

Self-configuring Survivable Techniques for Quality of Service Enabled Internet ¹

Yu Liu ^{*}, David Tipper ^{*}, Deep Medhi ^{**}, Anotai Srikitja ^{*}

^{*}Department of Information Science and Telecommunications
University of Pittsburgh
135N Bellefield Ave, Pittsburgh, PA 15260, USA

^{**}Department of Computer Networking
University of Missouri-Kansas City
5100 Rockhill Road, Kansas City, MO 64110-2499 USA

Due to the distributed administration, large geographic coverage, and expensive resource cost, communication networks are one of the most vulnerable parts in the current information infrastructure. Both failures and malicious attacks are difficult to eliminate in such systems. Recent advances in fiber transmission and switching/routing techniques have dramatically increased the communication capacity of links. Moreover, merging large amount and multiple classes of services over the same communication link is also common nowadays. An adverse consequence of these advances is an increasing network vulnerability since a small network failure or network attack can significantly reduce the capability to deliver services in large-scale information systems. Hence, there is a need for greater focus on spare capacity design and network restoration techniques to mitigate the impact of failures and attacks. While there is a body of work on providing network survivability for circuit switched networks (e.g., trunk diversity) and ATM networks, little work has appeared for the Next Generation Internet (NGI). The NGI will provide QoS services in addition to traditional best effort service and some QoS services will likely follow fixed routes and thereby be subject to single point failure/attacks.

We have begun research on survivability techniques for the NGI based on a multi-network scenario which includes multiple interconnected networks with different technologies and multi-vendor equipment with both wireline and wireless infrastructure. Our research is concentrating on the following areas [1,2]:

- The development of design models/algorithms to provide a specified quality of service (QoS) under single and multiple attack/failure conditions.
- Developing network management algorithms (e.g., provisioning of backup routes, rerouting algorithms, etc.), which make optimum use of network resources after an attack/failure (both large and small types) in support of critical services. The restoration algorithms will be suitable for automatic invocation by network components, resulting in a self-configuring system that adapts to the changing fault/attack environment.
- Studying the transient network congestion that occurs after a failure and incorporating its effect into the design of the network and the traffic restoration algorithms. Thus not only will a critical network user be provided service continuity, but the service quality will be maintained to the highest degree possible.

¹The work is supported in part by DARPA F30602-97-1-0257.

Recent research results

One focus of our recent results is survivable network design. In general, a backbone network includes multiple nodes in different geographic locations with long distance communication links constructing a mesh-type topology. Both those links and nodes are vulnerable to the failures and attacks. One survivability scheme for mesh networks consists of reserving capacity along backup paths for all traffic flows and switching the affected flows upon failure/attack. Each backup path, in general, requires more resources compared to its corresponding working path in order to absorb transients after a failure. The network redundancy can be reduced through spare capacity sharing where two overlapped backup paths can share their capacity reservations if their working/primary paths are disjoint and assuming only a single device fails at a time.

A novel and simple spare provision matrix (SPM) method was developed to implement the spare capacity sharing operation. The primary advantage of using SPM is its application in aggregating information for the backup path routing. We have shown that such backup path routing can be implemented as a link state routing protocol with the complexity of link state information at $O(L^2)$, where L is the number of links in the network. Consequently, *per-flow based information*, which is a major difficulty in providing bandwidth pre-allocated backup paths dynamically in a QoS enabled next generation Internet [3], is not necessary anymore.

Based on above analysis, an on-line algorithm, successive survivable routing (SSR), is proposed to approximate the optimal spare capacity allocation (SCA) solution. The algorithm routes link-disjoint backup paths for individual traffic flows, one at a time. According to the current network information including SPM, each traffic flow keeps updating its backup path as long as this backup path is not carrying any traffic load. This allows distributed online computation. Numerical results show its advantages in terms of computation speed, distributed implementation, adaptability to traffic fluctuation, and capability in achieving lower capacity redundancy over the entire network. These attractive properties are supportive evidence for the application of SSR in not only the general mesh-type backbone networks like SDH, WDM, ATM and IP/MPLS, but also other fault tolerance scenarios like parallel computing architecture and transportation networks [4].

Additionally, in order to find how close an algorithm is from the optimal solution, we have been working on several centralized algorithms for the spare capacity allocation (SCA) problem. A genetic algorithm has been formulated to find the sub-optimal solution within seconds [7]. It has the advantages in dealing with the non-linear cost function and fast solution speed (polynomial time bound). Simulated annealing has been used for the same problem and can achieve the optimum within several minutes [3]. The best (optimal for small network) solutions are found by integer programming techniques like the branch and bound (BB) algorithm in hours. It is an enumeration algorithm for the NP-hard SCA problem. In order to scale this algorithm, limiting the search space is a general method. We have found a random scaling scheme to limit the search space of the original SCA problem. The results show that we can reduce the solution searching time significantly and still be able to find the optimal solution [8]. All these algorithms, as

well as infeasible lower bounds from LP relaxation, are compared in our publications to provide a global view of the available SCA solutions in various networks [3,4,7,8].

A simulation comparison between the pre-active backup path routing (reserve bandwidth before failure) and dynamic fault recovery routing (request after failure) has been performed [5]. Using the Network Simulator (ns2), the packet-level performance metrics can be investigated in details. This work provides a framework to compare the tradeoffs between the set two important restoration schemes in the distributed routing networks.

Another interesting topic is to design the survivable virtual private network (VPN) in IP/MPLS network where destination-based label switching path (LSP) trees are used for packet forwarding. VPN survivability has not been studied extensively before because both the tree design and spare capacity design are hard problems themselves. However, it is critical in the next generation Internet and deserves detailed study. In [6] we present a mathematical programming model for VPN design and heuristic algorithms are used to finding the sub-optimal solutions [6]. Further improvements of these algorithms are under study currently.

In conclusion, our recent research results have provided several fundamental building blocks for a self-configuring survivable multi-network architecture in a QoS enabled Internet environment.

Selected publications

- [1] D. Medhi and D. Tipper, "Multi-Layered Network Survivability--Models, Analysis, Architecture, Framework and Implementation: An Overview," Proc. of the DARPA Information Survivability Conference and Exposition (DISCEX'2000), Hilton Head Island, SC, January, 2000.
- [2] D. Tipper, D. Medhi, W. Yurcik, R. Cotter, "On Survivable Multi-Networks for Information Systems Survivability," ISW'98, Orlando, FL, October 1998.
- [3] Yu Liu, David Tipper, Peerapon Siripongwutikorn, "Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing," submitted to INFOCOM'01, available at <http://www2.sis.pitt.edu/~yliu/pub/>
- [4] Yu Liu, D Tipper, "A matrix method for spare capacity allocation," submitted to ICC'01, available at <http://www2.sis.pitt.edu/~yliu/pub/>
- [5] Anotai Srikitja, David Tipper, Deep Medhi, "On Providing Survivable Services in the Next Generation Internet," Proceedings of IEEE Military Communications Conf. (Milcom'99), Atlantic, NJ, Oct., 1999.
- [6] Anotai Srikitja, David Tipper, Deep Medhi, "Virtual private network design for the next generation Internet," In the 5th INFORMS Telecommunications Conferences, BOCA 2000, Boca Raton, FL, March 2000
- [7] A. Al-Rumaih, D. Tipper, Y. Liu, and B. Norman, "Spare Capacity Planning for Survivable Mesh Networks," Proceedings IFIP-TC6 Networking 2000, Paris, France, May 14-19, 2000.
- [8] Yu Liu, David Tipper, "Scaling Spare Capacity Design Techniques for Survivable Network," In the 5th INFORMS Telecommunications Conference, BOCA 2000, Boca Raton, FL, March 2000