Dependability evaluation of a class of multi-loop topologies for local area networks

by W. Earl Smith
Kishor S. Trivedi

Local area networks have been developed using both ring and bus topologies. Multi-loop and multi-connected topologies have been proposed to improve the throughput and dependability of single-loop networks. We evaluate the dependability of a class of multi-connected loop topologies called forward loop, backward hop (FLBH) networks and compare them to simple ring networks.

1. Introduction

Unidirectional loop network architectures [1–3] provide an attractive alternative to broadcast bus architectures in the design of local area networks (LANs) because interface hardware and control software are less complex. The addition of links to a simple loop so as to form multi-connected loops promises improvements in both performance and dependability. The purpose of this paper is to carry out reliability and availability analysis of a multi-connected loop called the forward loop, backward hop (FLBH) [4] network and to compare it to simple loop networks.

Raghavendra and Silvester [4] compare the delays, throughput, and alternate routing capabilities of three double-loop topologies, the daisy chain [5], the distributed double loop computer network (DDLCN) [6], and the forward loop, backward hop network. The FLBH is actually a class of networks that includes the other two topologies. Each node has a forward link connected to its neighbor and a backward link connected to another node at a (skip) distance h. For instance, $h = 1$ for DDLCN, $h = 2$ for daisy chain, and $h = 4$ for the 16-node FLBH network shown in **Figure 1**.

A measure of importance in comparing these networks is the distance in number of links or hops that must be traversed to communicate between any two farthest nodes. Let N be the number of nodes in the network.

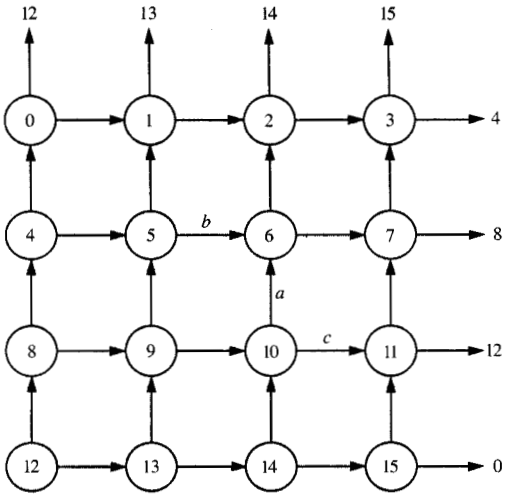

Figure 1

Optimal 16-node FLBH network.

The shortest routes between two farthest nodes consist of $(h-1)$ forward hops and b backward hops, where b is given by

$$b = \left\lfloor \frac{N}{h+1} \right\rfloor, \tag{1}$$

with $\lfloor x \rfloor$ denoting the largest integer less than or equal to x.

The number of distinct routes between two farthest nodes in FLBH networks is given by

$$N_R = 1 + \binom{b+h-1}{h-1}, \tag{2}$$

where $\binom{n}{i}$ denotes the number of combinations of n distinct objects selected i at a time [7],

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

By setting $h = \sqrt{N}$, we maximize N_R and obtain an optimal FLBH network. For this case, $b = h - 1$. Hwang [8] has noted that the selection of $h = \sqrt{N}$ does not guarantee a network of minimum diameter and is not optimal in that sense. However, we refer to an optimal FLBH network as one with this value of h, and we consider only integer values of h. Raghavendra and Silvester [4] discuss the terminal reliability of an FLBH network. The reliability of these networks is enhanced by providing multiple routing paths. This assertion is based on the following intuitive arguments:

1. Terminal reliability is proportional to the number of alternate routes.
2. Terminal reliability is inversely proportional to the average hop distance.

Raghavendra and Silvester have observed that for this optimal FLBH network, the fraction F_{DN} of double-node faults resulting in a trapped-node situation is

$$F_{DN} = \frac{2}{N-1}. \tag{3}$$

This occurs when two nodes fail at a distance $\sqrt{N}+1$ apart.

Quantitative reliability analysis of loop topologies has been scarce. Yu et al. [9] develop models for a token ring with a bypass mechanism. Raghavendra and Silvester address two-terminal reliability of FLBH networks. In this paper, we develop a reliability model for the FLBH class of networks in terms of nodes and communication links where transmitters and receivers are included as part of the communication link. We develop reliability models for nonrepairable networks and availability models for repairable networks. For small networks, we can obtain exact results, but for large networks we propose an approximate solution method. Upper and lower bounds are also proposed that are relatively tight for the cases shown. Results for FLBH networks are compared to those for single-loop networks.

In Section 2, we discuss the initial modeling assumptions. Section 3 describes the reliability model and develops the approximation for our solution method. In Section 4, the reliability results for the FLBH network are presented and compared to simple ring networks and to rings with node bypass. Finally, Section 5 contains the availability analysis and comparisons.

2. Modeling assumptions

As shown in **Figure 2**, a communications adapter for a LAN consists of a transmitter for each outbound link, a receiver for each inbound link, and control circuitry. Since analog and digital circuits are difficult to combine on a single chip, these units are usually packaged separately. This model exploits that separation by defining a *link* to include a transmitter, a receiver, and the communication medium connecting them. A *node* contains the remaining circuitry, which provides control and access to the transmitters and receivers and is assumed to be the same for both single-loop and multi-loop networks. By viewing the network in this way, we may progress from a single-loop architecture to multi-connected architectures using the same model.

Comparisons will reflect differences in the numbers of links and the ways in which they are connected.

The purpose of the network modeled here is to provide continuous, active communication between N nodes such as may be required for automated manufacturing or air traffic control. The following assumptions are utilized to construct our model:

- All components are assumed to have constant failure rates. Links fail at a rate λ_L and nodes at a rate λ_N. Times to failure of all components are assumed to be mutually independent.
- Network failure is caused by any combination of link faults that results in one or more disconnected nodes.
- Any node fault or a network failure is assumed to cause system failure.
- Since the failure rate for wiring is very low compared to that for other link components, differences between wiring lengths in links can be ignored, and links may be modeled as having identical failure rates.

The structure of the model and the assumptions for causes of system failure allow us to determine the reliability of FLBH communication systems, $R_s(t)$, as the product of the reliability of the nodes and the reliability of the interconnection network. Thus,

$$R_s(t) = R(t) \times R_N(t), \tag{4}$$

where the reliability of the nodes is $R_N(t) = e^{-N\lambda_N t}$ and $R(t)$ is the reliability of the FLBH interconnection network which is to be determined.

3. Reliability model

An FLBH network of N nodes has $2N$ links. In the worst case, the state space of the Markov chain model will be exponential in the number of links (i.e., 2^{2N} states). Even for small networks, the state space will be so large that effective reduction techniques such as lumping [10, 11] or aggregation [12] must be considered.

Najjar and Gaudiot [13] have considered a similar problem for multiprocessor systems using hypercube interconnection networks. They define a system to be disconnected whenever there are two or more disconnected components in the network graph. They compute this disconnection probability after i failures ($i > 0$) and use these probabilities to compute state-dependent coverage factors. For our problem, we have adopted a notation consistent with that of Raghavendra and Silvester, as shown in Equation (3), and proceed to analyze the FLBH network using Markov chain methods similar to those of Najjar and Gaudiot. First, we develop the state-dependent disconnection probabilities for small networks; we then propose bounds and an approximation for larger networks.

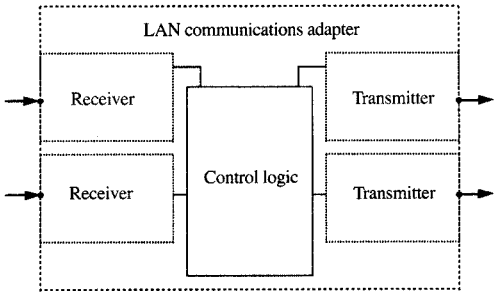

Figure 2

Node and link model elements.

• *State-dependent disconnection probabilities*

For each node in this network, there are exactly two link faults that will isolate the node from inbound messages and two other links that can fail and, if they do, prevent the node from sending outbound messages. Let F_{iL} be the conditional probability that the ith link fault causes a network failure given that the network was operational with $(i-1)$ link faults. Obviously, $F_{0L} = 0$. Observe that no single link fault will cause network failure; hence, $F_{1L} = 0$. Any of the $2N$ links may fail first. Any of the remaining $2N-1$ links is equally likely to be the second link to fail, but only two of these will result in network failure. Thus, the fraction of second-link faults causing network failure is

$$F_{2L} = \frac{2}{2N-1}. \tag{5}$$

Observe that the FLBH network is represented by a directed graph [14] in Figure 1, and that links are represented as directed arcs incident on network nodes which form the vertices of the digraph. Links may be of two types, either a forward loop link or a backward hop link. Also, links have an orientation relative to each node. Two links are incident *into* each node and two links are incident *out of* each node. The following definitions are useful in evaluating the network for other values of F_{iL}.

Definition *Corresponding links* are defined relative to two nodes. To be corresponding links, the links must be of the same type, either forward loop or backward hop. They must also have the same orientation, incident either into or out of the respective node.

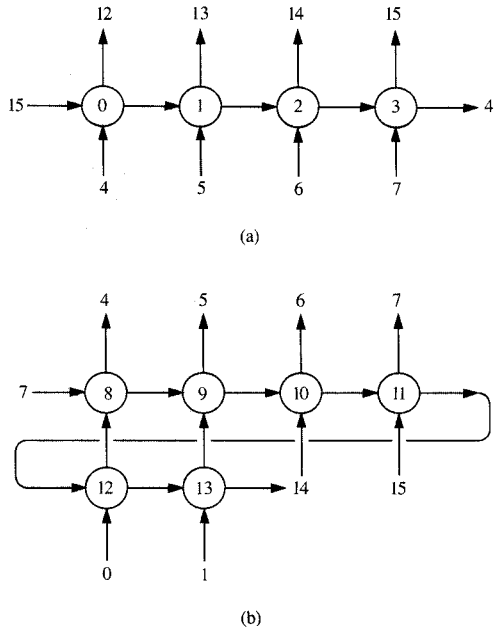

Figure 3

Node clusters from a 16-node FLBH network: (a) A four-node cluster illustrating Lemma 1. (b) A forward node cluster illustrating Lemma 2.

Definition A *critical link* is a link whose fault causes the network to fail. This depends on the current state of the network.

Definition A *forward node cluster* is a proper subset of all nodes that are consecutively numbered along the forward loop. Note that nodes in a cluster are connected such that each node, except the two end nodes, shares its two forward loop links with two other nodes in the subset. The two end nodes share only one forward loop link with other members of the subset. Nodes 3, 4, 5, and 6 in Figure 1 form a forward node cluster.

Definition A *backward node cluster* is a proper subset of all nodes such that these nodes are separated by a distance $h = \sqrt{N}$ and are interconnected by backward hops. There may be up to $\sqrt{N}$ nodes in a backward node cluster, in which case, a backward hop loop is formed. Nodes 0, 4, 8, and 12 in Figure 1 form a backward node cluster and a backward hop loop.

Lemma 1
A forward node cluster of size k ($2 \leq k \leq \sqrt{N}$) can be disconnected only if both of the links incident *into* or both of the links incident *out of* a node in the cluster have failed and, hence, the single node itself has become disconnected.

Proof Since we chose a backward hop distance of $\sqrt{N}$, all backward hop links connected to nodes of a cluster of size $\sqrt{N}$ or smaller must connect to other nodes outside the cluster. Thus, to disconnect the cluster, all inbound (outbound) links must fail. This requires that all inbound (outbound) backward hop links must fail along with the inbound (outbound) forward loop link. Thus, one node will have the inbound (outbound) forward loop link and backward hop link failed when the cluster is disconnected. □

In **Figure 3(a)**, we have depicted a four-node cluster from the network with 16 nodes shown in Figure 1. Note that failure of links from nodes 4, 5, 6, 7, and 15 disconnects this cluster from inbound communications, but that only failure of the links from nodes 4 and 15 is required to disconnect node 0.

Lemma 2
The disconnection of forward node clusters of size $> \sqrt{N}$ requires the failure of $\sqrt{N}$ backward hop links and one forward loop link.

Proof From our definition of a forward node cluster, there will be one inbound forward loop link to the cluster and one outbound forward loop link from the cluster. Call the node connected to the inbound link the first node in the cluster, and the node connected to the outbound link the last node in the cluster. By choosing the backward hop distance of $\sqrt{N}$, we require that the first node and the next $\sqrt{N} - 1$ nodes chained to it via the forward loop must all connect to nodes outside the cluster via outbound backward hop links. Similarly, we require that the last node and the previous $\sqrt{N} - 1$ nodes chained to it via the forward loop must all connect to nodes outside the cluster via inbound backward hop links.

Since disconnection of the cluster requires failure of all inbound (outbound) links, there must be $\sqrt{N}$ inbound (outbound) backward hop links and one inbound (outbound) forward loop link that have failed. Now, however, the set of nodes connected to the inbound (outbound) backward hop links does not include the node connected to the inbound (outbound) forward loop link. Single-node disconnection conditions are not met. □

In **Figure 3(b)**, network failure is caused by faults in the backward hop links to nodes 4, 5, 6, and 7 plus the forward loop link to node 14, disconnecting outbound communications from the cluster.

Lemma 3
A backward node cluster can cause network disconnection only if single-node disconnection conditions are met or if all forward loop links at a distance $\sqrt{N}$ have failed.

Proof Consider any backward node cluster where each node is at a distance $\sqrt{N}$. If there are exactly $\sqrt{N}$ nodes in the cluster, all backward hop links are contained within the cluster. Only the $\sqrt{N}$ forward links into the cluster or the $\sqrt{N}$ forward links out of the cluster must fail to cause network disconnection. By definition, these links must be at a distance $\sqrt{N}$.

If the cluster is of size $< \sqrt{N}$, there must be at least one inbound and one outbound backward hop link. To disconnect this cluster, all inbound links or all outbound links must have failed. Therefore, one node must have the inbound backward hop link and an inbound forward loop link to fail, or one node must have the outbound backward hop link and an outbound forward loop link to fail. In either case, single-node disconnection conditions are met.

If the cluster is of size $> \sqrt{N}$, it can be constructed by adding clusters from adjacent backward hop loops in one of two ways:

- Adding another cluster from the adjacent backward hop loop on the inbound side of the original cluster will cause the combined cluster to keep the disconnection conditions for the outbound links of the initial cluster. On the inbound side, if the added cluster is of size $\sqrt{N}$, the combined cluster will require faults on all forward loop links into the added cluster. Otherwise, the inbound side will include single-node disconnection conditions for at least one node, that being a node in the added cluster.
- Adding another cluster from the adjacent backward hop loop on the outbound side of the original cluster will cause the combined cluster to keep the disconnection conditions for the inbound links of the initial cluster. On the outbound side, if the added cluster is of size $\sqrt{N}$, the combined cluster will require faults on all forward loop links out of the added cluster. Otherwise, the outbound side will include single-node disconnection conditions for at least one node, that being a node in the added cluster. □

Lemma 2 states that at least $\sqrt{N} + 1$ total link faults are required to disconnect a forward node cluster of size greater than $\sqrt{N}$. Lemma 3 shows that at least $\sqrt{N}$ total link faults are required to disconnect a backward node cluster of size $\sqrt{N}$ or larger. If we examine the network for less than $\sqrt{N}$ total link faults, we are looking at disconnected node clusters of sizes smaller than $\sqrt{N}$ which can, by Lemmas 1 and 3, be evaluated using the conditions for single-node disconnection. We now develop the expressions for the disconnection probabilities for link faults when the total number of link faults is less than $\sqrt{N}$.

After one link fault, we have noted that there are two links that are critical links and $(2N - 3)$ links that are not critical links. If one of the $(2N - 3)$ links becomes the second link to fail, we wish to determine the probability F_{3L} that the network does not survive a third link fault. There are two cases to consider:

1. If the second link that failed is a corresponding link at a distance $(\sqrt{N} + 1)$ from the first, only three of the remaining nonfaulty links are critical links. In fact, one of these three will cause one node to lose outbound communication and will cause a second node to lose inbound communication. Relative to any first link fault, there will be exactly two of these links. For example, note that if links *b* and *c* in Figure 1 are the first two links to fail, both nodes 6 and 10 become disconnected if link *a* becomes the third link to fail.
2. For the other $(2N - 5)$ links that can become the second link to fail, there will be four critical links.

The total number of triple-link faults that are possible is the number of ordered sequences of three links out of $2N$ links minus the number of sequences of three faults that cannot occur because the network would not survive the previous two faults. Given that the network has not failed after faults have occurred on the first two links in the sequence, and that there are $2(2N)$ sequences of two link faults causing network failure, there will be $2(2N)(2N - 2)$ sequences of three link faults that cannot occur. Thus, for $\sqrt{N} > 3$,

$$F_{3L} = \frac{2N[4(2N - 5) + 3(2)]}{2N(2N - 1)(2N - 2) - 2(2N)(2N - 2)} \tag{6}$$

$$= \frac{8N - 14}{(2N - 2)(2N - 3)}. \tag{7}$$

Similar analysis shows that the fraction of possible fourth-link faults causing network failure is

$$F_{4L} = \frac{24N^2 - 120N + 150}{(2N - 3)(4N^2 - 18N + 20)}, \tag{8}$$

which is valid for $\sqrt{N} > 4$.

Closed-form expressions for F_{iL} $(4 < i < \sqrt{N})$ can be determined. For F_{iL} $(i \geq \sqrt{N})$, we must consider all fault conditions which disconnect a cluster of any size. However, Lemmas 1 and 3 allow us to determine the $2N$ conditions for disconnecting single nodes and to use them to evaluate disconnection of clusters of size $< \sqrt{N}$. Lemma 2 establishes that there will be $\sqrt{N} + 1$ links in

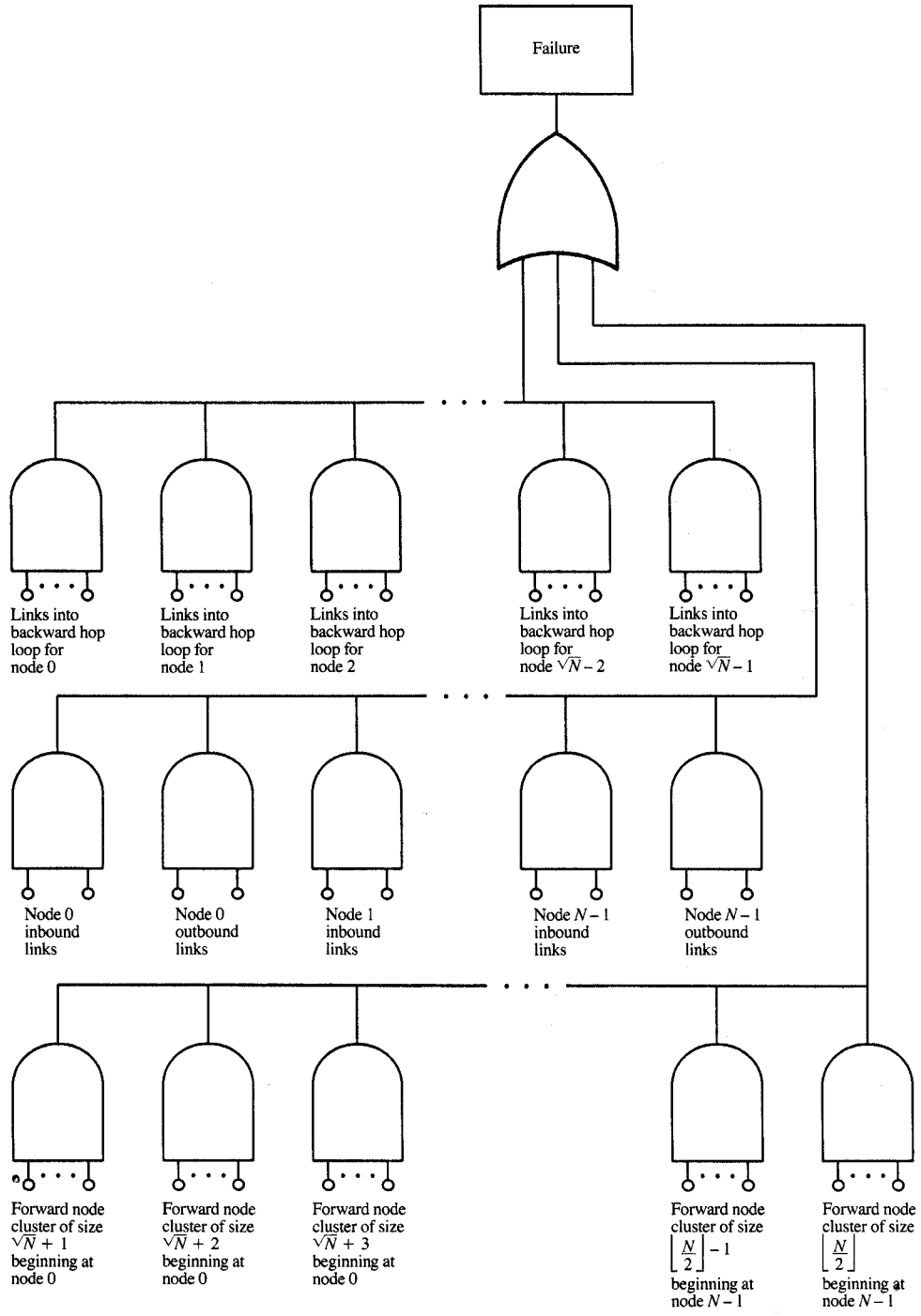

Figure 4

Fault tree for FLBH network failure.

each cutset that disconnects either inbound or outbound communication for forward node clusters of size $> \sqrt{N}$. Also, note that disconnecting inbound communication from a forward node cluster of size j is the same as disconnecting outbound communication for a cluster of size $N - j$. Thus, we also need all combinations of cutsets for forward node clusters of size $\sqrt{N} + 1$ up to $\lfloor N/2 \rfloor$. Finally, we must also consider the $\sqrt{N}$ conditions that cause disconnection of backward node clusters of size $\sqrt{N}$. These failure conditions can be represented by means of a fault tree of the form shown in **Figure 4**. The total number of inputs (basic events) to the fault tree is the number of network links $2N$. The total number of gates (internal nodes) G_{FLBH} required in the fault tree is

$$G_{\text{FLBH}} = 2N\left(\left\lfloor \frac{N}{2} \right\rfloor - \sqrt{N} + 1\right) + \sqrt{N}. \tag{9}$$

We have used HARP [15] in an interesting but originally unintended manner to solve the counting problem on hand for $N = 9$ and partially for $N = 16$. HARP can generate the set of link fault combinations that form the set of critical links by using the fault tree in Figure 4. By generating the state space, we determined the count of the number of possible transitions C_i to network failure states and the total number of transitions S_i out of all states with $(i - 1)$ link faults. These counts are shown in **Table 1**. Exact values for $F_{i\text{L}}$ are computed from

$$F_{i\text{L}} = \frac{C_i}{S_i}. \tag{10}$$

In **Figure 5** we plot the fraction of ith-link faults that cause network failure, given that the network had not failed after $(i - 1)$ link faults. For networks of four nodes and nine nodes, we are able to compute $F_{i\text{L}}$ for all i. For a 16-node network, values of $F_{i\text{L}}$ are plotted for only small values of i because of computation and memory limitations.

• *Disconnection probability bounds and approximation*
Bounds for the values of $F_{i\text{L}}$ can be determined. Recall that there are two critical links following the first link fault. In the worst case, there will be two more critical links added after every additional link fault. Thus, these values of $F_{i\text{L}}$, which give the worst case or lower bound on network reliability, are

$$F_{i\text{L}}^{WC} = \min\left\{\frac{2(i-1)}{2N - i + 1}, 1\right\}. \tag{11}$$

Similarly, in the best case, there will be two critical links after the first link fault, but only one critical link will be added for each additional link fault. As a result, the values of $F_{i\text{L}}$ which give an upper bound on network reliability are

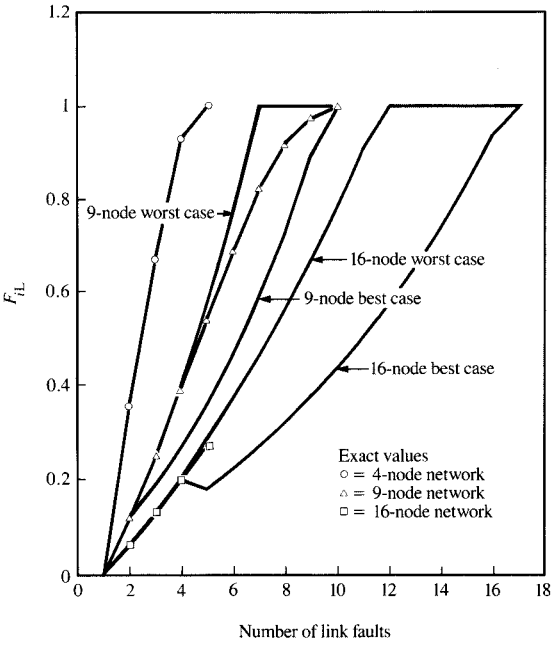

Figure 5
$F_{i\text{L}}$ for FLBH networks.

Table 1 Ratio of failure transitions to all transitions, C_i/S_i.

Number failed, i	*Number of nodes*		
	4	*9*	*16*
1	0/0	0/0	0/0
2	20/56	36/306	64/992
3	144/216	1062/4320	3648/27840
4	336/360	19062/48870	140064/701568
5	96/96	225072/417312	4263552/15722112
6		1712880/2499120	
7		7756560/9434880	
8		17010000/18461520	
9		14152320/14515200	
10		3265920/3265920	
11			

$$F_{i\text{L}}^{BC} = \frac{i}{2N - i + 1}. \tag{12}$$

In Figure 5, $F_{i\text{L}}^{WC}$ and $F_{i\text{L}}^{BC}$ are shown for $N = 9$ and $N = 16$.

The values of $F_{i\text{L}}$ are known or can be determined exactly for $N \leq 16$ and $i \leq 4$. For values of $i > 4$, $F_{i\text{L}}$ can be approximated as a linear function for up to $i = N - 1$

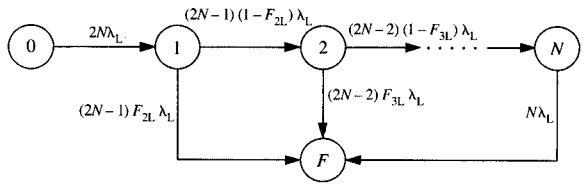

Figure 6

Markov chain for FLBH network without repair.

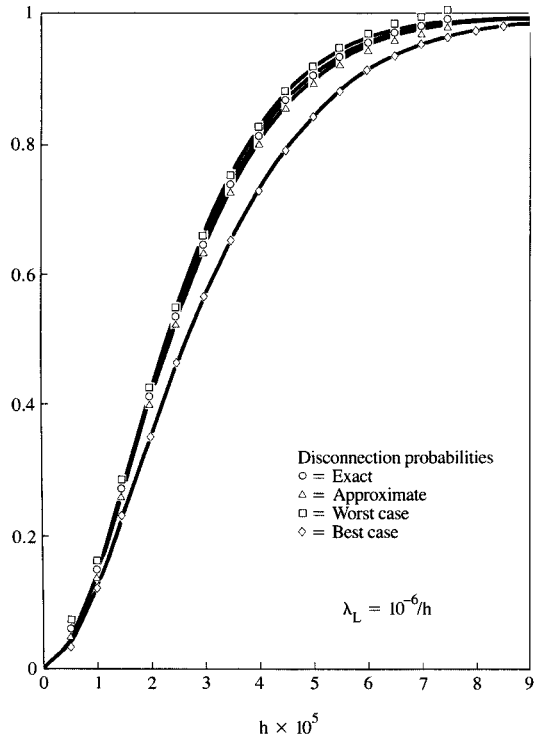

Figure 7

Unreliability of a nine-node FLBH network.

faults. For larger networks, we approximate the slope between F_{3L} and F_{4L} and calculate an estimate of F_{iL} as

$$F'_{iL} = \begin{cases} F'_{(i-1)L} + \frac{1}{N} + \frac{3}{2N^2} + \frac{3}{4N^3} & 4 < i < N, \\ 1.0 & i \geq N. \end{cases} \quad (13)$$

Using these estimated values of F_{iL} as the probability of network failure when exiting state $(i-1)$, we can construct a Markov chain of $N+2$ states. $N+1$ operational states are labeled from 0 through N, where the state index denotes the number of failed links in the network. The final state is the network failure state, labeled F. The rate $\lambda_{i-1,i}$ from state $(i-1)$ to state i is calculated as

$$\lambda_{i-1,i} = (1 - F_{iL})[2N - (i-1)]\lambda_L, \quad (14)$$

where λ_L is the failure rate of a single link. Similarly, the transition rate from state $(i-1)$ to the network failure state F is

$$\lambda_{i-1,F} = F_{iL}[2N - (i-1)]\lambda_L. \quad (15)$$

This Markov chain is shown in **Figure 6**.

4. Network reliability

The reliability $R(t)$ for the FLBH interconnection network can be determined from the Markov chain by solving for the state probabilities [7]. We require that state 0 be the initial state. We modify the failure rates and notation of [13] and give the state probabilities as

$$P_i(t) = \left[\prod_{j=1}^{i}(1 - F_{jL})\right]\binom{2N}{2N-i} e^{-(2N-i)\lambda_L t}(1 - e^{-\lambda_L t})^i. \quad (16)$$

Let $\delta_i(t)$ be the error in the ith state probability that is induced by the approximation method described earlier. For the FLBH network this can be determined from

$$\delta_i(t) = P_i(t) - P'_i(t), \quad (17)$$

where $P_i(t)$ is the ith state probability determined from the exact values of the F_{iL}, and $P'_i(t)$ is the corresponding state probability determined from the approximate values F'_{iL} given in (13).

We can compute the relative error $\Psi_i(t)$ as follows:

$$\Psi_i(t) = \frac{\delta_i(t)}{P_i(t)}. \quad (18)$$

Recall that we have closed-form equations to determine F_{iL} for $i < 5$. Substituting Equation (16), we find that the relative error in computing the state probabilities for $i \geq 5$ is not time-dependent. Thus,

$$\Psi_i = \begin{cases} 0 & i < 5, \\ 1 - \frac{\prod_{j=5}^{i}(1 - F'_{jL})}{\prod_{j=5}^{i}(1 - F_{jL})} & i \geq 5. \end{cases} \quad (19)$$

The reliability of the interconnection network is the probability that the network is in an operational state:

$$R(t) = \sum_{i=0}^{N} P_i(t). \quad (20)$$

Using the modeling tool SHARPE [16], we have evaluated the Markov chain in Figure 6 for $R(t)$ of a nine-node network with the link failure rate $\lambda_L = 10^{-4}$. The nine-node network was chosen because it was the largest network for which all of the F_{iL} factors were known precisely and an exact solution could be determined. Four variations of the Markov chain were examined. The unreliability for each case is shown in **Figure 7**. The variations are as follows:

1. Exact: The Markov chain is solved using exact values for F_{iL}.
2. Approximate: The Markov chain is solved using approximate values for F_{iL} as suggested in Equation (13). The exact solution and the approximate solution are indistinguishable in the graph.
3. Upper bound: The Markov chain is solved using the worst-case values, F_{iL}^{WC} for $4 < i < N$, with $F_{NL} = 1.0$. This yields an upper (lower) bound on unreliability (reliability).
4. Lower bound: The Markov chain is solved using $F_{iL} = F_{iL}^{BC}$ for all $4 < i < N$. This yields a lower (upper) bound for unreliability (reliability).

We find that the approximation [Equation (13)] for F_{iL} yields very good results, and that the upper and lower bounds are rather close. The maximal difference between upper and lower bounds in Figure 7 is 6.2%.

• *Mean time to failure*

Assuming that a faulty node always causes network failure, the reliability of the FLBH network, including nodes, is given by

$$R_S(t) = R(t)e^{-N\lambda_N t}. \tag{21}$$

By considering the imbedded Markov chain for the system described by Equation (21), the mean time to failure of the system, $MTTF_S$, can be derived as

$$MTTF_S = \sum_{i=0}^{N} \mu_i V_i, \tag{22}$$

where μ_i is the mean holding time in state i and V_i is the probability of reaching state i. Thus, for the FLBH network, we have

$$V_i = \prod_{j=1}^{i} (1 - F_{jL}) \frac{(2N - j + 1)\lambda_L}{(2N - j + 1)\lambda_L + N\lambda_N}, \qquad i > 0, \tag{23}$$

where $V_0 = 1$, and

$$\mu_i = \frac{1}{(2N - i)\lambda_L + N\lambda_N}. \tag{24}$$

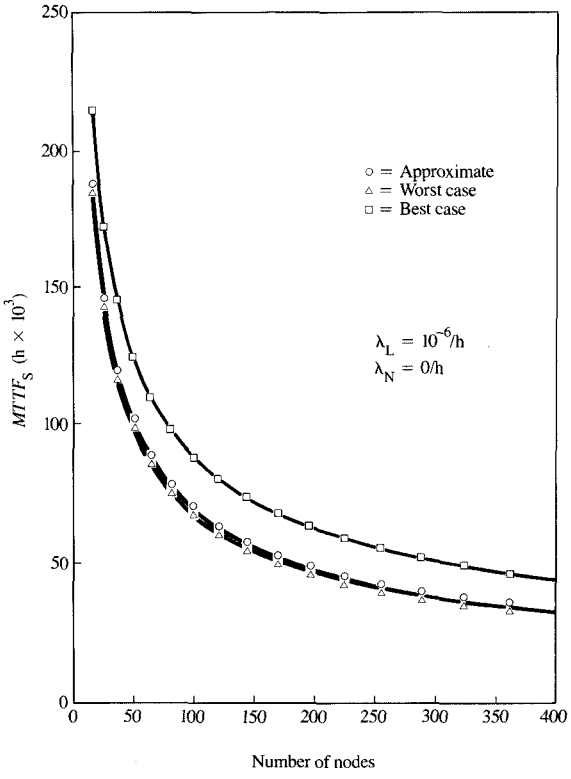

Figure 8

$MTTF_S$ for optimal FLBH networks.

Using the worst- and best-case values of F_{iL} from Equations (11) and (12), we can compute V_i^{WC} and V_i^{BC}. Using these values in Equations (22) and (23), we can determine the worst-case $MTTF$ for the optimal FLBH network,

$$MTTF_{WC} = \sum_{i=0}^{N} \mu_i V_i^{WC}, \tag{25}$$

and the best case,

$$MTTF_{BC} = \sum_{i=0}^{N} \mu_i V_i^{BC}. \tag{26}$$

In **Figure 8**, we show $MTTF_S$, $MTTF_{WC}$, and $MTTF_{BC}$ for optimal FLBH networks varying in size from 16 to 400 nodes. Here we have used the approximation method presented in Equation (13) to compute unknown values of F_{iL} for $MTTF_S$. We obtain a comparison of the interconnection of the FLBH network to that of the same size ring network by setting $\lambda_L = 10^{-6}$/h and $\lambda_N = 0$. Note that the approximation and the worst-case bound

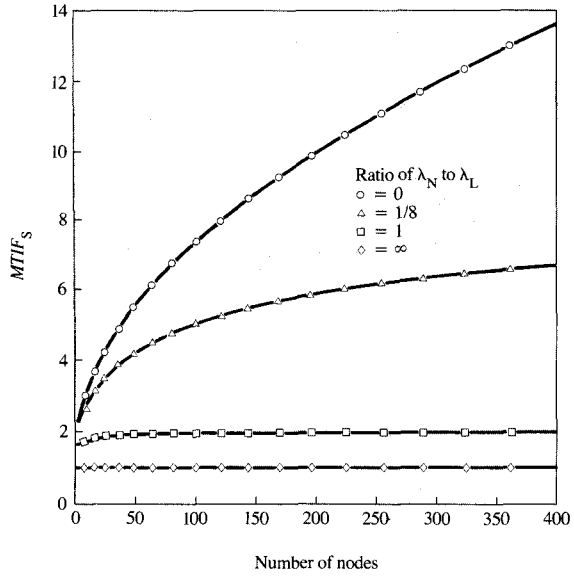

Figure 9

$MTIF_S$ for optimal FLBH networks vs. simple ring.

are nearly indistinguishable in the figure, and that the absolute difference between $MTTF_{BC}$ and $MTTF_{WC}$ is decreasing slightly as network size increases. This difference, relative to $MTTF_{BC}$, approaches 37% for large networks due to the fact that $MTTF_S$ decreases more quickly than the difference between the bounds.

• *Mean time to failure improvement factor*

In order to draw comparisons between network topologies, we use the mean time to failure improvement factor $MTIF_S$, which is defined by the ratio of $MTTF_S$ to the mean time to failure of the network that is being compared. Let $MTTF_R$ be the mean time to failure for a simple ring. Then,

$$MTTF_R = \frac{1}{N(\lambda_N + \lambda_L)}. \tag{27}$$

Comparing the $MTTF$ for the FLBH network to that of a simple ring, we compute the mean time to failure improvement factor $MTIF_S$,

$$MTIF_S = \frac{MTTF_S}{MTTF_R}. \tag{28}$$

For the optimal FLBH network, this is

$$MTIF_S = \sum_{i=0}^{N} \frac{N(\lambda_L + \lambda_N)}{(2N - i)\lambda_L + N\lambda_N} V_i. \tag{29}$$

Let ζ be the ratio of the node failure rate to the link failure rate. Thus,

$$\zeta = \frac{\lambda_N}{\lambda_L}. \tag{30}$$

In **Figure 9**, we show $MTIF_S$ for optimal FLBH networks consisting of M^2 nodes, $4 \le M \le 20$, for values of ζ ranging from 0 to the limiting case with ζ approaching ∞. We have again used approximation (13) for the values F_{iL}. Note that for finite ζ, $MTIF_S$ is an increasing function of the number of nodes. For these values of ζ, larger optimal FLBH networks offer a substantial improvement in $MTTF$ over simple rings with the same number of nodes. The two networks are equivalent in terms of $MTTF$ only when links are not allowed to fail, which is the case with $\zeta \to \infty$.

As a second comparison, consider a simple ring that has a bypass mechanism for failing nodes. This has been discussed in detail in [9]. For this network, the mean time to failure $MTTF'_R$ is

$$MTTF'_R = \sum_{j=M}^{N} \frac{N!}{j!} (\lambda_2 c)^{N-j} \prod_{k=j}^{N} \frac{1}{(k\lambda_2 + N\lambda_1)}, \tag{31}$$

where c is the probability that a node bypass is successful and M is the maximum number of nodes that can fail before the ring is declared down. We use $c = 0.9$ and $M = \lfloor N/2 \rfloor + 1$ in our example. We assume that a failed node that is not successfully bypassed will cause system failure, and that no bypass is provided for the optimal FLBH network. Also, the failure rates of the nodes and links of the ring network are not increased to compensate for the additional functionality that they possess.

In **Figure 10**, note that the mean time to failure improvement factor favors the FLBH network whenever $\zeta \le 1$, except for the case of ζ near 1 and $N = 4$ or 9. Even for $\zeta = 1.1$, FLBH networks larger than 256 nodes provide better $MTTF$. In fact, the FLBH network should be considered for even larger ζ, because our assumptions are somewhat favorable to the ring with bypass. The ring with bypass may operate in a degraded mode with up to M nodes bypassed, and this will reduce throughput and other performance measures. On the other hand, the FLBH network is considered to be down when a single node is down.

5. Availability model

We now allow failed links and nodes to be repaired by a single repair facility and assume that repair times are exponentially distributed with mean $1/\mu$. The repair strategy employed is to always repair the element that caused the network to fail first, then repair any other failed elements. Once the network has failed, no other

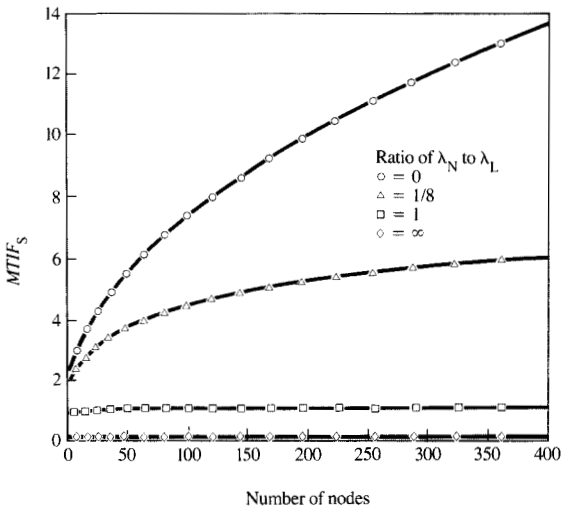

Figure 10

$MTIF_S$ for optimal FLBH networks vs. ring with node bypass.

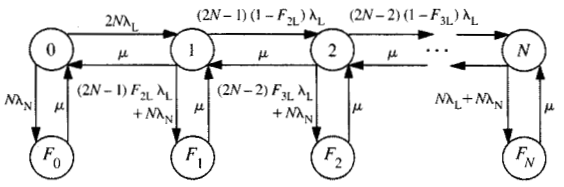

Figure 11

Markov chain for optimal FLBH network with repair.

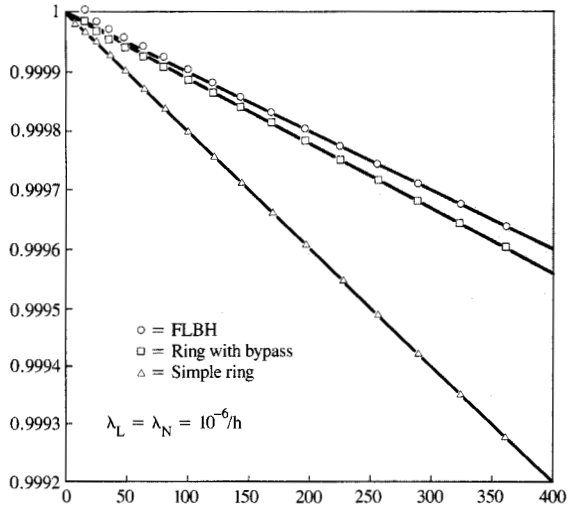

Figure 12

Availability of FLBH network vs. ring networks.

elements are allowed to fail until the network becomes operational again. We assume that repair rates are orders of magnitude higher than failure rates and use $\mu = 1$/h here.

The Markov chain in Figure 6 is modified as follows:

- A repair arc with rate μ is added from state i to state $i - 1$ for $1 \leq i \leq N$.
- The network failure state F is split into N failure states labeled F_1 through F_N. From state i, the arc that previously went to state F goes now to state F_i. Also, to account for node faults, an arc with rate $N\lambda_N$ emanates from state i to state F_i for $0 \leq i \leq N$.
- A repair arc with rate μ is added from state F_i to state i for $i \geq 0$.

For this new Markov chain shown in **Figure 11**, we can easily determine steady-state probabilities [7] from which we obtain the steady-state availability.

In **Figure 12**, we compare the steady-state availability of the optimal FLBH network to that of a simple ring with the same number of nodes ranging from 4 to 400. The FLBH network offers substantial improvement for larger networks.

If we now allow the simple ring to bypass faulty nodes with a constant probability of success c, we have found that the Markov chain models for the two networks are nearly duals of one another. The Markov chain in Figure 11 becomes the Markov chain of the ring with bypass by

1. Interchanging λ_N and λ_L.
2. Substituting the constant coverage factor c for the $(1 - F_{iL})$ terms.
3. Replacing the $2N$ factors with N.

In Figure 12, we have also plotted the availability of a ring network that bypasses faulty nodes with a coverage

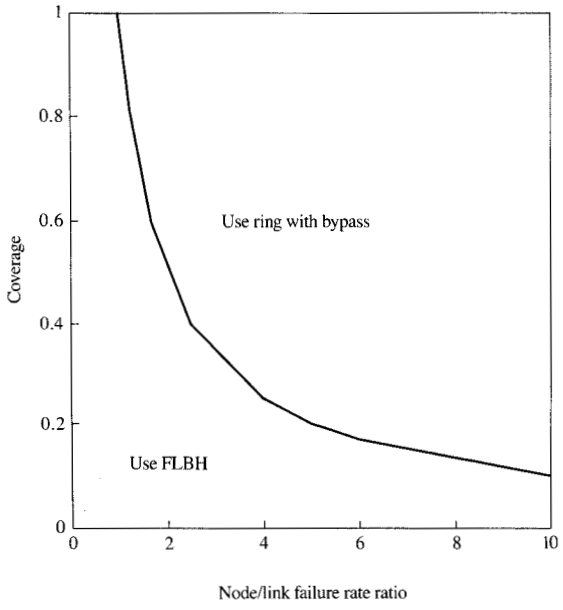

Figure 13

Availability of FLBH vs. ring network with node bypass.

factor $c = 0.9$. For this combination of coverage factor and failure rates, the FLBH network has higher availability for all sizes of networks.

Now vary the ratio of node failure rates to link failure rates ζ, and compute the coverage factor that causes the FLBH network and the ring network with node bypass to have the same availabilities. Because of the near duality of the Markov availability models for the two networks, the results show only a very slight variation in the number of nodes N, which is ignored. Thus, the effects of a constant coverage factor for node failures on the ring are compared to the link fault tolerance for the FLBH network. The results are plotted in **Figure 13**. For any combination of c and ζ beneath the curve, the FLBH network has higher availability. As expected, a ring with bypass becomes advantageous as the failure rate for the node in the adapter shown in Figure 2 increases and becomes larger than the failure rate associated with the link elements. This assumes that node failures can be tolerated on the ring if nodes can be successfully bypassed to remove them. These results confirm that the FLBH network is the network of choice in many cases when network availability is a primary consideration.

6. Conclusions

In this paper, we have evaluated the reliability and availability of the forward loop, backward hop class of networks. We have analyzed the probability that a subset of nodes becomes disconnected from the network, causing the network to fail. We have developed an approximation for these probabilities for use on larger networks where the computation of exact values is prohibitively expensive. These disconnection probabilities are then utilized as state-dependent branching (coverage) factors in Markov chain models. We have also developed simple yet close upper- and lower-bound models for the reliability of the FLBH network.

Even with the severe restriction that a node fault always causes the FLBH network to fail, we have shown that the FLBH network offers improvement in reliability over simple rings and some ring networks with node bypass. In fact, even in the case where the FLBH network is less reliable, it may offer a better combination of performance and reliability than a ring network with node bypass. We have also identified the conditions under which the availability of the FLBH network is better than that of the simple ring network with node bypass.

References

1. R. C. Dixon, N. C. Strole, and J. D. Markov, "A Token-Ring Network for Local Data Communications," *IBM Syst. J.* **22,** 47–62 (1983).
2. D. Farmer and E. Newhall, "An Experimental Distributed Switching System to Handle Bursty Computer Traffic," *Proceedings of the ACM Symposium on Problems in the Optimization of Data Communications*, 1969, pp. 1–23.
3. J. R. Pierce, "Network for Block Switching of Data," *Bell Syst. Tech. J.* **51,** 1167–1175 (1972).
4. C. S. Raghavendra and J. A. Silvester, "A Survey of Multi-Connected Loop Topologies for Local Computer Networks," *Computer Networks & ISDN Syst.* **11,** 29–42 (January 1986).
5. A. Grnarov, L. Kleinrock, and M. Gerla, "A Highly Reliable Distributed Loop Network Architecture," *Proceedings of the 1980 International Symposium on Fault Tolerant Computing*, October 1980, pp. 319–324.
6. M. T. Liu, *Distributed Loop Computer Networks*, Academic Press, Inc., New York, 1978.
7. K. S. Trivedi, *Probability and Statistics with Reliability, Queueing and Computer Science Applications*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1982.
8. F. K. Hwang, "Comments on 'Reliable Loop Topologies for Large Local Computer Networks,'" *IEEE Trans. Computers* **C-36,** 383–384 (1987).
9. Philip Yu, K. S. Trivedi, and W. E. Smith, "Reliability and Performance Analysis of a Ringnet," *Proceedings of the IFIP International Symposium on Local Communication Systems: LAN & PBX*, November 1986, pp. 111–123.
10. M. L. Shooman and A. E. Laemmel, "Simplification of Markov Models by State Merging," *Proceedings of the 1987 Annual Reliability and Maintainability Symposium*, pp. 159–164.
11. J. G. Kemeny and J. L. Snell, *Finite Markov Chains*, Van Nostrand-Reinhold, Princeton, NJ, 1960.
12. Andrea Bobbio and K. S. Trivedi, "An Aggregation Technique for the Transient Analysis of Stiff Markov Chains," *IEEE Trans. Computers* **C-35,** 803–814 (September 1986).

13. W. Najjar and J. L. Gaudiot, "Reliability and Performance Modelling of Hypercube-Based Multiprocessors," *Proceedings of the 2nd International Workshop on Applied Mathematics and Performance/Reliability Models of Computer/Communication Systems*, University of Rome II (Italy), May 1987, pp. 305–319.
14. Narsingh Deo, *Graph Theory with Applications to Engineering and Computer Science*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1974.
15. Joanne Bechta Dugan, K. S. Trivedi, Mark K. Smotherman, and Robert M. Geist, "The Hybrid Automated Reliability Predictor," *AIAA J. Guidance, Control & Dynam.* **9**, 319–331 (May–June 1986).
16. R. Sahner and K. S. Trivedi, "Reliability Modeling Using SHARPE," *IEEE Trans. Reliability* **R-36**, 186–193 (June 1987).

Received April 27, 1989; accepted for publication July 18, 1989

W. Earl Smith *IBM Communication Systems Division, P.O. Box 12195, Research Triangle Park, North Carolina 27709.* Dr. Smith received his B.S.E.E. degree from North Carolina State University in 1971 and his M.S.E.E. and Ph.D. degrees from Duke University in 1982 and 1989, respectively. He joined IBM in 1982 at the Research Triangle Park Development Laboratory working on telecommunications products. Later, he helped to develop the method for isolating and predicting errors in the IBM Token Ring local area network. Dr. Smith assumed a leadership role in the development of *Augmented Phone Services*, an IBM Personal Computer software product to assist the hearing impaired. Currently, he is a designer for subsystem reliability and serviceability in the 3174 Establishment Controller. Dr. Smith's research interests are in the areas of communications network design, reliability and availability analysis, and fault-tolerant computer architectures. He is a member of Eta Kappa Nu, Tau Beta Pi, and the Institute of Electrical and Electronics Engineers.

Kishor S. Trivedi *Department of Computer Science, Duke University, Durham, North Carolina 27706.* Dr. Trivedi received the B.Tech. degree from the Indian Institute of Technology (Bombay), and the M.S. and Ph.D. degrees in computer science from the University of Illinois, Urbana-Champaign. He is the author of *Probability and Statistics with Reliability, Queuing and Computer Science Applications*, published by Prentice-Hall. Dr. Trivedi's research interests are in computing system reliability and performance evaluation. He is currently Professor of Computer Science and Electrical Engineering at Duke University. Dr. Trivedi has served as a principal investigator on various projects for the U.S. Air Force Office for Scientific Research, the U.S. Army Research Office, Burroughs, IBM, NASA, NIH, and NSF, and as a consultant to a number of industry and research laboratories. He was an editor of the *IEEE Transactions on Computers* from 1983 to 1987, and is currently an editor of the *Journal of Parallel and Distributed Computing.*