A Framework for Characterizing Disaster-Based Network Survivability

Soung C. Liew, *Member, IEEE,* and Kevin W. Lu, *Member, IEEE*

Abstract— **This paper formulates a general framework that includes and extends the existing definitions for network survivability. Based on this framework, network survivability is characterized by a survivability function rather than a single-value survivability measure, and various quantities of interest can be derived from the function. Examples are the expected survivability, the worst-case survivability, the r-percentile survivability, and the probability of zero survivability. The survivability function is especially useful for the study of large-scale disasters. For illustration, we derive the survivability function in closed form for a simple ring network under link failures. We also discuss the general procedure for finding survivability functions for complex networks, and show that the survivability function reveals useful information about a network. This framework provides a unified and practical approach to analyzing and designing highly survivable communications networks.**

I. Introduction

INTEREST in reliable and robust communications networks has been on the rise recently [1]–[3]. The studies of network integrity generally fall under three major categories.

1) Network availability deals with the fraction of time the network is in service [4]. For example, a metric was proposed to measure the loss of traffic in units of DS3 min/year [5].

2) After-failure survivability assumes that some failure has occurred. Usually, the worst-case single or isolated failure (e.g., a single link failure) is considered [1], [3].

3) Disaster-based survivability considers what happens in the wake of a disaster. The occurrence of a disaster event is a given. In the case of a large-scale disaster, several link failures, for example, could happen simultaneously. In general, the network may fail totally, partially, or not at all [6].

Most recent work on network survivability belongs to the first two approaches. This paper clarifies several important issues and proposes a probabilistic framework for the study of disaster-based survivability. To date, the characterization of network survivability still lacks a unified framework, particularly one that also applies to large-scale disasters. Our formulation both includes and extends the existing definitions for network survivability.

Since network survivability deals with network integrity in the wake of some undesirable event, an issue, then, is the specific event being addressed and the meaning of network integrity. Examples of undesirable events are severe thunderstorm, tornado, hurricane, earthquake, fire, flood, tsunami, cable cut, an undetected software bug, and other disasters that in some way or another affect the normal operation of the overall network. Since different types of disasters may occur with different frequencies and may affect the network differently, network survivability under different disaster types should be studied separately.

Manuscript received July 15, 1992; revised February 8, 1993. A short version of this paper was presented at IEEE ICC'92.

The authors are with Bellcore, Morristown, NJ 07960-6438.

IEEE Log Number 9212469.

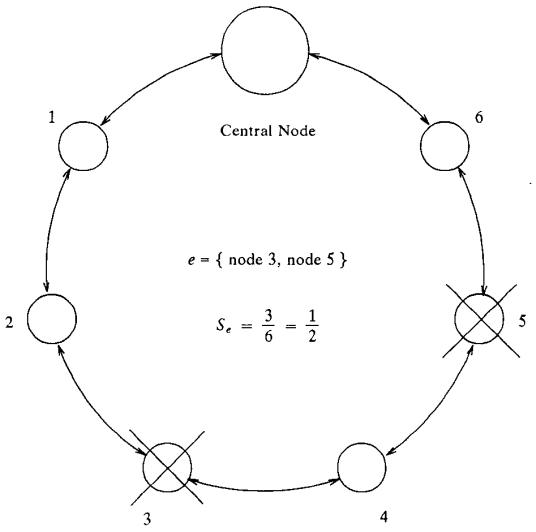

Fig. 1. A ring network with node failures due to a thunderstorm.

It is important to specify clearly the disaster type of interest. Given that the disaster in question has occurred, there are also many ways to describe network integrity. For instance, it could be defined as the traffic volume, the number of connected subscribers, the network operator's revenue, the grade of service, or other network characteristics that are related to the remaining "goodness" of the network. The point of emphasis here is that before we embark on a definition of network survivability, it is also important that we first specify what feature of the network we wish to capture. If the selected feature, say x, of the network can be quantified, such as in the above examples, we can then define network survivability, S, as the fraction of x that remains after an instance of the disaster type under consideration has happened.

In general, S is a random variable rather than a fixed quantity, and we propose that network survivability be characterized by a survivability function rather than a single-value survivability measure. As an example, consider Fig. 1, in which we want to study the number of remaining nodes connected to a central node in a ring network under, say, a

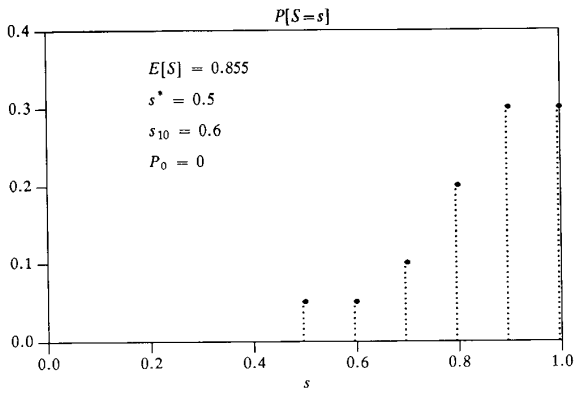

Fig. 2. Various quantities of interest based on a survivability function.

severe thunderstorm. Some of the nodes may be destroyed by lightning. Depending on which nodes are destroyed, the value of S may be different. Suppose that the set of inoperative nodes can be characterized probabilistically; then we have a sample space $E = \{e\}$ consisting of all subsets of nodes, each assigned a probability measure representing the likelihood the subset of nodes are the ones that malfunction. Thus, for each sample point e, we have a probability P_e and a survivability S_e, where S_e is the fraction of nodes connected to the central node. From this, we get the survivability function

$$P[S = s] = \sum_{e:S_e=s} P_e \tag{1}$$

the probability that a fraction s of the nodes are connected to the central node.

The reason for concentrating on a survivability function rather than a single survivability value, as in many previous studies, is that a number of different quantities of interest can be derived from the function, each capturing a particular network characteristic. For instance, we can obtain the expected survivability $E[S]$, the worst-case survivability s^*, the r-percentile survivability s_r, and the probability of zero survivability P_0 as follows:

$$E[S] = \sum_s sP[S = s] \tag{2}$$

$$s^* = \min_{P[S=s]>0} s \tag{3}$$

$$s_r = \max_{P[S\le s]\le r/100} s \tag{4}$$

$$P_0 = P[S = 0]. \tag{5}$$

Note that larger values of $E[S]$, s^*, s_r, and $(1-P_0)$ correspond to networks that are more survivable, but each parameter captures a different aspect of network survivability. For illustration, we show the above quantities based on a fictitious survivability function in Fig. 2.

As a detailed example of using the framework, Section II considers a simple ring network under link failures whose survivability function can be derived in closed form. The network survivability function in general cannot be obtained so easily, and the use of a computer may be necessary. Section III discusses the general procedure for calculating survivability functions; and Section IV follows the procedure to find survivability functions for a network. Finally, Section V summarizes this paper.

II. Survivability of a Centralized Ring Network Under Link Failures

We now discuss in detail an example of simple ring network, and define its network survivability as the fraction of nodes connected to the central node under link failures. We assume that all links are bidirectional. This, for example, could be a self-healing ring with the central node being the central office and the other nodes being the remote terminals in a subscriber loop network [3]. To simplify derivation, we also assume the number of nodes to be very large.

Let us first suppose that n link failures have occurred, and that a link failure is equally likely to be located anywhere within the network. For simplicity, we assume the locations of the n failures to be independent (although we can certainly accommodate dependency among failures in our framework by judiciously mapping probabilities to sample points). We want to derive the corresponding survivability function, $P[S = s|n]$. The value of n will be randomized later. Certainly, for $n = 0$ or 1, no node will be disconnected from the central node. So, we shall assume $n \ge 2$ in the following. To the extent that the number of nodes is very large, S becomes a continuous random variable rather than a discrete random variable, and we should focus on its probability density function $p_S(s|n)$ rather than its probability distribution function. The problem becomes similar to that of making n random cuts on a rubber band of unit length, and finding the length $s \in [0, 1]$ of the segment containing the central node. As shown in the Appendix, the probability density of s can be found to be

$$p_S(s|n) = n(n-1)s(1-s)^{n-2}. \tag{6}$$

Note that the above expression is for $n \ge 2$. For $n = 0$ or 1, the survivability is 1 with probability 1. Figs. 3 and 4 show the probability density and distribution functions, respectively, for various values of $n \ge 2$. We see that the probability density function tends to "skew" toward lower values of s as n increases, conforming to our intuition that the survivability of the network becomes worse as the number of link failures increases. The various single-value survivability measures that we mentioned previously can also be easily derived as follows:

$$E[S|n] = \int_0^1 sp_S(s|n)ds = \frac{2}{n+1} \tag{7}$$

$$s^* = \min_{p_S(s|n)>0} s = 0 \tag{8}$$

$$s_r = \theta : \left(\int_0^\theta p_S(s|n)ds = r/100\right)$$
$$= \theta : (-(1-\theta)^n - n\theta(1-\theta)^{n-1} + 1 = r/100) \tag{9}$$

$$P_0 = 0. \tag{10}$$

Notice that although the worst-case survivability is 0, the probability of zero survivability is 0. This is due to the continuity of random variable S.

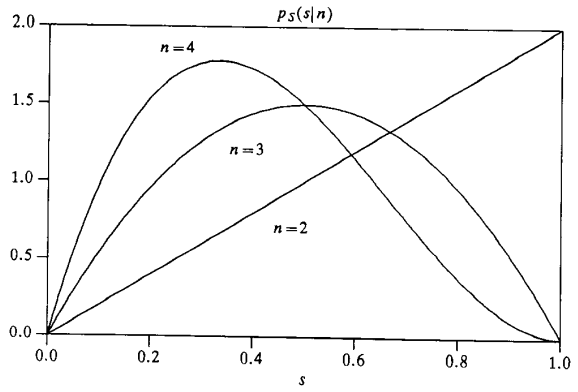

Fig. 3. Survivability density functions for a ring network.

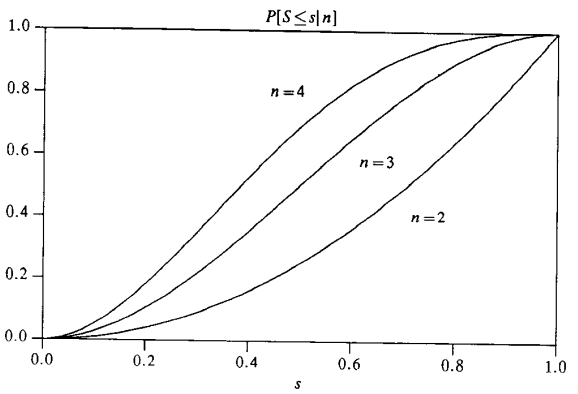

Fig. 4. Survivability distribution functions for a ring network.

In general, the number of link failures n is also a random variable for a given disaster type. Let N_c be the random variable associated with the number of cuts. Then,

$$\begin{aligned} p_S(s) &= \sum_n p_S(s|n)P[N_c = n] \\ &= \delta(s-1)(P[N_c = 0] + P[N_c = 1]) \\ &\quad + \sum_{n=2}^{\infty} n(n-1)s(1-s)^{n-2}P[N_c = n] \end{aligned} \tag{11}$$

where $\delta(x)$ is the impulse function [7]. Let

$$N_c(z) = \sum_{n=0}^{\infty} z^n P[N_c = n] \tag{12}$$

be the moment-generating function of N_c, and let $N_c^{(2)}(z)$ be the second derivative of N_c with respect to z [8]. Then,

$$\begin{aligned} p_S(s) &= \delta(s-1)(P[N_c = 0] + P[N_c = 1]) \\ &\quad + sN_c^{(2)}(1-s). \end{aligned} \tag{13}$$

For the Poisson distribution, which is applicable to a large uniform network

$$P[N_c = n] = (\overline{n})^n e^{-\overline{n}}/n! \tag{14}$$

where $\overline{n}$ is the mean number of cuts for the disaster type under consideration

$$N_c(z) = e^{\overline{n}(z-1)}. \tag{15}$$

Thus, we have

$$p_S(s) = \delta(s-1)(e^{-\overline{n}} + \overline{n}e^{-\overline{n}}) + \overline{n}^2 s e^{-\overline{n}s}. \tag{16}$$

It is easy to derive the following survivability quantities:

$$E[S] = \frac{2}{\overline{n}} - e^{-\overline{n}}\left(1 + \frac{2}{\overline{n}}\right) \tag{17}$$

$$s^* = \min_{p_S(s)>0} s = 0 \tag{18}$$

$$\begin{aligned} s_r &= \theta : \left(\int_0^{\theta} p_S(s)ds = r/100\right) \\ &= \theta : (1 - e^{-\overline{n}\theta}(1 + \overline{n}\theta) = r/100) \end{aligned} \tag{19}$$

$$P_0 = 0. \tag{20}$$

III. General Procedure for Finding Survivability Function

The previous section deals with a simple case where the survivability function can be found in closed form. For more general networks, or with other definitions of network integrity, the survivability may not be so easily obtained. Automated computation using a computer program may be necessary. The general procedure is as follows:

1) specify disaster type to be studied;
2) define "goodness" of networks;
3) list the sample points $\{e\}$, or all combinations of events that may happen under the disaster type being considered;
4) determine the survivability S_e;
5) determine or assign probability of each event e; and
6) calculate survivability function $P[S = s] = \sum_{e:S_e=s} P_e$.

We now describe the above steps in more detail. Before calculating the survivability function, one should first specify the type of disaster and the definition of the "goodness" of networks. This is important since different disaster types may have different effects on networks. For instance, a severe thunderstorm may render more than one node inoperative, whereas a cable cut usually destroys only transmission between two nodes. Thus, damage to the network and the probabilistic characterization will be different in these two cases. Moreover, we may also obtain different results depending on the features of the network for which we are calculating survivability. For example, definitions for "goodness" may be the number of subscribers connected to a central node, as in the example of the preceding section, or the revenue collected by the network operator. If some subscribers contribute to the revenue more than others, the survivability based on these two definitions would be different. This also suggests that the network operator could give high priority to the network survivability of major subscribers.

The next step is to list all possible combinations of events that could happen under the given disaster type. However, this may not be as simple as it sounds. The ring network in the previous section is a special case in which the sample points

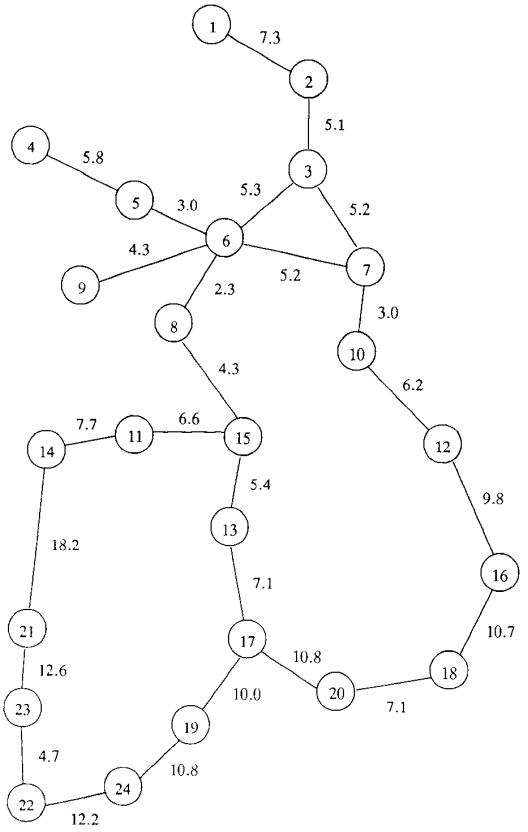

Fig. 5. A network for survivability characterization.

can be enumerated easily. Given a more general network and a different definition for "goodness," listing all the sample points may be difficult and can only be done effectively by a computer. In addition, the sample space may simply be too large, and we may want to eliminate sample points which are very unlikely to happen.

Once the sample points have been listed, the next step is to calculate the survivability measure for each sample point. This calculation will depend on our definition of survivability. If the definition is the number of nodes connected to a particular central node, as in our example above, then we would need an efficient algorithm that can determine whether there is a path to and from the central node for each node. Instead of concentrating on a general algorithm that can determine the survivability of any given network, one may want to identify more efficient algorithms by exploiting the particular network structures being considered. For instance, the solution to the ring network above can be obtained exactly without any sophisticated algorithm.

To each sample point, we can assign a probability measure representing the likelihood of its occurrence. Strictly speaking, assignment of probabilities to sample points should be based on past observations or experience. However, if the disaster under consideration happens so rarely (e.g., a nuclear attack) that past observations are not available, then one will need to use his or her judgement when assigning probabilities. In this case, a study of the sensitivity of results to variations in probability assignment is also necessary in order to establish the confidence level one would have of the results. For special cases in which the problems being considered have a homogeneous or uniform structure, we can assign probabilities uniformly. For example, in our ring network in the previous section, each link is equally likely to fail.

Once the above steps have been done, it is routine to calculate each point of the survivability function by summing the probabilities of all sample points with the same survivability.

TABLE I
DS3 DEMANDS BETWEEN NODES OF A NETWORK

Node Pair		DS3's	Node Pair		DS3's
1	6	3	6	17	1
2	6	2	6	18	5
3	6	4	6	19	1
3	7	1	6	22	2
4	6	4	7	8	1
5	6	3	14	15	2
6	7	11	15	21	3
6	8	1	16	18	1
6	9	1	17	18	1
6	10	3	18	19	1
6	11	1	18	20	2
6	12	4	21	22	4
6	13	1	22	23	1
6	15	2	22	24	2
6	16	1	Total DS3's		69

IV. FINDING SURVIVABILITY FUNCTION FOR A NETWORK

For illustration, this section follows the general procedure described above to find survivability functions for the network shown in Fig. 5. This network consists of 24 nodes and 26 links, and the number associated with each link is its length in miles. We assume a total of 69 DS3 (44.736 Mb/s) fiber-optic transmission systems between 29 node pairs as individually listed in Table I. For those node pairs with more than one route between them, we choose the shortest one; that is, no diverse routes are assumed.

Following the general procedure in Section III, we first specify hurricanes, which may cause multiple link failures, as the disaster type for study. Second, we are interested in the total number of surviving DS3's under link failures. This definition of network integrity corresponds to the revenue generated by the DS3's. For single link failures caused by localized disasters such as a cable cut, the network survivability can be easily found by counting the number of DS3's lost for the particular link as listed in Table II. However, for the network of 26 links, there are $2^{26} = 67,108,864$ possible combinations of link failures under a large-scale disaster such as a hurricane. For simplicity, we assume that more than four link failures are highly unlikely. Thus, there are $17,901$ possibilities of link failures, including 26 single, $\binom{26}{2} = 325$ double, $\binom{26}{3} = 2600$ triple, and $\binom{26}{4} = 14\,950$ quadruple link failures. Then, for each event e, the survivability S_e is simply the number of surviving DS3's divided by the total of 69.

TABLE II
DS3'S LOST DUE TO LINK FAILURES OF A NETWORK

Failed Link		DS3's	Failed Link		DS3's
1	2	3	11	15	6
2	3	5	12	16	6
3	6	9	13	15	5
3	7	1	13	17	4
4	5	4	14	21	3
5	6	7	16	18	6
6	7	25	17	19	4
6	8	10	17	20	2
6	9	1	18	20	4
7	10	13	19	24	2
8	15	8	21	23	4
10	12	10	22	23	5
11	14	5	22	24	4

To determine the probability P_e of each event e, we assume that link failures are independent and the probability of a link failure is proportional to its length, l_i; that is,

$$P[\text{link } i \text{ fails}] = \epsilon l_i, \qquad 0 < \epsilon < \frac{1}{\max_i l_i}. \tag{21}$$

The probability of no link failures is then

$$P[\text{no link failure}] = \prod_i (1 - \epsilon l_i). \tag{22}$$

In practice, ϵ is set to reflect the extent of damage expected of the hurricane, and hence we define

$$\epsilon = \frac{\rho}{\max_i l_i}, \qquad 0 < \rho < 1. \tag{23}$$

With ϵ determined, the probabilities of single, double, triple, and quadruple link failures are simply as follows:

$$P[\text{only link } i \text{ fails}] = \epsilon l_i \prod_{n \neq i} (1 - \epsilon l_n) \tag{24}$$

$$P[\text{only links } i \text{ and } j \text{ fail}] = \epsilon^2 l_i l_j \prod_{n \neq i,j} (1 - \epsilon l_n) \tag{25}$$

$$P[\text{only links } i, j, \text{ and } k \text{ fail}] = \epsilon^3 l_i l_j l_k \prod_{n \neq i,j,k} (1 - \epsilon l_n) \tag{26}$$

$$P[\text{only links } i, j, k, \text{ and } m \text{ fail}] = \epsilon^4 l_i l_j l_k l_m \prod_{n \neq i,j,k,m} (1 - \epsilon l_n). \tag{27}$$

Based on the values of S_e and P_e derived above, we are ready to calculate the survivability function in (1). Although there are 17 901 events in total, many of them have exactly the same survivability. In addition, for clarity of illustration, we condense all survivabilities within the intervals $(0.02i - 0.01, 0.02i + 0.01]$ to the points $0.02i$, $i = 1, 2, \cdots, 50$. Figs. 6 and 7 show the survivability (density) functions for $\rho = 0.1$ and 0.2, respectively. It is worth noting that, when we increase ρ from 0.1 to 0.2, the probability of no link failure (at $s = 1$) decreases significantly from 0.341 to 0.11, the expected survivability $E[S]$ decreases from 0.925 to 0.834, and the 10-percentile survivability s^* is unchanged simply because it is independent of ρ. Although the worst-case survivability is about 0.28, it corresponds to two events of quadruple link failures (links 3–6, 5–6, and 6–7 with link 6–8 or 8–15), and its probability is less than 10^{-6}. On the other hand, for $s = 0.92$ and $\rho = 0.2$, there are 117 possible events with a combined probability of 0.123. The observations above suggest that the survivability function can reveal more insightful information than just the worst-case survivability or any other single-value measure alone.

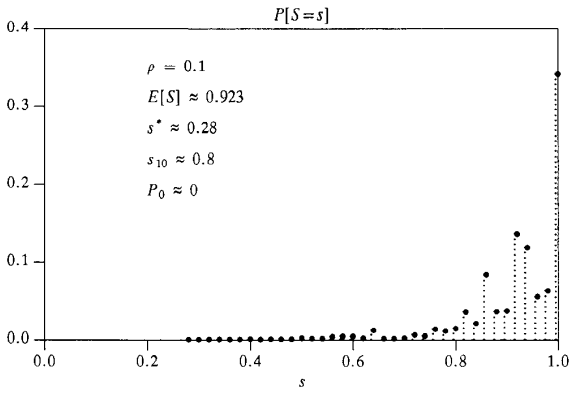

Fig. 6. Survivability function of a network under large-scale disaster.

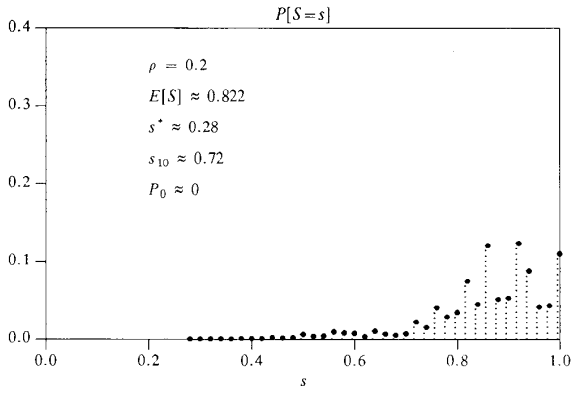

Fig. 7. Survivability function of a network under large-scale disaster.

V. CONCLUSIONS

We have described a general framework for characterizing network survivability that includes and extends the existing

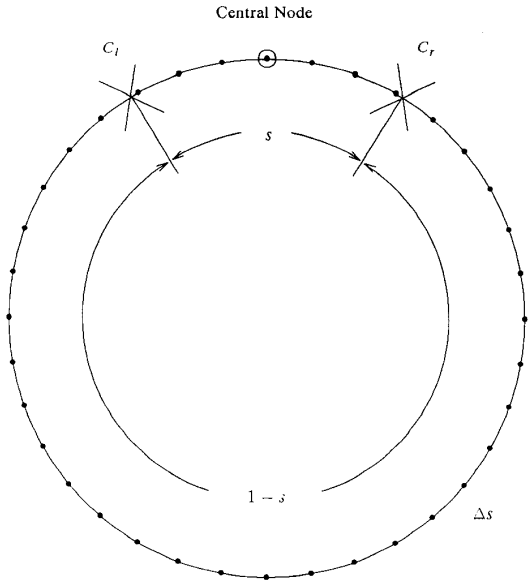

Fig. 8. Illustration for deriving survivability function of a ring.

definitions. Based on this framework, network survivability is characterized by a survivability function rather than a single-value survivability measure; and various quantities of interest can be derived from the function. Examples are the expected survivability, the worst-case survivability, the r-percentile survivability, and the probability of zero survivability. In particular, we derived the survivability function in closed form for a simple ring network under link failures. We also discussed the general procedure for finding survivability functions for complex networks, and showed that the survivability function reveals useful information about a network. Although our illustrating examples assume link failures to be independent, our framework can accommodate situations that involve dependency among failures; the added complexity for computing the survivability function remains to be studied further. In short, this framework provides a unified and practical approach to analyzing and designing highly survivable communications networks.

APPENDIX

This Appendix derives the results in (6). Since S is continuous here, there are an infinite number of sample points in the sample space E. To avoid this nonessential technicality, we first artificially make the sample space finite by dividing the rubber band into many small segments, each of length Δs. The desired result is obtained by letting Δs approach zero. If there is no more than one cut on each segment, which is true when Δs is very small, the size of the sample space, or the number of ways the n cuts can be done, is

$$\frac{1}{\Delta s}\left(\frac{1}{\Delta s}-1\right)\cdots\left(\frac{1}{\Delta s}-(n-1)\right)\approx\frac{1}{(\Delta s)^n}. \tag{A1}$$

Since each of these sample points is equally likely,

$$P_e\approx(\Delta s)^n \qquad \text{for all } e \tag{A2}$$

and

$$P[S=s|n]=\sum_{e:S_e=s}P_e=N_s(\Delta s)^n \tag{A3}$$

where N_s is the number of ways to make n cuts that result in a survivability of s.

To find N_s, let's first denote the cuts by $C_1, C_2, \cdots, C_n$. As far as survivability is concerned, only the two cuts adjacent to the central node, C_l and C_r, are important (see Fig. 8), since their locations completely define the value of S. Out of the n cuts, there are $n(n-1)$ ways of choosing two cuts to be C_l and C_r. The number of ways one can arrange the remaining $(n-2)$ cuts in the segments away from the central node and outside C_l and C_r is

$$\left(\frac{1-s}{\Delta s}\right)\left(\frac{1-s}{\Delta s}-1\right)\cdots\left(\frac{1-s}{\Delta s}-(n-3)\right)\approx\left(\frac{1-s}{\Delta s}\right)^{n-2}. \tag{A4}$$

Given that the segment containing the central node is of length s, there are $s/\Delta s$ ways of putting the two adjacent cuts, ranging from putting C_l right next to the central node and C_r at a distance of s to the central node, to putting C_r right next to the central node and C_l at a distance of s to the central node (see Fig. 8). Thus,

$$N_s=n(n-1)\left(\frac{1-s}{\Delta s}\right)^{n-2}\frac{s}{\Delta s}. \tag{A5}$$

By definition,

$$p_S(s|n)=\lim_{\Delta s\to 0}\frac{P[S=s|n]}{\Delta s}=n(n-1)s(1-s)^{n-2}. \tag{A6}$$

ACKNOWLEDGMENT

The authors would like to thank T.-H. Wu for providing the network example and valuable comments. They are also indebted to D. N. Deutsch for his thorough review and useful suggestions.

REFERENCES

[1] T.-H. Wu, *Fiber Network Service Survivability*. Norwood, MA: Artech House, 1992.
[2] Special Issue on Surviving Disaster, *IEEE Commun. Mag.*, vol. 28, June 1990.
[3] J. Sosnosky and T.-H. Wu, "SONET ring applications for survivable fiber loop networks," *IEEE Commun. Mag.*, vol. 29, June 1991.
[4] R. E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing: Probability Models*. New York: Holt, Rinehart, Winston, 1975.
[5] Y. Kane-Esrig *et al.*, "Survivability risk analysis and cost comparison of SONET architectures," in *Conf. Rec. IEEE Globecom '92*, pp. 841–846.
[6] Technical Report on Network Survivability Performance, Standards Committee T1A1.2, 1993.
[7] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York: McGraw-Hill, 1965.
[8] L. Kleinrock, *Queueing Systems, Vol. 1: Theory*. New York: Wiley, 1975.

Soung C. Liew (S'84–S'87–M'87–M'88) received the S.B., S.M., E.E., and Ph.D. degrees in electrical engineering from Massachusetts Institute of Technology, Cambridge, in 1984, 1986, 1986, 1988, respectively.

From 1984 to 1988 he was a Research Assistant in the Local Communication Networks Group at the M.I.T. Laboratory for Information and Decision Systems, where he investigated fundamental design problems in high-capacity fiber-optic networks. He was also a Teaching Assistant for a graduate course on data communication networks. In March 1988 he joined Bellcore, Morristown, NJ where he has been a Member of Technical Staff in the Network Systems Research Laboratory. He is currently taking a leave of absence from Bellcore and is Senior Lecturer in the Chinese University of Hong Kong. He has conducted research and published actively in various areas related to broadband communications, including wavelength-division-multiplexed optical networks, high-speed packet-switch designs, system-performance analysis, routing algorithms, network-traffic control, and reliable and survivable networks. His current research interests include interconnection networks, broadband network control and management, distributed and parallel computing, fault-tolerant networks, and optical networks.

Dr. Liew is a member of Sigma Xi and Tau Beta Pi.

Kevin W. Lu (S'81–M'85) received the B.S. degree in control engineering from National Chiao Tung University, Taiwan, in 1979, and the M.S. and D.Sc. degrees in systems science and mathematics from Washington University, St. Louis, MO, in 1981 and 1984, respectively.

In August 1984 he joined Bellcore, Morristown, NJ, where he is currently a Member of Technical Staff in Applied Research. His research interests include modeling, analysis, and optimization for the communications network systems. His current research activities are related to fiber in the loop and network survivability. He was Adjunct Professor at Rutgers Graduate School of Management, Newark, NJ, and Special Lecturer with the Department of Electrical Engineering at Columbia University, New York, NY, in 1989.

Dr. Lu is a member of Sigma Xi and has been active in the Optical Communications Committee of the IEEE Communications Society. He was the recipient of the Bellcore Award of Excellence in 1987 for his work on technological and market obsolescence of telephone network equipment. He was recently a co-recipient of the Bellcore 1992 Team Award for his work on developing economic models for fiber in the loop.