and Raphaël Marinier (2009) presented a chosen-plaintext attack of plaintexts in its adaptive version. The predictive-coding-based (PCB) steganography can embed a large amount of bits into the code stream of lossless compression with high imperceptibility. Guangjie Liu et al (2005) proposed that steganalytic method can easily find the presence of a secret message with small error probability. To enhance the scheme’s security, a modified one is proposed, which preserves the prediction errors’ distribution by choosing the optimum adjustment parameter.

An image steganography system, in which the data hiding (embedding) is realized in bit planes of sub band wavelets coefficients obtained by using the Integer Wavelet Transform (IWT). To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas are
defined by a complexity measure used in the Bit-Plane Complexity Segmentation Steganography (BPCS). Ramani et al (2007) proposed a system which shows a high data hiding capacity, while keeping a high fidelity of stego-image.

Kalavathi. Alla, R. Siva Ram Prasad (2005) analysed that the methods of Steganography have been mostly applied on images, audios, videos and text files while the major characteristics of these methods are to change in the structure and features so as not to be identifiable by human users. Naji et al (2009) implemented the system computation between Cryptography and Steganography which embeds information in unused area 2 within EXE files to find a secure solution to cover file without change the size of cover file.

Osamah Abdulgader and Al-rababah (2005) described that one of the main obstacle of the data hiding in audio is to develop a system, which has the quality to include a big amount of data and without affecting the quality of sound. Yu et al (2005) proposed a method which is superior to previous methods that can make a satisfying balance among the most concerned criteria in steganography which are imperceptibility, hiding capacity, compression ratio and robustness against attacks. The performance of the proposed method is evaluated by several experiments on gray-level images with different textural properties.

Yang Wen-chuan and Chen Yu (2010) proposed a solution for supporting low-delay services for the MAC layer and it can realize the dividing of the real time and non-real-time services, and then build a new MAC mechanism serving for different service class by amending the source code of NS2. Freund and Schapire (1999) introduced the boosting algorithm AdaBoost, and explained the underlying theory of boosting, including an explanation of why boosting often does not suffer from over writing as well as boosting's relationship to support-vector machines.
Xingwen Zhao and Fangguo Zhang (2011) described two major flaws. One is that valid group members outside the receiver set can still decrypt the ciphertext, which contradicts the authors' definition for IBBE. The other is that, given a valid private key, it is easy to generate private keys for other people without interacting with Private Key Generator (PKG). Wu Ho and Lee (2004) discussed clustering algorithm, called progressive exponential clustering (PEC) that is applied to increase the embedding capacity by avoiding redundancy. Meanwhile, a cluster expansion algorithm is also developed in order to further increase the capacity without sacrificing imperceptibility.

Wu and Hwang (2005) proposed a new adaptive least-significant-bit (LSB) steganographic method using pixel-value differencing (PVD) that provides a larger embedding capacity and imperceptible stegoimages. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels.

Wang et al (2001) performed data hiding by taking difference value of three and two neighbouring pixels by adapting Zig-Zag traversing scheme (ZZTS). This method enhances security and the quality of image in spite of high capacity of concealed information. Error correction mechanism using hamming code is applied to ensure reliable secret communication. (Mohammed Abbas Fadhil Al-Husainy 2012) proposed method which provides good confusion and diffusion properties that ensures high security due to mixing the two Boolean operations: XOR and Rotation that are done on the bits of the pixels in the image.

Li Chang-Gang et al (2002) analysed that the secret-key and algorithm cannot be separated effectively. This does not satisfy the requirements of the
modern cryptographic mechanism and are prone to various attacks. Li and Zheng (2002) discussed image encryption techniques try to convert an image to another one that is hard to understand and Cheng-Hung Chuang et al (2011) proposed protection of digital images against illegal copying and distribution has become an important issue.

Tseng and Pan (2002) proposed a steganography scheme for hiding a piece of critical information in a host binary image. That scheme ensures that, in each image block of the host image, as many can be hidden in the block by changing at most 2 bits in the block. Tseng et al (2002) proposed a scheme that can conceal as many as bits of data in the image by changing, at most, two bits in the host image. This scheme provides a higher security, embed more information, and maintain a higher quality of the host image than available schemes.

Tzeng and Tsai (2003) proposed an Enhancement of security in detecting tampered images which is achieved by randomly generating the codes and embedding them into randomly selected locations in the image blocks. Tseng and Chnag (2004) proposed a novel high capacity data hiding method based on JPEG. In this method, employer’s capacity table to estimate the number of bits that can be hidden in each DCT component so that significant distortions in the stego-image can be avoided.