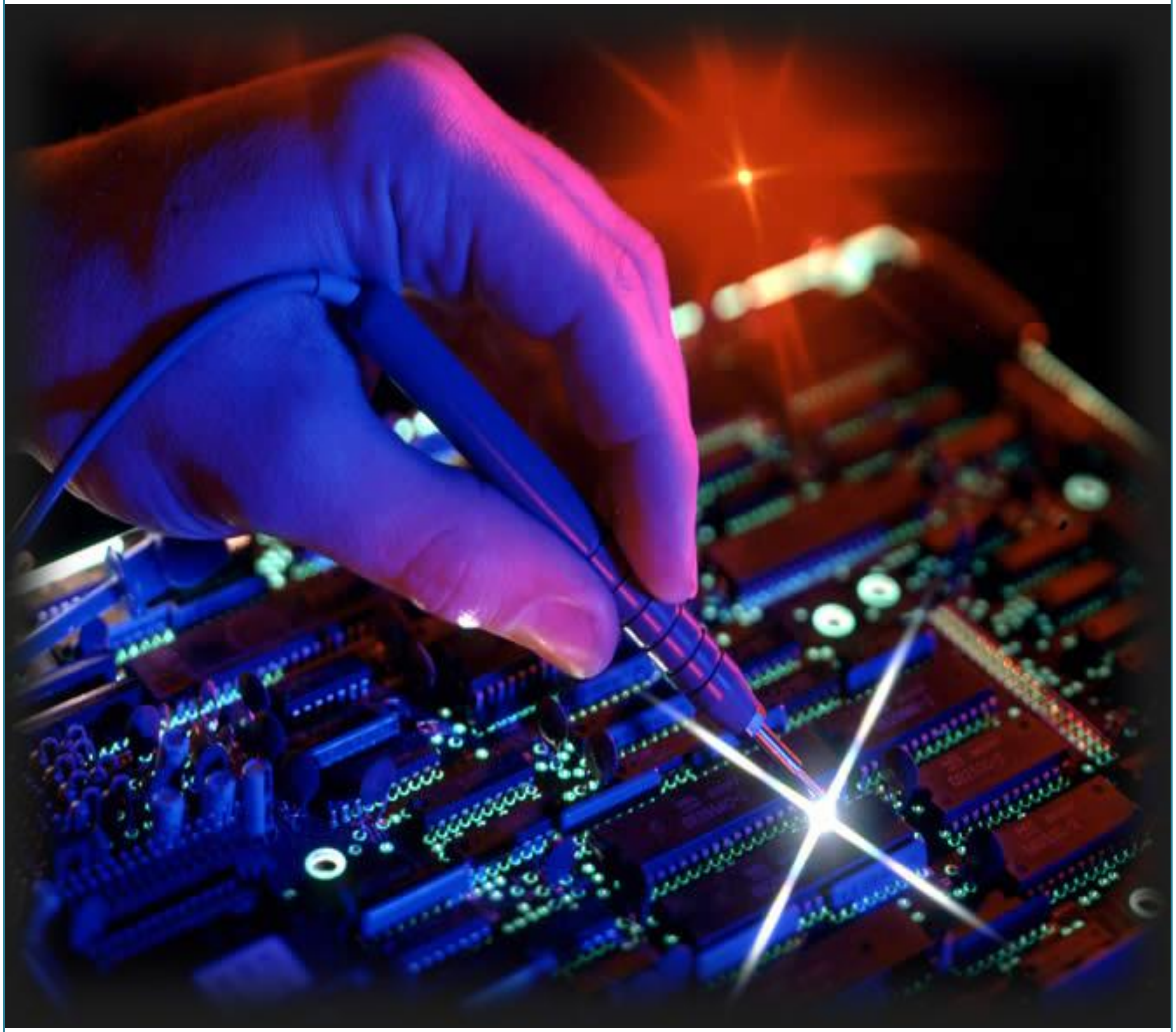
INTERNATIONAL JOURNAL OF COMPUTATIONAL ENGINEERING RESEARCH (IJCER)

ISSN: 2250-3005

VOLUME 1 Nov-Dec 2011 ISSUE 1



Email : ijceronline@gmail.com **Url : www.ijceronline.com**

INTERNATIONAL JOURNAL OF COMPUTATIONAL ENGINEERING RESAERCH (IJCER)

EDITORIAL BOARD

CONTENTS :

BYPASS THE LOOPS IN ENORMOUS NETWORKS

D Kishore Kumar
Assistant Professor, Department of Information Technology, GITAM University

ABSTRACT: ***In general comprehensive networks have chance of frequent failures; this can be failures of links between the routers when they communicate for the routing table which results in loop occurrence. Routers have the terrible feature of updating their routing tables where its convergence time depends on its routing protocols. Here in this paper, a new advanced attempt is made that saves the convergence time as well as the packet losses. The mechanism is Refreshing with Fast Merging (RFM) which regularly amends the forwarding routing tables with very less time. Here we have taken a complicated network of routers for stimulation later there occurs failures in links. These loops can be evaded and shown by constructing a shortest path tree.***

KEYWORDS: ***Refreshing with Fast Merging (RFM), Shortest Path Tree, Link failures***.

INTRODUCITON: Earlier Research networks are Inter network Protocol networks which carried best effort packets where the link state Intra domain routing protocols were used in enormous networks [1]. All these protocols are used in LSP's. Internet service providers mainly obtain links failures as key problem.

Temporary loops when link fails can be occurred due to change in topology. Points of presence used network Point **-** to **-**point link and Local Area Network point to point link Internet gateway Protocol will gather as soon as possible. When the link is not protected locally.

Internet Gateway Provider metrics are the source of changes in Internet Protocol networks. When there is increase in sudden traffic then this Internet gateway provides metric come in to play. A router sometimes facesinternal failures which are the means of software update. The routers keep on updating their forwarding information base the resources are kept up until this job is done and links to forwarded packet will not come in to influence here. When a router is failed then the packets reaching to this router will be deviated to the adjacent router through fast Reroute Technique to a node. So that finally packets reach safely to destination.

OUR APPROACH: University studies have proved that in a large backbone networks routers frequently fail their links. The Internet has been very important personal assistance to every person and also the users are increasing day by day as well as the services are more depended on the Internet. In provide 24*7 reliability to the customers Internet Service Providers should take care of the failures. The routers need to be quickly updated about their adjacent routers in case of failures. So that forwarding packets will not affect the destination. OSPF which is widely used routing protocol for the link advertisements in response to charge in topology which again results in new routing table. This will happen nationwide sometimes which also results in delay in traffic sometimes packets may also be dropped [1].
RFM [3] will mainly achieve two goals
1) evade loops andforward 2) optimal time delay.
RFM prevents when packets losses due to lack of valid routes.
Optimal time delay can be achieved when forwarded packets move along with shortest path as well as network is ready for any change. The disadvantages in this technique results that each packet should also maintain cost of the remaining path to move to the destination. This results in larger byte to the header.

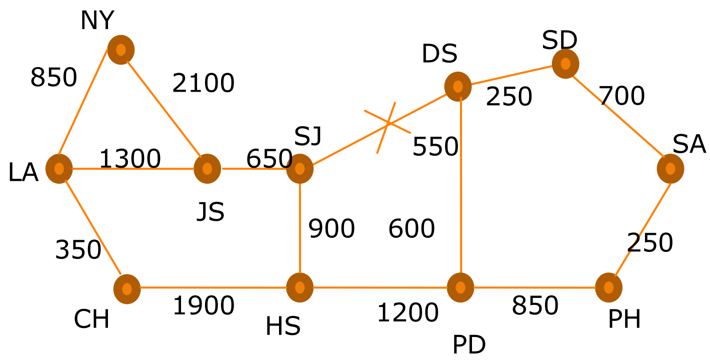
HANDLING LOOPS: During Reverse Shortest path Tree calculations, all the routers independently maintain its waiting list with respect to down link. The refreshing routing table of the Router updated its Forwarding Information Base for a destination.Selecting the outgoing interfaces for destination when updating its Forwarding Information Base according to its new topology is considered for the removal or the metric increase of all the affected links. Completion messages means of a link sent by the router in the form of FIB for all the final destinations before the event [4].If has not updated its FIB for destination, it cannot have sent a completion message for any of the failing links that it uses to reach. The failing links that a router on uses to reach are used by to reach, so that cannot have received all the necessary completion messages for any of those links. In other words, did not send a completion message for the links that it uses to reach. Thus, locks the FIB update for those links long its paths towards them. We provide the pseudo code that implements the ordering with completion messages. A router will compute the reverse shortest path to process the metric increase of a set of link tooted on each link belonging to, that it uses in its current, outdated shortest path tree. The ranking is associated with it [5]. This depends on the next hop or the router to record the path in the list. Neighbors receive completion messages with the link. When the rank is zero with the help of the given link then the forward information base is updated directly for the final destinations via link, and lately sends the completion messages to the corresponding next hop or the router.

When there occur waiting list for the process then it reaches neighbors and starts considerations for the rank via the link. When the waiting list is empty then the times collapses for the update of FIB

```
for each Link X→ Y Є S do
        if X→Y ЄSPTold(R) then
        Link RSPT= rSPT (X → Y);
        LinkRank = depth(R, Link RSPT );
        I(X → Y) = Nexthops (R, X → Y);
        ifLinkRank == 0 then
        foreach d: X → Y ЄPathold(R , d) do
        UpdateFIB(d);
        end
        foreach N Є I(X → Y) do
                send(N, CM(X → Y));
        end
        end
        else
        WatingList(X → Y)=Childs(R,LinkRSPT);
        StartTimer(X → Y, LinkRank * MAXFIBTIME);
        end
end
end
        Upon reception of CM(X → Y) from Neighbor N:
        WatingList(X → Y).remove(N);
        Upon (WaitingList(X → Y).becomesEmpty()
        Timer(X → Y).hasExpride());
        foreach d: X → Y Є Path(R,d) do
        UpdateFIB(d);
        end
        foreach N Є I(X → Y) do
        send(N,CM(X → Y));
        end
```

Pseudo code for Avoiding Link Failures\

We consider a network to explain how to avoid the transient loops occur in the network by converging link state routing protocol. The American cities are connected in this network like San Jose (SJ),San Antonio (SA), Los Angeles (LA), New York (NY), Jack Sonville (JS), Chicago (CH), Houston (HS), Dallas (DS), San Diego (SD), Phoenix (PH), Philadelphia (PD)



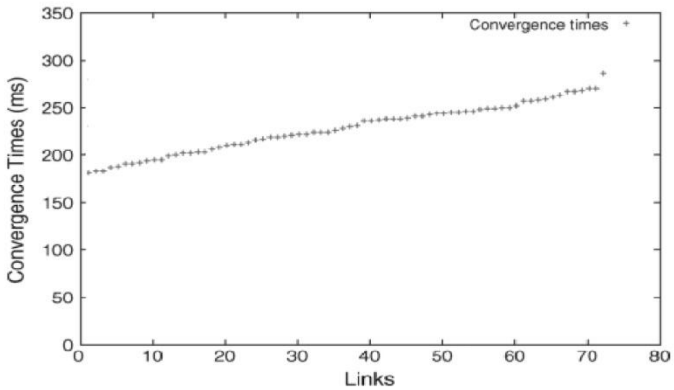
Example: Internet topology with Internet Gateway Protocol Costs

To understand this problem, let us consider the Internet2/Abilene backbone.1 Fig. 1 shows the IGP topology of this network. Assume that the link between SJandDS fails but was protected by an MPLS tunnel between DSandSJ via PDandHS. When PD receives a packet with destination JS, it forwards it to DS, which forwards it back to PD, but inside the protection tunnel, so that SJ will DE capsulate the packet, and forwards it to its destination, JS.

This suboptimal routing should not last long, and thus after a while the routers must converge, i.e., adapt to the new shortest paths inside the network, and remove the tunnel. As the link is protected, the reach ability of the destinations is still ensured and thus the adaptation to the topological change should be done by avoiding transient loops rather than by urging the updates on each router. The new LSP generated by DS indicates that DS is now only connected to SDandPD. Before the failure, the shortest path from PH to SJ, JS, NYandLA was via SA, SDandDS. After the failure, SA will send its packets to SJ, JS, NYandLA via PH, PDandHS. During the IGP convergence following the failure of link SJ−DS, transient loops may occur between SAandPH depending on the order of the forwarding table updates performed by the routers. If SA updates its FIB before PH, the packets sent by SA to SJ via PH will loop on the PH-SA link. To avoid causing a transient loop between PHandSA, PH should update its FIB before SA for this particular failure. A detailed analysis of the Internet2 topology shows that transient routing loops may occur during the failure of most links, except NY−JSandNY−LA. The duration of each loop will depend on how and when the FIB of each router is updated. Measurements on commercial routers have shown that updating the FIB may require several hundred of milliseconds. Transient routing loops of hundred milliseconds or more are thus possible and have been measured in real networks. As shown with the simple example above, the transient routing loops depend on the ordering of the updates of the FIBs. In the remainder of this paper,. This proof is constructive as we give an algorithm that routers can apply to compute the ranks that let them respect the proposed ordering.

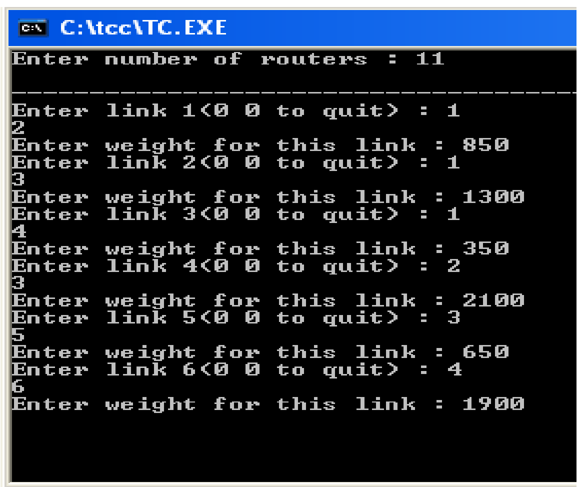
CONVERGENCE TIMES IN ISP NETWORKS: In this section, we analyze by simulations the convergence time of the proposed technique, in the case of a link down event. The results obtained for link up events are very similar. Indeed, the updates that are performed in the FIB of each router for the shutdown of a link impact the same prefixes for the linkup of the link. The only difference in the case of a link up is that the routers do not need to compute a reverse Shortest Path Tree. As no packet are lost during the convergence process.

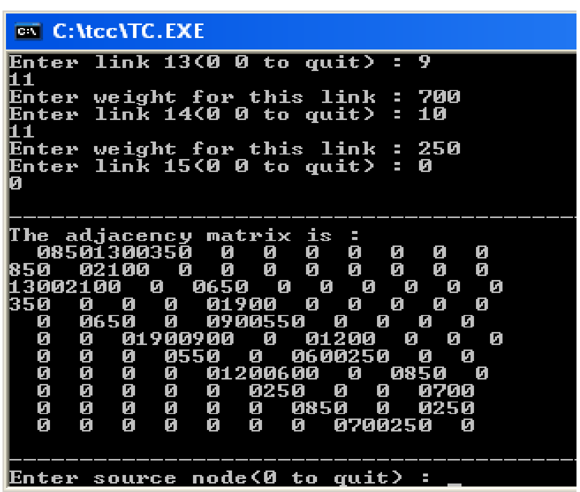
Lsp_process_delay	[2,4]ms
Update_hold_down	180ms
rspt_computation_tome	[3,5]ms
Completion_message_process_delay	[2,4]ms
Completion_message_sending_delay	[2,4]ms

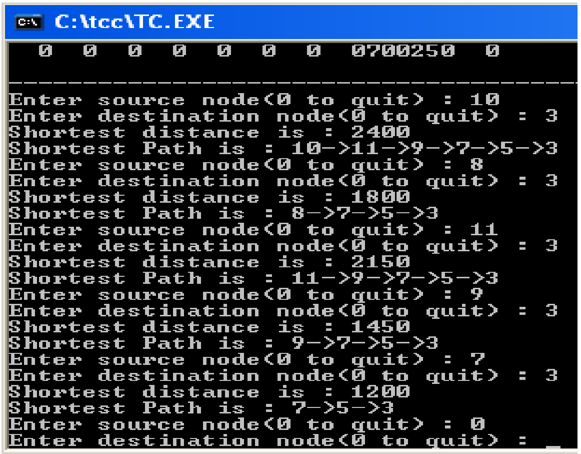


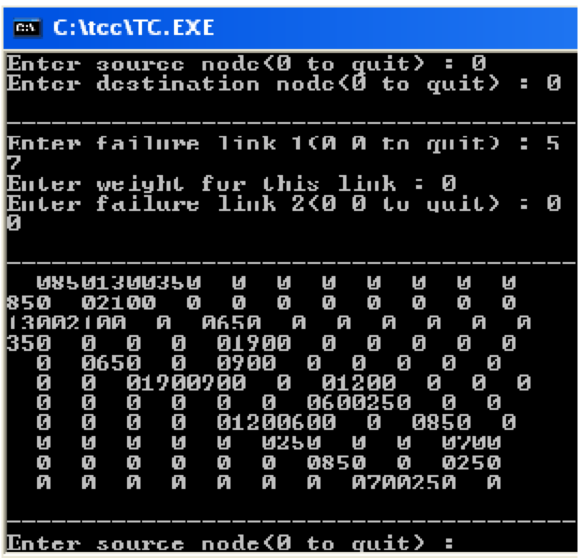
We cannot define the convergence time as the time required bringing the network back to a consistent forwarding state, as it would always be equal to zero. What is interesting to evaluate here is the time required by the mechanism to update the FIB of all the routers by respecting the ordering.

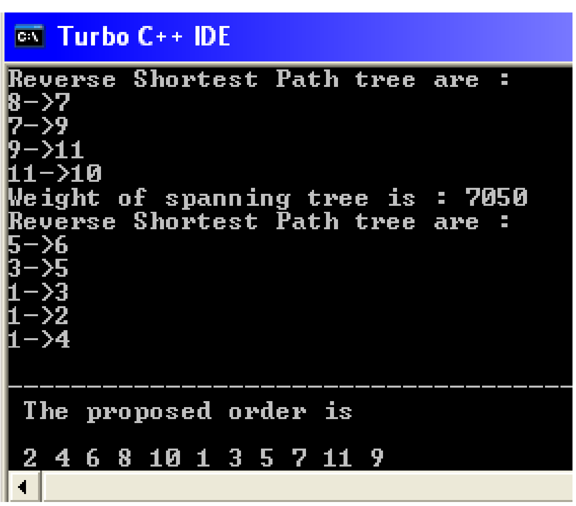
EXPERIMENTAL RESULTS:






C:\tcc\TC.EXE
0 0 0 0 0 0 0 0700250 0
Enter source node(0 to quit) : 10
Enter destination node(0 to quit) : 3
Shortest distance is : 2400
Shortest Path is : 10->11->9->7->5->3
Enter source node(0 to quit) : 8
Enter destination node(0 to quit) : 3
Shortest distance is : 1800
Shortest Path is : 8->7->5->3
Enter source node(0 to quit) : 11
Enter destination node(0 to quit) : 3
Shortest distance is : 2150
Shortest Path is : 11->9->7->5->3
Enter source node(0 to quit) : 9
Enter destination node(0 to quit) : 3
Shortest distance is : 1450
Shortest Path is : 9->7->5->3
Enter source node(0 to quit) : 7
Enter destination node(0 to quit) : 3
Shortest distance is : 1200
Shortest Path is : 7->5->3
Enter source node(0 to quit) : 0
Enter destination node(0 to quit) :


C:\tcc\TC.EXE
Enter source node(0 to quit) : 0
Enter destination node(0 to quit) : 0
Enter failure link 1(0 0 to quit) : 5
7
Enter weight for this link : 0
Enter failure link 2(0 0 to quit) : 0
0
850 02100 0 0 0 0 0 0 0
350 0 0 0 01900 0 0 0 0 0
0 0650 0 0900 0 0 0 0 0
0 0 01700700 0 01200 0 0 0
0 0 0 0 0 0 0600250 0 0
0 0 0 0 01200600 0 0850 0
0 0 0 0 0 0 0850 0 0250
Enter source node(0 to quit) :


Turbo C++ IDE
Reverse Shortest Path tree are :
8->7
7->9
9->11
11->10
Weight of spanning tree is : 7050
Reverse Shortest Path tree are :
5->6
3->5
1->3
1->2
1->4
The proposed order is
2 4 6 8 10 1 3 5 7 11 9

CONCLUSION:

Enormous networks consist of many topologies described above. Router keeps updating their routing table with a Forward Information Base Technique. Updates sometimes causes looped in order to evade them we came up with a technique called RFM (Refreshing and Fast Merging) where packet losses can also be evaded. This is most common in enormous networks. We have proposed aRefresh applicable for the failures of protected links and the increase of a link metric and another ordering for the establishment of a new link or the decrease of a link metric. We also came up with Experimental Results which shows our approach for optimizing this problem.

REFERENCES

[1] P. Francois and O. Bonaventure, "Avoiding transient loops during IGP Convergence in IP Networks," in *Proc.IEEE INFOCOM*, March 2005.

[2] ISO, "Intermediate system to intermediate system routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (iso 8473)," ISO/IEC, Tech. Rep. 10589:2002, April 2002.

[3] P. Pan, G. Swallow, and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels," May 2005, Internet RFC 4090.

[4] M. Shandand S. Bryant, "IP Fast Reroute Framework," October 2006,

[5] A. Shaikh, R. Dube, and A. Varma, "Avoiding Instability during Graceful Shutdown of OSPF," in *Proc. IEEE*

[6] C. Alaettinoglu, V. Jacobson, and H. Yu, "Towards millisecond IGP congergence," November 2000, internet draft, draft-alaettinoglu, ISISconvergence-00.

[7] M. Shand and S. Bryant, "IP Fast Reroute Framework," October 2006.

[8] A. Shaikh, R. Dube, and A. Varma, "Avoiding Instability during Graceful Shutdown of OSPF," in Proc. IEEE.

TWO INPUT PID FUZZY C MEANS POWER SYSTEM STABILIZER

K.R.Sudha[1] Y. Butchi Raju[2]

[1]Department of Electrical Engineering, AU college of Engineering, Andhra University, Visakhapatnam, India

[2] Research Scholar, Department of Electrical Engineering, AU college of Engineering, Andhra University, Visakhapatnam, India

Abstract

Power System Stabilizer (PSS) must be capable of providing appropriate stabilization signals over a broad range of operating conditions and disturbances. Traditional power system stabilizers rely on linear design methods. In the present paper, a novel approach for design of PSS using Fuzzy C Means is presented. The proposed Fuzzy C Means PSS (FCMPSS) is trained with the pre-designed two input PID fuzzy logic PSS(FLPSS). The simulation results of the proposed FCMPSS are compared to those of conventional stabilizers and the pre-designed Fuzzy PSS for a Single Machine Infinite Bus (SMIB) system. The effect of system parameter variations on the proposed stabilizer performance is also examined. The results show the Robustness of the proposed FCMPSS and its ability to enhance system damping over a wide range of operating conditions and system parameter variations.

Keywords: Fuzzy C Means , Power system stabilizer, Dynamic stability.

1. INTRODUCTION

The basic function of a PSS is to extend stability limits which are characterized by lightly damped or spontaneously growing oscillations in the 0.2 to 2.5 Hz frequency range [1]. This is accomplished via excitation control to contribute damping to the system modes of oscillation. Consequently, it is the stabilizer's ability to enhance damping under least stable condition. A PSS can be most effectively applied if it is tuned with the understanding of the characteristics of the power system associated. Considerable efforts have been directed towards developing an adaptive PSS. Machine Learning is considered as a subfield of Artificial Intelligence and it is concerned with the development of techniques and methods which enable the computer to learn. In simple terms development of algorithms which enable the machine to learn and perform tasks and activities. Machine learning overlaps with statistics in many ways. Over the period of time many techniques and methodologies were developed for the design of PSS using machine learning tasks[1]-[4].

The fuzzy logic approach is emerging as a compliment to the conventional approach. The most important advantages of fuzzy controller is that there is a very little mathematical computation [5][[6][7] involved in this method and this control method will not increase the order of the system. It is realized that this method of control can perform very effectively when the operating conditions change rapidly and also when the system nonlinearities are significant. These features make very attractive for power system applications. One of the hallmarks of fuzzy logic is that it allows nonlinear input/output relationships to be expressed by a set of qualitative "if – then rules." Nonlinear control and process models may all be expressed in the form of fuzzy rules. Most fuzzy systems are hand crafted by human expert to capture some desired input/output relationships that the expert has in mind. However often an expert cannot express his or her knowledge explicitly and for many applications, an expert may not even exist. Hence there is considerable interest in being able to extract fuzzy rules from experimental input/output data. The motivation for capturing data behavior in the form of fuzzy rules is easy to understand. An expert can check the rules for completeness and fine-tune or extend the system by editing the rule base. Obviously, it is difficult for human experts to examine all the input/output data from complex system to find the number of proper rules for fuzzy system. To cope with this difficulty, much research effort has been devoted to develop alternative design methods. Recently, methods for extracting fuzzy rules have incorporated clustering techniques.

A common concept of more or less all the clustering techniques is that they are prototype based that are characterized by clustering prototypes Ci. ,i=1,2,….c. Prototypes are used to capture the distribution of data in each cluster. The cluster center ci is instantiation of the attribution utilized to illustrate the domain. The various applications of the unsupervised learning based data clustering can be summarized as:

- It can group data with no label.
- It can be applied for fuzzy and neural modelling as well as to real time modelling
- It can be easily applied for detection of faults and its isolation.
- It is helpful in learning the parameters and structure both in fuzzy and neuro-fuzzy model

2. CLUSTERING:

Clustering is the unsupervised classification[8][9] of patterns (objects, data items or future vectors) into groups (clusters). The main aim of clustering is to divide data set in a way that the data belonging to one cluster is as similar as possible. The idea is to identify the number of sub classes 'c' of clusters in a universe 'x' composed of 'n' data samples and divide 'x' into 'c' clusters. One of the easiest method is the distance between the observed data and if one is able to measure the distance between the all observed data then it can be expected that the distance between the points in the same cluster will be less when compared to the distance between the points indifferent clusters. Based on the requirements the user can decide the number of clusters needed that can be best suit the given purpose.

2.1 BASIC CLUSTERING ALGORITHMS:

The idea to define an objective function and to minimize it for achieving clustering is being used universally for a long time. Apart from basic cluster algorithms many developments, modifications and proposals have been given that aims at improving the performance of the existing cluster algorithms related to a particular problem The basic forms of clustering are crisp or Hard C-Mean (HCM) clustering and soft or Fuzzy C-Mean (FCM) clustering.

2.1.1 Hard C-mean Clustering (HCM)(or) K-Means:

Bezdek developed a powerful classification method for accommodating fuzzy data popularly known as Hard C-Mean (HCM) or K-means clustering, is an algorithm based on finding data clusters in a data set such that an objection function of dissimilarity (or distance) measure is minimized. In most cases this dissimilarity measure is chosen as the Euclidean distance.

A set of n vectors xj , j =1,2.., n , are to be partitioned into c groups Gi, i =1,2,..c . The objective function, based on the uclidean distance between a vector xk in group j and the corresponding cluster center ci , can be defined by

$$J = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \left(\sum_{k.x_k \in G_i} \left\| x_k - c_i \right\|^2 \right) \quad \text{------(1)}$$

Where $J_i = \sum_{k.x_k \in G_i} \left\| x_k - c_i \right\|^2$ is the objective function within group i .

The partitioned groups are defined by a cXn binary membership matrix U, where the element uij is 1 if the jth data point xj belongs to group i , and 0 otherwise. Once the cluster centers ci are fixed, the minimizing uij for equation (1) can be derived as

$$u_{ij} = \begin{cases} 1 \cdots if \left\| x_j - c_i \right\|^2 \le \left\| x_j - c_k \right\|^2, \, foreach, k \ne i \\ 0 \cdots otherwise. \end{cases} \quad \text{------(2)}$$

This means that xj belongs to group i, if ci is the closest center among all centers.

On the other hand, if the membership matrix is fixed, i.e. if uij is fixed, then the optimal center ci that minimizing equation (1) is the mean of all vectors in group i :

$$c_i = \frac{1}{|G_i|} \sum_{k.x_{k \in G_i}} x_k \quad \text{------(3)}$$

where $|G_i|$ is the size of G_i or $|G_i| = \sum_{j=1}^{n} u_{ij}$.

The algorithm is presented with a data set xi =1,2,.. n ; it then determines the cluster centers ci and the membership matrix U iteratively using the following steps:

Step 1: Initialize the cluster center, ci , i=1,2,.. c. This is typically done by randomly selecting c points from among all of the data points.

Step 2: Determine the membership matrix U by Equation (2).

Step 3: Compute the objective function according to Equation (1). Stop if either it is below a certain tolerance value or its improvement over previous iteration is below a certain threshold.

Step 4: Update the cluster centers according to Equation (3). Go to step 2.

The performance of the HCM algorithm depends on the initial positions of the cluster centers, thus it is advisable to run the algorithm several times, each with a different set of initial cluster centers.

Strengths and Weaknesses:

K-means is simple and can be used for a wide variety of data types. It is also quite efficient, even though multiple runs are often performed. Some variants, including bisecting K-means, are even more efficient, and are less susceptible to initialization problems. K-means is not suitable for all types of data however. It cannot handle non-globular clusters or clusters of different sizes and densities, although it can typically find pure sub clusters if a large enough number of clusters is specified. K-means also has trouble clustering data that contains outliers. Outlier detection and removal can help significantly in such situations. Finally, K-means is restricted to data for which there is a notion of a center (centroid).

2.1.2 Fuzzy C-Mean Clustering (FCM):

The main disadvantage of HCM is that it has to assign each data point to exactly one and only one cluster. Also the points which can belong partially to several clusters should be assigned to one cluster only. This drawback is overcome by using FCM clustering. Fuzzy cluster analysis allows gradual membership of data points to clusters measured as degrees in [0,1]. This gives the flexibility to express that the data points can belong to more than one cluster. However, FCM still uses an objective function that is to be minimized while trying to partition the data set. The membership matrix U is allowed to have elements with values between 0 and 1. However, the summation of degrees of belongingness of a data point to all clusters is always equal to unity:

$$\sum_{i=1}^{c} u_{ij} = 1, \forall j = 1, 2..., n \qquad \text{------(4)}$$

The objective function for FCM is a generalization of Equation (1):

$$J(U, c_1, c_2 ... c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}^m d_{ij}^2 \qquad \text{------(5)}$$

Where uij is between 0 and 1; ci is the cluster center of fuzzy group i .

$d_{ij} = \|c_i - x_j\|$ is the Euclidean distance between the ith cluster center and the jth data point; and $m \in [1, \infty)$ is a weighting exponent.

The necessary conditions for Equation (5) to reach its minimum are

$$c_i = \frac{\sum_{j=1}^{n} u_{ij}^m x_j}{\sum_{j=1}^{n} u_{ij}^m} \quad \text{and} \qquad \text{------(6)}$$

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{d_{ij}}{d_{kj}} \right)^{2/(m-1)}} \qquad \text{------(7)}$$

The algorithm works iteratively through the preceding two conditions until the no more improvement is noticed. In a batch mode operation, FCM determines the cluster centers ci and the membership matrix U using the following steps:

Step 1: Initialize the membership matrix U with random values between 0 and 1 such that the constraints in Equation (4) are satisfied.

Step 2: Calculate c fuzzy cluster centers, 1, , ci i=1,2….c , using Equation (6).

Step 3: Compute the objective function according to Equation (5). Stop if either it is below a certain tolerance value or its improvement over previous iteration is below a certain threshold.

Step 4: Compute a new U using Equation (7).Go to step 2.

3. SYSTEM MODEL

The small perturbation block diagram of a synchronous machine connected to infinite bus system [2] is considered. The exciter is assumed to be of the thyristor type. Amortisseur effects, armature resistance, armature pψ terms and saturation are neglected. The linearized model parameters K1 to K6 vary with operating conditions with the exception of K3. The stabilization problem is to design a stabilizer, which provides supplementary stabilizing signals to increase the damping torque of the system.

An infinite bus is a source of constant frequency and voltage either in magnitude and angle. A schematic representation of this system is shown in fig 1.

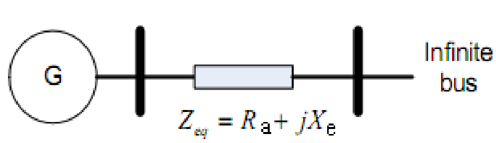


Fig1 Single Machine Connected to infinite busbar

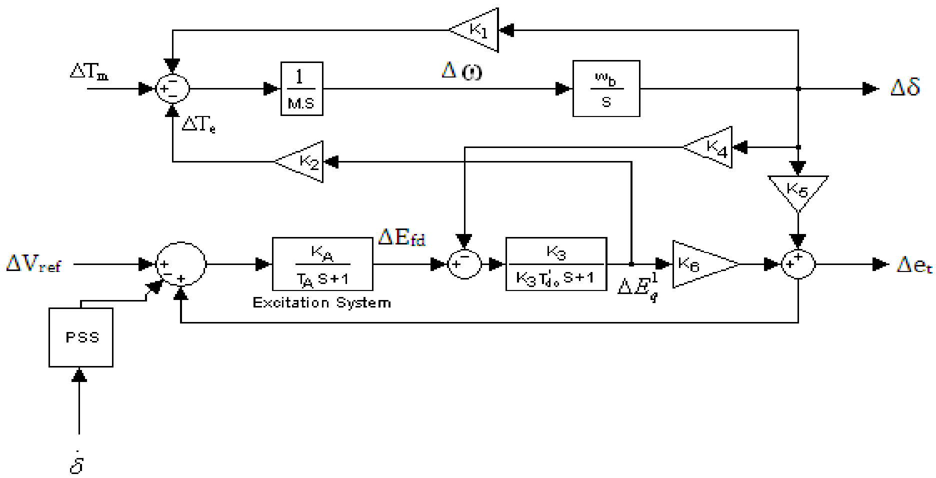


Fig.2 Block diagram representation of the system

4. THE DESIGN OF THE PROPOSED FUZZY CONTROLLER:

Step 1: The Normal Fuzzy controller is designed heuristically with rules shown in Table -4.1
Step 2: The Fuzzy C-Means PSS is tuned to the pre-designed fuzzy PSS .
Step 3: The input space is divided into desired number of clusters using Fuzzy C-Means and the cluster centers are identified. These centers represent the rules of the proposed FCMPSS.
Step 4: The FCMPSS is designed. The designed FCMPSS is tested for a single machine infinite bus system for different operating conditions.

Rule 1	If $X(\dot{\delta})$ is N and $X(\ddot{\delta})$ is N then output is PB
Rule 2	If $X(\dot{\delta})$ is N and $X(\ddot{\delta})$ is Z then output is PS
Rule 3	If $X(\dot{\delta})$ is N and $X(\ddot{\delta})$ is P then output is Z
Rule 4	If $X(\dot{\delta})$ is Z and $X(\ddot{\delta})$ is N then output is PS
Rule 5	If $X(\dot{\delta})$ is Z and $X(\ddot{\delta})$ is Z then output is Z
Rule 6	If $X(\dot{\delta})$ is Z and $X(\ddot{\delta})$ is P then output is NS
Rule 7	If $X(\dot{\delta})$ is P and $X(\ddot{\delta})$ is N then output is Z
Rule 8	If $X(\dot{\delta})$ is P and $X(\ddot{\delta})$ is Z then output is NS
Rule 9	If $X(\dot{\delta})$ is P and $X(\ddot{\delta})$ is P then output is NB

5. NUMERICAL SIMULATION:

In the small signal model the parameters K1-K6 except K3 are functions of the operating condition. K3 is the impedance factor and it is constant. The data as in [21] as follows

xd=1.6 , x'd=0.32 , xq=1.55 ,T'do=6 s, H=5 s, Ta=0.05, Ka=100 ,wb=377 rad/s ,xe =0.4, Re=0.0. All resistances and reactances are in Per unit and time constants are in seconds.

Operating condition	Constants					
	k_1	k_2	k_3	k_4	k_5	k_6
1+j0	1.174	1.468	0.36	1.879	-0.117	0.3011
1+j0.5	1.01	1.149	0.36	1.47	-0.097	0.4184
1-j0.5	1.566	1.729	0.36	2.21	-0.1006	0.798
0.5+j0	0.942	1.07	0.36	1.37	0.5448	0.4391

Table 4.1 k_1 to k_6 Constants at different operating conditions

4.2.1 Simulation Results: The dynamic response of the system with the proposed Two input Single out put PSS, FLPSS and CPSS for 0.05 step change in ΔVref is shown in figures 4.2 to 4.5.

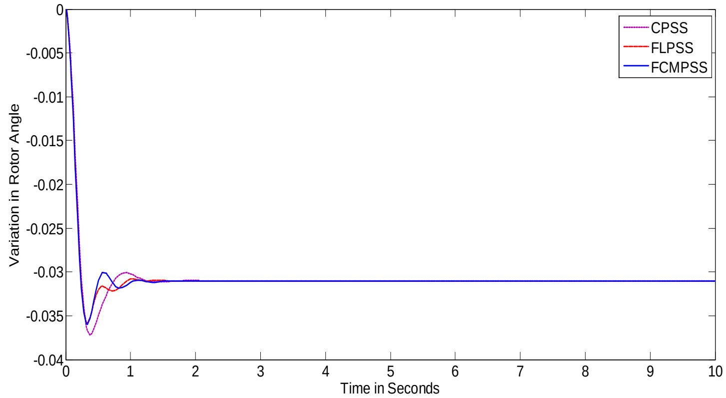


Figure 4.1 (a) Response with CPSS, FLPSS, and FCMPSS for the operating point 1+j0

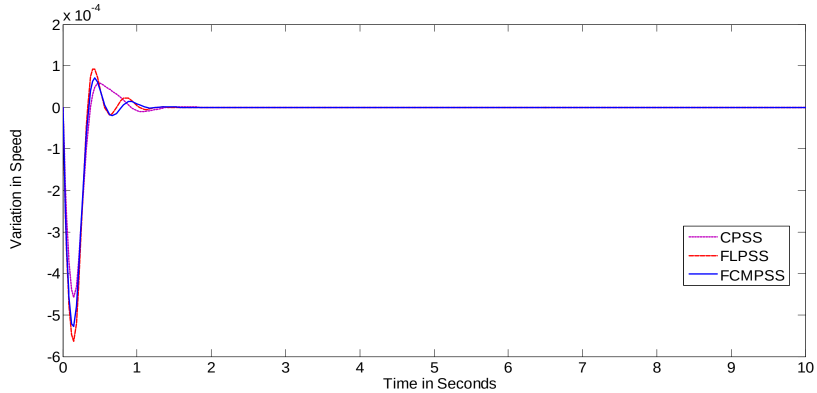


Figure 4.1(b) Response with CPSS, FLPSS, and FCMPSS for the operating point 1+j0

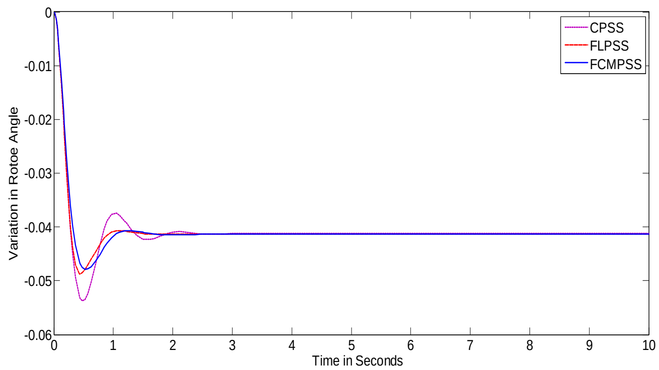


Figure 4.2(a) Response with CPSS, FLPSS, and FCMPSS for the operating point 1+j0.5

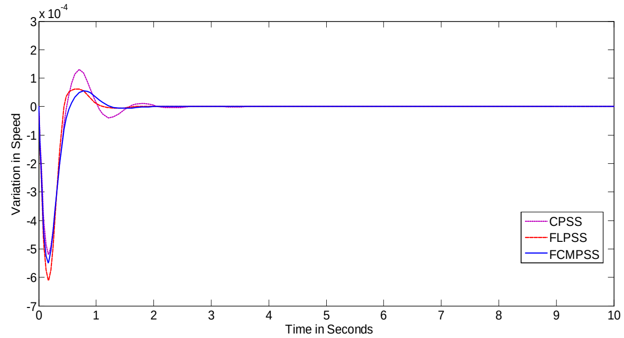


Figure 4.2(b) Response with CPSS, FLPSS, and FCMPSS for the operating point 1+j0.5

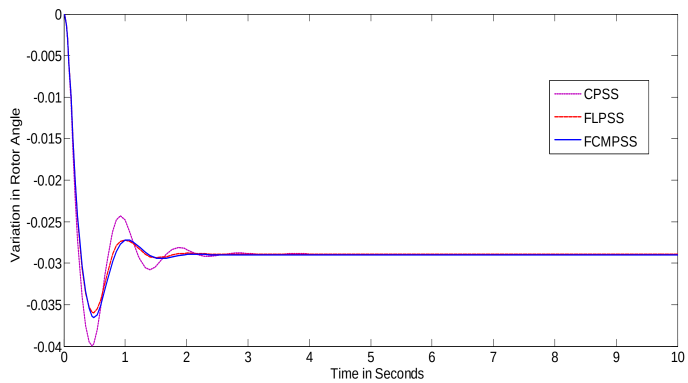


Figure 4.3(a) Response with CPSS, FLPSS, and FCMPSS for the operating point 1-j0.5

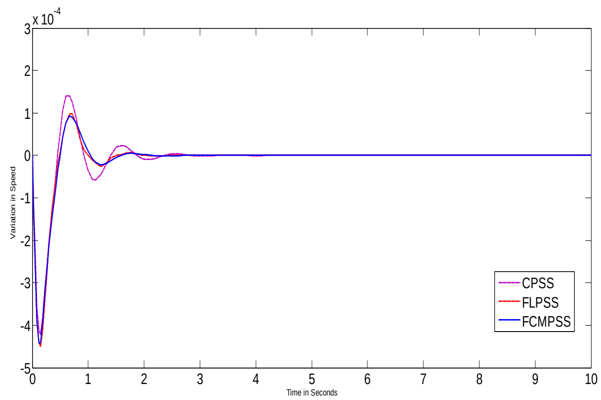


Figure 4.4(b) Response with CPSS, FLPSS, and FCMPSS for the operating point 1-j0.5

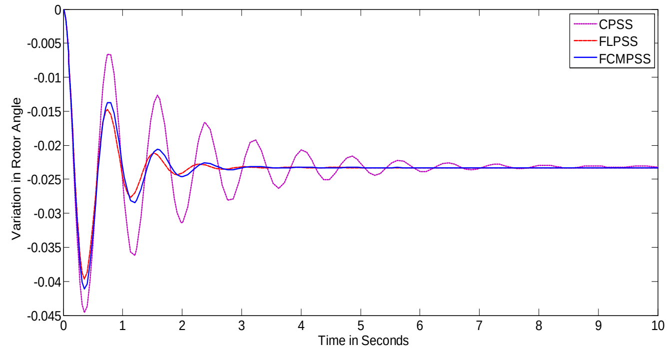


Figure 4.5(a) Response with CPSS, FLPSS, and FCMPSS for the operating point 0.5+j0

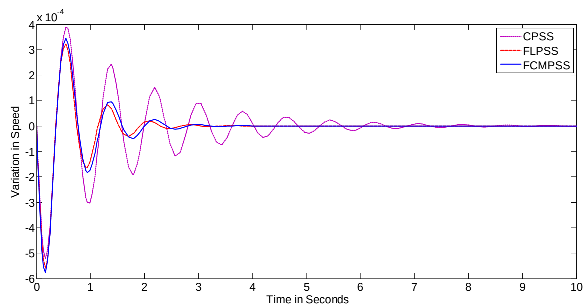


Figure 4.5(b) Response with CPSS, FLPSS, and FCMPSS for the operating point 0.5+j0

5. CONCLUSIONS:

In this study FCM based Power System Stabilizer (FCMPSS) is presented to adapt the PSS parameters to improve power system dynamic stability. Time domain simulations of the system with FCMPSS given a good speed deviation and change in rotor angle response at different type of loading condition. The results show that the performance of the FCMPSS parameters yields the less settling time and less overshoots as compared with conventional PSS parameters.

ACKNOWLEDGMENT:

This work was supported by grants from the All India Council for Technical Education (AICTE) project under RPS Scheme under file No. F.No.8023/BOR/RID/RPS- 94/2008-09.

REFERENCES:

[1] E.V.Larsen and D.A.Swann "Applying Power system stabilizers :General concepts Part I,II,III ",IEEE Transactions on Power Apparatus and systems, Vol. PAS-100, No6 June 1981. pp 3017-3044

[2] F. P. deMello and C. Concordia, "Concept of Synchronous Machine Stability as Affected by Excitation Control," IEEE Transactions on Power. Apparatus and Systems, Vol. PAS-88. April 1969. pp.316-329.

[3] K.R.Sudha, K.A.Gopala Rao "Analytical Structure of Three Input Fuzzy PID Power System Stabilizer with Decoupled Rules" WSEAS Trans. on CIRCUITS and SYSTEMS, June 2004 pp965-970

[4] K.R.Sudha, K.A.Gopala Rao "Analytical Structure of PID Fuzzy Logic Power System Stabilizer Proceedings of IASTED Modelling ,Simulation,and Optimization MSO2004 August 2004

[5]. Ying H., W. Siler and J.J. Buckley, "Fuzzy Control Theory: a Nonlinear Case," Automatica, vol. 26, pp.513-520, 1990

[6]. Ying H., Fuzzy Control and Modeling: Analytical Foundations and Applications, IEEE Press, 2000.

[7]. Ying H., "Deriving analytical input-output relationship for fuzzy controllers using arbitrary input fuzzy sets and Zadeh fuzzy AND operator", IEEE Trans. Fuzzy Syst., vol.14, pp. 654-662, 2006.

[8]. Bezdek.J. C., Pattern Recognition with Fuzzy Objective Function Algorithms, Plenum Press, NY, 1981.

[9]. Chiu S. Fuzzy model identification based on cluster estimation. 1994, Journal of Intelligent and Fuzzy Systems; 2:267–78.

Fuzzy Reliability Analysis in Interconnection Networks

Dr. Sudarson Jena
Associate Professor
Dept. of Computer science & Application
GITAM University, Hyderabad, A.P, INDIA

Ms. K. Deepthi
Asst. Professor
Dept. of Computer science & Engineering
GITAM University, Hyderabad, A.P, INDIA

Abstract
Multiprocessors are quite suitable for task-based applications for the fact that they can support graceful degradation. However the uncertainty associated with the failure ,needs to be addressed for these systems. This paper proposes the fuzzy reliability model for multiprocessor interconnection systems, which takes into an account of uncertainty process. The effect of processor failure rate and coverage on fuzzy reliability is investigated.

Keywords: Reliability, Coverage, Failure rate, Fuzzy reliability, Interconnection network,

I. Introduction
Advances in computer technology and the need to have the computers communicating with each other have led to an increased demand for reliable parallel computing systems. The multiprocessing systems typically consist of an ensemble of processors. They have found wide applications in real time environments and are becoming increasingly popular for large commercial application as well. Researchers in the past have developed techniques for the combined analysis of performance and reliability [2][3]. Reliability of an interconnection system depends upon the reliability of its components. However, for large parallel processing systems, it is very difficult to evaluate the probability of many failures since they might have never occurred before. Also for a system working in an ever-changing environment, feedback does not help much in estimating system reliability using classical statistics. The conventional statistical methods fail to give correct measures of reliability of a parallel computer network. The reason may be, due to insufficiency of failure data, variations due to different reporting sources, variations in application, fluctuations in environmental conditions etc**.,** if they are not due to erroneous modeling.

The multiprocessor systems are quite suitable for task-based applications because of their ability to support graceful degradation. Graceful degradation in multiprocessors can be accomplished through automatic reconfiguration and recovery capabilities provided by the on-line maintenance units [1]. However, the system designer must be certain that faults and errors are detected promptly, so that the redundant processing modules can be utilized. Models that can predict the reliability of systems incorporate a parameter called Coverage(C).

Definition 1. The coverage (C) = Pr{System recover | fault occurs} reflects the ability of the system to automatically recover from occurrence of a fault during normal system operation.
In a practical situation, the error handling naturally depends on the detection of the error, but can range from error correction or masking, to instruction retry, to complete reconfiguration of the system, and thus coverage can be a very difficult parameter to predict in a real life parallel computing environment. Because of system dependencies and the attribute of graceful degradation it is hard to interpret the meaning of success (failure) in a multiprocessor interconnection system. These systems often react to a detected failure by reconfiguring to a state, which may have a decreased level of performance. In these situations, subsystem or component failures may result in the performance degradation.

All the previous analysis on parallel computers has addressed its various aspects using the conventional statistical procedures. However, the uncertainty associated with the system functioning has not received enough attention. The conventional analysis using probability concepts alone is not adequate to treat such imprecise nature of systems performance data. Thus, it has become necessary to develop a new kind of formalism to capture the subjectivity and the impression of failure data for use in reliability analysis. Fuzzy set theory provides a powerful approach for solving these kinds of problems involving uncertainties [4][5]. By resorting to this concept a degree of uncertainty needs to be allocated to each value of the probability of failure and thus different aspects of uncertainty i.e. possibility and probability are treated simultaneously. The concept of fuzzy reliability has been proposed and developed by several authors[7][8].Nahman [6] presented a method for assessment of reliability of non-series parallel network using fuzzy logic. Tripathy et al. [5] have proposed a method to evaluate fuzzy reliability of MIN's. Narasimhan et al. [7] presented a method for evaluating fuzzy reliability of a communication with fuzzy elements capabilities and probabilities. Bastani et. al [8] considered the reliability modeling continuous processor control systems. But none of the methods discussed above suggested a general method of evaluating fuzzy reliability of a multiprocessor interconnection systems where there lies a large degree of uncertainty in system failure. In this paper we present a general and efficient fuzzy probability method for computing reliability of multiprocessor interconnection networks viz. hupercube and star based network..

The rest of the paper is organizes as follows. Section II of this paper presents a topological details of Hypercube and Star graph multiprocessor interconnection networks. In section III Reliability model of multiprocessor system is discussed. Fuzzy reliability analysis has been carried out in section IV. Results are discussed in Section V. Section VI concludes the paper.

II. Topological details

In order to examine the fuzzy reliability of cube-based and a permutation graph based multiprocessor one must consider their topological features in details. The multiprocessors considered here are Hypercube [9], and Star graph[10].

Hypercube

The n-dimensional hypercube can be modeled as a graph $H_n(V, E)$ with the node set V_n and the edge set E_n, where $|V_n| = 2^n$ and $|E_n| = n2^{n-1}$ nodes. The n-dimensional hypercube have 2^n nodes and $n2^{n-1}$ links. The 2^n nodes are distinctly addressed by n-bit binary numbers with values from 0 to 2^n-1. Each node has link at n-dimensions ranging from (lowest dimension) to n (highest dimension) , connecting to n neighbours. An edge connecting nodes $X = x_n x_{n-1}$---------------x_1 and $Y = y_n y_{n-1}$------------y_1 is said to be the dimension j or to the j^th dimensional edges if their binary address $x_n x_{n-1}$--------x_1 and $y_n y_{n-1}$--------y_1 different bit position j only , $x_j \neq y_j$. An edge in H_n can also be represented by n character string with one hypen (-) and n-1 binary symbols {0,1} . For example, in a H_4, the string 00-1 denotes the edge connecting nodes 0001and 0011. The degree of the n-dimensional hypercube is n. Fig. 1 shows the 4-dimentional hypercube.

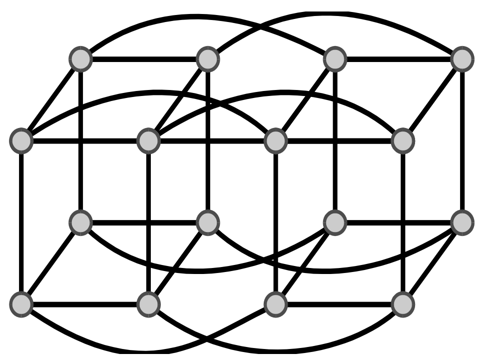


Figure 1. 4-dimensional hypercube (N=16,n=4)

Star graph

Star graph has more complex structure rather than binary n-cube. The n-dimensional star graph S_n is an edge and node symmetric graph containing n! nodes and $(n-1)n!/2$ links. Each node is labeled by a distinct permutation set of integers{1-----n} .Two joints are linked with a link i if and only if the label of the one can be obtained from the label of the other by swapping the first digit (conventionally the leftmost) and the i^th digit where $1<i<n$. *For example:* in S_5 two nodes 12345 and 42315 are neighbors and joined via a link labeled 4. 4-dimentional star graph is shown in fig.2.

Star Graph has been extensively studied for its applications and structured properties . We summarize some of its properties that are relevant to our discussions.

i. The star graphs are members of Cayley group graphs. A star graphs S_n has n-1 generators g_1, g_2-------------g_n where g_i swaps the 1^st symbol with the i^th symbol of any permutation . Each generator has its own inverse i.e the star graph is symmetric. Also the star graph S_n is an $(n-1)$ regular graph with n! nodes $n!(n-1)/2$ edges.

ii. Since Star graphs are vertex symmetric, one can always view the distance between any two arbitrary nodes as the distance between the source node and the identity permutations by suitably renaming the symbols representing the permutations.

iii. It is easy to see that only permutations of n elements can also be specified in terms of its unique cycle structure with respect to the identity permutation. For example 345216 ={135,24,6}. The maximum number of cycles in a permutation of n elements is n and minimum number is 1 .The length of the cycle is defined to be number of symbols present in the cycle.

iv. The dimension of S_n is given by $D_n=[3(n-1)/2]$.

The star graph is an attractive alternative to the hypercube and compares favorably with it in several aspects. For example, the degree of S_n is n-1 i.e sub-logarithmic in the number of nodes of S_n while a hypercube with $\Theta(n!)$ nodes has degree $\Theta(\log n!) = \Theta(n\log n)$, i.e logarithmic in the number of nodes. The same can be said about the diameter of S_n .

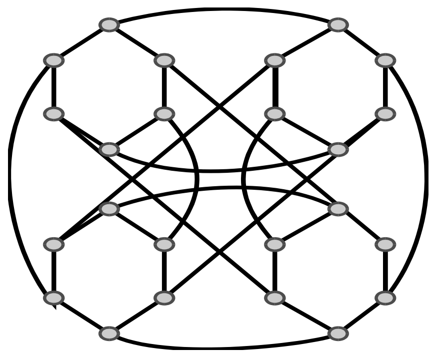


Figure 2. 4-dimensional Star graph

III. Reliability Model of Multiprocessor System

The evaluation of reliability over a systems life cycle is characterized by the notions of stability, growth and decrease that can be stated for the various attributes of reliability. These notions are illustrated by failure intensity, i.e number of failures per unit time. For building a model for multiprocessor, we consider a general case, where, the system consists of N identical processing nodes.

Initially, all the N processors are in fully operational state. Let this state be denoted as S_N. In the event of occurrence of a fault, the fault is detected and the system is reconfigured, or else if the fault is of permanent type, then the failed processors are logically isolated from the system, whereas other processors continue to perform their job without interruption. Let

S_i = The state of the system with *i* operational processors, and there are N+1 states in total.

C = System coverage factor,

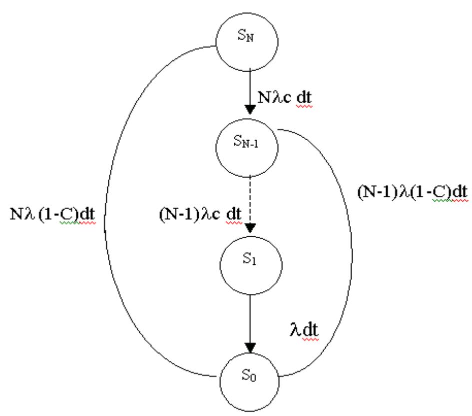


Figure 3. Markov diagram for multiprocessor system.

The Markov Transition diagram for the multiprocessor system can be easily constructed as shown in Figure 1. Now, mathematically, this system can be represented by the following equations.

$$\frac{dp_N}{dt} = -N\lambda_P P_N \qquad (1)$$

$$\frac{dp_i}{dt} = i\lambda_p p_i + (i+1)\lambda_p c p_{i+1} \qquad (2)$$

i =1,2,3………..N-1

$$\frac{dp_0}{dt} = ip_1 + \lambda_P(1-c)j = \sum_{j=2}^{N} jp_j \qquad (3)$$

where $p_i(t)$, i=0,1,2,3……N represents the probability that the system remains in the state S_i at time t. Now, imposing the boundary conditions and assuming

$P_N(t) = 1$, for t=0, we have,

$$P_i(t) = C^{N-1} e^{-i\lambda_P t} \binom{N}{i} (1 - e^{-i\lambda_P t})^{N-1} \quad (4)$$

i= 1,2,3…..…..N

and the system reliability is given by

$$R(t) = \sum P_i(t) \quad (5)$$

where i belongs to successive states.

The above analysis considers the states of a multiprocessor as distinct. However, in a practical situation, because of the system's ability to work in a degraded mode, it is difficult to interpret a state of a multicomputer as success (failure). For the purpose, we consider the states of a multiprocessor as fuzzy state. Consequently, the transition from a fuzzy success state to a failure state can also be considered as a fuzzy event.

IV. Fuzzy Reliability Analysis

Uncertainty and imprecision of information is expected to prevail as the network becomes complex, and even the degree of dependence between the components may not be described deterministically. Under such circumstances, it is difficult to obtain precise reliability measures for a system. Fuzzy set is one of the best tool to model and evaluate such situation. Reliability of a network or node may be evaluated as high, medium and low with the reliability grade scale ranging from 0 to 100% and the membership function of grades ρ in the sets of high, medium, low may overlap partially which corresponds to the nature of the linguistic attributes, i.e same grades may be both medium & low or high & medium. This section presents fuzzy reliability measures of multiprocessor interconnection networks. The following assumptions are made for the development of fuzzy reliability in multiprocessor interconnection network.

Assumptions

i) Initially, all components of the system are in good conditions.
ii) The link failure and link success probability is assumed to be fuzzy numbers.
iii) Failures cannot be determined with certainty
iv) Repair facility is not available
v) Processing modules may fail with a constant exponential failure rate λp

A multiprocessor system in general, consists of much valuable units. Therefore, naturally all failure events incur some economic loss in addition to bringing performance degradation to the overall system. The economic aspect though important, is often ignored while modeling the behavior of a system. In what follows, we build a model for multiprocessor incorporating all the above measures in equation 5.

Let A be a fuzzy set defined on the universe of U. It can be expressed as a set of a ordered pairs $\{x, \mu_A(x)\}$, denoted by

$$A = \{x, \mu_A(x)\} \quad (6)$$

where, x= fuzzy number

$\mu_A(x)$ = membership function bounded by a value between the interval [0,1]

= degree of membership of x in A

Let P denote the probability measure over the universe U, then the probability of A denoted by Pr(A), can be expressed as

$$Pr(A) = \int_A dP \quad (7)$$

Or equivalently, where a finite or countable number of elements $\{x_i\}$, i={1,2,….n} constitutes the universe of discourse, the probability of a fuzzy event A with membership function $\mu_A(x)$ becomes

$$\Pr(A) = \sum_{i}^{n'} \mu_A(x_i) \quad (8)$$

where, P_i is the probability measure corresponding to x_i and n is the number of points constituted by the universe.

Let U= $\{S_1, S_2, \ldots\ldots S'_n\}$ denote the universe of discourse. On this universe, we define a fuzzy success state S and a fuzzy failure state F,

$$S = \{S_i, \mu_S(Si), i=1,2\ldots n'\}$$

$F = \{S_i, \mu_F(Si), i=1,2,\ldots\ldots n'\}$

The transition from fuzzy success state to the fuzzy failure state is denoted as T_{SF}. Since a multiprocessor system behaves stochastically in the time domain.

Defination 2.

Fuzzy reliability (FR) of the system in $[t_0, t_{0+1}]$ as: $R(t_0, t_{0+t}) = Pr\{T_{SF}$ does not occur in the time interval $[t_0, t_{0+t}]\}$.

Since both S and F are fuzzy states, the transitions between them are consecutively fuzzy events. This justifies our approach to assume T_{SF} as fuzzy event. We can define T_{SF} on the universe U_T

$U_T = \{m_{ij}\}$; i, j = 1,2,….n',

Where, m_{ij} = transition from state S_i to S_j with membership function:

$\{\mu_{TF}(m_{ij})\}$; i, j = 1,2,….n

i.e. $T_{SF} = \{m_{ij}, \mu T_{SF}(m_{ij})\}$; i.j=1,2,…..n

$$\beta_{F/S}(S_i) = \frac{\mu_F(S_i)}{\mu_F(S_i) + \mu_S(S_i)}$$

Then, $\beta_{F/S}(S_i)$ can be viewed as the grade of membership of S_i. It is reasonable to say that the transition from S_i to S_j makes the transition from S to F possible to some extent if and only if

$\beta_{F/S}(S_j) > \beta_{F/S}(S_i)$ holds.

Therefore ,

$$[\mu T_{SF}(m_{ij})] = \begin{cases} \beta_{F/S}(S_j) - \beta_{F/S}(Si); & \text{when } \beta_{F/S}(S_j) > \beta_{F/S}(S_i) \\ 0; & \text{when } \beta_{F/S}(S_j) \le \beta_{F/S}(S_i) \end{cases}$$

Based on the above discussions, the general expression of fuzzy reliability process is developed. Incorporating the concept of fuzzy success/ failure state in equation 5. The Fuzzy reliability can be evaluated as

$$FR(t) = \sum_{i=1}^{N} \{1 - \mu T_{SF}(m_{ij})\} P_i(t)$$

Considering the economic loss to nonlinearly increase by a factor x', with increase in the number of faulty modules , we define

$$\mu_S(S_i) = \frac{i}{N}$$

$$\mu_F(S_i) = 1 - \left(\frac{i}{N}\right)^{x'}, \quad i=0,1,2,\ldots,N$$

It can be noted that here, the conventional concept $\mu_F(S_i) = 1 - \mu_S(S_i)$ does not hold good. It may also be noted that $Pr(F) \neq Pr(T_{SF}).Pr(S)$

Therefore, the degree of the membership function becomes

$$\mu_{T_{SF}}(m_{N_i}) = \frac{\mu_F(S_i)}{\mu_F(S_i) + \mu_S(S_i)} = \frac{1 - (\frac{i}{N})^{x'}}{1 - (\frac{i}{N})^{x'} + \frac{i}{N}} \quad \text{where, } i = 0,1,\ldots, N$$

Now, Fuzzy Reliability of a system is expressed as

$$FR(t) = \sum_{i=t}^{N} \{1 - \mu T_{SF}(m_{ij})\}.Pr\{S_i \mid t_0\} = \sum_{i=1}^{N} \frac{(\frac{i}{N})^{x'}}{1 - (\frac{i}{N})^{x'} + \frac{i}{N}} C^{N-i}.e^{-i\lambda_p t} \binom{N}{i} (1 - e^{-\lambda_p t})^{N-i}$$

V. Results and Discussions

In this section, results on various fuzzy reliability measures of multiprocessor interconnection networks are presented. Fig. 4 and fig. 5 shows the effect of processor failure rate (**λ_p**) on the fuzzy reliability of star based and hypercube networks. From these figures, it is observed that at time t=500 hrs, coverage c=1.0 and economic loss factor x'=2, the effect of variation of **λ_p** on the fuzzy reliability of a 5- dimensional star (SC_5) is more, compared to 5- dimensional(HC_5). Further, with the increase in processor failure rate, the fuzzy reliability of both star and hypercube multiprocessor networks decreases. For example, when the processor failure rate increases from 0 to 0.0004, the fuzzy reliability of SC_5 and HC_5 gradually decreases.

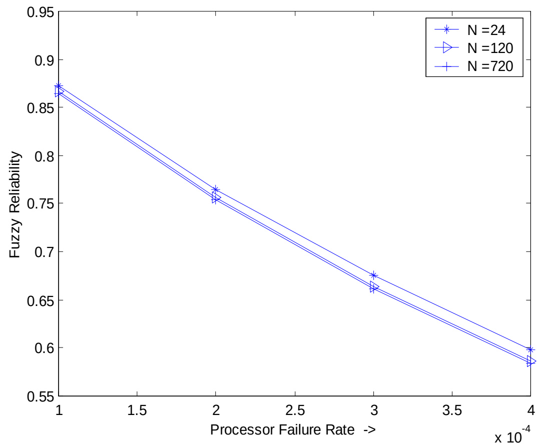


Figure 4 Fuzzy reliability of star graph multiprocessor with processor failure rate

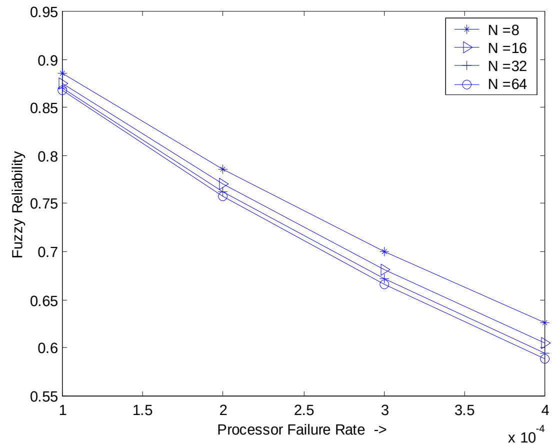
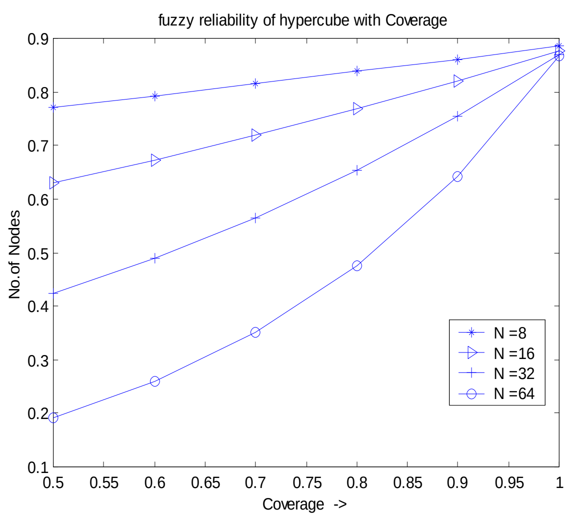


Figure 6Fuzzy reliability of Hypercube multiprocessor with Coverage

Figure 5 Fuzzy reliability of hypercube multiprocessor with processor failure rate



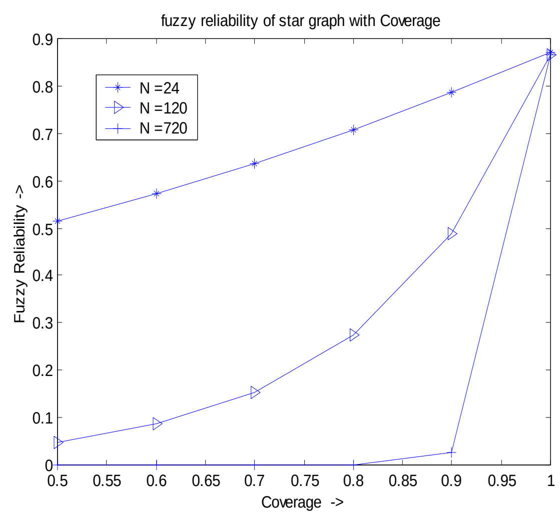


Figure 7 Fuzzy reliability of Star based multiprocessor with Coverage

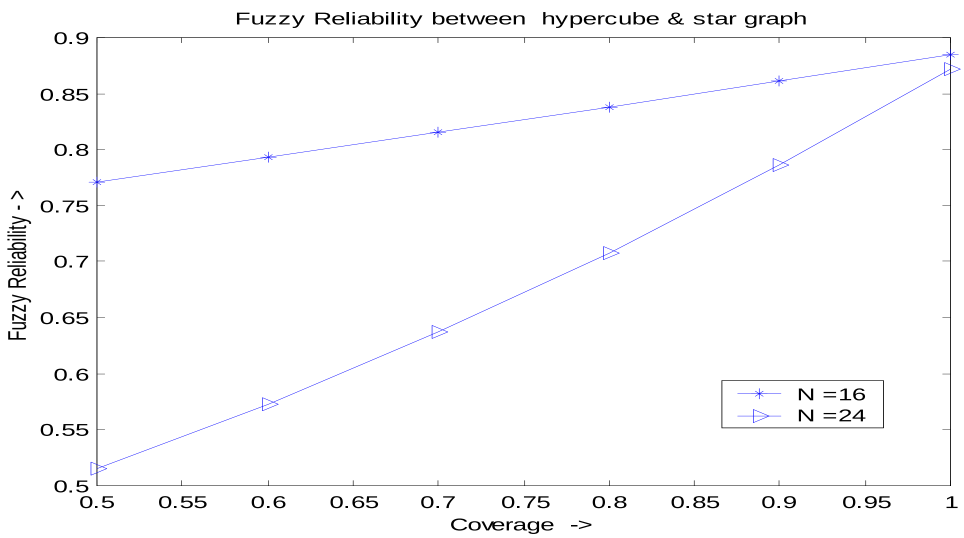


Figure 8 Comparision of Fuzzy reliability between Hypercube and Star graph

Again the fuzzy reliability of hypercube decreases with increase in dimensions. The rate of decrease is more from dimension 3-4 as compared with the decrease from 4-5. Fig.8 compares the fuzzy reliability of both hypercube and star based network. It is observed that with increase in the system coverage, the fuzzy reliability of hypercube improves more compared to star based network.

VI. Conclusion

In this paper the reliability aspect of multiprocessor systems have been discussed. The paper develops fuzzy reliability model for grace fully degrading multiprocessor system. The fuzzy reliability model has been evaluated for two classes of multiprocessor interconnection system viz: hypercube and star graph. Results for fuzzy reliability of various processor failure rate and coverage have been presented. It is observed that fuzzy reliability improves more in hypercube than star graph with increase in the system coverage.

References

1. B.R.Orgerson and R.F Fretters, A Reliability Model for gracefully degrading and standby sparing systems, *IEEE Trans. Comput*, C-24(5),517-525,1975.
2. N.L Benitez and K S Trivedi, Multiprocessor Performability Analysis, *IEEE Trans. Relib*, 42(4), 579-587, 1993.
3. J.T. Blake and K S Trivedi, Reliability Analysis of Interconnection Networks using Hierarchical Composition, *IEEE Trans. Relib*. 38,111-120, 1989.
4. A Kaufmann and M.M. Gupta, Fuzzy Mathematical Models in Engineering and Management Science, *Elsevier Science Publishers*, The Netherlands, 1988.
5. C.R Tripathy, R.N.Mohapatro and R.B. Mishra, A Method for evaluation of Fuzzy Reliability of MINS, *Comp.Sc. and inf. Journal*, 25(4),17-29,1995 .
6. J.Nahman, Fuzzy Logic based Network Reliability Evaluation, *Microelectron. Reliab*., 37(8), 1161-1164, 1997
7. S. Narasimhan and S.Asgarpoor, A Fuzzy- based approach for generation system reliability evaluation, *Electric Power Systems Research*, 53, 133-138, 2000.
8. F.B.Bastani, I.R.Chen and T.Tsao, Reliability of systems with fuzzy- failure criterion, *proc. Annual Reliab. And Maint. Symp*., 1994, 442-448.
9. S. Abraham and K. Padmanabhan, Performance of the direct binary n-cube networks for multiprocessors, *IEEE Trans. Computers*, 37(7), 1000—1011, 1989.
10. S.B Akers et al. The Star graph: An attractive alternative to the n-cube, *Proc. Intl. Conf. Parallel processing*, 1987, 393-400

CYBER BULLYING AND ACADEMIC PERFORMANCE

Dr. Qais Faryadi
Faculty of Science and Technology
Department of Computer Science
Universiti Sains Islam Malaysia
USIM

ABSTRACT
This research investigates the emotional and physiological effects of cyber bullying on the university students. The primary objective of this investigation is to identify the victims of cyber bullying and critically analyze their emotional state and frame of mind in order to provide them with a workable and feasible intervention in fighting cyber bullying. In this research a triangulation method (quantitative, qualitative and descriptive) is employed in the investigation. The instruments used in this study, in which 365 students participated, included questionnaires, interviews, checklists and observations. The results of the study indicated that a significant number of the respondents 35 (13%) had suffered emotionally due to cyber bullying. Furthermore, 300 (85%) of the respondents indicated that in their views cyber bullying causes emotional and psychological stress. Further, majority of the respondents 255 (70%) agreed that cyber bullying adversely affects students' academic performance. Results further designate that 60 (16.6%) of the respondents specified that they had bullied someone inside the university at least 2 or 3 times a month while 4 (1.1%) of the participants said that they had bullied someone outside the university at least 2 or 3 times a month. It is interesting to note that majority of the students 75 (20.8%) signify that they have heard bullying taking place inside the university.

Index Terms: Computer, internet, bullying, student, emotional psychology

INTRODUCTION
Modern technology is continuously evolving, and in recent times, it has manifested itself in a very serious social problem, namely cyber bullying. Modern technology is like a double-edged sword; on one hand it gives us connectivity, on the other it increases emotional stress (Michel, 2011). As such, young internet users, including students, may be at the mercy of cyber bullies. The victims, under great emotional stress, are unable to concentrate on their studies, and thus their academic progress is adversely affected (Juliana, 2010). Unfortunately little attention is given to this global problem by institutions of higher learning, teachers, parents and emergency service providers. The depressive effect of cyber bullying prevents students from excelling in their studies (Lauren, 2011).

Bullying in schools and universities are causing unimaginable problems to students, parents and to educational institutions. Unfortunately little has been done to help those victims who are continuously trapped in the name of modernization and digitalization (Watson, 2010). Researchers agree that the stressful impact of bullying is escalating with the rapid expansion of technological advancement (Justin, 2011). Many students who are victims of cyber bullies suffer silently; they are reluctant to complain to the authorities or their parents owing to the social stigma attached to victims of bullies (Susan, 2011). As such, parents, teachers and institutional authorities have to be on the lookout for such occurrences.

PROBLEM STATEMENT
Cyber bullying is an online aggressive behaviour in the digital space. Bullying is a form of peer aggression which can be as damaging as any form of conventional aggression (Mickie, 2011). The problem investigated in this research concerns cyber bullying that disturbs university students psychologically and emotionally. Bullying also prevents students from achieving good grades. It seems that technologies are in some ways creating more stress on our young in the form of cyber bullying rather than to help them progress. Research findings have shown that young students who become victims of cyber bullies suffer great stress (Elizabeth, 2010). Hence there is an urgent need to understand the problems faced by the victims so that concrete and proactive measures can be taken by university authorities, teachers and parents to address this global problem.

LITERATURE REVIEW

The Internet has created a new paradigm shift in communication. Today our youth are addicted to using electronic communication tools. It is an undeniable fact that electronic-based communication has transformed our lives tremendously, but unfortunately, there is a dark side to this technological advancement. Cyberspace is a potential site for violence, victimization and oppression (Faye, 2011). According to Olweus (1993), "a student is being bullied or victimized when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other students." Hence, bullying is showing aggressive behavior to a person without any prior provocation with the intention of causing harm.

It also denotes that the harm is done repeatedly over time and there is a disparity in strength and power between the victims and cyber criminals. Electronic bullying or cyber bullying, according to Kowalski (2011) simply indicates using the Internet to cause psychological and emotional disturbances. Olthof (2011) defines cyber bullying as a *strategic behavior* of an individual to dominate another individual or a group of individuals. Online Oxford Dictionary defines cyber bullying as *the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.* Cyber bullying is defined by Wikipedia as a deliberate act of aggression using technological advances such as internet to cause harm to a person. This aggression can be repeated, deliberate hostility. Cyber-bullying occurs *"when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person"* (http://en.wikipedia.org/wiki/Cyber-bullying).

Cyber bullying causes grave harm to an individual or group of people by exposing their personal data, real names and addresses to criminals with malicious intent to the targeted individual or group. *Cyber bullying can include such acts as making threats, sending provocative insults or racial or ethnic slurs, gay bashing, attempting to infect the victim's computer with a virus, and flooding an e-mail inbox with messages* (WatIs.com).

According to Olweus, (1986, 1993) the following are some symptoms of victims of cyber bullying:

1. Anxious, insecure, unhappy and have low self-esteem
2. Cautious, sensitive, quiet, withdrawn and shy
3. Depressed and engaged in suicidal ideation much more often than their peers
4. Do not have a single good friend to discuss problems.
5. Often physically weaker than their peers in the school.

The following are some characteristics of cyber bullies:

1. Often involved in other antisocial activities such as drug use.
2. Impulsive and easily angered
3. Strong need to dominate other students.
4. Show little empathy toward students who are victimized
5. Often physically stronger than other students in the class.
6. Often defiant and aggressive, including to parents and teachers.

Cyber bullying also happens when a person's name is used to publish undesirable materials online, thus causing character assassination of the victim. Character assassination can be done through e-mail, chat room, sms, calls, social network, twitter, MySpace, Facebook, discussion boards, on-line forums, blogs, instigation and rumors. Recent findings indicate that cyber bullying is becoming a pervasive problem around the world and it is increasing alarmingly. (John, 2011). The psychological effects of cyber bullying in our society and institutions cannot be ignored any longer (Bulent, 2009). As the social networking domain expands in cyber space, it inevitably creates more opportunities for cyber criminals to victimize young, unsuspecting internet users (Allison, 2009). Research findings have shown that cyber bullying causes emotional and physiological damage to defenseless victims. (Yavuz, 2010).

SIGNIFICANCE OF THE RESEARCH

1. The finding of this research provides up to date information about the nature and extent of cyber bullying among the university students.
2. The finding of this research will assist the university authorities, lecturers and parents to take more effective steps to combat cyber bullying.
3. Records of interviews, observations and questionnaires are valuable assets for future researchers in finding workable solutions to cyber bullying.

METHODOLOGY

This research applied a triangulation method to carry out the investigation. Data were collected using quantitative, qualitative, observation and descriptive methods. The study applied direct or passive observation in the investigation. In passive observation the researcher has no influence on the students. The qqualitative method was used to collect and analyze data while the quantitative method was used to further strengthen the qualitative data. In research it is better to use both eyes rather than one (Thompson, 2004). Research further indicates that qualitative methodology is very naturalistic and conducted in real time with the investigator in control (Bogdan & Biklen, 2003; Golafshani, 2003). Faryadi, 2010).

POPULATION AND SAMPLE

This study was conducted at a university level in Malaysia. Student enrolment was around 8,000 students (at the time of writing); 365 first year students were randomly chosen to participate in the study. Students' parents were given special questioners so that their feedbacks might reveal significant information about their children's unusual behavior.

INSTRUMENTS

The data for this study were collected through the following instruments: (1) Questionnaires for students' parents; (2) Questionnaires for students; (3) Interviews with selected students; (4) Observation of participants and field notes.

VALIDITY AND RELIABILTY OF THE INSTRUMENTS

Even though the questionnaires used in this study were derived from a well known psychologist and theorists, the researcher submitted the questionnaires to a panel of linguistic experts and English Language experts for their perusal. Furthermore, copies of the research questions, problems, goals, objectives were also submitted to these professionals for further advice. The feedback obtained from these experts was useful for increasing the validity of the instrument. A set of reliability tests was also conducted to determine the Cronbach's Alpha reliability coefficient. The Cronbach's Alpha reliability coefficient was noted at .945, indicating that all the instruments used in this study were satisfactory and reliable.

DATA COLLECTION PROCEDURE

The instruments for the study were administered by the researcher. All the data in the questionnaires were also personally collected by the researcher. The whole process took one week.

DATA ANALYSIS PROCEDURE

The framework for data analysis in this study was adopted from the model developed by Miles and Huber man (1994) to describe the major phases of the data analysis. The primary tools used to analyze collected data were the Statistical Package for Social Sciences (SPSS version 16.0) and Microsoft Excel to determine means, standard deviations, frequencies, counts and percentages of the data. A combination of deductive and inductive analyses was used to organize the collected data. Data were then categorized and meaningfully reconfigured. Crucial data were selected and focused, simplified and abstracted for easy comprehension. Data conformity and validity were verified. Data were cross-checked several times to determine their validity and reliability.

RESULTS

The results signify that cyber bullying indeed affected students academically as well as emotionally. Ninety-five percent of the participants (95%) denoted that they were scared and worried about cyber bullying in the classrooms. The majority of the respondents 300(85%) were of the view that if concrete action was not taken to curb cyber bullying, many students would be affected emotionally. Furthermore, the majority of the respondents 255(70.8%) held the view that cyber bullying had an adverse effect on the victims' academic performance. Data collected from the parents 55 (22%) indicated that their children are worried without apparent reasons. Parents further indicated that they suspect cyber bullying might be the main cause of their mood change. Few parents (10%) designated that their children are depressed most probably due to cyber bullying.

Results from observation specify that 35% of the population in the class showed sign of worries on their faces. The instruments used to collect data were video recording, note taking and digital photography. Many extra ordinary incidents such as students' gesture, facial expressions and body languages are simply self-explanatory about difficulties they face in the class.

SUMMARY OF THE RESEARCH INSTRUMENTS AND THE RESPONDENTS

No	Instruments	Respondents	Sample	Collection
1	Questionnaire	Parents	360	250 (69.4%)
2	Questionnaire	students	360	300 (83.3%)
3	Interviews	Students	50	50 (100%)
4	Observation	Students	360	100%

Table 1 Summary of the Research Instruments and the Respondents

Table 1 shows the summary of the instruments and the responses. It is interesting to observe that the data collection was smooth and satisfactory. Results indicate that out of 360 parents 250 (69.4%) agreed to participate in the study while out of 360 students 300 (83.3%) were took part in the research. Unstructured interviews were conducted to determine the effect of cyber bullying in their academic performance. Students were divided into five groups for better communication and management.

It is worth mentioning that the questions tendered to the participants were not formal questionnaires. The prime purpose of having informal questions was to make participants feel free and keep talking. Majority of the participants (85%) interviewed indicated that cyber bullying indeed affects students academic performance such as their grades. To a question *do you think bullying causes students to suffer psychologically and emotionally?* Majority of the participants (99%) were of the view that bullying in fact causes psychological and emotional effects on students. To another question *do you think bullying can affect students' academic performance such as grade?* 99% of the participants viewed cyber bullying indeed affects students' performance in the exam.

A two- hour observation was undertaken in the lecture hall to critically observe students behavior change. Results from observation and field notes indicated that there was no specific or immediate mood change in the classroom. However, when students went out of the classroom, observation showed sign of worry on their faces as some looked confused.

STUDENTS PARTICIPANTS BY GENDER

Boys	Girls	Age	TOTAL
35	325	21	360(100%)
PARENTS BY GENDER			
Male	Female	Age	Total
125 (50)	125 (50%)	43	250 (83.3%)

Table 2 student participants by gender.

Table 2 points out that majority of the participants are 21 years old female while parents participants were intentionally chosen equally. Table 3 also shows significant number of students N= 360 (100%) and their parents N= 250 (83.3%) has participated.

STUDENTS CLASS OBSERVATION AND CHECKLIST RESULTS

Table 3
Class

No	Evaluation Criteria	Responses
1.	Did the students enter the class in a happy mode?	(No)
2.	Did the students pay attention to the teacher?	(No)
3.	Did the students ask any questions during the lesson?	(Yes)
4.	Were the students motivated in the class?	(No)
5.	Did the students retain the lesson and continue to learn?	(No)
6.	Did the students remain happy in the class?	(No)
7.	Did the students understand the lesson?	(Yes)
8.	Did the students complain about class condition?	(Yes)
9.	Were the students confident in the class?	(No)
10.	Did the students annoy the teacher? (Mood change)	(Yes)

Observation Results

The above class observation and checklists signify that majority of the responses 60% (6 out of 10) were negative based on pre determined checklists. It is interesting to note that only 4 out of 10 (40%) are positive. It shows that majority of the students were not happy in the class perhaps due to some sort of emotional disturbance (Cyber Bullying).

SUMMARY OF IMPORTANT QUESTIONNAIRES FOR STUDENTS 1

	Do you think bullying causes students to suffer psychologically and emotionally?	Do you think bullying can affect students' academic performance such as grade?	Have you ever been cyber bullied **inside** the University?
Yes	300 (85%)	255 (70.8%)	35 (13.8%)
No	60 (5%)	55 (15.2%)	300 (83.3%)
Sometimes	0%	0%	0%
Most probably	0%	0%	5 (1.3%)
Once or twice	0%	0%	20 (5.5%)

Table 4 summary of important questionnaires for students 1

Table 4 signifies that majority of the respondents 300 (85%) agree that bullying indeed causes devastating impact on students emotion and equally causes unimaginable psychological problems among the youths. It is of value to note that majority of the students 255 (70%) agreed that cyber bullying has a negative effect on students academic performance while only 55 (15.2%) have indicated to the contrary. A significant number of participants 35 (13.8%) have mentioned that they indeed been bullied by cyber criminals inside the university. 20 (5.5%) of the respondents clarified that they been bullied by cyber criminals at least once or twice inside the university. Only 5 (1.3%) respondents designated that most probably they had been bullied.

SUMMARY OF IMPORTANT QUESTIONNAIRES FOR STUDENTS 2

	Have you bullied anyone **inside** the university?	Have you ever bullied anyone **outside** the University for Fun?	Have you ever heard of bullying taking place inside the university? **(Yes/No)**
It has only happened once.	20 (5.5%)	26 (7.2%)	75 (20.8%) Yes
2 or 3 times a month.	60 (16.6%)	4 (1.1%)	21 (5.8%) NO
Several times a week.	1 (0.27%)	4 (1.1%)	
I never had been bullied.	80 (22.2%)	80 (22.2%	

Table 5 summary of important questionnaires for students 2

Table 5 shows that 20 (5.5%) of the respondents were of the view that they have bullied someone inside the university while 26 (7.2%) of the respondents clarified that it (bullying) had happened at least once. 60 (16.6%) of the students agreed that they have bullied someone at least 2 or 3 times a month while majority of the participants 80 (22.2%) indicated that they have never bullied anyone inside the university. It is interesting to note that 4 (1.1%) of the respondents indicated that they have bullied someone several times a week.

SUMMARY OF IMPORTANT QUESTIONNAIRES FOR PARENTS

	Does your child come home in a happy mode?	Does your child annoy you in the house? (Mood change)	Does your child complain that she/he is being bullied in the university?
Yes	200 (80%)	55 (12%)	15 (6%)
No	50 (20%)	150 (60%)	150 (60%)
Sometimes	0%	0%	0%
Once or twice	0%	0%	0%

Table 6 summary of important questionnaires for parents

Table 6 explains that a significant portion of the respondents 50 (20%) agreed that their children comes home not happy while the majority of the respondents 200 (80%) signified that their children comes home in a happy mood. It is important to note that 55(12%) of the respondents indicated that their children experience mood change in the house while 150 (60%) said that they did not notice any behavioral change on their children in the house. It is interesting to note that 15 (6%) of the parents indicated that their children complained that they are being cyber bullied in the university while majority of the parents 150 (60%) indicated not.

CONCLUSION

This study revealed that university students were not spared the detrimental effects of cyber bullying. The authorities at universities should take steps to curb cyber bullying. Victims of cyber bullies suffer from emotional and psychological stress, and inevitably their grades will deteriorate. Institutions, teachers and parents must realize that cyber space is a risky place and must take effective steps to protect the victims. The following steps are needed to protect students from becoming victims of cyber criminals:

1. Identify cyber bullying problems in the university and discuss the problem with the students and their parents.
2. Appoint internet safety team in the university to monitor internet activities.
3. Create bullying prevention policies that include lessons on cyber bullying.
4. Make rules and regulations for acceptable use of technology. Get students, teachers and parents to sign a pledge to report cases of cyber bullying.
5. Provide educational materials for parents and students on Internet safety.
6. Ensure that cellular phone policies are enforced consistently.
7. Encourage students to participate in programs that outline internet responsibilities.
8. Develop a program for senior students to teach younger students about Internet safety.

IMPLICATIONS OF THE STUDY

Policy makers have an important role to play in re-shaping the University for the Better. Users, lecturers as well as Education Ministry must support university policy makers to redesign a system that can help students overcome their fear while in cyberspace. The findings of this study indicate that communication between students, parents, teachers and the University is not strong to fight cyber crimes. Malaysian policy makers should support university planners by providing them with state of the art technology and funds to continue their fight against cyber criminals. The following are some constructive suggestions:

1. Support and create an environment that protects students from cyber criminals all the time.
2. Support the creation of an environment that offers confidence to the students.
3. Support the allocation of funds for buying technology so that students can be protected.
4. Support and provide sovereignty in information technology faculty so that they decide what to buy to fight crimes in cyberspace.

LIMITATIONS OF THE STUDY

The results of this study are subjected to the following limitations: First, this research conducted only on first year students with 350 samples. As thus, the results cannot be generalized. Further investigations are needed to examine how other students such as masters and PhD students are coping with cyber bullying. Second, further examinations are necessary with longer period of time as well as more samples to test whether cyber bullying indeed affected them academically. Third, it is beyond the control of this research to avoid human factor such as bias to cyberspace and affected students.

REFERENCES

Beebe, J. Elizabeth, (2010). The Prevalence of Cyber Bullying Victimization and Its Relationship to Academic, Social, and Emotional Adjustment among College Students. ProQuest LLC, Ph.D. Dissertation, University of Northern Colorado.

Bogdan, R. C., & Biklen, S. K. (2003). *Qualitative Research for Education: An introduction to theories and methods* (4th Ed.). PP. 4-7, Boston: Allyn and Bacon.

Bulent,. D. (2009). Psychological Needs as a Predictor of Cyber Bullying: A Preliminary Report on College Students, Educational Sciences: Theory and Practice, v9 n3 p1307-1325.

Faryadi, Q. (2010). Developing an Effective Interactive Multimedia Instructional Design to Teach Arabic Language, p. 80, Al-Mehrab e-Publisher, Kuala Lumpur, Malaysia,

Faye, M. ; Cook, C. ; Saini, M. l; Wu, Meng-Jia; MacFadden, R. (2011). Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review, Research on Social Work Practice, v21 n1 p5-14.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8(4),* 597-606.

Hanson, W. Creswell, J. Plano; Kelly and Creswell, D. (2005). Mixed Methods Design in Counselling Psychology. *Journal of Counselling Psychology, 52 (2),* 224-235.

John., S. Van, A., Richard; Gable, R. A., (2011). Cyberbullying: Prevention and Intervention to Protect Our Children and Youth. Preventing School Failure, v55 n2 p88-95

Juliana, R. (2010). Text-Bullying: Associations with Traditional Bullying and Depression among New Zealand Adolescents. *Journal of School Violence, v9* n1 p74-97 2010

Kowalski, R. M.; Fedina, C. (2011). Cyber Bullying in ADHD and Asperger Syndrome Populations. Research in Autism Spectrum Disorders, v5 n3 p1

Lauren, M.; Ratliffe, K. T., (2011). Cyber Worlds: New Playgrounds for Bullying, Computers in the Schools, v28 n2 p92-116.

Michel, W. Heirman, W. (2011). Cyber bullying: Predicting Victimisation and Perpetration, Children & Society, v25 n1 p59-72.

Miles, M.B, and Huberman, A.M. (1994). *Qualitative Data Analysis,* 2nd Ed., p. 10-12. Newbury Park, CA: Sage.

Olthof, T.; Goossens, Frits A.; Vermande, Marjolijn M.; Aleva, Elisabeth A.; van der Meulen, Matty, (2011). Bullying as Strategic Behavior: Relations with Desired and Acquired Dominance in the Peer Group. *Journal of School Psychology*, *v49 n3* p339-359 Jun 2011

Olweus, D. (1996). Bullying In Schools: Facts And Intervention, Research Centre for Health Promotion, University of Bergen, Norway

Patchin, Justin W.; Hinduja, Sameer, (2011). Traditional and Non-traditional Bullying among Youth: A Test of General Strain Theory. Youth & Society, v43 n2 p727-751 Jun 2011

Susan., D.; Butler, C., W.; Emmison, M. (2011). "Have You Talked with a Teacher Yet?" How Helpline Counsellors Support Young Callers Being Bullied at School, Children & Society, v25 n4 p328-339.

Thompson, P. (2004). Researching Family and Social Mobility with Two Eyes: Some Experiences of the Interaction between Qualitative and Quantitative Data. *International Journal of Social Research Methodology*, *7 (3)*, 237-257.

Watson, Scott E. J.; Vannini, N. Woods, Sarah; D., Kerstin; Sapouna, Maria; Enz, Sibylle; Schneider, W.; Wolke, D.; Hall, L.; Paiva, A.; Andre, E.; Aylett, R., 2010). Inter-Cultural Differences in Response to a Computer-Based Anti-Bullying Intervention, Educational Research, v52 n1 p61-80

Wong-Lo, Mickie; Bullock, Lyndal M. (2011). Digital Aggression: Cyber world Meets School Bullies, Preventing School Failure, v55 n2 p64-70

Yavus, A. ; Sahin, Y., Levent; Eristi, B., (2010). Cyber bullying Victimization among Turkish Online Social Utility Members, Educational Technology & Society, v13 n4 p192-201.