Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FAULT DETECTION AND GROUPING OF ERRORS IN MPLS NETWORKS

[1]VENKATA RAJU S, [2]GOVARDHAN A, [3]PREMCHAND P
[1]Research Scholar, Dept. of Computer Sciences and Engineering,
Univ. College of Engg, Osmania University,Hyderabad-500007, India
[2]Professor, Dept. of Computer Science and Engg, JNTUH,Kukatpally, Hyderabad
[3]Professor and Dean, Faculty of Engineering,
Univ. College of Engg,Osmania University, Hyderabad
E-mail: venkataraju0775@gmail.com

ABSTRACT

On MPLS/GMPLS networks, heavy data loss occurs within the minimum duration of time, during fault prevalence. It is difficult to handle these faults as it may cause critical network survivability issue. Most of the research estimates the failure probability, bandwidth and delay of all routes using the traditional shortest path algorithm which leads to huge delay and overhead. In order to detect the fault in real time scenario, in this paper, we propose information based fault detection and grouping for fault detection in GMLPS/MPLS. In this technique, fault detection is based on the data present in the network. This involves the detection of router fault, link failure, and fault at nodes. In order to enhance the fault detection of an MPLS network, it has been considered forward detection and backward detection. This detection technique provides the next generation researchers a chance to detect the fault detection and solution techniques according to information already present in the network and the real need of the network. Simulation results show that the proposed approach provides high detection accuracy with reduced loss and delay.

Keywords- *Delay, Bandwidth, Grouping Of Errors*

1. INTRODUCTION

1.1 MPLS

Recently communication has grown rapidly in a client server model [12]. Multi-protocol Label Switching (MPLS) is a broadband technique which, supports and strengthens IP services. MPLS includes Label Edge Router (LER), which is responsible for attaching appropriate labels on the packet. LER are of two types and they are ingress or egress router. A label is a signature to transmit data in the network. The labeled packets are forwarded or routed through the path known as Label Switch Path (LSP). During transmission, the final LER is responsible for removing label from the packets. [19] MPLS is a connection oriented technique. MPLS provides reliable services according to the customer demands and profit goals, network requirements. [2]. It works at the second layer and a third layer of the network. [3]

MPLS networks consist of more than one clients and more than service providers. A node can do the work of source, destination, routers. There are lots of switching devices, routers, multi-plexures and demulti-plexures. A node can act in multiple works. The different switch level path follows different protocols to transmit their message to the next node. A switch can send a message in any direction in the networks. The data packet used in the transmission system carries required information and some extra bit of data. The extra amount data provide a proper direction to reach the destination, while ciphering of data provides a secure way of transmissions and other extra bits are added in multiple propose like error detection, probability of failure detection etc.

1.2 Problems of MPLS

MPLS is a complicated procedure [11]. Failures in MPLS network cause huge amount of data loss, which are resulting adverse effect on critical business applications and services [16]. In MPLS, failure of network components is reasoned by different reasons such as hardware/ software errors, fiber cut [8], power failures, malicious nodes and adversaries [13], architectural and procedural defects [9]. Simultaneous multiple failures are reasoned in MPLS as its topology consists of multiple links. [2]

A general failure that occurs in MPLS network is “black hole”. This failure happens in the network

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

due to anomalous termination of an LSP inside an MPLS network. [5] The failure may also be reasoned by a failed and broken MPLS tunnel. Delayed routing protocol convergence to mis-configurations to bugs in the individual router implementation is a serious consequence of black hole failure. [6]

Failures are complex in nature [10], Due to multi-layer architecture of MPLS. MPLS is dependent on physical transmission layer, as a result, the failure of a single component may lead to simultaneous failure of multiple components [7]. In MPLS, network survivability can be assured only by considering fault tolerance as a prominent QoS factor. The MPLS network architecture is connection oriented architecture. It is more susceptible to network failures. [18] In MPLS networks from link/node failures is an important issue. [9]

Faults in MPLS network results in large packet loss, poor quality of service and degrades network performance. So faults have to be discovered and recovered as soon as earliest. Fault tolerance is defined as the ability of the network to respond and recover quickly from the failure. Fault recovery techniques can free the network from faults and can make the MPLS network fault most tolerant. [19, 3]

The implementation of path protection technique implicitly permits redundancy in network resources. Thus, while designing fault tolerant technique, the capacity share allocation factor has to be considered. [14] [15] The failure recovery technique incurs a time delay and this delay may vary from an approach to another. This delay factor influences both network topology and recovery technique. In addition to delay factor, packet loss ratio is also an important factor that affects failure recovery technique. The time required to detect fault node causes more packets to be dropped. To alleviate this issue, buffering mechanism has to be used in order to reduce packet loss ratio. On the other hand, addition of buffering mechanism makes recovery more complex techniques. [18]

This technique shows a way to detect the failure from the available information at transmission node levels. The method is able to detect the node failure or link failure with mutual communication through different nodes.

First a fundamental structure of MPLS is described and some of the problems generally faced in the network are elaborated in the introduction part. Then the research is proceeding through some related work as described in section two. In the solution part a brief description of the problems facing in our previous paper is given. Then the paper enters into the detection techniques with references to our previous paper. Finally a proven conclusion is given to the future work.

2. RELATED WORK

Maria Hadjiona et.al [16] have proposed a hybrid fault-tolerant algorithm for MPLS Networks. The proposed algorithm is the first to employ both path restoration mechanisms typically used in MPLS networks: protection switching and dynamic path rerouting. In addition, it is the first algorithm to adequately satisfy all four criteria which we consider very important for the performance of the restoration mechanisms in MPLS networks: fault recovery time, packet loss, packet reordering and tolerance of multiple faults.

The hybrid algorithm maintains four data structures: (i) a Shortest Path Tree (SPT) where the root is the node that will execute the calculations, (ii) an array of lengths which contains the length of the shortest paths between the SPT root and all other nodes, (iii) a priority queue for nodes, (iv) a list maintained by the ingress LSR (Label Switching Router) and contains the working and alternative LSP. The first three data structures are the ones also used by the Otel algorithm.

Eusebi Calle [3] shows some parameters which are affecting the transmission system in the network. Generally these effects are resulting in huge loss of data. Here the author has taken different timings for the error detection. The terms used in timing concept are fault detection time, hold off time notification time, back off time, switch over time etc. The author focuses a method which is finding a probabilistic method to find a path for the secure data transmission. After probabilistic calculation he added a shortest path algorithm for a secure data transmission. It is a standard way to detect the failures. Still timing in everything needs synchronization of the whole network. Synchronization is a costly process in the networks.

Muhammad Kamran et.al [19] have proposed a new fault recovery protocol, which is based on protection switching domain and uses explicit routing and TCL. The authors compared the proposed protocol with the NS2 rerouting fault recovery protocol.

The rerouting fault recovery protocol uses rerouting domain for fault tolerance .It computes a recovery path on demand after the occurrence of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

fault whereas proposed fault recovery algorithm is for protection switching domain in which recovery paths are pre-computed. The proposed fault recovery protocol took less time to switch over the traffic to the recovery path as compare to rerouting fault recovery protocol. The time which is needed for the rerouting fault recovery protocol took to recover from a particular fault is a time for sending FIS to the ingress plus time to compute a backup path and sending traffic to it .In proposed fault recovery protocol total time is just to send FIS to ingress then ingress will automatically transfer the traffic to the backup port because it has already stored backup paths. As Network Simulator NS2 is an open source simulator has the advantage over other simulators like Graphical Network Simulator (GNS) that its files are easier to modify and source files are freely available.

Radim Bartos et.al [20] have proposed an approach to providing fault tolerance in MPLS networks based on the concept of "domain protection". In their method protection paths for all working paths that terminate in an egress router are calculated simultaneously. The proposed method guarantees that every protected node is connected to two protection paths placed in a way that no single link failure would cause simultaneous loss of connectivity between a node and the egress router on both protection paths. The use of dual protection paths permit decoupling the protection path placement from the working path placement and allowing much greater flexibility.

Several heuristic methods are employed within the algorithm. They improve the quality of the protection path placement without increasing the asymptotic complexity of the algorithm. Their Simulation results show that the proposed algorithm provides protection that is better than Fast Reroute scheme. The algorithmic complexity of the proposed model is less than that of RSVP Backup Tunnels while providing comparably good protection. The proposed model guarantees independence of the working and protection path placement.

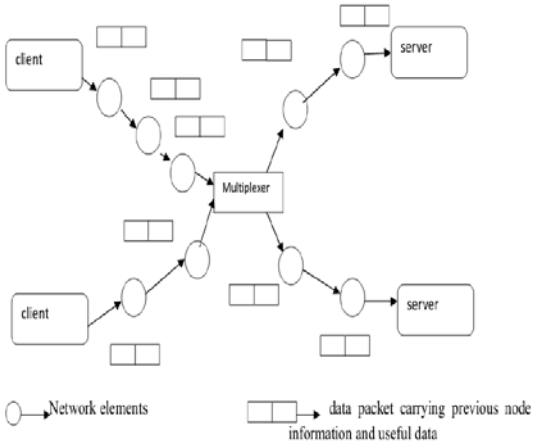
3.PROBLEM IDENTIFICATION AND PROPOSED METHODOLOGY

3.1 Problem Identification

Our previous paper [1] focuses on a secure link on MPLS. But when there is an error occurs in the network it is hard to detect the location. Some fundamental things to be considered in the error detection is bandwidth and time delay. The previous paper shows how to detect the bandwidth and delay. It is also finding a methodology to find the probability of error in different paths. Still it is unable to find the specific error found at any node or at a link. It is also not able to alert the network about the failure which can be resolved. [2] [3] A number of authors are showing techniques of failure correction without grouping the failure. [4] A lot of work has been done for finding shortest path algorithm. Some of shortest path algorithms are able to find the shortest path only considering the distance matrix [5]. Some of other algorithms are focusing about the traffic in the shortest path algorithm. But these papers do not show any methods for MPLS. The shortest path does not consider about other factors like bandwidth, delay, failure probability in finding their position of failure. Our previous methods do not show any detection technique which can detect the failure and recognize it certain type so that error correcting method becomes easier.

3.2 Proposed Methodology

The proposed methodology focuses on failure detection in link level and node level.



The data packet is carrying the information about some factors which are the fundamental need of network. For the failure detection this method is considered the bandwidth ratio, delay, and timer. Every node (n_{i+1}) in the network sends an acknowledgement to the sender node (n_i) after getting information. Every node has the ability of grouping of fault data packet information to find the fault in the network. Every node (….. n_i, n_{i+1},……) has a timer which is reset or set to zero after each data packet transmission. Optimized information about the required bandwidth ratio and delay is stored at every node for detection of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

failure. The data packets carry the information of delay from neighbor node and the bandwidth of the link from a neighbor node to the node. A predetermined value for the timer is set before the initialization of the network. The time of every node is set to a certain value at the time of initialization of the network. Every node is given identification ID. Every data packet has also identification id.

The sender node (n_i) generates a data packet it keeps its information and sends it to destination through long range data transmission packets. The nodes (n_i) add the information like available bandwidth, current time in data packets and send it to the neighbor nodes (n_{i+x}, here x can be of positive or negative). Procedure for Detection of bandwidth and delay is given in the previous paper [1]. Every data packet is given a unique ID number which is a combination of packet number [PN], sender ID (n_1) and last traveled nodes ID (n_i). After getting a data packet a node (n_{i+1}) first verifies the destination. Then it examines the information available in it. The node (n_i) just gets the information field which holds the data of the bandwidth (BW) and delay (D) and the timer (T). The node calculates the ratio of bandwidth (BW_i/BW_s, here's' for standard) and delay (D). Then it changes the data packet number (PN). The data packet number is changed only in the last node (n_i) address. Available bandwidth field (BW), delay (D) and timer (T) fields are also refreshed. The refreshed data packet is sent to the next node (n_{i+1}).

3.2.1 Procedure for numbering the data packet

Generally the entire field of a data packet in a network is sent as a character array. So it is proposed to make a character array for producing a unique number for every data packet. Every node has a node ID having X alphanumeric characters. The number of the data packet is also an alpha numeric. Suppose it is of N characters. The nodes which are also the part of the network are having X alphanumeric characters in it. Here the values of X and N was determined at the time of initialization of the network. The size (value) of X depends upon the number of the nodes present in the network. The value of N depends upon the amount of data packet is required to send. Suppose X_1 is the last node travelled nodes ID. Data packet generation follows as-

3.2.2 Estimation of Available Bandwidth

The available bandwidth is determined based on the channel status and idle periods of the shared wireless media. As the transmission and reception of the data packets from other nodes affects the channel status, this method takes neighbor nodes behavior into consideration. The idle time (IT_i) consists of number of idle periods for the period of examining time interval t and each node sums up all the idle periods in order to estimate the aggregate idle time. [17]

The ideal ratio δ for every time period t is computed using Eq (1)

$$\delta = IT_i / t \quad (1)$$

Thus the available bandwidth BW is given in Eq (2)

$$BW = \delta * B_c \quad (2)$$

Where B_c = raw channel bandwidth

3.2.3 Estimation of Delay

Let T_{i1} represent the time at which the data packet originates from the node (n_i).

Let T_{i2} represent the time at which a data packet is received at the originator node (n_i).

Let D_{qi} be the queuing delay at node n_i.

The round trip time (RTT) is defined as the difference between the transmission and reception time of the data packet in the node. [18] This is given using Eq. (3)

$$RTT = (T_2 - T_1) \quad (3)$$

The delay (D_i) is estimated based on the round trip time and queuing delay using Eq. (4)

$$D_i = RTT - D_q \quad (4)$$

Here the unit of delay is in Nano seconds.

3.2.4 Calculation of Bandwidth Ratio

To know the distraction of the bandwidth in the network from the fundamental requirement of the network a formula based on standard bandwidth and the bandwidth information received from the previous node is used. The formula is given in equation 5.

$$BW_r = BW_{rec}/BW_s \quad (5)$$

Here, BW_r is bandwidth ratio.

BW_{rec} is the bandwidth information send by the previous node (n_i).

BW_s is the standard bandwidth determined at the time of initialization of network.

The factor BW_r has no unit as it is a constant ratio of two similar factors.

Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2.5 Time taken in travel through the medium

The time is estimated based on the time of receiving (T_1) the data packet at the node (n_{i+1}) and sending time (T_2) of previous node (n_i) is given in Eq.6.

Travelling Time (TT) = T_1 (n_{i+1}) -T_2 (Ni) (6)

Here, T_1 (n_{i+1}) is the receiving time of the current node (n_{i+1}).

T_2 (n_i) is sending time of the previous node (n_i).

3.2.6 Details about data packet

The data packets are mainly divided into two parts. One part is for carrying the data; the other part is for information at the current node (n_i). The information present at the current node (n_i) is about the bandwidth available and current time (T_i) and the delay (D_i) till the current node (n_i). The method of calculation of bandwidth, delay is given in our previous paper [1].

Available bandwidth	Current time	Delay till node	Data	Destination

(Fig 2: Showing Data Packet For Transmission)

3.2.7 Failure Detection at every node

For the failure detection at every node level, a set of standard data is kept in a table that is present on every node. The standard should be calculated before the initialization of the network. A change in value of M% [M is a variable] is allowed. The change of values [value of M] should be chosen as per the requirement of the network. The table contains attributes like standard bandwidth, Incoming bandwidth and bandwidth ratio, delay till now, standard time interval to receive the data packet from the previous node (T_{i+1}-T_i), current time (T_{i+1}), the percentage of change in time. There is another table present which is grouping the different type of errors into categories or groups. The tables are given below.

Data packet no	Current time	Time carried in data packet (T_2 (Ni))	Change in time. ()	Standard bandwidth (BW_s)	Bandwidth in the data packet (BW_i)	Standard bandwidth ratio (BW_r)	Percentage of error in bandwidth. (BW_e)
……	……..	…….	……..	…….	…….	……..	……..

(Fig 3: Showing Table Of Information Getting From Data Packets At Nodes)

When a node sends any data packet to any node it is keeping the track of sending information. It starts a timer waits for the standard time to get the acknowledgement from the next node. The table is given below.

Data packet number	Transmitting (Sending) time	Expected time for acknowledgement receive	Status

(Fig 4: Showing The Table Present At The Node For Sending Information)

If the node is getting any acknowledgement at a certain time distant then it is called to be attacked by the black hole. So black hole detection is a forward detection. It is detected at the previous node (n_i). If the time of travel is more than the standard time of travel then then the problem is detected as link failure (link from n_i to n_{i+1}). Change in bandwidth more than M% is also symptomatic of link failure as bandwidth is purely depend upon link or medium. If the time of travel is good still delay varies a lot from the last delay then the problem is found to be in the previous node (n_i). The link and node failure are detected at current node (n_{i+1}). So the method defines the detection of failure at node and link as back word detection. At the time of every node is set to the same value so the method can easily detect. Grouping of failed data packets transmission has enabled researchers to find the type of the failure that is a node or link or black hole at a specific time. As the last nodes (n_i) ID is a part of uniform identification no of the data packet, node and link can be easily detected.

Delay	Time	Error
……	……	Node/link
……..	……	Node/link
……..	…….	Node/link

(Fig 5: Shows Backword Error Detection)

3.3 Detailed procedure

Step-1- The sender generates the data packet in the required manner as given in part 3.2. The data packet is numbered as according to the section 3.2.1. The data packet is generated in the procedure given in section 3.2.5. The data packet carries the

Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information like bandwidth, delay and current time in it. The detail of generating this field is given in the sections 3.2.4 and 3.2.5. It starts the timer and waits for the standard time to get the acknowledgement from next node.

Step-2- when another node gets the data packet which is acting as a node or router in the network, it changes the data packet number. It updates the data field present in it like bandwidth and timer and delay. Then it sends the next nodes. The current node is also given acknowledgement to the previous node.

Step-3-The error is determined at node levels and link levels as given in the parts 3.2.7. Then the the errors are grouped as given in 3.2.7.

4.SIMULATION RESULTS AND DISCUSSION

4.1 Simulation Setup

We simulated the design of our Information Based Fault Detectio and Grouping Of Errors in MPLS Networks (FDG) with Network Simulator (NS-2) [21].we consider the simulation topology given in Fig 6. The topology consists of 18 nodes.Different link bandwidth and delay are set for the all the links.

The Exponential traffic is used with packet size 2000 bytes. We have taken the metrics received bandwidth, end-to-end delay and packet loss ratio for evaluation. Loss ratio is given by the ratio of average number of packets lost at the receivers to the average number of packets sent. We compared our results with the HFTA strategy [16]. The results are described in the next section.

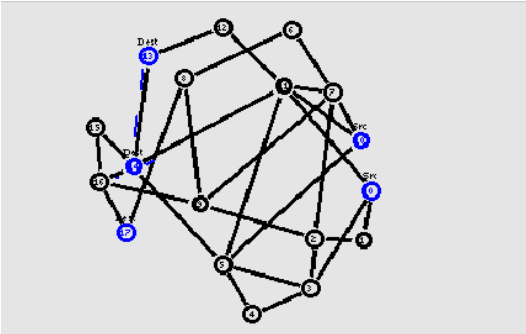


Fig 6. Simulation Topology

4.2 Results

In this section, the results for the given topology are provided by varying the number of faults and time. We vary the number of faults from 1 to 5 which involves both node and link level failures**.**

In this experiment, we vary the exponential traffic rate as 250,500,750 and 1000kb.

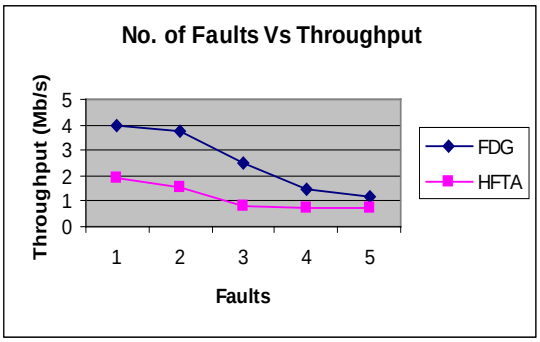


Fig 7: No. Of Faults Vs Throughput

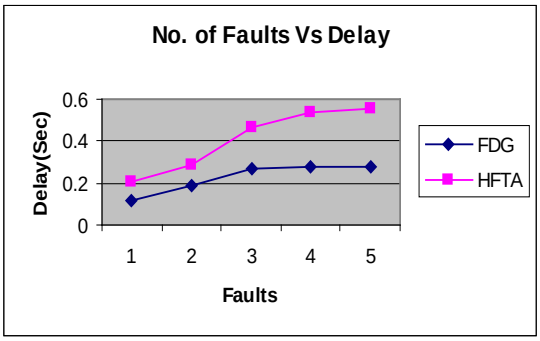


Fig 8: No. Of Faults Vs Delay

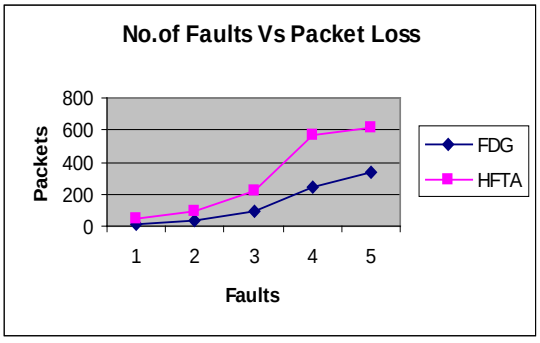


Fig 9: No. Of Faults Vs Packet Loss

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

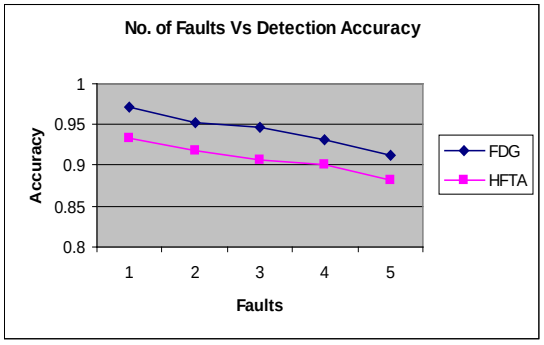


Fig 10: No. Of Faults Vs Detection Accuracy

When the number of faults is increased, it involves more fault detection activities and hence the delay is increased. Fig 8 shows that delay is increased when the number of faults is increased from 1 to 5. But FDG involves 43% lesser delay than HFTA, as per Fig 8.

Naturally the packet loss will be more if the number of faults that occurred is more. Fig 9 shows that the packet loss is increasing when the faults are increased from 1 to 5. Ultimately, the increase in packet loss results in decrease of throughput as shown in Fig 7. But FDG has 60% lesser packet loss and 53% higher throughput, when compared to HFTA.

The detection accuracy is depicted in Fig 10. It shows there is a decline of detection accuracy, when there are more faults. But FDG attains 3.6% more accuracy, when compared with HFTA.

5. CONCLUSION

The paper first identifies the fundamental needs of a network. Then the paper proceeds to a procedural way which is able to find the errors in a ratio. This proposed method is able to detect the failure of the neighbor node easily. This does not take any overhead of any hardware and central system. This method is able to identify the errors in node levels and link levels. The method is able to group the errors. After detection of failure it is helping the researchers to invent a different type of failure correction idea for different failure. The error is detected and immediately informed to the neighbor node for further prohibition of communication. Simulation results show that the proposed approach provides high detection accuracy with reduced loss and delay.

REFERENCES

[1] S.Venkata Raju, A Govardhan, P.Premchand, "Swarm based Fault Tolerant Routing in MPLS Networks" *International Review on Computers and Software*,Vol.5, No.3, March 2013.

[2] Jong Tae Park, Senior Member, IEEE, Jae Wook Nah, and Wee Hyuk Lee," Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks"**,** *IEEE Transactions On Dependable And Secure Computing*, vol. 5, no. 3, july-september 2008

[3] Eusebi Calle," Enhanced fault recovery methods for protected traffic services in GMPLS networks", February 2004

[4] G.H. Shirkoohi, K. Hasan," Enhanced TDR Technique for Fault Detection in Electrical Wires and Cables" *2nd International Symposium on NDT in Aerospace* 2010

[5] Kamesh Madduri_ David A. Bader_ Jonathan W.Berry† Joseph R. Crobak," An Experimental Study of a Parallel Shortest Path Algorithm for Solving Large-Scale Graph Instances", 2007

[17] P. Revathi and R. Balasubramanian, "Efficiency Analysis on QoS Multicast routing protocols under Cross-layer Approach with Bandwidth estimated Admission Control", *International Journal of Algorithms, Computing and Mathematics* Volume 2, Number 3, August 2009 © Eashwar Publications

[7] Dennis Arturo Ludeña Romaña1, Kenichi Sugitani2, and Yasuo Musashi3," DNS based Security Incidents Detection in Campus Network" *International Journal of Intelligent Engineering and Systems* 1 (2008) 17-21

[8] Jing Wu1, Chengcheng Guo, Puliu Yan, Jianguo Zhou," Traffic Balance after Link Failures Using Few Weight Changes", *International Journal of Intelligent Engineering and Systems* 2(2008)40-47

[9] Jong Tae Park, Senior Member, IEEE, Jae Wook Nah, and Wee Hyuk Lee," Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks", *IEEE Transactions On Dependable And Secure Computing*, vol. 5, NO. 3, july-september 2008

[10] Łukasz Saganowski 1 , Michał Chora´s 2,∗ , Rafał Renk 3 , Witold Hołubowicz 4 ," Signal-based Approach to Anomaly Detection in IDS Systems", *International Journal of Intelligent Engineering and Systems* 4 (2008) 18–24 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11] Jianqing Liu¤, Rongkai Lu," Monitoring Network through SNMP-based System" *International Journal of Intelligent Engineering and Systems*, Vol.5, No.1, 2012

[12] XiboWang, Zhen Zhang," Design of Embedded WEB Remote Monitoring System Based on mC/OS-II Operating System", *International Journal of Intelligent Engineering and Systems*, Vol.5, No.1, 2012

[13] Olivier Klopfenstein," Robust pre-provisioning of local protection resources in MPLS networks", 2007

[14] E. R. Naganathan, S. Rajagopalan," Effective Traffic Management in MPLS using Traffic Flow Analysis Based ACO Algorithm", *European Journal of Scientific Research* ISSN 1450-216X Vol.72 No.3 (2012), pp. 482-489

[15] Mohammad HossienYaghmae, Fahimeh Jafari" A New Fault Tolerant Routing Algorithm For GMPLS/MPLS Networks"2004

[16] Maria Hadjiona, Chryssis Georgiou, Maria Papa, Vasos Vassiliou," A Hybrid Fault-*Tolerant Algorithm for MPLS Networks*", 2008

[17] Noureddine Kettaf, Hafid Abouaissa, Thang Vuduong† and Pascal Lorenz," A Cross layer Admission Control On-demand Routing Protocol for QoS Applications", *IJCSNS International Journal of Computer Science and Network Security*, vol.6 No.9B, September 2006

[18] Sahel Alouneh, Abdeslam En-nouaary, Anjali Agarwal,"A Multiple LSPs Approach to Secure Data in MPLS Networks", *Journal Of Networks*, vol. 2, no. 4, august 2007

[19] Muhammad Kamran and Adnan Noor Mian, "Multiple Fault Tolerance in MPLS Network using Open Source Network Simulator", *Proceedings of the 4th International Conference on Open-Source Systems and Technologies* (ICOSST '10), 2010

[20] Radim Bartoˇs and Mythilikanth Raman," A Heuristic Approach to Service Restoration in MPLS Networks", 2002.

[21] Network Simulator: http:///www.isi.edu/nsnam/ns