QoS Assurance in Unreliable Networks

Kiran K[1], Nitin R[1], and Sridhar V[2] (email: sridhar@satyam.com)
[1]Dept. of Computer Science, RVCE, Bangalore
[2]Applied Research Group, Satyam Computer Services Ltd., Bangalore, India 560 025

I. QoS Issues

Network survivability refers to the capability to maintain service continuity in the presence of faults within QoS networks. In general, survivability techniques can be deployed at access layer, transport layer and / or Intelligent layer. Medhi and Tipper [1] describe an approach considering a pair of diverse paths for every survivable demand request and the backup path is used in case there is a failure. RSVP signaling is assumed to be used to reserve resources along a fixed route (explicit path reservation) to provide QoS. Further, primary path information is included in the signaling message during backup path reservation.

A major issue in providing QoS in routing is related to locating a QoS satisfying route. There are approaches discussed in the literature in which source selects the alternate routes based on the dynamic states of the network such as load information. Such source routes are used for handling specialized traffic requirements. Given an application's requirement of end-to-end path reliability, the multipath dynamic source routing technique described in [2] seeks to discover multiple disjoint paths to satisfy such a requirement. In a multiple path routing, data transmission fails if and only if all disjoint paths fail at the same time. This approach builds the routes in an incremental manner ensuring about the path reliability requirements. Nasipuri and Das [3] propose an approach in which all intermediate nodes of a primary path are provided with disjoint alternate routes. The destination node, that has all possible routes due to flooded query message, replies to each intermediate node to accomplish the identification of necessary alternate paths.

Hot redundancy failure protection with additional bandwidth overhead needs to be effectively considered along with cold standby with a compromise on restoration time to provide a cost effective solution. Cost is always an issue and the challenge is to provide an acceptable level of service for a set of failure scenarios in a cost effective manner. In this paper, we propose a source-routed, partially multicasted, alternate path based QoS assurance approach operating at transport layer. Further work towards the study of shared alternate paths across multiple unicast and multicast connection requests is under progress.

II. QoS Assurance

The system architecture of the proposed approach that is cost-sensitive and tolerates multiple failures is shown in Fig. 1. Note that as compared with the approaches discussed in the literature, the proposed approach makes best use of available paths from source to destination without imposing any constraints on the nature of these paths (from reliability point of view). Furthermore, the proposed approach takes into consideration the reliability of not only links but also of nodes in computing path reliability. This technique will be quite useful when the network is loaded. The goal of our proposed approach is to achieve the best possible exploitation of network resources to assure negotiated QoS by using multiple paths.

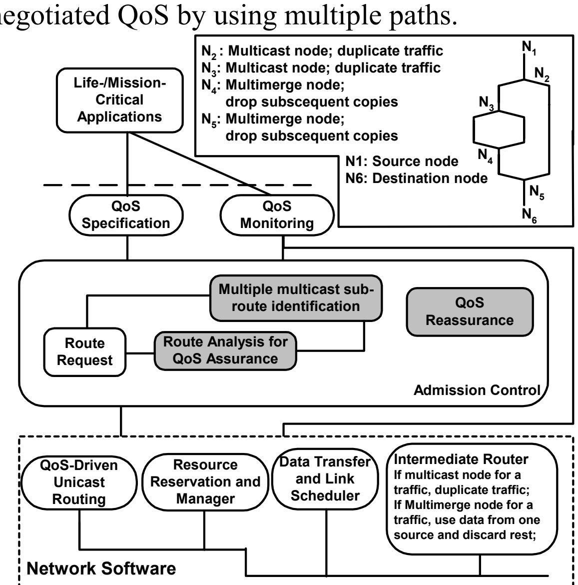


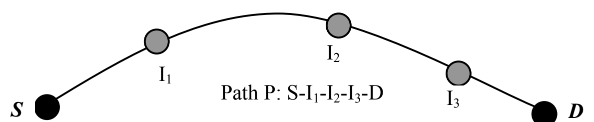
Figure 1: QoS Assurance Architecture

The problem of assuring agreed-upon QoS essentially involves the setting up of reliable redundant paths. These reliable paths bypass problematic nodes which might impair the ability of the network to satisfy previously agreed upon QoS requirements. Under QoS based routing, paths for flows would be determined based on some knowledge of resource availability in network as well as the QoS requirements of the flows.

Copyright 2002 Chillarege Press

We propose an approach that dynamically determines minimum number of alternate paths that together satisfy QoS assurance conditions based on the current state of the network. Our proposed approach to ensure QoS assurance is described in the following steps: (1) The source, destination and required QoS assurance (τ) are specified and an initial path (P) is obtained; This step is executed during connection set-up time. (2) Estimate $QoS_A(P)$ of the path (QoS assurance). (3) If $QoS_A(P) < \tau$, find a set of alternate, disjoint paths (Q) such that $QoS_A(P \cup Q) \geq \tau$; If no such path can be found, return FAILURE. (4) If P is changed to P' due to network failure, then reassure $QoS_A(P')$ and if required find Q' in an incremental manner (QoS reassurance). The above steps determine the QoS assurance of a path (P) and enhances the same by identifying alternate, disjoint paths (Q). The objective is to duplicate the transmission of data along these multiple paths so as to achieve reliable data transmission in spite of network node and link failures. Note that during reassurance, service is not interrupted due to the transmission of data along the alternate paths.

A. *Computation of $QoS_A(\,)$*



S: Source node; ***D***: Destination node; I_i: Intermediate node

α_i: < $\alpha_{i1}, \alpha_{i2}, \alpha_{i3}, \ldots$>; β_j: < $\beta_{j1}, \beta_{j2}, \beta_{j3}, \ldots$>;

Each $0 \leq \alpha_{ik}, \beta_{jl} \leq 1$ is scaled and weighted; Examples α_i : α_{i1} =1-(system load/system capacity); α_{i2} = Normalized system uptime; α_{i3} = 1 – (No. of critical alarms/Total No. of alarms); β_j: β_{j1}= 1 - Normalized link delay; β_{j2} = Normalized link uptime;

Figure 2: Path Reliability Measures

Let M_N and M_L be matrices of multiple reliability measures (refer to Fig. 2) associated with nodes and links respectively in a path P with R_i and r_j being the reliability of a node and a link respectively.

$$\begin{array}{c|ccc|l} M_N & \alpha_1 & \alpha_2 & \alpha_3 & \\ I_1 & \alpha_{11} & \alpha_{12} & \alpha_{13} & R_1(\alpha_{11},\alpha_{12},\alpha_{13}) \\ I_2 & \alpha_{21} & \alpha_{22} & \alpha_{23} & R_2(\alpha_{21},\alpha_{22},\alpha_{23}) \\ I_3 & \alpha_{31} & \alpha_{32} & \alpha_{33} & R_3(\alpha_{31},\alpha_{32},\alpha_{33}) \end{array}$$

$$\begin{array}{c|cc|l} M_L & \beta_1 & \beta_2 & \\ S-I_1 & \beta_{11} & \beta_{12} & r_1(\beta_{11},\beta_{12}) \\ {}_1-I_2 & \beta_{21} & \beta_{22} & r_2(\beta_{21},\beta_{22}) \\ {}_3-I_3 & \beta_{31} & \beta_{32} & r_3(\beta_{31},\beta_{32}) \\ I_3-D & \beta_{41} & \beta_{42} & r_4(\beta_{41},\beta_{42}) \end{array}$$

$QoS_A(P)$ is defined as

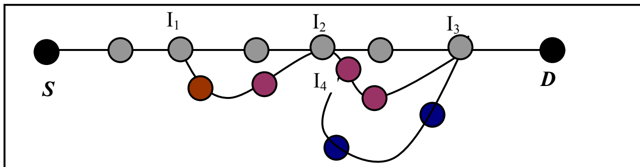
$$\prod_{i=1}^{3} R_i(\,) \times \prod_{j=1}^{2} r_j(\,)$$

B. *Computation of Q*

Input: Path P; Output: $Q = \{Q_1, Q_2, \ldots\}$; Constraints: Path P and paths in Q_i are mutually disjoint; Exit condition: $QoS_A(P \cup Q) \geq \tau$ or no such Q exists; N_C is the set of critical nodes in a path

The procedure is as follows: (1) P is analyzed and N_C is determined. In one of the approaches, $QoS_A()$ can be used for this determination. (2) Using N_C as basis, determine $Q_1=\{Q_{11}, Q_{12,\ldots}\}$ such that Q_1 is a set of alternate disjoint paths (mutually and also with respect to P) and collectively bypass N_C. (3) Estimate $QoS_A(P \cup Q_1)$; If this is greater than or equal to τ, accept path and exit; (4) Let Q_1 be Q_i. (5) For each element $Q_{i1} \in Q_i$,compute N_c; based on N_c, compute alternate paths and update Q_{i+1} (refer to Step 2). (6) Repeat Step 5 until exit condition is met; Note that $Q = Q_1 \cup Q_2 \cup \ldots$.

C. *Computation of $QoSA(P \cup Q)$*



S: Source node; ***D***: Destination node; I_i: Intermediate node
$p^1 = QoS_A$(Path from S to I_1); $p^2 = QoS_A$(Path from I_1 to I_2) ‖ q_{11}; $p^3 = QoS_A$(Path from I_2 to I_3) ‖ q_{12}; $p^4 = QoS_A$(Path from I_3 to D); $q_{11} = QoS_A$(Alternate path from I_1 to I_2); q_{12} = min (QoS_A(Path from I_2 to I_4), q_{12}^2); $q_{12}^2 = QoS_A$(Path from I_4 to I_3) ‖ QoS_A(Alternate path from I_4 to I_3); $QoS_A(P \cup Q) = \min(p^1, p^2, p^3, p^4)$

Figure 3: Multipath Reliability Computation

The computational procedure is shown in Fig. 3. Overall QoS_A is computed by recursively applying parallel / serial reliability equations to sub-paths.

III. QoS Reassurance

Reassurance involves the maintenance of agreed-upon QoS during renegotiation and reestablishment of paths/sub-paths due to failure of nodes/links. This can be achieved, during the session, by finding alternate paths to bypass vulnerable nodes/links wherever a network failure is indicated.

References

1. Medhi D and D. Tipper, "Multi-layered Network Survivability," Proc. DIS-CEX'2000, 2000.
2. Roy Leung et al, "MP-DSR: A QoS-aware Multi-path DSR Protocol for Wireless Ad-Hoc Networks," Proc. 26th LCN, 2001.
3. Nasipuri A and Samir Das, "On-demand multipath routing for mobile ad hoc networks," Proc. 8th IC3N, 1999.

Copyright 2002 Chillarege Press