
# A path protection method using congestion control in IP/MPLS networks as an underlying network in Smart Grids

**B. Mobasheri, M.H. Yaghmaee Moghadam**

**Payamnour University of Tehran, Mashad Electrical Distribution Company(MEDC)**
**(mobasheri_khi@khi.ac.ir, yaghmaee@ieee.org )**

**Paper Reference Number: 07-11-2849**
**Presenter: B. Mobasheri**

**Abstract**

To provide a reliable backbone network, fault tolerance should be considered in the network design. Multiprotocol label switching (MPLS) based backbone network, is used to provide traffic engineering (TE) and high speed networking. The fault-tolerant issue which is one of the aspects of QoS, focuses on how to protect the traffic of a label switched paths (LSP) against node and link failures. Fault tolerance techniques are very useful to maintain the survivability of the network by recovering from failure within acceptable delay and minimum packet loss while efficiently utilizing network resources.

In this paper, based on the modified (k, n) threshold sharing scheme with multi-path routing, we propose a relationship between k and n by considering the priority levels of incoming traffics, we apply a congestion method to reduce the packet loss. The traffics that are going to be injected to our IP/MPLS network are received from a Smart Grid sub-networks. The approach introduces very low recovery delay and low packet loss while giving desirable throughput of the network. In addition, it can easily handle single and multiple path failures. We validate the analytical results through simulations in *OPNET*.

**Keywords:** Failure tolerance, Priority levels, Smart Grids, Packet Loss, Multiple path failures

## 1. Introduction

The multiprotocol label switching (MPLS) as a new forwarding technology for meeting the requirement of explosive traffic. In addition to fast forwarding, fault tolerance is also an important issue in the network design. If an Internet service provider (ISP) adopts the MPLS technology to design its backbone network, a fault-tolerant mechanism is also necessary to protect the traffic of a label switched path (LSP) against node and link failures. Huang, Sharma, Owens and Makam (2002) defined the LSP as a transmission path in the MPLS network. MPLS provides mechanisms in IP backbones for explicit routing using label switched paths (LSPs), encapsulating the IP packet in an MPLS packet. When IP packets enter a MPLS based network, label edge routers (LERs) assign a label identifier based on classification of incoming packets and relating them to their forward equivalence class(FEC). Once this classification is complete and mapped, packets are assigned to corresponding labeled switch paths (LSPs), where label switch routers (LSRs) place outgoing labels on the packets. In this basic procedure all packets which belong to a particular FEC follow the same path to the destination, without regards to the original IP packet header information. Awduche, Berger, and Gan(2001) used the constraint based label distribution protocol (CR-LDP) or RSVP-TE, an extension of the resource

reservation protocol, to distribute labels and bind them to LSPs. MPLS has many advantages for traffic engineering. It increases network scalability, simplifies network service integration, offers integrated recovery, and simplifies network management. However, MPLS is very vulnerable to failures because of its connection oriented architecture. Path restoration is provided mainly by rerouting the traffic around a node/link failure in a LSP, which introduces considerable recovery delays and may incur packet loss. As Makam, Huang and Sharma(2002) has mentioned, such vulnerabilities are much costly to time-critical communication such as real-time applications, which tolerate a recovery time in the order of seconds down to 10's milliseconds. Therefore, service disruption due to a network failure or high traffic in the network may cause the customers significant loss of revenue during the network down time, which may lead to bad publicity for the service provider as Bhandari(1999) has mentioned. To prevent such bad consequences, routers and other system elements in MPLS networks should be resilient towards node or link failures. In other words, MPLS networks should implement efficient mechanisms for ensuring the continuity of operations in the event of failure anywhere in the network. This aspect is usually referred to as fault tolerance. In other words, fault tolerance is defined as the property of a system to continue operating properly in the event of failure of some of its parts.

In IETF, two well-known recovery mechanisms (protection switching and rerouting) have been proposed. In protection switching a backup LSP is pre-established and configured at the beginning of the communication in order to reserve extra bandwidth for each working path. At the other hand in rerouting technique no backup LSP is established in advance but after a failure occurs; hence, extra bandwidth is reserved upon the happening of failures. Pre-established path protection is the most suitable for restoration of MPLS networks in real-time due to fast restoration speed. Barenghi and Pelosi(2011) declare that the dynamic protection model, however, does not waste bandwidth but may not be suitable for time sensitive applications because of its large recovery time .

Protection techniques can be compared one to another based on parameters like type of failures handled, end to end delay, and packet loss. The first parameter determines whether the protection technique recovers from single or multiple failures. The second parameter indicates how much time is required by the technique to route traffic from the source to destination. Finally, the last parameter gives the percentage of packets lost due to failures. In this paper, we use an approach for fault tolerance in MPLS networks using a modified (k,n) threshold sharing scheme(TSS) with multi-path routing introduced by Alouneh, Agrwal and En-Nouaary(2009). An IP packet entering MPLS network is partitioned into n MPLS packets, which are assigned to n disjoint LSPs across the MPLS network. Receiving MPLS packets from k out of n LSPs is sufficient to reconstruct the original IP packet but only single failures are supported.

Mobasheri and Yaghmaee (2012) used priority levels for the incoming demands from sub-networks of a smart grid entering the IP/MPLS backbone. Based on these levels, the traffic demands will be given their desired services. For the IP/MPLS network to tolerate multiple failures, using modified TSS, in this paper introduce a relationship between k and n to handle multiple failures instead of just handling single failures. Still it allows the reconstruction of the original packet with a negligible packet loss and end to end delay due to congestion control being applied to the network flows. Consequently leading to better throughput of the network.
The rest of this paper is organized as follows. We will have a brief introduction to Smart Grids in section 2. Section 3 is devoted to related work. Section 4 introduces our proposed relationship for k and n and applies a congestion control method to the underlying network to become more applicable in Smart Grids and discusses the main issues related to it. Section 5 presents the performance evaluation and the simulation results. Section 6 concludes the paper.

## 2. Smart Grids

New standards and initiatives in the electric power grid are moving in the direction of a smarter grid. Media attention has focused prominently on smart meters in distribution systems, but big changes are also occurring in the domains of protection, control, and Supervisory Control and Data Acquisition (SCADA) systems. Fadul, Hopkinson, Sheffield, Moore and Andel(2011) declare that these changes promise to enhance the reliability of the electric power grid and to allow it to safely operate closer to its limits, but there is also a real danger concerning the introduction of network communication vulnerabilities.

A set of technologies, commonly regrouped under the names of smart metering and smart power grid has been proposed to raise the production, transmission and distribution efficiency of the present of power grid infrastructures through accommodating a two-way flow of electricity and metering data. A smart grid promises reduced vulnerability to unexpected hazards, lower energy prices, increased use of renewable resources, and fewer energy shortages. The technological challenges encompass problems ranging from the integration of high-speed, low-latency telecommunications infrastructures (that can process large-scale data securely across a multiple network components) to the processing of large volumes of data received in near real-time from a multitude of remote sensors and field devices.
In this sense, the ICT structure of the new smart grid will converge to a full fledged informative system, effectively speeding up the processing of the metering information on a large scale. However, the major concerns about smart grids are posed by the potential security problems raising from the network transmission of end-user's metering data. This is why a reliable infrastructure network is needed to transmit the smart grids' demands to the destination . According to Mobasheri and Yaghmaee (2012), each sub-network in a smart grid is given a priority level. Based on these levels, the sub-networks having the highest priority is given the needed service first and so forth for the others. Some of these sub-networks are namely: Voice, Video, SCADA, AMI networks.

## 3. Related work

The recovery approaches in MPLS are either pre-established protection or dynamic protection. Since our approach is based on n pre-established paths between the ingress and egress routers, the following discussion is limited to existing pre-established protection schemes only.

The protection technique discussed by Li, Buddhikot, Chekuri and Guo(2005) is "1+1"protection. In this technique path recovery is provided without packet loss or recovery time. The resources(bandwidth, buffers, and processing capacity) on the recovery path are fully reserved, and carry the same traffic as the working path, requiring substantial amount of dedicated backup resources. Selection between the traffic on the working and recovery paths is made at the path merge LSR (PML) or the egress LER. In this scheme, the resources dedicated for the recovery of the working traffic may not be used for anything else.
Rajeev and Muthukrishnan(2001) declare that to support differentiated services, normally if the network is safe, the capacity of the backup paths is utilized to carry packets belonging to lower priority class types (e.g. best effort). In case of failure, the lower class traffic is blocked to support backup for high priority traffic.

The paper by Haskin et al.(2001) is also based on pre-established alternative path. The backup path is comprised of two segments. The first segment is established between the last hop working switch and the ingress LSR in the reverse direction of the working path. The second segment is built between the ingress LSR and the egress LSR along an LSP that does not utilize any working path. In Fig. 1, if the link between LSR4 and LSR9 fails, all the traffic in working path is rerouted along the backup path, LSR 3–2–1–5–6–7– 8–9. Optionally, as soon as LSR1 detects the reverse traffic flow, it may stop sending traffic downstream of the primary path and start sending data traffic directly along
the second segment.

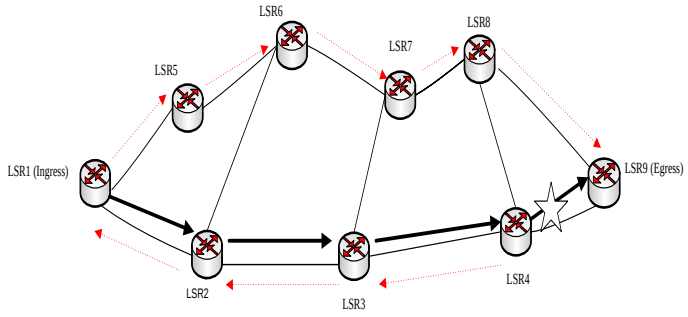


Figure 1: Path restoration examples Haskin et al.

The paper by Alouneh, Agrwal and En-Nouaary(2009) present an approach for fault tolerance in MPLS networks. The approach uses a modified version of the (k, n) threshold sharing scheme (TSS) with

multi-path routing wherein k out of n LSPs are required to reconstruct the original message. Threshold sharing scheme is a very well-known concept used to provide security.

At the ingress each IP packet is partitioned into m blocks. The m blocks will be packed in one MPLS packet which will be sent through one LSP. Using this method n MPLS packets are formed and sent through n paths. MPLS packets generated are sent in the same order in which the IP packets were received by the ingress router, therefore the MPLS packets at each LSP will also be received in order if there is no MPLS packet lost due to transmission errors. To identify packet lost due to transmission errors, Alouneh, Agrwal and En-Nouaary(2009) proposed to use sequence numbering.

When arriving at the egress, by receiving traffics from k paths out of n, the original IP packet can be reconstructed. Alouneh, Agrwal and En-Nouaary(2009) proposed to use k=n-1 this means the single failures are supported. In this paper we mainly consider the multiple failure aspect of the scheme by proposing a new relationship between k and n for high priority traffics.

In networking, different traffics may require different kinds of treatment. Therefore, our approach should be able to consider multiple classes of QoS services. There are four types of traffics traversing through the network, as indicated previously in table 1. The first and second type are high priority traffics. High priority traffics do not tolerate packet loss, and therefore cannot be pre-empted. The third and fourth type are grouped into low priority traffics. This type has no stringent traffic requirements such as recovery delay or packet loss, and accordingly can be pre-empted.

| Priority level | Sub-network |
|---|---|
| 1 | Voice |
| 2 | Video |
| 3 | SCADA |
| 4 | AMI |

Table 1: Priority levels of a Smart Grid traffics

## 4. Appling congestion control in an IP/MPLS network using a (k,n) threshold sharing scheme as a recovery approach to be more applicable in Smart Grids

In this paper, by choosing to use IP/MPLS network as an infrastructure in smart grids and considering the different priority levels in traffic demands, we focus on the high priority traffics and their need of safe transmission through the network. These traffics should be transferred through the underlying network in minimum delay time and packet loss and at the same time if multiple failures occur in the network, the network should be able to manage the failure in an acceptable manner.

To have even more reduction in packet loss we apply a congestion control method to the network. The congestion control method work as follows: When the queues considered for each level of traffic overloads, the packets drop from the queues tails therefore the injected traffic forms a congestion in the network. At this time a notification signal will be send back to the source and the rate of the incoming packets will be decreased. In this way the traffic will be control until the network recovers from the congestion.

*The proposed algorithm:*

1. Traffics enter the Ingress router at the edge of the IP/MPLS domain
2. The ingress router reads the FEC of the incoming packet and places the packet in the right queue
3. If the packets' source was located in a high priority sub-network in the smart grid, k and n will be calculated from the equation below:

$$k > n / 2 \qquad (1)$$
$$3 \leq k \leq n - 2$$
$$n \geq 6$$

4. In case the source was located in a low priority sub-network, k and n will have the following relationship:
   k=n-1
5. To recall from Alouneh, Agrwal and En-Nouaary(2009) receiving traffics from k paths out of n, at the egress node, is enough to reconstruct the original packet.

In case of a failure happening in any intermediate node /link through the IP/MPLS network, the upstream node realizes the failure and piggybacks the sequence number of the last packet passed successfully through the faulty node/link. By receiving the sequence number at the ingress node, the packets with the following sequence numbers will be sent again.

Based on Eq.(1) a failure occurring in a LSP, carrying the high priority traffics like Voice or Video through the IP/MPLS network, needs at least 6 failure-free LSP in order to pass the traffic through the underlying network. If less than 6 paths is found, the higher priority traffics preempt the lower ones and their needed bandwidth will be allocated to them and the low priority traffics have to wait until their needed bandwidth frees up. At the same time at least 3 simultaneous failures can happen in the network, without effecting the affected traffic. The same scenario is used for the lower priority traffics but the relationship between k and n will be different. In low priority traffics, like demands coming from AMI networks which are not real-time networks, we use the same scheme used in Alouneh, Agrwal and En-Nouaary(2009), i.e. k=n-1. Still the same recovery method, in time of failure, will be applied for low priority traffics.

It is worth to note that our proposed relationship can provide multiple path failures by increasing the number of n disjoint paths. To help us better understand our proposed algorithm, the following illustrates the distribution and reconstruction processes through an example.

### *4.1. An example of the distribution process*

Fig. 2 shows an example of how the distribution process apply a (4,7) modified threshold sharing scheme using our proposed algorithm onto an IP packet. The IP packet is first divided into *m* blocks $S_1$, $S_2$,…$S_m$ where each block is a multiple of *k* bytes. The original TSS is implemented using Lagrange interpolations for polynomials. The polynomial function is as shown in Eq.(2), where *p* is a prime number, coefficients $a_0,a_1,\ldots a_{k-1}$ are unknown elements over a finite field $Z_p$, and $a_0=M$ is the original message.

$$f(x)=(a_{k-1}x^{k-1}\_\ldots+a_2x^2+a_1x+a_0) \bmod p \qquad (2)$$

It can be easily seen that there are three coefficients, $a_0,a_1,a_2$ and $a_3$, for a (4,7) scheme where $k$=4. Each block is therefore divided in k equal parts and these coefficients are assigned values from the block.

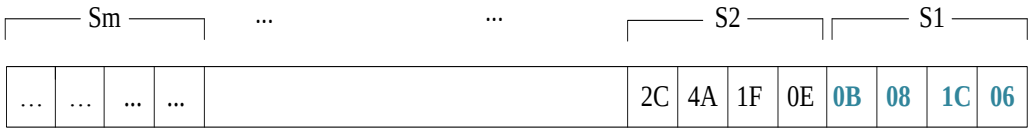

Figure2: Division of an IP packet into m blocks

For example $a_0$=06, $a_1$-28(1C in hex), $a_2$=08 and $a_3$=11(0B in hex) for the block $S_1$. Next m quadratic equations $fS_1,x)$, where 1≤j≤m, are generated using the four coefficients from each of the m blocks, that is, every block generates a quadratic equation. Each quadratic equation is solved n times using the n different $x_i$, 1≤i≤n, values as agreed between a sender (ingress) and a receiver (egress). Each MPLS packet payload therefore consists of m encoded values obtained from the m quadratic equations using the same $x_i$ value, as shown in Fig.1. Each LSP corresponds to a $x_i$ value.
For example, for block $S_1$, the equation generated is:

$$F(S_1,x)=11x^3+8x^2+28x+6 \bmod 257.$$

The above equation is solved for different n values as follows:

$$f(S_{j=1},x=1)=53$$

$f(S_{j=1},x=2)=182$
$f(S_{j=1},x=3)=459$
$f(S_{j=1},x=4)=950$
$f(S_{j=1},x=5)=1721$
$f(S_{j=1},x=6)=2838$
$f(S_{j=1},x=7)=4367$.

### *4.2. An example of the reconstruction process*

Now, we consider the example of Fig. 1 to illustrate how the reconstruction of the original IP packet is done at the egress router. Fig. 3 shows the process after receiving any $k$ of the $n$ MPLS packets of Fig. 2. In the figure, MPLS packets received from the LSP1, LSP2, LSP3 and LSP4 is considered. Recalling from Alouneh, Agrwal and En-Nouaary(2009) since both ingress and egress routers use the same polynomial functions, the order of coefficients $a_0,a_1,\ldots,a_{k-1}$ are already preserved and does not depend on the location of failure or the path that has failed.

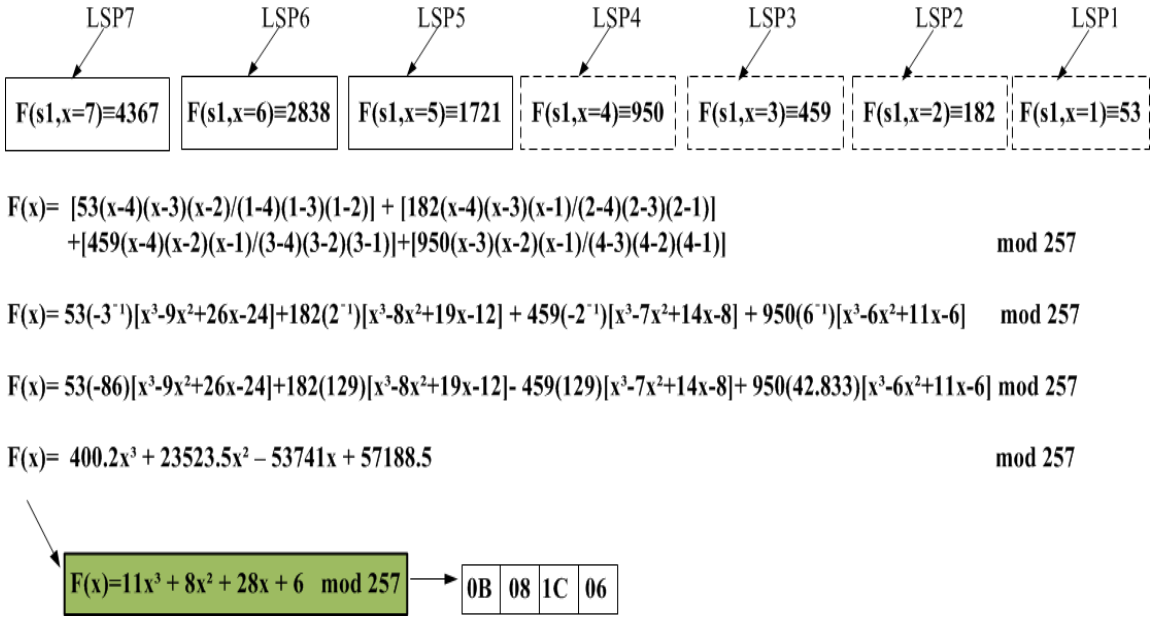


Figure 3: Reconstruction process in the egress router applying a (4,7) modified TSS.

For block $S_1$ the following four equations are used to obtain the function $f(s_1,x)$ using Langrage Interpolation:

$(a_0+a_1(1)+a_2(1)(1)+a_3(1)(1)(1))\equiv 53$ (mod 257); from LSP1,
$(a_0+a_1(2)+a_2(2)(2)+a_3(2)(2)(2))\equiv 182$ (mod 257); from LSP2,
$(a_0+a_1(3)+a_2(3)(3)+a_3(3)(3)(3))\equiv 459$ (mod 257); from LSP3,
$(a_0+a_1(4)+a_2(4)(4)+a_3(4)(4)(4))\equiv 950$ (mod 257); from LSP4.

LSP5, LSP6 and LSP7 are considered to fail somewhere in the network, so they are not able to carry their traffics to the destination. So using the Lagrange linear interpolation the polynomial function is obtained:

$F(S_1,x)=11x^3+8x^2+28x+6$ mod 257

where the original values of the coefficients for block $S_1$ obtained are $a_3=11$(0×0B in hex), $a_2=8$(0×08 in hex), $a_1=28$(0×1C in hex) *and* $a_0=6$(0×06 in hex).

## 5. Performance evaluation

This section is devoted to performance analysis we did to evaluate our approach. We are especially going to measure and analyze the packet loss, end to end delay and throughput of the underlying network and be able to manage multiple failure happening in the network. Three different failure situations is considered throughout our simulations.

Simulations were performed on 3 GHz Intel Pentium 4 CPU processor with 2 GB memory running under XP operating system to measure the time taken by the modified TSS scheme to distribute the original IP packet to n MPLS packets and reconstruct it at the ingress and egress routers, respectively. Too be closer to reality and to achieve the true results we used the exponential distribution to generate and distribute the packets through the IP/MPLS network and each node uses drop tail queue.

This scheme is implemented in OPNET and the experimental results show negligible packet loss and low end to end delay. Applying the congestion control method, the results show more reduction in the above mentioned criteria.

### *5.1. The performance evaluations before applying the congestion control method*

*Scenario1:*

Table 2 shows the amount of traffic for each level of priority, injected to the network. As can be seen the highest amount of traffic injected to the network belongs to the lowest level of priority. The rate of the packet production is considered to be 1500 packets/sec and the rate of the packet entrance to the network is 800 packet/sec.

| Traffic priority | Traffic injection | Packet production rate | Packet entrance rate |
|---|---|---|---|
| 1 | 10% | 1500 | 800 |
| 2 | 20% | | |
| 3 | 30% | | |
| 4 | 40% | | |

Table 2: Scenario1-Most of the incoming traffic belongs to the low priority traffics.

Fig.4 shows the end to end delay time of the packets arriving safely at the destination. When the probability of failure happening in the network is 1%, the end to end delay reaches its highest level. This is because the congestion occurs and there is no control on it. The amount of traffic injected to the network is almost twice the traffic entering the network. Thus the queues overload and the packets have to wait in the queues to get turn to pass. In case the failure reaches 10% and 30% more packets destroy in the network due to failure. Thus the packets waiting in the queues get the turn to pass through the network more quickly.

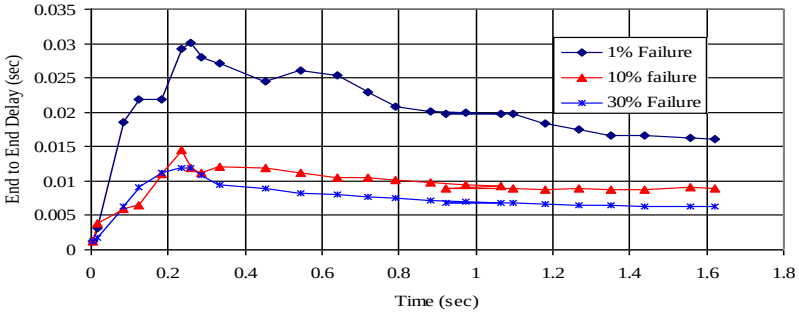


Figure 4: End to End Delay of packets in three different failure situations

Fig.5 shows the same failure situations with packet loss. Considering the absence of congestion control, at 1% and 10% failure situations, the network tolerates low packet loss but it increases as the failure grows in the network.

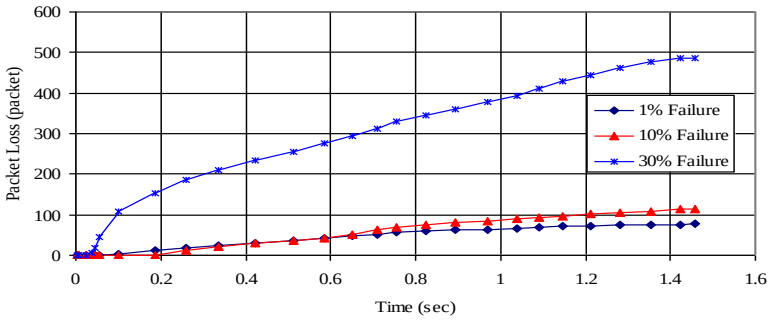


Figure5: No. of packet loss in different failure situations

The graph shown in fig.6 shows the ratio of the number of packets sent originally from the ingress node through failure-free LSPs, to the number of packets received at the destination successfully. In other words the graph shows the throughput of the network. Again at 1% and 10% failure situations the throughput of the network gets close to 1; as desired. But when the network tolerates 30% failure, because of the absence of congestion control and the increased packet loss, it takes some time for the network to reach a steady state.

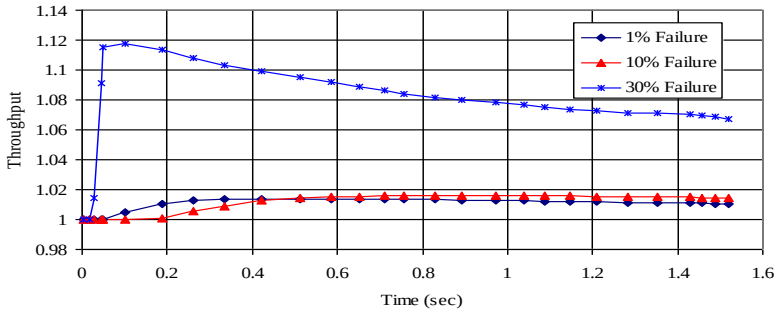


Figure 6: Throughput of the network in different failure situations

*5.2. The performance evaluations after applying the congestion control method*

*Scenario 2:*

Table 3 shows the amount of traffic for each level of priority, injected to the network. In this scenario the highest amount of traffic injected to the network belongs to the highest level of priority and the congestion of the network traffics is under control. The rate of the packet production is 1000 packets/sec and the rate of the packet entrance to the network is 800 packet/sec.

| Traffic priority | Traffic injection | Packet production rate | Packet entrance rate |
|---|---|---|---|
| 1 | 40% | 1000 | 800 |
| 2 | 30% | | |
| 3 | 20% | | |
| 4 | 10% | | |

Table 3: Scenario2-Most of the incoming traffic belongs to the high priority traffics.

Figures 7 through 14 compare three different states of the modified TSS; the original modified TSS, modified TSS using our proposed relationship between k and n and the state in which the congestion of the network is

controlled. The evaluated criteria, as already mentioned, are the packet loss, end to end delay and the throughput of the IP/MPLS network. All of these are evaluated in three different failure situations.

From all the above mentioned criteria, packet loss is the only one that takes the most effect, when using congestion control in a network. So we start to evaluate the packet loss first to see how it changes in compare to the state in which the congestion control is not applied.

Fig. 7 shows the no. of packet losses of the network. Using the proposed relationship for k and n and also applying the congestion control to the network, the no. of packet loss of the network remains zero, but the TSS shows a few loss of packets.

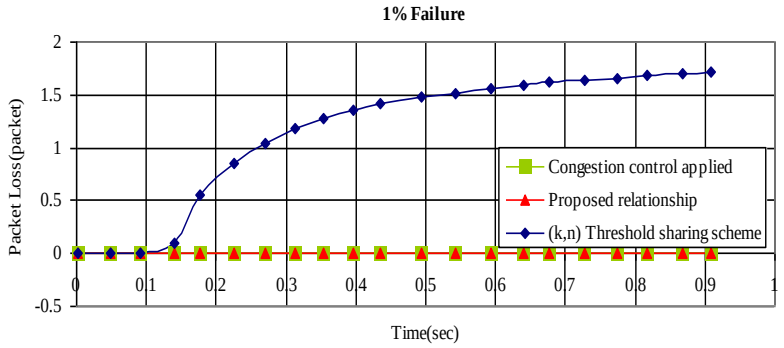


Figure 7: Comparison of no. of packet losses in three different states with 1% failure

Consider fig.8 where the packet loss reaches zero when the congestion control is applied to the network whereas by using the proposed relationship the packet loss reaches to 10 packets and with the TSS almost twice more.

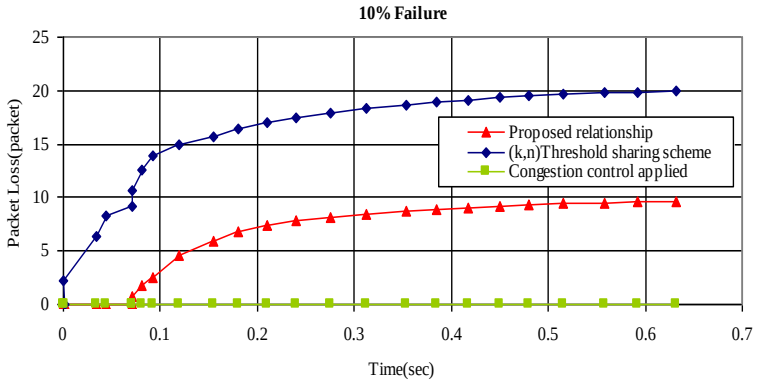


Figure 8: Comparison of no. of packet losses in three different states with 10% failure

In fig.9, once more controlling the congestion of the network traffics results in low packet loss even when the probability of failure reaches its highest level. As it is expected because of the high failure occurrence in the network, the packet loss cannot be absolutely zero. The figure also shows the no. of packet loss of the TSS, where it is relatively high and using the proposed relationship is somewhere in between.

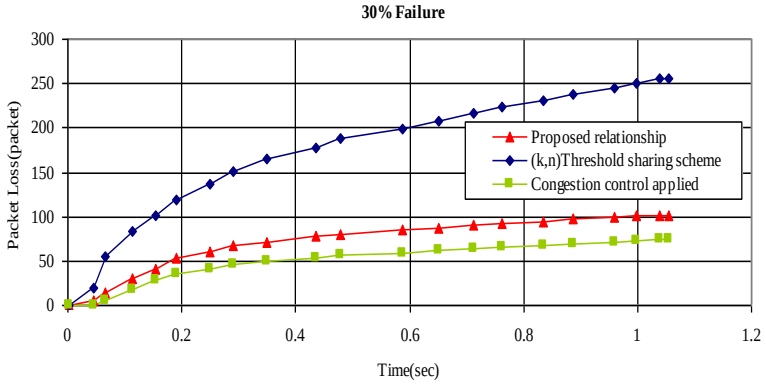


Figure 9: Comparison of no. of packet losses in three different states with 30% failure

Fig.10 shows the amount of end to end delay of packets when there is 1% failure probability in the network. As it can be seen the original TSS shows the highest amount of end to end delay. When using the proposed algorithm without controlling the congestion, this amount decreases, but it reaches below 4 milliseconds when we applied the congestion control method to the network.

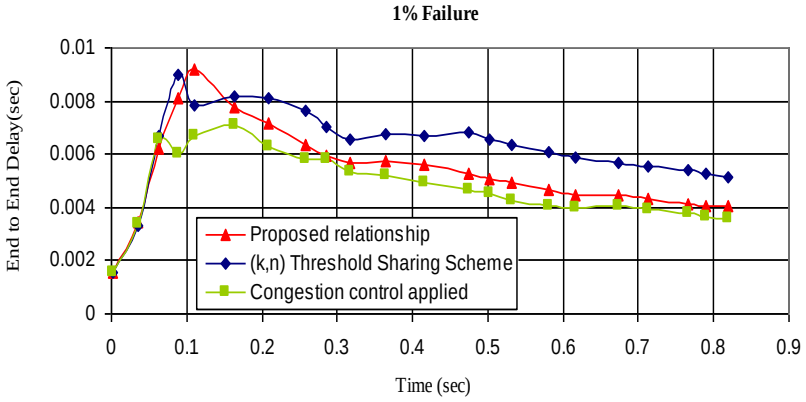


Figure 10: Comparison of the packets' End to End Delay in three different states with 1% failure

Fig.11 shows the state when the network probability of failure reaches 10%. In this case, again, using congestion control method shows better results and the original TSS has the highest score.

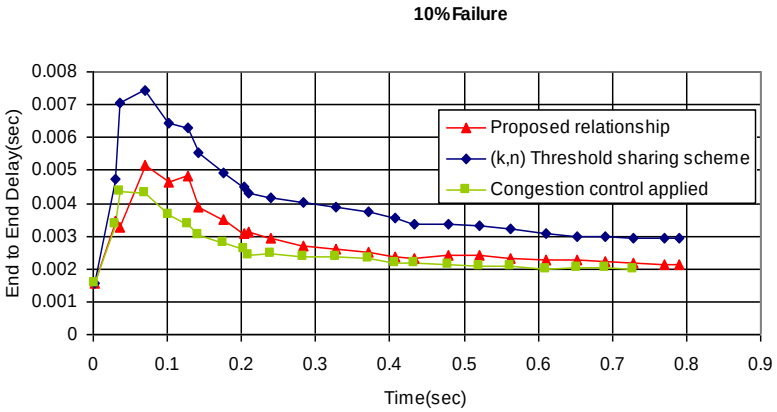


Figure11: Comparison of the packets' End to End Delay in three different states with 10% failure

In fig. 12, the network experiences its highest probability of failure. Here again when the network congestion is controlled, the end to end delay obtains the lowest level among the two other methods.

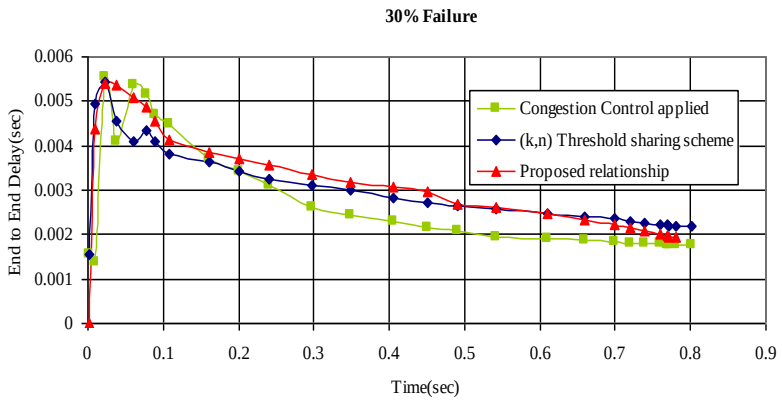


Figure 12: Comparison of the packets' End to End Delay in three different states with 30% failure

After considering the packet loss and the end to end delay of incoming traffics it is time to see how the network throughput acts in three failure situations. As you know the no. of packet losses have a considerable effect on the network throughput. When the failure occurrence of the network is very low, like 1%, that means almost all of the packets reach the destination and that insures a desired network throughput.
But because the original TSS does not use any congestion control method, the throughput of the network is not as good as the other two states. This can be seen in fig.13.

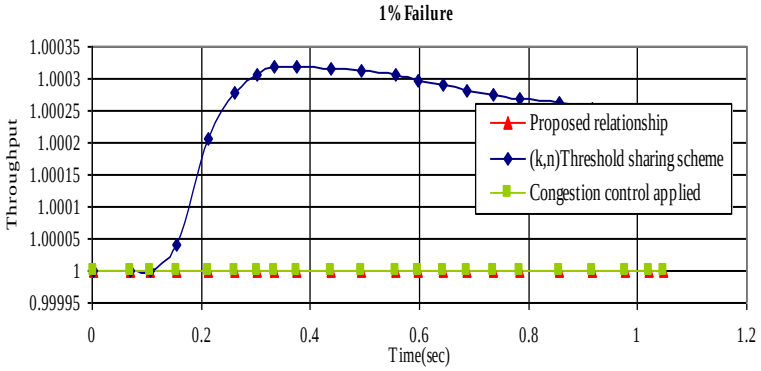


Figure 13: Comparison of the throughput of the IP/MPLS network in three different states with 1% failure.

Fig. 14 demonstrates an interesting result. In this case the network failure is supposed to be 10%. And still by controlling the traffic congestions the throughput of the network is very fine. As can be seen in the fig. the original TSS takes some time for the throughput to reach a steady state.

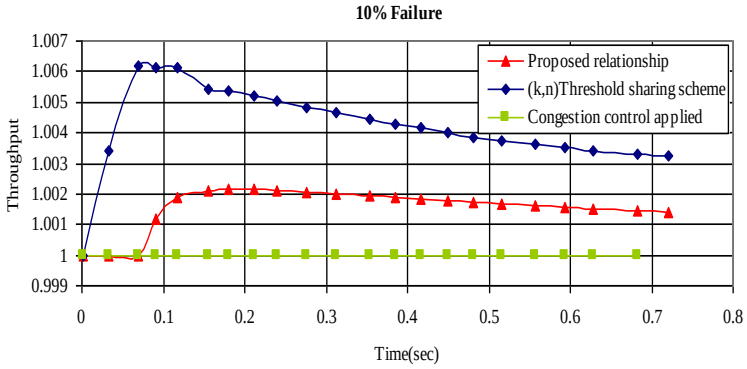


Figure 14: Comparison of the throughput of the IP/MPLS network in three different states with 10% failure

Finally in fig.15, when the network failure reaches its highest level the throughput of the network, when applying a congestion control, reacts much better than the TSS and after almost 1.5 second reaches a desire state and this is because of a few packet loss that naturally happen in the network at this situation.

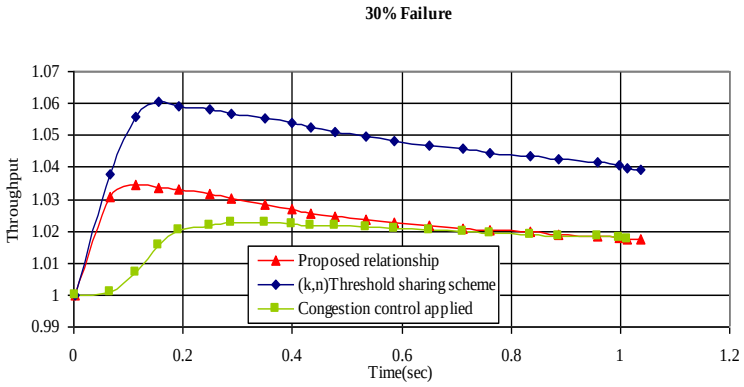


Figure 15: Comparison of the throughput of the IP/MPLS network in three different states with 30% failure

The above obtained figures show that in the case we use the congestion control for traffics flows in the network, even in situations where the network experiences its highest probability of failure, our main aim which was moderating multiple failure occurrences in the underlying network, is finely achieved.

## 6. Conclusion

Based on a modified Threshold Sharing Scheme(TSS) with multipath routing, this paper has presented an efficient relationship between two main factors in the TSS, which are the number of LSPs carrying network traffics from the source and the number of LSPs which have reached and delivered the traffics to the destination. We applied our proposal in Smart Grid networks, where the arriving demands have different priority levels, and the infrastructure used is especially chosen to be an IP/MPLS network. The recovery path protection used in this paper is a fault notification message to the router that is responsible for rerouting the traffic and sending the packets which were unable to reach the destination because of a node/link failure happening somewhere in their passing LSPs, in their sequence order. A congestion control method is also used to decrease the packet loss of the network. Our proposal considers multiple failure happening in the underlying network and the simulation results show an appropriate end to end delay time, packet loss and the throughput of network traffics in three different failure situations. Our approach can be very useful in time-critical applications running on networks susceptible to failures.

## Reference


Alouneh S., Anjaili Agrwal, Abdeslam En-Nouaary(2009), A novel path protection scheme for MPLS networks using multi-path routing, *Computer Networks 53 pp*. 1530-1545.

Awduche D., L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow(2001), RSVP-TE: Extensions to RSVP for LSP Tunnels, IETF, RFC 3209.

Barenghi A. and Gerardo Pelosi(2011), Security and Privacy in Smart Grid Infrastructures, *22nd International Workshop on Database and Expert Systems Applications*.

Bhandari R.(1999), Survivable networks, Algorithms for Diverse Routing, Kluwer *Academic Publishers*.

Fadul J., Kenneth Hopkinson, Christopher Sheffield, James Moore and Todd Andel(2011), Trust Management and Security in the Future Communication-Based "Smart" Electric Power Grid, *Proceedings of the 44th Hawaii International Conference on System Sciences* .

Haskin D.(2001), A method for setting an alternative label switched paths to handle fast reroute, *Internet Draft.*

Huang, C., Sharma, V., Owens, K., Makam, S., (2002). Building reliable MPLS networks using a path protection mechanism. *IEEE Commun. Mag. 40 (3)*, 156–162.

Makam K., C. Huang, V. Sharma(2002), Building reliable MPLS networks using a path protection mechanism, *IEEE Communication Magazine* ,156–162.

Mobasheri B., Yaghmaee Moghadam M.H.(2012), Applying a priority-based IP/MPLS management scheme in Smart grids, 6th *International Symposium on Advances in Science and Technology*,Kuala Lumpur, Malaysia .

V. Rajeev V., C.R. Muthukrishnan(2001), Reliable backup routing in fault tolerant real-time networks, in: *Proceeding of the Nineth IEEE International Conference on Networks*, pp. 184–189.