УДК 681.324

FAST REROUTING METHOD IN MPLS NETWORKS IN CASE OF FAILURES

HAZEM HATAMLEH

The problem of nonlinearity identification in experimental data is considered with application of appropriate statistical tests. An analysis of known statistical nonlinearity test is presented that is based on Fisher relation, and a new simplified test is proposed that can be used in conditions of incomplete experimental or statistical data. The empirical statistical nonlinearity criterion is computed on the basis of existence of a link between the values of respective cumulative sum and sample based standard deviation. It was empirically established that there exists a close link between the proposed and existing tests in the sense of similarity of final testing results. To find the critical values of statistics that are necessary for statistical decision making with the use of the simplified test appropriate computational experiments have been fulfilled. It has also been established that the test proposed can be used successfully in conditions of complete and incomplete experimental data. The practical application of the test proposed to actual data proved the similarity of results obtained with various approaches.

INTRODUCTION

Rapid growth of real-time traffic, which is transmitted via IP networks, sets not only high demands to a quality of service, but also to network survivability. Currently, the degree of survivability in the Internet is defined only as ability finding and installing an alternative routes in case of crash. Today MPLS is becoming a key technology of transmission in the core network. Networks with MPLS technology — technology oriented on connections, are even more sensitive to failure. Therefore, the development of methods of traffic protection from failures in a service is an important task.

The goal of this paper is to develop a fast rerouting algorithm to protect traffic that would provide the best use of bandwidth and performance requirements to a quality of service (QoS).

FAST REROUTING METHOD

In networks with MPLS technology three approaches to a problem of traffic protection from failures to service one of label switched route are used.

The main point of method of global recovery (global protection) is that when denial occurs in result of router or communication channel breakdown, the router

which finds failure, sends RSVP-message to a border router of region, which calculates new routes for traffic, which was transmitted through the channels or node, which failed, and redirects traffic to a new route.

The main point of method of global security (global protection) is that reserve routes on which traffic will be routed in the event of failure are calculated and determined simultaneously with the main routes. When the failure is detected, a border router immediately begins to redirect traffic to a reserve route.

The idea of fast rerouting method, which is a method of local protection, is shown in Fig. 1.

In Fig. 1 T1 is the main label-switched (LS) route, by which traffic is passed from router R2 to R6, T2 — the main LS-route, by which the traffic is passed from router R7 to R9.

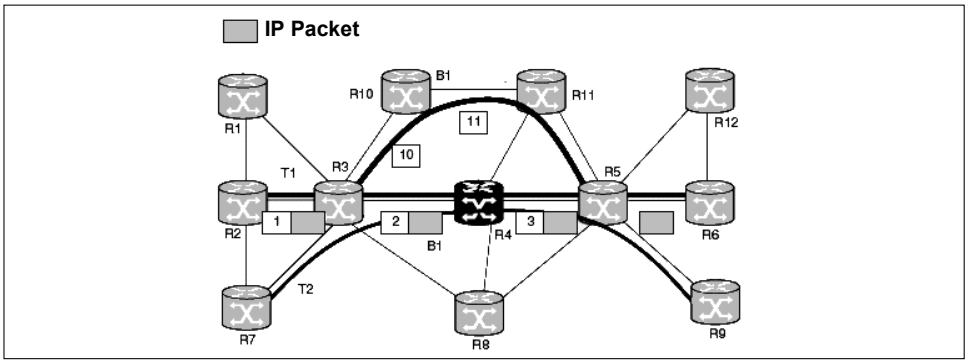

Fig. 1. Fast rerouting

Let the router R4 has failed. In this case, router R3, through which routes T1 and T2 pass, reveals the lack of communication through the path R1-R4. The router R3 finds a new route for all flows that follow through that communication channels and establish a tunnel B1: R3-R10-R11-R5 and redirect all traffic through that tunnel. Traffic rerouting along this tunnel was performed to add one more label to a package with a stack labels. When a packet reaches to a node R5 this label is removed from the stack and a packet follow through the main route.

REQUIREMENTS FOR NETWORK RECOVERY METHODS

Evaluation of the recovery mechanisms of the network requires consideration of several parameters: recovery time, size of network, bandwidth and quality of service parameters use, etc.

Obviously, the recovery time of the global recovery method will be the largest, because it contains failures detection time, time of failure transmission to the border router, the calculation time and a new route establishment time.

As for recovery time in a local protection mechanism, it consists only of time we need to pass the message about the failure to the border router. And in fast rerouting method traffic redirection begins as soon as the router, closest to the area, where a failure has occurred, detect it.

An important parameter when security algorithms work is the size of network, as the number of nodes in the network is growing, the load to routers is also increasing, because it is associated with the need to store additional information about the reserve routes and of the time of route calculation is also increasing.

For the protection algorithms (global and local) the important is reservation of additional bandwidth that is available when the network works without interruption. The mechanism of global protection sets a reserve route that duplicates the main route. In contrast to this mechanism, the local rerouting method can establish reserve tunnels that duplicate only a part of the route. Therefore they can be used by all routes that pass through an area which is protected by him. In addition in local protection is possible sharing of bandwidth of the tunnel. Tunnel B1 on the Fig. 1 can be used not only to protect the traffic that passes along the route R3-R4-R5, but also to protect areas R3-R8-R5.

For some traffic types it is important to maintain a quality of service. During the voice transmission isn't allowed reducing of the service quality for a long period of time. So it is important that recovery mechanisms ensure the quality of service.

The problem of ensuring quality of service is much more complicated when equipment breaks down and loses part of precious resources and solving of this problem is more complicated than when the network is working normal. Obviously, not all types of traffic can use reserve tunnels, as there would be significantly increased bandwidth use, that leads to overloads. That's why, only high-traffic routes should be protected by the protection mechanisms. To the rest of traffic, we use the method of the global recovery.

Also in connection with the problem of guaranteeing quality of service in MPLS networks is the notion of priority service (preemption), the main point of which is at times, when bandwidth isn't enough, capacity of low priority traffic may be directed to transmit high priority traffic. Thus, all the above requirements should be considered when restoration algorithms are developed in case of network failures.

ALGORITHM FOR FINDING RESERVE ROUTES

A distinctive feature of the proposed local rerouting algorithm from the other similar algorithms is an algorithm for finding reserve tunnels, which considers the quality of the service indicators and works in a decentralized manner.

MPLS network is given as a graph $G = (V, E)$, where $V = \{v_j\}$, $j = \overline{1,n}$ is a set of nodes — MPLS routers, $E = \{(r, s)\}$ is the set of communication channels. Each node in a network is characterized by the intensity of processing of the incoming packets — $\{\lambda_i\}$ each channel is characterized by its bandwidth capacity — $\{\mu_{rs}\}$.

Subscribers connected to the router form the input flow, which is described as a requirements matrix of input Poisson flows of the *k*-th class $H^{(k)} = \left\| h_{ij}^{(k)} \right\|$, $i, j = \overline{1,n}$, $k = \overline{1,K}$, where $h_{ij}^{(k)}$ — the intensity of input flow of *k*-th class transferred from node i to node j.

For each type of transferred data the following indicators of QoS should be set: the average delay — $T_{\text{Delay}}^{(K)}$, $\sigma_{\text{Delay}}^{(K)}$ is delay variation (jitter), the probability of packet loss — $P_{\text{Delay}}^{(K)}$ and the following constraints for the desired levels of QoS should be satisfied:

$$T_{\text{Average}}^{(K)} \le T_{\text{Delay}}^{(K)},$$

$$P_{\text{Average}}^{(K)} \le P_{\text{Delay}}^{(K)},$$

$$\sigma_T^{(k)} \le \sigma_{T\,\text{Delay}}^{(K)}. \quad (1)$$

Expressions formulas for finding the average delay, delay variation and packed loss probability were obtained in work [1].

Assume in time t router discovered that one of his neighbors can't answer and he needs to redirect traffic $h_{ij}^{(k)}$ to bypass the router, which failed. Assume that at time t router knows network status, that is, the loading of channels: $\rho(t) = \{\rho_{rs}^{(k)}(t)\}$. The loading of the channel is the ratio of volume of traffic to the bandwidth.

1. Find conditional metrics by the formula, which is obtained in work [2]:

$$l_{rs}^{(k)}(t)\Big|_{\rho^{(k)}=\rho_{rs}^{(k)}(t)}. \quad (2)$$

2. By the matrix we find the shortest path given the fact that the channels have sufficient bandwidth capacity:

$$\min_{(r,s)\in\pi_{ij}^{\min}} \{(1-\rho_{rs})\mu_{rs}\} > h_{ij}^{(k)}. \quad (3)$$

If the algorithm does not find ways, then it generates denial to service as the network is unable to transfer this amount of data in a given time. Otherwise, proceed to step 3.

3. Distribute this flow on the found path.

4. Check of constraints (1) fulfillment. When they are fulfilled, the router establishes a LS-path, and starts the data transfer. In a different way, proceed to step 5 and try to redistribute the flows that are passing through this router.

5. Repeat steps 1–3 for finding distribution of the flows $V^{(k)} = [v_{rs}^{(k)}]$, using at the step 1 conditional metrics:

$$l_{rs}^{(k)}(t)\Big|_{F^{(k)}(t+1)} \quad (4)$$

6. Check the condition of possible optimization of the flow distribution $F(t+1)$:

$$\sum_{(r,s)\in E} l_{rs}^{(k)} f_{rs}(k) > \sum_{(r,s)\in E} l_{rs}^{(k)} v_{rs}(k). \quad (5)$$

If this condition is true, then go to step 8, otherwise STOP — problem is unsolvable at the given input parameters.

7. Find the first requirement (i, j_1), for which the inequality (6) is valid

$$\sum_{(r,s)\in E} l_{rs}^{(k)} f_{rs}^{ij_1}(k) > \sum_{(r,s)\in E} l_{rs}^{(k)} v_{rs}^{ij_1}(k), \quad (6)$$

where $\hat{\pi}_{ij_1}$ — path of the requirement transmission (i, j_1), that is used in the current distribution $F(t+1)$, $\pi_{ij_1}^{\min}$ is the shortest path in the metrics $l_{rs}^{(k)}(t)$. The

flow of the requirement packets (i, j_1) redirecting from the path $\pi_{ij_1}^{\min}$ to path $\hat{\pi}_{ij_1}$ and find a new flow.

8. Check the performance of the conditions (1). If they are true, then it's the end of the second stage, else go back to step 7, choose the next request that satisfies the condition (1).

In a result of the algorithm performance we obtaina new route and distribution of flow of class k, which satisfies constraints (1).

RESULTS OF EXPERIMENTS

For experimental research the corresponding algorithm was implemented as part of software kit «MPLS Net Builder». The work of decentralized local rerouting algorithm was compared with the work of the centralized global security algorithm.

Algorithms of routes protection from overloading use a significant part of network resources, that's not used during normal work of the network. That's why, an important indicator of the work of algorithm is the number of reserve routes that are set to protect the major routes from failures. In Fig. 2 dependence of number of the reserve tunnels from network size is shown. From the Fig. 2 we may see that for local rerouting algorithm this dependence is linear and creates a smaller number of reserve tunnels. This means that in contrast to the global protection algorithm, where a reserve route is created for each primary route, in the local rerouting algorithm one reserve tunnel is created to protect each part of the route, but due to the assumption that at in the same time the failure of only one channel or hub may happen the sharing use of tunnels by different routes enables total number of tunnels to be smaller.

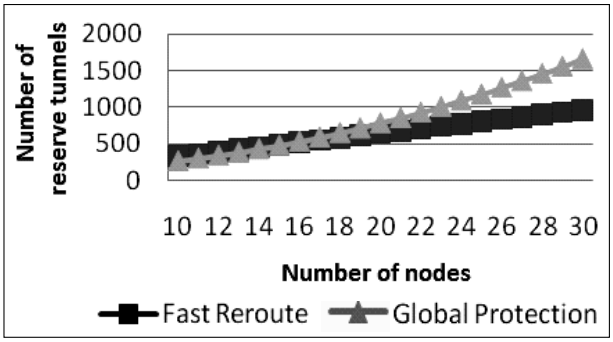

Fig. 2. The number of reserve tunnels

A similar effect has sharing of throughput capacity of channels on the over-overall throughput capacity, that use routes. In Fig. 3 the total bandwidth capacity used by reserve tunnels is shown. As the bandwidth capacity of the tunnel in the local rerouting algorithm is used by the various routes, the reserve local tunnel can protect immediately several different parts of the network. As we can see from

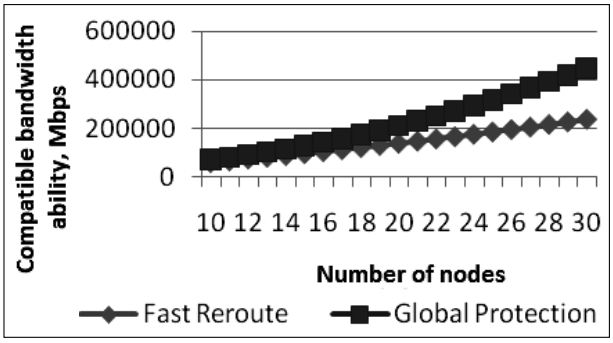

Fig. 3. Compatible bandwidth usage

from the presented dependence at the Fig. 2, the greater is the number of nodes in the network, the more effective is usage of local rerouting.

Certainly, an important aspect of work of security algorithms is their ability to maintain high quality of service in the periods of network equipment failures. In Fig. 4 the curves of the average packet delay time with high requirements to quality of service during normal work of the network equipment and in the periods of failures when algorithm of local rerouting or global defense is used. As we can see when high-priority traffic is routed through a reserve route average time of delay increases, which is evident because reserve routes aren't optimal when compared with the main routes. But we also can see, that due to the fact that at local rerouting total delay time increases only by the value of delay needed to bypass a single channel or node of main route that failed, the average time of delay increase in the local rerouting algorithm is less than in the global protect algorithm.

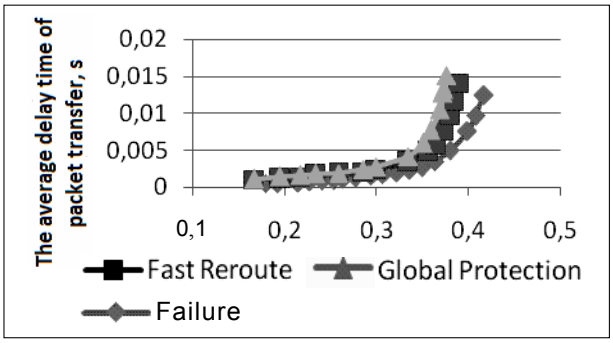

Fig. 4. The average delay time of packet transfer

CONCLUSIONS

As experimental investigations show, via program implementation the suggested algorithm has achieved the very high degree of utility of bandwidth capacity when compared with the centralized control method of setting paths, namely the indicator of bandwidth capacity saving reaches the value of 5. This means that for centralized control of reserve paths we need 5 times more bandwidth capacity than for decentralized local rerouting algorithm. And additionally, all the requirements to the level of quality of service during transfer by the new routes are assured. The only disadvantage of this method is that the inner routers of MPLS area may not have sufficient computational capacity, in contrast to the border routers that perform global protection.

REFERENCES

1. *Zaichenko Y.P., Ahmed A.M. Sharadka*. Task distribution of flows of different classes in the networks with MPLS technology // Journal of NTU «KPI». Avg. Informatics, Management and Computing equipment. — 2005. — № 43. — P. 113–123.
2. *Zaichenko Y.P., Lavrinchuk O.M.* Decentralized algorithm of distribution of traffic flows in MPLS networks based on the state of channels and parameters QoS // Journal Cherkasy State Technological University. Avg. Technical Science. — 2010. — № 2. — P. 17–27.
3. *Bruce S. Davie, Adrian Farrel*. MPLS: next steps. — San Francisco: Morgan Kaufmann, 2008. — 432 p.

Received 25.05.2011

From the Editorial Board: the article corresponds completely to submitted manuscript