Recovering Guaranteed Performance Service Connections from Single and Multiple Faults†

Anindo Banerjea, Colin J. Parris, and Domenico Ferrari.

Tenet Group
Computer Science Division, UC Berkeley
and
International Computer Science Institute,
1947 Center St. , Suite 600
Berkeley, CA 94704-1105.
Tel: (510)-642-8919 Fax:(510)-643-7684
E-mail: {banerjea,parris}@tenet.berkeley.edu

TR-93-066

ABSTRACT

Fault recovery techniques must be reexamined in the light of the new guaranteed performance services that networks will support. We investigate the rerouting of guaranteed performance service connections on the occurrence of link faults, focussing on the aspects of route selection and establishment in the network. In a previous investigation, we explored some components of rerouting in the presence of single link faults in the network. In this paper we study the behavior of our techniques in the presence of multiple link faults in the network, and also examine the technique of *retries* to improve the success of rerouting. Our schemes are simulated on a cross-section of network workloads, and compared using the criteria of the fraction of the affected traffic that could be rerouted, the time to reroute and the amount of resources consumed in the network. A novel metric, the *Queueing Delay Load Index*, which captures both the bandwidth and delay demands made on the network by a connection, is used to present and analyze the results.

Keywords: Fault recovery, guaranteed performance, network management.

†This research was supported by the National Science Foundation and the Defense Advanced Research Projects Agency (DARPA) under Cooperative Agreement NCR-8919038 with the Corporation for National Research Initiatives, by AT&T Bell Laboratories, Hitachi, Ltd., Hitachi America, Ltd., Pacific Bell, the University of California under a MICRO grant, and the International Computer Science Institute. The views and conclusions contained in this document are those of the authors, and should not be interpreted as representing official policies, either expressed or implied, of the U.S. Government or any of the sponsoring organizations.

1. Introduction

Guaranteed Performance Communication[1] (GPC) has been recognized as an important service from future wide-area broadband-ISDNs [23]. Several GPC schemes have been proposed to date; however, they all assume adequate fault-free service from the underlying network. The high level management features needed for such schemes are still under investigation. Fault recovery is one of the critical features which must be added to make GPC schemes of practical use.

Fault recovery consists of the tasks of fault detection, recovery instigation, computing and distributing new state information, and rerouting the affected traffic. Our investigation focusses on the *rerouting* of GPC connections in a network with redundant connectivity after the occurrence of link faults. In a previous paper [24] we investigated rerouting to recover from single faults in the network along two orthogonal components. In this paper we extend the investigation to multiple faults, which aggravates the problem of *route collisions* (see Section 4.2). We also borrow the idea of retries from the world of telecommunication failure recovery [10], and explore the effect of adding retries to our schemes under single and multiple faults.

In Section 2 we look at related work in the area of GPC schemes and network fault management. In Section 3 we examine the reasons for choosing this approach to fault recovery. In Section 4 we present a model of the network in which our fault recovery schemes work, and a model of the fault recovery process. In Section 5 we present our experimental design. In Section 6 we present and analyze our results. In Section 7 we summarize our results and mention directions of future research.

2. Related work

In [24] we investigated fault recovery for GPC networks in the presence of single link faults along two components: the *locus of reroute* (which determines the section of the failed route over which a reroute is attempted) and the *reroute timing* (which determines when the actual attempt to acquire resources over the new route is performed). These approaches and the results of our investigation are summarized in Sections 4 and 6. Apart from this paper, we have not come across any investigation of fault recovery for GPC schemes in the literature. However, a significant amount of work has been published in the area of GPC schemes (without fault recovery), and of fault recovery in other contexts.

Several investigators have proposed schemes for GPC service in packet switched networks. The Tenet group [2] has devised an approach [1] to the provision of such services, which we assume as part of our underlying network model and describe briefly in Section 4. The *guaranteed service* proposed in [2] meets the definition of GPC as used in this paper, as opposed to the *predictive service* proposed in the same

[1] Defined as communication with guaranteed bounds on performance parameters such as bandwidth, delay, jitter and loss rates.

[2] At the University of California at Berkeley and the International Computer Science Institute.

paper. The Session Reservation Protocol [3] provides deterministic guarantees and follows an approach similar to that of the Tenet group. The Heidelberg Resource Administration Technique (HeiRAT) [5] uses the ST-II protocol to reserve bandwidth resources for unicast and multicast connections. The Asynchronous Time Sharing (ATS) approach [4] provides a menu of QOS classes to the client, while the Flow Protocol [25] allows clients to specify an average throughput bound and compute the resulting delay bounds. PlaNET [26] performs bandwidth reservation using an equivalent bandwidth model. All these schemes have some basic similarity; indeed it can be argued [1] that any scheme that provides a similar service with the same set of assumptions about the network must to have the properties of resource reservation, admission control, connection-orientedness with pre-computed routes, and a service discipline or policing strategy which protects one connection from another. This leads us to believe that it may be possible to devise an abstract model of GPC schemes which is independent of the details of the particular scheduling mechanism, admission control test, etc. but captures enough information to allow management schemes to be built on top of these data transfer schemes. Our fault recovery schemes make as few assumptions as possible about the underlying GPC schemes, hence we believe that they would work well with any of the above GPC service schemes.[3]

Fault recovery in telecommunication networks has been presented in [6] in the context of a layered model of the transport network. At the highest layer, the *switched layer*, the unit of communication and fault recovery is the *call*. The recovery action taken at this layer is to update the routing database in order to correctly route new calls around the fault [7,8]. Existing calls are lost and have to be redialed by the end systems. At the *Cross-connect layer* the units of communication and recovery are *trunks* (e.g. DS1 or DS3),[4] which have fixed bandwidth requirements and relatively stable routes. This makes the network relatively stateful and the fault recovery mechanism attempts to preserve this state. Recovery approaches used at this level include pre-computing and storing the configurations for a large failure set [9,10,11], and running dynamic distributed algorithms to find short routes [12,13,14,15].

Conventional computer data networks are mostly based on a connection-less paradigm (e.g. Internet). Fault recovery in these networks consists of recomputing routing information to route new data correctly. In the Internet no performance guarantees are given, though the protocols attempt to reduce congestion and network instabilities [16,17,18]. AN1 [19] and AN2 are local area networks designed for high survivability. AN1 is packet switched and connection-less, while AN2 is ATM based, connection-oriented and supports CBO (fixed bandwidth) traffic. However, both networks stop data forwarding during the network state acquisition and routing table computation; this technique only works in local area networks.

---

[3] However our simulations test the performance of these schemes in the concrete context of the Tenet scheme, since the resource reservation and scheduling disciplines are simulated in detail.

[4] The trunks in turn appear as the links in the network topology seen by the next higher layer: the switched layer.

3. Motivation

Fault recovery for GPC networks is different from that for conventional data networks because GPC networks need to maintain performance bounds and keep network state during recovery. It has more in common with recovery in the cross-connect layer of the telecommunication network, where the trunks have bandwidth requirements and relatively stable paths. However in the cross-connect layer, there are relatively few trunks which belong to a small number of classes (e.g. DS1, DS3), whereas in a GPC network the connections would in general have peak and average bandwidth specifications, delay, jitter and loss-rate requirements, and the number of possible combinations preclude approaches such as pre-computation and storage of all configurations. As such, more distributed dynamic schemes, which provide good but sub-optimal solutions, have to be investigated.

Our investigation focusses on the aspect of rerouting, where we think the hardest problems of failure recovery lie. One possible approach to fault recovery is to move this function to the application layer, i.e. recompute the network topology and state so as to route new requests correctly, but allow all affected connections to be lost and re-established by the applications. This idea is clean and appealing, but there are strong practical reasons to incorporate at least some fault recovery within the network. Application initiated fault recovery would result in all the affected connections being retried within a short time after the fault, especially if the applications have requirement for quick recovery. Thus all affected connections will compete for resources during the rerouting phase, causing *route collisions*. Spreading the attempts out in time and space (over different routes) would increase the probability of success of the attempts. This sort of cooperation is harder at the application level. In addition, there is state within the network which can be reused to reduce the amount of work which needs to be done. It may be possible to restrict the exchange of messages to the affected portion of the connection to speed up the recovery and increase the probability of success. The response time of the reroute will also be faster, the lower the level at which this recovery action is initiated. For instance, if the recovery action is initiated by the node adjacent to the failed link, then the recovery will be faster than if the error message must first propagate to the application layer. Another (perhaps debatable) advantage is that the user is not involved in the recovery action. Finally, a scheme for automatic recovery could also be used to move traffic off a link, in response to increased error rates or as a management action.[5] In this case, only the fault detection mechanism would need to be modified to allow the recovery mechanism to be triggered manually or by error rate thresholds. Thus there are strong reasons to consider placing recovery mechanisms within the network. It is therefore important to explore the various possibilities for network initiated automatic rerouting systematically.

Our previous investigation explored two components of rerouting against a cross-section of network loads using evaluation criteria that captured the impact of the fault on the client and the network. In this paper we add the component of multiple retries, borrowing the idea from the telecommunication world

[5] For example, to allow a connection with unusually high requirements to be established, or for maintenance.

[10], and compare the possible benefits resulting from this approach against the other techniques. We also examine in this paper the effect of multiple isolated faults within the same *recovery cycle*,[6] where isolated means that the faults affect disjoint sets of channels. Since the logical topology seen by computer networks is actually overlaid on a lower physical topology, with logically separate trunks sometimes existing on the same physical fiber, multiple isolated faults are not such an unlikely occurrence. Multiple non-isolated faults are more unlikely since they would arise from the simultaneous failure of two distinct physical links.[7] We would like to look at the effect of the temporary increased routing load caused by two simultaneous faults trying to use the remainder of the network to reroute their affected channels. Our earlier investigation shows us that the major difficulty with rerouting in GPC networks is route collisions and we expect multiple isolated faults to aggravate this problem.

4. Model

In this section we provide the network model. This model includes the model of the guaranteed performance scheme (i.e. the Tenet model) and that of the fault recovery scheme. In conjunction with the detailed description of the fault recovery model, the underlying support mechanisms (i.e. the fault detection and control mechanism and the routing mechanism) will also be presented.

4.1. The Tenet Scheme

The Tenet scheme allows the network to provide guaranteed performance communication services. In this service a guaranteed performance connection (*a real-time channel*) is an abstraction that defines communication services with guaranteed traffic and performance parameters in a packet-switched network[1]. A channel's traffic is characterized by: $X_{\min}$, the minimum packet inter-arrival time, X_{ave}, the average packet inter-arrival time over an averaging interval I, and, $S_{\max}$, the maximum packet size. The performance requirements available to channel are: D,the maximum delay permissible from the source to the destination, J, the maximum delay jitter[8], Z, the probability that the delay of the packet is smaller than the delay bound, and, W, the buffer overflow probability. In the Tenet scheme a channel is *established* and then data is transferred. Channel establishment occurs in the following sequence: a real-time client specifies its traffic characteristics and performance requirements to the network; the network determines the most suitable route for this channel using its traffic characteristics and performance requirements; the network translates the end-to-end parameters into local parameters at each node, and attempts to reserves resources at these nodes accordingly. Channel establishment is source routed and occurs in two passes (i.e.

[6] The interval from the occurrence of a fault to when the last connection affected by that fault is either successfully rerouted or reroute attempts are aborted.

[7] We assume that the logical network layout and the routing on top of that does not cause a connection to traverse the same physical link twice.

[8] Jitter is defined here as the difference between the delays experienced by any two packets on the same connection.

the round trip from the source host to the destination host). Resources, corresponding to the lowest possible delay, are reserved at each node along the forward pass. This is required because the exact reservation required to meet the end-to-end requirements depends upon the resource state on the downstream nodes; thus, a scheme which reserves less resources at an earlier node might fail to meet the end-to-end delay requirement, if a downstream node is heavily loaded and cannot provide a low delay bound. Our scheme thus over-books resources on the forward pass, and along the reverse pass these resources are appropriately relaxed to reflect the actual needs of the channel. To determine the availability of resources, each node uses the Tenet algorithms or admissions tests, which are based on the service discipline. Research by Ferrari et al.[20] has shown that a broad spectrum of service disciplines may be used in the Tenet framework, however, in this paper we have chosen Rate Controlled Static Priority (RCSP) queuing as it decouples the bandwidth and delay resources while providing simple admissions tests.

4.1.1. Rate Controlled Static Priority (RCSP) Queuing

The RCSP service discipline can be logically divided into a rate controller and a scheduler. The rate controller ensures that all sources obey their input traffic description by calculating the expected arrival time of a packet using its traffic description. If at any time a packet violates its traffic description by arriving before its expected arrival time, this packet is held until such a time that its traffic description is not violated. Packets are then passed on to the scheduler which maintains several levels or priorities and serves packets First-Come-First-Serve (FCFS) within each priority starting at the highest priority queue at which packets are waiting and ending at the Non-Real-Time queue[9]. The separation of the rate controller and the scheduler provides the decoupling of the bandwidth and delay resources.

The admission control test, provided below, is performed at each node during channel establishment in order to provide guaranteed performance service communication in a network of servers with RCSP scheduling. The test proceeds as follows: For a request with the traffic specification ($X_{min}, X_{ave}, I, S_{\max}$) and a delay bound requirement D_k (where $D_1, D_2, D_3, .., D_l$ are the delays associated with each of the l priority levels in the switch), if for all priority levels p greater than or equal to k:

$$\sum_{j=1}^{j=c_p} \left\lceil \frac{D_p}{X_{\min_j}} \right\rceil * S_{\max_j} + \left\lceil \frac{D_p}{X_{\min}} \right\rceil * S_{\max} + S_{maxP} \le D_p * L \qquad (1)$$

then the new channel can be accepted (at the priority level k). c_p is the current number of channels at or above the priority level p, $X_{\min_j}$ is the minimum interarrival time of packets corresponding to the jth connection at that priority level, S_{maxP} is the largest packet size that can be transmitted over the link, and L is the link speed. Proofs of the correctness and sufficiency of this test are presented in [22].

The purpose of the test is to guarantee that a packet belonging to any priority level p experiences at most a delay bound of D_p before it is transmitted, assuming that all previously queued packets at this level

[9] Packets in the Non-Real-Time queue are only served after the lowest level RCSP queue's packets have been served.

and all packets at higher priority levels will be transmitted prior to it. Therefore, adding a channel at level k contributes *work* to all equal and lower priority levels $p \geq k$. The admission test ensures that the total *work* at any level p cannot exceed the delay bound D_p for that level, where *work* at level p is defined as

$$W_p = \sum_{j=1}^{j=c_p} \left\lceil \frac{D_p}{X_{\min_j}} \right\rceil * \frac{S_{\max_j}}{L} + \frac{S_{maxP}}{L} \qquad (2)$$

4.2. The Failure Recovery Model.

In this section we will present our model of failure recovery which is based on the Tenet guaranteed performance services scheme. We will begin by giving a brief overview of rerouting to provide the proper context for our work. We will then describe our model and discuss the specific components that we intend to investigate.

As mentioned previously, fault recovery can be divided into the tasks of fault detection, recovery instigation, computation and distribution of new routing information, and channel rerouting. The focus of this investigation is the rerouting task, which can be further subdivided into *route selection*, determining the new route, and *alternate route establishment*, transferring the channel onto the new route. Optimal solutions of *route selection* involve exponential computational complexity, and all other solutions involve trade-offs between time and goodness of the solution. *Alternate route establishment*, which changes the resource state in the network to reflect these new routes, involves cooperation, since network resources must be shared.

In the literature [6], the approaches to rerouting have been classified along three axes: *Centralized vs. Distributed schemes*, *Link rerouting vs End-To-End rerouting*, and *Pre-computation vs dynamic computation of routes*. In an integrated high-speed packet-switched network that provides guaranteed performance service connections, we believe the most useful approach to be a distributed, dynamic computation approach. The problems introduced by a centralized scheme, i.e. scalability, reliability of the central control unit, and congestion and computational bottlenecks at the control unit, lead us to believe that a distributed scheme would be more efficient. Also, the dynamic nature of multimedia traffic, which will most likely pervade these networks, will render the pre-computation of routes ineffective. Rerouting will need to be done dynamically. In our investigation we will compare Link and End-To-End rerouting.

In our failure recovery model, a fault is detected by the node upstream of the faulty link, which informs all nodes in the network of the topology change by route update messages. The detector also instigates recovery on affected nodes (i.e. source nodes of affected connections) by sending a reroute message. These nodes then perform route computations and attempt to reroute as many of the affected connections as possible, while satisfying their initial traffic and performance requirements. Our model for fault recovery contains the following components: the method used for fault detection, the routing algorithm used to find a new route for a given channel, the constraints on the route selection, the timing of the alternate establishment attempt, and the maximum number retries that are performed. In our investigation, we

focus on the last three components, which together comprise the rerouting scheme. We fix or make simplifying assumptions about the other components.

We examine rerouting along the lines of three orthogonal components: *the locus of reroute*, *reroute timing*, and *retries*. One of the goals of this investigation is to establish the significance of these components, as such we have chosen easily analyzed yet broadly encompassing instances of each. The *locus of reroute* component indicates the node which performs reroute selection, and the portion of the current route traversed by the connection upon which a reroute attempt will be made. We consider three locus of reroute types: *Global reroutes*, *Local reroutes*, and *Hybrid reroutes*. With a Global reroute, which corresponds to the *end-to-end* rerouting of [6], the path of the rerouted connection is determined at the source node based on the current network load and the traffic and performance characteristics of the connection. As all information available to the node is considered in determining this route, this scheme would tend to distribute load evenly through out the network. With a Local reroute, the rerouted connection traverses the original route but bypasses the failed link. The route computation is performed by the node upstream of the failed link, and determines a path segment from this node to the node downstream of the failed link. This segment is combined with the unaffected portion of the old route, removing any redundant links or loops. The *route establishment* still traverses the entire new route, in order to balance resource along the length of the route. This type of locus of reroute reuses the maximum amount of previously reserved resources, and in a highly loaded network may have a higher probability of success than a Global reroute. It also localizes the effect of the reroute to the immediate neighborhood of the fault, which might improve performance for multiple faults. It corresponds roughly to *link rerouting* of [6], except that the complete round-trip for *route establishment* implies better resource balancing, higher success rates, but longer establishment times. A Hybrid reroute combines the previous two types of locus of reroutes; a Local reroute is first attempted, however, if a local path cannot be found, a Global reroute is initiated. In all types of locus of reroutes the traffic and performance characteristics of any rerouted connection must be maintained after the reroute.

The *reroute timing* component provides the starting time of the reroute attempt. This component seeks to mitigate the effect of route collisions and database inconsistencies. *Route collisions* occur when an establishment request, during the forward pass along a link, consumes a large fraction of the remaining resources on the link (see Section 4.1), thus causing an immediately following forward pass establishment request to fail due to lack of resources, even though on the reverse pass the former establishment request would have relaxed its resource reservations such that the latter could have had its resource request honored. Reducing route collisions would increase the probability of establishing a connection. *Database inconsistencies* can also cause reroute attempts within a small time interval of each other to interfere. Had there been sufficient time between connection reroute attempts the routing database may have reflected a more accurate network load and the latter of the two reroutes would have chosen a different path through the network.

Three possible approaches are considered for the timing component: *Immediate*, *Random(n)*, and *Sequential*. Under Immediate timing, reroute attempts are initiated by the controlling node as soon as a failure is reported to it. This approach depicts the least cooperation and possibly the most expected interference. Under Random(n) timing, the reroute attempt time is determined by generating a random value from a uniform distribution over an interval of duration n. This random value is added to the current time with the result being the reroute starting time. This approach does introduce some level of cooperation as all controlling nodes use the same algorithm. Under Sequential timing, all reroutes attempts are handled sequentially with only one controlling node initiating a reroute attempt at any given time. When all the reroute attempts of a single affected connection are completed only then are reroute attempts made on another connection. Sequential timing reduces route collisions and database inconsistencies but at the cost of much higher average time to reroute.

The *retries* component indicates if retries are permitted on a reroute attempt. The retry mechanism removes the saturated link (at which the previous reroute failed) from consideration, incorporates new information presented by recent database update messages, and attempts to calculate a route from the source to the destination. Retries are repeated on failure up to a pre-determined limit; different values of the limit give us different possible approaches within this component.

The recovery schemes presented (i.e. all combinations of the approaches of the three components) are fairly simple and may not translate directly to practical implementations. However, as the objective of our investigation is to look at the significance and impact of the components, we choose approaches that span the entire spectrum of the each component. For example, Sequential timing with retries, while it may not be practical from the stand point of the time to reroute, will give us an idea of the best possible performance, in terms of rerouting success, which may be achieved by a perfect timing strategy with the maximum number of retries. Sequential provides a standard against which we can compare other more practical timing schemes. In our experiments we will explore the solution space of our recovery model by examining all combinations of the three components.

The rerouting schemes presented above utilize two mechanisms, the *fault detection and control mechanism* and the *routing mechanism*. The fault detection and control mechanism recognizes faults, informs the routing mechanism that new route update messages are needed, and disseminates fault messages to the source nodes of the affected connections. The process of fault detection is complex and is not investigated in this paper. We assume that when a link is characterized as faulty, low level validation has been performed to eliminate transient faults and oscillations. The fault message provides the relevant reroute scheme information to all affected connections. The routing mechanism is a combination of the routing algorithm and the route update mechanisms and is described in the next section.

4.3. The Routing Mechanism.

The routing algorithm used in rerouting is based on the DCM Routing Algorithm [21] and determines a route from the source node to the destination node taking into consideration the traffic and performance characteristics of the connection, the current network load, and the locus of control. The goals of the routing algorithm are to maximize throughput, balance the network load, obtain routes in a timely manner, and to maximize the probability that the route provided by the algorithm will be successfully established[10]. The routing algorithm calculates a minimal-cost route where the cost of the route is the sum of the costs of the links comprising the route. The cost of a link is a delay value, which is the sum of the minimum queuing delay offered by the starting node to a real-time channel with these traffic characteristics, the transmission delay, and the propagation delay along the output link. The transmission and propagation delay are fixed costs, however, the queuing delay in the scheduler is variable, and dependent on the current channel resource reservations and the traffic characteristics of this new channel (see Section 4.1.1., equation 1).

The DCM routing algorithm proceeds in two steps. In the first step a directed graph is created in which the nodes correspond to switches and hosts in the network and the edges to the links connecting these switches and hosts. The weights attributed to each edge represent the link costs. The link cost are computed just prior to applying the algorithm thereby using the most recent link information obtained from routing update messages. In the second step a constrained, modified version of the Bellman-Ford[11] algorithm is then applied to this graph to determine a possible route. In this algorithm consecutive searches are performed on all 1, 2, .., N-2-hop paths from the source to the destination node until the delay condition $\sum_{l(s,d)} d_l \leq D$ is satisfied, where D is the delay bound of the channel, d_l is the weight of link l, (s, d) is the path from the source s to the destination d, and N is the number of nodes in the network. A *constraint* is placed on the number of possible searches by stopping at the first *hoplevel*[12] at which the delay bound condition is satisfied, and choosing the minimum cost path within the same level.

The DCM routing algorithm maximizes throughput by minimizing the number of intermediate nodes encountered along the path from the source to the destination host. The load balancing criterion reduces call blocking by distributing the load more evenly throughout the network. The algorithm limits its search space, thus reducing its computation time, thereby providing routes in a timely manner. It also increases the probability that channel establishment will be successful as it determines the link queuing delays based on the traffic characteristics of the channel and the most recent resource reservation information.

Routing updates are currently done on a per-channel-establishment basis. This is accomplished by having every node broadcast the load values of its links to all other nodes after it sends the reverse channel

---

[10] That is, the route will be established with the traffic and performance specifications given by the client.

[11] The fundamental Bellman-Ford algorithm [22] searches for the shortest paths between a specified source and destination node starting from all possible one-hop paths and continuing until the N-2-hop paths are examined.

[12] This *hoplevel* is the number of hops from the source to the destination node.

establishment message to the previous node on the new channels route; each receiving node updates its local link-state table. This broadcast is done along a minimum spanning tree.

5. Experimental Design

This section provides a framework for our experiments by discussing the metrics by which we evaluate the various rerouting schemes, and the other experimental factors that we need to consider. First we present a new index, the *Queuing Delay Load Index* that will be used to characterize the network load and to define our performance metrics.

5.1. Load Index

A major problem to be addressed by any investigation which seeks to compare schemes involving guaranteed performance connections is the choosing of an index which is able to characterize the network load imposed by one or more guaranteed performance connections. As this imposed load is dependent on the number of connections, their bandwidth, delay, and jitter requirements, and the links traversed by each of these connections, a general solution to this problem is quite complex. However, we have devised a simple index which meets the above requirements using the concept of *work* as defined in the RCSP (Rate Controlled Static Priority) service discipline.

In RCSP, placing a channel in the network at priority level l adds work to all lower levels. This is evidenced by a low delay channel adding a greater amount of work, since it is placed at a high-priority level (small l) thereby increasing the call blocking probability at all levels $m > l$. If the delay requirement is larger, it can be placed at a lower priority level (larger l) effecting fewer levels and contributing less work. This situation prompts us to consider the sum of the *work* (specified by equation 2) across all levels as an index of the load on the node. A large increase in this index will be caused by a high priority channel as it will reflect the *work* component at a greater number of levels, while a channel at the lowest priority level will only reflect the work done at one level. We call this index of the load on the network the Queuing Delay Load Index.

Figure 1 depicts the ability of this index to capture the effect of the bandwidth, delay and path-length components in the overall load on the network. Graph *i* illustrates the response of the index with respect to the delay requirement of a channel on an empty network. As shown in the graph the load index decreases as the delay requirement is lessened. The graph flattens out beyond 200ms as the connection is now placed at the lowest level in the RCSP queues and further increases in the delay bound do not effect the priority level of the channel. Therefore with all other components fixed, the index decreases monotonically with respect to the end-to-end delay bound. Graph *ii* indicates that the load index increases linearly with respect to the bandwidth of the traffic, with the gradient of the line dependent on the delay bound of the channel. Graph *iii* shows the linear increase of the index with respect to the path length (the delay bound and the bandwidth are constant). Finally, graph *iv* shows us that the index is additive, i.e. two channels existing

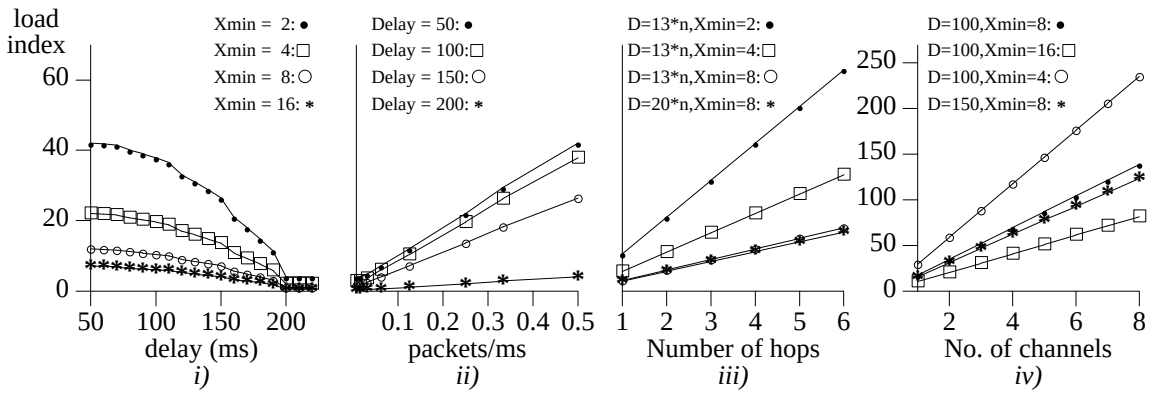

Figure 1. Queuing Delay index vs. other load indices.

together in the network create a load index equal to the sum of their individual indices in an empty network, provided that they do not interfere. Interference could cause a channel to take a longer path or occupy a higher priority level, leading to higher network load indices. These graphs indicate that this index is a good characterization of the overall load on the network, and that it can be reliably used to characterize the load on the network and to compare the behavior of the rerouting schemes.

To aid in our comparison of rerouting schemes we define the Empty Network Delay index (END index) of a channel as the load index measured by establishing the channel in a empty network. Measuring this index in an empty network allows us to eliminate second order effects, such as interference with other channels. Under the assumption that the routing scheme chooses the shortest available path and the admission scheme places the channel at the lowest appropriate priority level, the value of the END index is the smallest increase in the overall load index which can be caused by successfully establishing this channel under all load conditions. It is thus a measure of the intrinsic resource requirement of a channel, as opposed to the actual amount of resources consumed, which depends on the state of the network and the ability of the routing schemes to place the channel on the best path. The END index can be used to compare rerouting schemes schemes which successfully reroute different sets of channels under identical conditions, by comparing the sum of the END indices of one set against the other.

5.2. Metrics

The metrics used to compare the performance of the rerouting schemes are: the rerouting success ratio (SR); the average and maximum time to reroute a connection; and the excess load consumed by the reroute.

The success ratio is the fraction of the affected traffic that could be successfully restored by the rerouting scheme and is calculated by summing the END indices (defined previously) of the successfully rerouted channels, and expressing this value as a percentage of the total affected traffic. Comparing the ratio rather than the absolute value of the amount of traffic successfully rerouted makes our analysis

independent of the load. The average and maximum time to recover the affected connections are calculated over the set of successfully rerouted channels by subtracting the time at which each successfully reroute channel is established from the time of the fault and taking the average and maximum values of each set.

The excess load consumed by the network is a calculated based on the resources consumed by the successfully rerouted channels and the minimum amount of resources required to support this set of channels. The actual resources consumed by the successfully rerouted channels is measured by calculating the network load index after the rerouting is complete and again after tearing down all the successfully rerouted channels, and subtracting the two values. The minimum resources required to support this set of channels can be approximated by the sum of the END indices, since the END index of a channel represents the amount of resources required if the routing and relaxation is not constrained by the presence of other channels. The excess of resources can thus be expressed as a percentage by $\frac{(required - minimum)}{minimum} * 100$.

5.3. Experimental Factors

In our experiments we kept the network topology and the routing scheme fixed, and varied all of the rerouting components. The network topology used was that of a simple 5x5 square *mesh* as it is simple enough to allow us to verify any unusual results manually, while at the same time providing a diverse number of possible routes between any host pairs. The routing scheme used was described in Section 4.3.

In the experiments described in this paper the fault model, the workload, and the rerouting schemes are the factors that we vary. In the fault model, one link fault or two isolated link faults were allowed during a recovery cycle. As discussed previously, isolated faults exercise the abilities of the rerouting schemes under increased route collisions. The workload is composed of the set of channels which were established prior to the fault in the network. In our investigation we examined the performance of the rerouting schemes at four different workload levels. In terms of the network load index defined in Section 5.1, the load levels were *low* = 270, *medium* = 620, *medium-high* = 790, and *high* = 858. In order to provide some insight into the characteristics of these values, sample index values (taken from our experiments) and corresponding bandwidth loads are presented here. In this sample workload the *low* workload level corresponded to a 15.8% average bandwidth utilization and a 63.3% bandwidth utilization (maximum) on the heaviest loaded link; *medium* corresponded to a 32.0% average and a 84.7% maximum; *medium-high* corresponded to a 41.2% average and a 87.3% maximum; and *high* corresponded to a 44.5% average and a 86.7% maximum; The numbers shown above correspond to only one of a number of workloads which we generated and used for our simulations at each workload level. It should be stressed that the load index captures more than the bandwidth information, and a set of channels with identical bandwidth requirements but different delay requirements would give us different load index values.

Workloads were statistically generated with the channels in the workload taken from three classes, with bandwidth requirements corresponding to a one way low quality video conference channel (*Class A*),

a CD quality audio channel (*Class B*), and a telephone quality audio channel (*Class C*). The distribution of these is chosen so that 30% of the channels belong to Class *A*, 30% to Class *B*, the the rest to Class *C*. The host pairs were selected randomly to lie along the periphery of the mesh. The delay requirements of the channels were also generated statistically, to lie uniformly in the range $[x+50, x+100]$ ms, where x is the one way propagation delay between the source and the destination of the channel. Thereafter different numbers of channels were generated with the above statistical properties to get different values of the workload index. The specific values of the workload index that we used were chosen by studying the rerouting success ratio(SR) across a much more densely chosen set of workload points and observing the regions in which behavior was relatively stable. The workload points chosen represent the midpoints of these stable regions. Thereafter a number of workloads were generated with load index at or very close to each of the four values shown, and within each specific workload the simulations repeated with different random seeds fed to the simulator. The results of all of the simulation runs were averaged (or the maximum across the set taken in the case of metrics such as max time to reroute) to increase confidence in our experiments. The simulation results are specific to the topology and the statistical distribution imposed on the workload, hence we do not attempt to consider the actual values of the measured performance metrics as significant. Instead, we only compare the relative performance of the routing schemes. We did not calculate the statistical confidence because we use these results for rough comparisons and not to provide precise numbers. Thus we merely assured ourselves that the variation between experiments at the same workload level were small compared to the differences which we use to draw conclusions.

The rerouting schemes were explored along all possible combinations of the three components of locus of reroute, timing, and retries. With regard to the retry component, initial baseline experiments were conducted with 0, 2, 4 and 8 retries and our results showed that, under the current topology and workload model, no retry attempts succeeded beyond 4 retries and there was little difference between the results at 1, 2 and 4 retries. Thus the results presented here only show *no retries* and retries with an upper limit of 4 attempts. We also restrict ourselves to only one of the random approaches, Random over 1500ms, since the earlier paper explored the component in more detail. Thus simulation experiments were conducted along five dimensions, i.e. the three components of rerouting (which comprise the rerouting scheme), the workload, and the number of faults. Our experiment set included all possible combinations across these five dimensions. The results of these experiments and their analyses are presented in the next section.

6. Results and Analysis

The results of our experiments are presented in Figures 1 and 2. Figure 1 show our results with a single fault simulated in the network, while Figure 2 shows the results for two simultaneous isolated faults. Each scheme is simulated with and without retries and the results for no retries are shown as a white bar, while the bar for retries has stripes or dots. Graphs *i* to *vi* show the success ratio of the various schemes across four different values of the network load. Graphs *i*, *iii*, and *v* keep the rerouting component fixed and

allow us to compare the timing approaches, while graphs *ii*, *iv*, and *vi* show the same data but fixing the timing component within each graph to allow us to compare the rerouting schemes. Graphs *vii* to *ix* show the maximum and average time to reroute the channels, the average is shown as the lower solid (or striped for the retry case) bar, while the maximum is shown as the upper bar drawn with dashed lines (filled with dots in case of retries). Graphs *x* to *xii* show us the excess resources consumed by the schemes in the network across the same four network loads.

Looking at the single fault results, we note that without retries (the plain white bars) Local rerouting performs poorly with respect to the amount of traffic rerouted (Figure 1, graphs *ii*, *iv*, and *vi*) while Global and Hybrid are comparable. Comparing the timing approaches (graphs *i*,*iii*, and *v*) we see that success ratio improves from Immediate to Random to Sequential as expected, but the trade-off is in the maximum time to reroute (graphs *vii* to *ix*) since Immediate takes only 300ms while Sequential takes up to 10 seconds. Ransom takes a little more than the interval over which the randomization is done, in this case 1500ms. Graphs *x* to *xii* have to be more carefully interpreted since they show the amount of resources above the minimum resources required by the set of successfully rerouted channels expressed as a percentage of the minimum resources. As such it only makes sense to call a scheme more efficient than another is it has a comparable or better success ratio than the latter at the same workload, and at the same time uses less resources. Thus Global is more efficient than Local or Hybrid at low load. These conclusions are similar to the results published in [24] in which single faults without retries were explored.

If we look at the multiple retries (the striped bars in the same graphs) the first surprising observation is that retries do not seem improve the success ratios. For example in graph *i* at medium-high and high loads we note that the network is capable of supporting some extra load (since Sequential and Random do better than Immediate) but adding retries to Immediate timing does not bring about the expected improvement. Looking at the excess resources graphs we even note a few places where the resources used in the network increase without much improvement in the success ratio on adding retries (e.g. Local rerouting with Sequential timing at high load). Also even though the retry mechanism was set to retry up to four alternate paths, the time to reroute graph for Immediate timing (graph *viii*) shows that the maximum time to reroute was 300 ms which corresponds roughly to two round trip times on the longest paths in the workload. This indicates that at no time did a second or later retry on a long path succeed.

A careful analysis of the event traces from our simulations shows us that the reason for the poor performance of the retries is that the main cause of reroute failure is the temporary over-booking of resources on the forward pass of reroute, a second channel which makes an attempt or retries during that period has a higher chance of being blocked due to the temporarily unavailable resources. This is supported by the fact that Randomizing the reroute attempts over an interval of 1500ms is much more effective than the retry mechanism. In addition, the mechanism of retries examined here (based upon telecommunications rerouting schemes) does not retry along the same path, if an earlier attempt fails at a link, it tries a different path. This is counter productive since the link was probably only temporarily blocked by a forward reservation

and then cleared within one round trip time. Comparing the success of Randomization against this performance suggests a different way of performing retries more suitable to our environment. Instead of immediately retrying along a *different* path the mechanism should wait for an interval and then use the new routing information which comes in during the interval to compute a new path (which may actually turn out to be the same as the old path). We are currently adding this version of retries to our simulator and intend to experiment with the length of the interval and the use of randomization.

Figure 2 shows a similar set of graphs for two simultaneous faults in the network. We first look at the schemes without retries, the plain white bars. The most striking observation is that Local rerouting does not do much worse compared to the other schemes. In fact all the schemes perform comparably with respect to success ratio, with Global a bit better for Immediate timing and Hybrid a bit better for Random and Sequential timing. The cause we ascribe to this behavior is that Hybrid and Local are better at confining the effect of the fault to the immediate vicinity, and the two faults thus interfere less. With Global the two faults interfere due to route collisions and it loses the advantage it had over Hybrid and Local with single faults. Across the timing approaches the behavior is similar to the single fault case, Immediate reroutes the least amount of traffic, Sequential the most. Looking at the excess resource we note that for comparable success ratios, Global rerouting is most efficient.

When we add retries to the schemes (the striped bars), we note that it helps Hybrid the most, so that Hybrid with retries performs consistently equal or better than any other rerouting schemes with respect to success ratio. We note that retries have the most affect in the case of Immediate timing, since that is the case where a lot of reroute attempts fail due to collisions at the first try. We also note that retries brings down the excess resources consumed by Hybrid and Local, because the retry path is always calculated using a routing algorithm like Global which looks at the whole network. However in terms of success ratios, the gain from retries is smaller than the gain from randomization; in all cases Random without retries does as well or better than Immediate with retries. This supports our earlier conclusion about the applicability of this specific mechanism of retries in such networks.

Our overall conclusion is that a Hybrid schemes with the modified version of retries and a randomization interval picked according to the recovery response time required by the clients is best to reroute GPC connections.

7. Conclusion.

In this paper we have presented an investigation into the rerouting of guaranteed performance connections affected by single and multiple faults in the network. In our environment rerouting, while avoiding the faulty links, must also ensure that the traffic and performance guarantees previously supported along the old routes will be supported along the new ones. The goal of a rerouting scheme is to minimize the effect of the fault on the network and the client, by rerouting as much of the traffic as possible, as quickly and efficiently as possible. To aid in our investigation we chose criteria, or metrics of success, that reflect

this goal. These criteria were: the amount of affected traffic that was recovered by the scheme (i.e. the success ratio SR); the amount of network resources that were wasted in the rerouting process; and, the average and maximum time taken to establish the successfully rerouted connections. A new index, the *Queuing Delay Load* index, was designed that captures both the bandwidth and delay resources reserved by a connection, and was used in examining these criteria. This index is very useful as it allows us to compress these two resources along one dimension, thereby facilitating the proper comparisons of the rerouting schemes.

Rerouting was examined along three orthogonal components: the *locus of reroute*, the *timing*, and the *retries* components. The locus of reroute determines the node which selects the new route and the constraints under which this route is selected, the timing component determines the time at which the recovery attempt should begin, and the retries component determine whether a reroute attempt is retried should the attempt fail. There are three locus of reroute approaches; Local, Hybrid, and Global. There are also three different reroute timings approaches: Immediate, Random and Sequential, and two approaches to retries, no retries permitted and retries permitted up to a given maximum. The cross product of the approaches in the three components spans the complete rerouting scheme space.

All rerouting schemes were examined across a cross-section of workloads, and the approaches were compared along the lines of the criteria mentioned above. These comparisons were achieved by using extensive simulation experiments. We found that retries implemented exactly as in the telecommunications model did not significantly improve the rerouting success of our schemes. We noted that randomization over time was a more powerful technique to improve rerouting success. We concluded that routing collisions make it more important to retry at a different time, rather than along a different path. We suggested an alternative retry mechanism which would randomize the retry in time, but would not insist on a different route, which we intend to evaluate using simulation. On introducing multiple isolated faults into our experiments, we noticed that the relative performance of Global rerouting dropped, since the reroutes caused by the different faults interfered more for Global rerouting. Hybrid rerouting performs comparably to Global under single faults and is less adversely affected by multiple faults, as a result it offers better overall performance. Randomization continues to be more effective than retries as a means of improving success rate.

Work in progress includes the investigation of the modified retry mechanism suggested above, making our schemes robust to multiple non-isolated faults in the network, and experimenting with other topologies, statistical workload distributions and routing schemes.

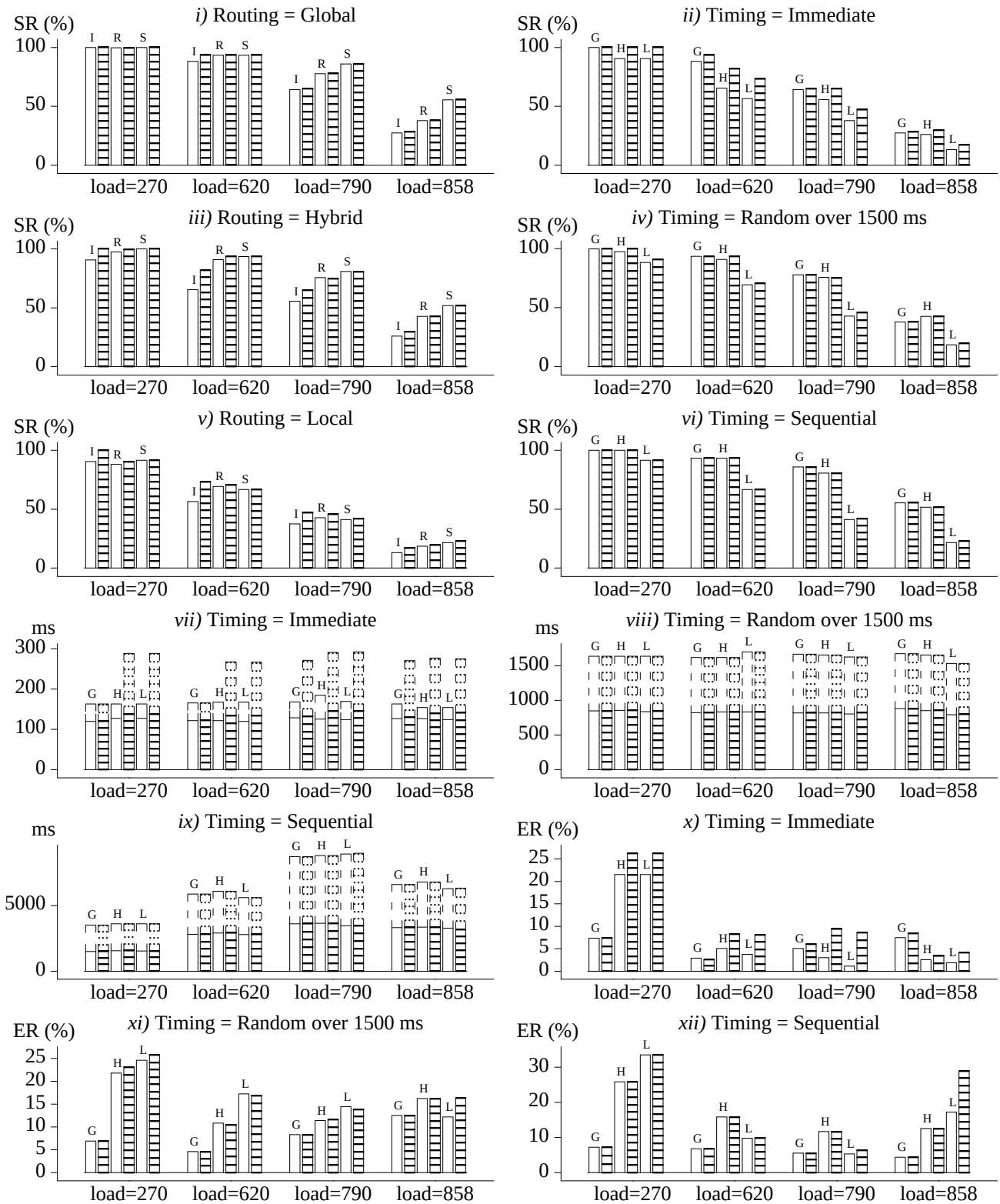

Figure 2. Single fault. Graphs *i*,*iii*, and *v* show the success ratio for different loads and timing approaches keeping the routing component constant, graphs *ii*, *iv*, and *vi* keep the timing component constant. Graphs *vii*-*ix* show the maximum and average time to reroute. Graphs *x*-*xii* show the excess resources consumed by the scheme in the network.

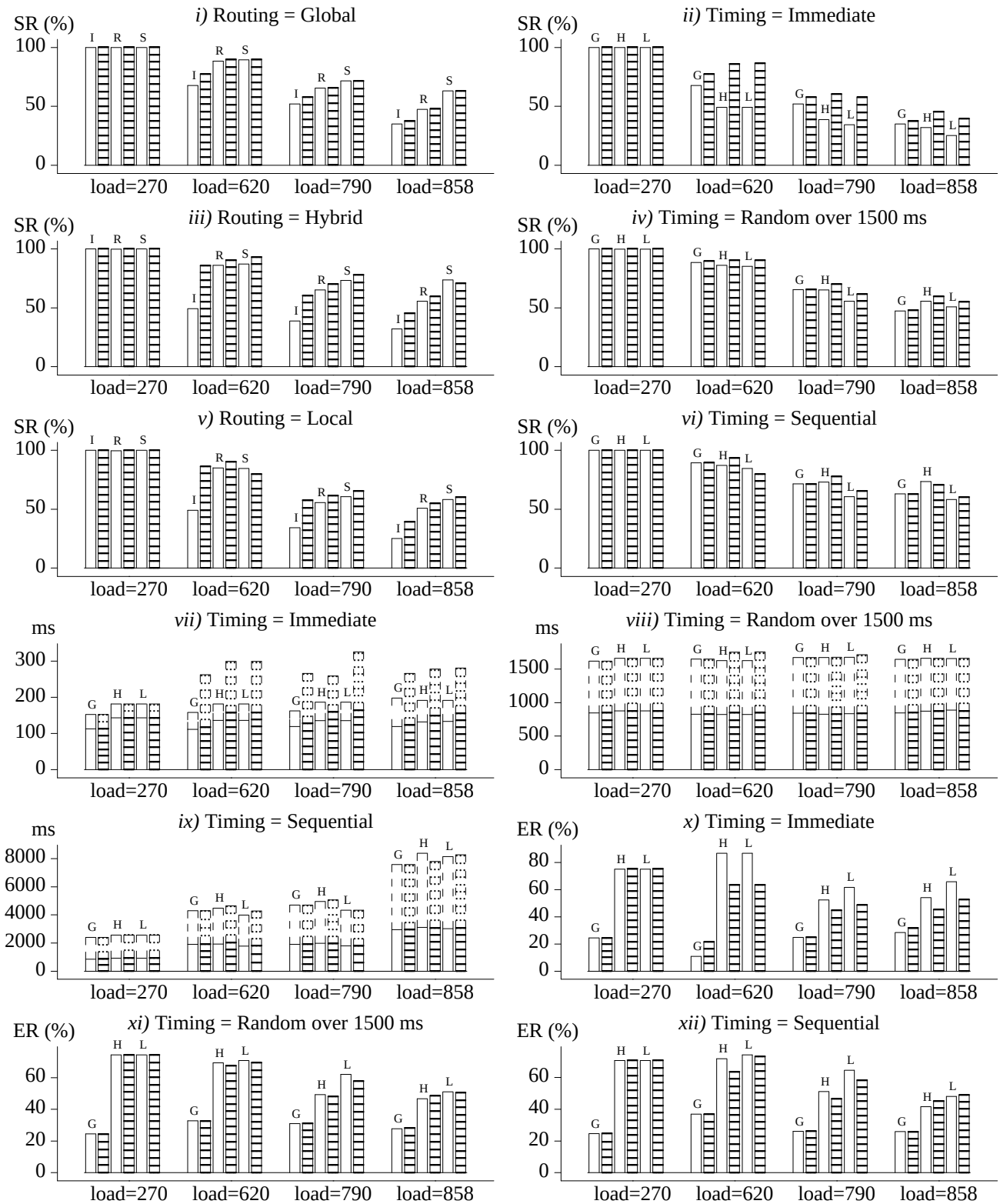

Figure 3. Multiple isolated faults. Graphs *i*,*iii*, and *v* show the success ratio for different loads and timing approaches keeping the routing component constant, graphs *ii*, *iv*, and *vi* keep the timing component constant. Graphs *vii*-*ix* show the maximum and average time to reroute. Graphs *x*-*xii* show the excess resources consumed by the scheme in the network.

Bibliography

[1] Domenico Ferrari, Anindo Banerjea, and Hui Zhang, ‘‘Network Support for Multimedia: A discussion of the tenet approach’’, Technical Report No. TR-92-072, International Computer Science Institute, Berkeley, CA, November 1992.

[2] David Clark, Scott Shenker, and Lixia Zhang, ‘‘Supporting Real-Time applications in an Integrated Services Packet Network: Architecture and Mechanisms’’, In *Proceedings of ACM SIGCOMM’92*, pages 14-26, Baltimore, Maryland, August 1992.

[3] David P. Anderson, Ralf Guido Herrtwich, and Carl Schaeffer, ‘‘SRP: A Resource Reservation Protocol for Guaranteed Performance Communication in Internet.’’, Technical Report TR-90-006, International Computer Science Institute, Berkeley, CA, February 1990.

[4] J. Hyman and A. Lazar, ‘‘MARS: The Magnet II Real-Time Scheduling Algorithm’’, In *Proceedings of ACM SIGCOMM’91*, pages 285-293, Zurich Switzerland, September 1991.

[5] C. Vogt, R. Herrtwich, and R. Nagaragan, ‘‘HeiRAT - The Heidelberg Resource and Administration Technique: Design Philosophy and Goals’’, IBM Technical Report No. 43.9243, IBM ENC, Heidelberg, 1992.

[6] Robert Doverspike, ‘‘A Multi-Layered Model for Survivability in Intra-LATA Transport Networks’’, In *Proceedings of IEEE GLOBECOM ’91*, Phoenix, Arizona, pp. 2025-2031, December 1991.

[7] K. R. Krishnan and T. J. Ott, ‘‘Forward Looking Routing: A New State Dependent Routing Scheme’’, In *Proceedings of the 12th International Teletraffic Congress* (ITC), Torino, Italy, June 1988.

[8] V. P. Chaudhary, K. R. Krishnan, and C. D. Pack, ‘‘Implementing Dynamic Routing in the Local Telephone Networks of USA’’, Teletraffic and Datatraffic in a Period of Change, ITC-13, A. Jensen and V. B. Iversen (Editors), Elseviers Science Publishers B. V. (North Holland).

[9] Brian A. Coan, Will E. Leland, Mario P. Vecchi, Abel Weinrib, and Liang T. Wu, ‘‘Using Distributed Topology Update and Preplanned Configuration to Achieve Trunk Network Survivability’’, In *IEEE Transactions on Reliability*, Volume 49, Number 4, October 1991.

[10] M. Barezzani, E. Pedrinelli, and M. Gerla, ‘‘Protection Planning in Transmission Networks’’, In *Proceedings of SUPERCOMM / International Conference on Communications ’92*, Chicago, June 1992.

[11] Makiko Yoshida and Hiroyuki Okazaki, ‘‘Cooperative control over logical and physical networks for multiservice environments’’, In *IEICE Transactions*, Vol. E.74, No. 12. December 1991.

[12] W. D. Grover, ‘‘The Self-Healing Network: A Fast Distributed Restoration Technique for Networks using Digital Cross-connect Machines’’, In *Proceedings of IEEE Global Telecommunications Conference*, pp. 28.2.1-28.2.6, December 1987.

[13] C. Han Yang and S. Hasegawa, ‘‘FITNESS: Failure Immunization Technology for Network Service Survivability’’, In *Proceedings of IEEE Global Telecommunications Conference*, pp. 47.3.1-47.3.6, November/December 1988.

[14] H. Komine, T. Chuja, T. Ogura, K. Miyazaki, and T. Soejima, ‘‘A Distributed Restoration Algorithm for Multiple Link and Node Failures of Transport Networks’’, In *Proceedings of IEEE Global telecommunications Conference*, pp. 403.4.1-403.4.5, December 1990.

[15] H. Sakauchi, Y. Nishimura, and S. Hasegawa, ‘‘A Self-healing Network with an Economic Spare-Channel Assignment’’, In *Proceedings of IEEE Global Telecommunications Conference*, pp. 403.1.1-403.1.6, December 1990.

[16] J. McQuillan et al., ‘‘The New Routing Algorithm for the ARPANET’’, In *IEEE Transactions on Communications*, Vol. COM-28, May 1980.

[17] William T. Zaumen and J. J. Garcia-Luna-Aceves, ‘‘Dynamics of Distributed Shortest-Path Routing Algorithms’’, In *Proceedings of the 21st ACM SIGCOMM Conference ’91*, Zurich, Switzerland, September 3-6, 1991, *Computer Communications Review*, Vol. 21, No. 4, ACM Press.

[18] J. J. Garcia-Luna-Aceves, ‘‘A Unified Approach for Loop-Free Routing Using Link States or Distance Vectors’’, In *ACM Computer Communication Review*, Vol. 19, No. 4, pp. 212-223, 1989.

[19] M. Schroeder, A. Birell, M. Burrows, H. Murray, R. Needham, T. Rodeheffer, E. Satterthwaite, and C. Thacker, , ‘‘Autonet: A High-Speed Self-Configuring Local Area Network Using Point-To-Point Links’’, *IEEE Journal Selected Areas in Communication*, Vol. 9, No. 8, pp. 1318-1335, October 1991.

[20] Domenico Ferrari, ‘‘Real-time Communication in an Internetwork’’ *Journal of High Speed Networks*, Vol. 1, No. 1, pp. 79-103.

[21] Colin Parris and Domenico Ferrari, ‘‘A Dynamic Connection Management Scheme for Guaranteed Performance Services in Packet-Switching Integrated Services Networks’’, Technical Report TR-93-005, Jan 1993, International Computer Science Institute, Berkeley, CA.

[22] Hui Zhang and Domenico Ferrari, ‘‘Rate-Controlled Static Priority Queueing’’, In *Proceeding of the IEEE INFOCOM’93*, April 1993, San Francisco, CA.

[22] R. Bellman, ‘‘On a routing problem’’, In *Quarterly of Applied Mathematics*, Vol. 16, 1958, pp. 87-90.

[23] Domenico Ferrari, ‘‘Client requirements for real-time communication services’’, In *IEEE Communications Magazine*, Vol. 28, No. 4, pp. 65-72, November 1990.

[24] Colin Parris and Anindo Banerjea, ‘‘An Investigation into Fault Recovery in Guaranteed Performance Service Connections’’, submitted to *SUPERCOMM/International Conference on Communication ’94*, also available as Technical Report No. TR-93-054, International Computer Science Institute, Berkeley, CA, September 1993.

[25] Lixia Zhang, ‘‘A new Architecture for Packet Switched Network Protocols’’, Ph.D Dissertation, Massachusetts Institute of Technology, July 1989.

[26] Israel Cidon, Inder Gopal, and Roch Guerin, ‘‘Bandwidth management and congestion control in PlaNET,’’ *IEEE Communications Magazine, pp. 54-64, October 1991.*