# RELIABILITY OF COMPUTER-COMMUNICATION NETWORKS*

Richard Van Slyke and Howard Frank
Network Analysis Corporation
Beechwood, Old Tappan Road
Glen Cove, N.Y. 11542

## Summary

A major consideration in the original design and in the expansion of any computer-communication network is the provision of a network which will be relatively invulnerable to failures of its components. This paper considers the reliability analysis of such networks. Two indices of reliability for a network are introduced. Methods for the calculation of these indices are illustrated by carrying out a detailed reliability analysis of the ARPA Computer Network. This analysis includes sensitivity calculations to protect against inaccuracies of measured system parameters and the evaluation of possible improvements in reliability through modification of network configuration.

## Introduction

The ARPA network is a store-and-forward computer network designed to interconnect many dissimilar computers located throughout the country. Each computer interfaces with the network by means of an Interface Message Processor (IMP). These IMPs are connected by fully duplex communication lines of typically 50 kilobit/second capacity. The reliability of such networks and their availability to users is the subject of this paper.

For analysis purposes, the ARPA network can be represented as a graph with lines corresponding to communication links and nodes corresponding to the Interface Message Processors. In earlier work[1] methods were described to choose network designs providing good response time at low cost. A minimum level of reliability was guaranteed by requiring that there exist at least two node disjoint paths between each pair of IMPs. Figure 1.1 represents a version of the ARPA network which is representative of the planned design at the end of 1971. This network consists of 23 nodes and 28 links and is used throughout the paper as an example.

In Section 2 we define two measures of network reliability. In Section 3 we assume nodes are perfectly reliable and we analyse the network with respect to the first measure. In Section 4 we allow both node and link failures and determine reliability according to the second criterion. In addition, modifications of the network which increase reliability are explored.

*This work was supported by the Advanced Research Projects Agency of the Department of Defense (Contract No. DAHC 15-70-C-0120).

## Two Network Reliability Criteria

Nodes and links can be in two states, failed or operative. Two nodes in the network can communicate if they both are operative and there exists a path of operable nodes and links between them. A simple and natural characterization of a failed or operative network is:
Criterion 1: A network is operative if every pair of operable nodes can communicate; otherwise it is failed. This is equivalent to: the network operates if all operating nodes are in one component; (a component is a maximal set of nodes in which each pair can communicate).

Criterion 1 is not completely satisfactory because it does not indicate the "degree" of disruption a failed network has experienced. For example, the failure of the single node 1 in the network shown in Figure 2.1 entirely prevents communication between the remaining nodes. In Figure 2.2 the failure of node 1 only prevents one operable node from communicating with the others.

Criterion 2: The fraction of communicating node pairs of a network is the ratio of the distinct pairs which can communicate to the total number of distinct node pairs.

Suppose nodes and links fail with known probabilities. Each node and link may have a different failure probability. However, we require that every link and node failure be an independent random variable. We seek to calculate either the probability that the network is failed or the expected number of node pairs cannot communicate.

Our model represents two situations; in the first, a catastrophic event such as an earthquake or hurricane may destroy network elements. Then, if elements fail with known probabilities, we seek the expected number of node pairs that can communicate after the event. In the second situation, links and nodes may continually fail and be repaired. We then wish to know either the time average of the number of node pairs communicating or the fraction of the time the network is connected. For this interpretation each element failure probability is the fraction of time it is not operational.

## Network Connectivity Probability

The IMPs in the ARPA system are very rugged, highly reliable units and preliminary information implies they can be made more reliable than their connecting lines. As a first approximation, we therefore assume the nodes are perfectly reliable. Initially, we assume that all links have the same failure probabilities.

If p represents the probability of a link failure, the probability, h(p), of the net failing is

$$h(p) = \sum_{k=0}^{NB} C(k)\ p^{NB-k}\ q^{k} \qquad (1)$$

where q=1-p, NB is the number of links in the net, and C(k) is the number of disconnected subnets with k operable links. Thus, the original probabilistic problem "reduces" to the combinatorial problem of determining the C(k). Several of the C(k) can be specified immediately. If the net has NN nodes, at least NN-1 links are required to connect all nodes. Thus C(k) = $\binom{NB}{k}$ for k<NN - 1. Moreover, if it takes at least c failed links to disconnect the net, C(NB-k) = 0 for k = 0, 1, ..., c-1. There are now NB-NN-c+2 unknown C(k). Since the ARPA net is designed to minimize cost, typically NB is not much larger than NN and c=2. Thus, for the example in Figure 1.1, the number of unknown terms is 28-23-2+2 = 5. There are 3 ways to find these terms: enumerating subnets with k links and counting the failed ones, sampling among subnets with k links and estimating C(k), or calculation of bounds on the missing terms. A more complete discussion of this is given in Reference 4. The essential feature is that when p is small (the situation for the ARPA net) only networks with small numbers of simultaneous failures are likely to occur. In (1), therefore the unknown C(k) with the largest k are most important. Consequently, a good approach is to enumerate the first few C(k) and estimate or sample the remaining ones. We illustrate this procedure on the ARPA net of Figure 1.1. Table 3.1 lists the number of subnets for all k and the number of k link subnets which are not connected for all k except k = 23 and k = 24.

The two unknown terms, C(23) and C(24), can be accounted for in two ways. The first uses the fact that if the removal of k links disconnects the net, the removal of any set of k+1 links containing these k links also disconnects the net. The details of the resulting estimation procedure are given in Appendix A. The resulting bounds on C(23) and C(24) are given in Table 3.2. The terms can also be obtained by sampling. For small p, C(24) makes the greatest contribution to the probability of the network failing, and we expend the most effort to estimate it. We utilize proportional stratified random sampling. Suppose we are interested in the range $0 \leq p \leq .1$. For p = .05, the probability of a network having 23 operational links is $\binom{28}{23}(.05)^5(.95)^{23} = .009439$ while the probability of a network having 24 operational links is $\binom{28}{24}(.05)^4(.95)^{24} = .037365$. If we are allowed a total of 1000 samples, we allocate these to the 23 and 24 link nets in proportion to their probability of occurence. Thus, we sample 24 link nets (1000)(.037365)/(.009439 + .037365) = 798.32 ≅ 798 times and 23 link nets, (1000)(.009439)/(.009439 + .037365) = 201.67 ≅ 202 times. The resulting estimates and their variances are shown in Table 3.3. In Table 3.4, upper and lower bounds for network failure probability for p between 0 and .1 in increments of .01 and from .1 to .9 in increments of .1 are given. Estimates of their values and the sample standard deviations are also shown. In general, the estimation procedure considers all terms not known _a priori_. In our example, these are C(26), C(25), C(24) and C(23). To be specific, suppose we wish to sample 1000 networks. For p = .05, the probability that a network with 26 links will occur is .24903; with 25 links, .11359; with 24 links, .03736; and with 23 links, .00944. We divide our 1000 samples among these 5 types of networks in proportion to their probability of occurring. This leads (approximately) to 608 samples of nets with 25 links and so on. Since there are only 378 networks with 26 links, it is most efficient to calculate C(26) by enumerating all 378 subnets. This allows 622 = 1000 - 378 samples to be allocated to networks with 23 through 25 operative links. Using proportional allocation, we obtain 440 samples for C(25), 145 for C(24) and 37 for C(23). The results are also displayed in Tables 3.3 and 3.4. In Table 3.5 the stratified simulation with a sample of size 1000 is compared with conventional simulation with the same sample size done by assigning a random number to each link and considering the link failed or operative depending on whether the random number is less than or greater than the link failure probability. As is evident, the stratified simulation is far more efficient than the conventional approach over the range of practical link failure probabilities.

Figure 3.1 illustrates the relationship between the upper and lower bounds given in the tables and the estimates of connectivity probability obtained by the stratified simulation.

<u>Average Fraction of Non-Communicating Node Pairs</u>

To find the expected number of communicating node pairs, we sample directly from the family of all subnets of the original network rather than use stratified sampling. This method, while less efficient, is easier to use in more general situations such as the case in which nodes can fail. The method operates by generating a random number for each node and link. If the random number is less than the failure probability, the corresponding element is removed; otherwise it is operative. We use the procedure described in Appendix C to yield the expected number of pairs not communicating _for a range_ of link and node failure probabilities with about the same computational effort as for one set of values of link and node failure probabilities.

For the first case, the results of a simulation on the 23 node, 28 link net in Figure 1.1

using equal probabilities for node and link failures and a sample of size 1000, are shown in Figure 4.1. Also shown are several results that illustrate the flexibility of the approach. These simulations tested ideas for increasing network reliability. In the first, the link connecting UTAH to NCAR was replaced by a link from NCAR to NASA thus creating an additional node disjoint path between the East and West Coasts. However, the reliability improvement as measured by the simulation was negligible and the two curves could not be shown separately in Figure 4.1. Next, the long serial chain from BBN to HARVARD to BURROUGHS to ETAC to MITRE to CM to CASE was examined. This chain is vulnerable since any two node or link failures in it disconnects the network. To relieve this situation, a link was added from LINCOLN to BURROUGHS. This generated a substantial improvement as shown in the figure. The third approach considered the installation of hardware at each IMP so that if an IMP failed, traffic could bypass it by being routed around it in one direction connecting two of the incident links. Any remaining links are effectively blocked. The directions of the bypasses chosen are shown in Figure 2.4.2. The result was a reduction in the expected fraction of node pairs not communicating almost to the level of the case of no-node failures. However, for low levels of unreliability, ($p \leq .03$) the improvement was not considered to be worth the expense of the hardware and software modifications that would be required.

Two additional simulations considered link failure and node failure separately. These simulations give an indication of the extent that any modification of the network design can lower the expected fraction of pairs communicating. If a node fails, at least 22 pairs cannot communicate (all nodes paired with the failed node) independent of the network structure. Thus, good network design cannot improve beyond the effect directly due to node failures, which for the ARPA net is the major factor affecting reliability.

The situation where link and node failure probabilities are not necessarily equal was also investigated. Preliminary data was available on the downtime for a subset of the communication lines in the ARPA network. The reliability of a link in the ARPA net was hypothesized to be a linear plus a constant term function of the link's length. Linear regression was used to fit a function to the available data. The least squares linear regression function was .00293 X + .904. This function gives the percent downtime as a function of the direct distance X in miles between nodes. A highly conservative failure probability of .03 was assigned to the nodes. The average failure probability over all the nodes and links was .0241. In Figure 4.3 the results of the simulation are displayed. Other points plotted were obtained by assigning a common value for each element failure probability (nodes and links) equal to the average element failure probability for the previous simulation. From the closeness of the results we conclude that for design purposes the assumption that links fail with equal probability is an excellent approximation.

We can also use Criterion 1 for networks with failing nodes and links. In Figure 4.4, the probability that the network is disconnected is compared for three situations. In the first two cases, nodes and links are assigned the same failure probability. First, the network is considered disconnected if any node pair cannot communicate. (That is, if any node has failed, the network is considered disconnected.) Second, the network is considered disconnected only if a pair of operable nodes cannot communicate. Finally, for comparison purposes, we give the probability of disconnection when nodes are perfectly reliable.

## Appendix A: Bounds for C(k)

If removing a set of k links disconnects a net, then removing any set containing it also disconnects the net. Similarly, if a subset of links forms a connected subnet, then any set containing the first is also connected. Using only these facts, if one knows the number, C(k), of disconnected k link subnets, one can give lower bounds for C(k') for $k' < k$ and upper bounds for C(k"), $k'' > k$.

Bounds can be obtained using Kruskal's Theorem.[2] An abstract complex is a finite set of points together with a class of subsets with the subset closure property; that is, if a subset belongs to the class, then so do all its subsets. The r-canonical representation of any non-negative integer n is $(n_r, \dots, n_i)$ where

$$n = \binom{n_r}{r} + \binom{n_{r-1}}{r-1} + \dots + \binom{n_i}{i} \qquad (1)$$

and $n_r$ is as large as possible so that $\binom{n_r}{r} \leq n$, $n_{r-1}$ is as large as possible so that $\binom{n_r}{r} + \binom{n_{r-1}}{r-1} \leq n$ and so on until equality is achieved. An r-set is a subset with r elements. For $r \leq r''$, f(n; r, r') is the greatest number of r'-sets in any complex having precisely n r-sets. If $r > r'$, f(n' r, r') is the smallest number of r'-sets in any complex having precisely n r-sets.

Theorem (Kruskal). If $n = \binom{n_r}{r} + \dots \binom{n_i}{i}$ is canonical, then

$$f(n; r, r,') = \binom{n_r}{r'} + \binom{n_{r-1}}{r'-1} + \dots + \binom{n_i}{r'-r+1} \qquad (2)$$

with the conventions that $\binom{0}{0} = 0$, $\binom{m}{k} = 0$ for $m < 0$ or $k < 0$, or $m < k$.

Kruskal's theorem gives us the following inequalities

$$C(k') \geq f(C(k);\ k,\ k') \text{ for } k \geq k'. \quad (3)$$

$$C(k') \leq f(C(k);\ k,\ k') \text{ for } k \leq k'. \quad (4)$$

Thus, for each $C(k)$ that we can calculate (or bound), we can get bounds on the remaining $C(k')$. In the ARPA net, c is small and links have small failure probabilities. In such cases, we can exactly calculate the first few terms $C(NB-c)$, $C(NB-c-1)$, ..., and then derive lower bounds for the remaining co-efficients. This yields a good lower estimate for $h(p)$ for p small. Good upper bounds are more difficult to determine. $C(NN-1)$ equals $\binom{NB}{NN-1}$ minus the number of trees and can be calculated by formula; upper bounds for $k$ $N-1$ then result from (4). Unfortunately, the terms which are most important for small p are the ones for which the estimates from (4) are least accurate. Further details can be found in Reference 4.

## Appendix B
## Determining Components of Networks

Consider a network $G=\langle \mathcal{N}, \mathcal{A} \rangle$ with node set $\mathcal{N}$ and link set $\mathcal{A}$ in which only some of the nodes or links are operable. We wish to find the number of components of the network. Each node will be assigned a label indicating which component it is in. The algorithm is as follows where $k := k + 1$ means k is replaced by $k+1$.

Step 0: Start with $\mathcal{A}_0 = \emptyset$ and assign each node a separate label. Set $k = 0$. Go to Step 1.
Step 1: If all operable links are in $\mathcal{A}_k$, stop. Otherwise add an operable link $a_k$ to $\mathcal{A}_k$ to form $\mathcal{A}_{k+1}$. Suppose $a_k = (m_k, n_k)$. Examine the labels of $m_k$ and $n_k$. If they are the same or if either $m_k$ or $n_k$ is inoperable repeat Step 1 with $k := k+1$. If not, go to Step 2.
Step 2: Change all the node labels which are the same as the label of $m_k$ (including $m_k$'s label) to the label of $n_k$. Set $k := k+1$ and go to Step 1.

When the algorithm terminates, each component is listed. It is important for future applications of the algorithm that we may introduce the operable links in Step 1 in any order we please.

It is convenient to maintain several other statistics of interest during the calculation. These include the number of components, the number of nodes in each component and the number of node pairs which are in the same component. This is carried out as follows. Initially, the number of components is NN, the number of pairs communicating, NP, is 0, and each component contains 1 node. Each time we reach Step 2, we combine two components, with say $t_1$ and $t_2$ nodes into a new component with $t_1 + t_2$ nodes. Also, we now have $t_1 \times t_2$ more node pairs which can communicate. Therefore, we set $NP=NP+t_1 \cdot t_2$. The number of components decreases by 1.

## Appendix C: Functional Simulation

Suppose for a network with NN nodes and NB links the probability of node i failing is $p_i$ and the probability of link j failing is $p_{NN+j}$. We start with no nodes or links and generate NN+NB random numbers, divide the ith by $p_i$ for $i = 1, \ldots, NN+NB$, and sort the resulting numbers in decreasing order. This yields a non-increasing sequence $r_1, r_2, \ldots, r_{NN+NB}$. We then add the node or links corresponding to $r_1$; then the node or link corresponding to $r_2$, and so to obtain $NP_1, NP_2, \ldots, NP_{NN+NB}$ when $NP_i$ is the number of pairs communicating after the ith link or node has been added. Then for $s \geq r_1$, the sample value is 0; for $r_1 \geq s \geq r_2$, the sample value is $NP_1$; for $r_2 \geq s \geq r_3$, the sample value is $NP_2$; and so on. Adding a link in this process corresponds to one step of the algorithm described in Appendix B. Adding a node corresponds to checking to see if any of the operable links incident to the added node can be added. The entire procedure for determing the NP for all s is essentially the same as applying the algorithm for determining connectivity once to the overall network. For s=1 the node and link failure probabilities are the nominal ones $1.p$, $1.p_2$, ..., $1.p_{nn}$, ..., $1.\ p_{NN+NB}$. For s=1/2 we obtain the expected number of pairs communicating for node and link failure probabilities $(1/2)p_1$, $(1/2)p_2$, ..., $(1/2)p_{NN}$, ..., $1/2, p_{NN+NB}$. Thus the method gives a sensitivity analysis when each element failure probability is varied proportional to s. For a more extended discussion, see Reference 4.

## References


1. Frank, H., Frisch, I.T., and Chou, W., "Topological Considerations in the Design of the ARPA Computer Network," AFIPS Conference Proceedings, Vol. 36, AFIPS Press [1970], pp. 581-587.

2. Kruskal, J.B., "The Number of Simplices in a Complex," in Mathematical Optimization Techniques, ed. R. Bellman, Berkeley: University of California Press [1963], pp.251-278.

3. Seshu, S. and Reed, M.B., Linear Graphs and Electrical Networks, Addison-Wesley [1971], p.157.

4. Van Slyke, R. and Frank, H., "Network Reliability Analysis", Networks, Vol. 1, No. 2, December, 1971.

TABLE 3.1

EXACTLY KNOWN C(k) FOR
23 NODE 28 LINK ARPA NET

| Number of links Operative | Number of links Failed | Number of Nets | Number of Failed Nets | Method of Determination |
|---|---|---|---|---|
| 0 | 28 | 1 | 1 | a |
| 1 | 27 | 28 | 28 | ↑ |
| 2 | 26 | 378 | 378 | │ |
| 3 | 25 | 3276 | 3276 | │ |
| 4 | 24 | 20475 | 20475 | │ |
| 5 | 23 | 98280 | 98280 | │ |
| 6 | 22 | 376740 | 376740 | │ |
| 7 | 21 | 1184040 | 1184040 | │ |
| 8 | 20 | 3108105 | 3108105 | │ |
| 9 | 19 | 6906900 | 6906900 | │ |
| 10 | 18 | 13123110 | 13123110 | │ |
| 11 | 17 | 21474180 | 21474180 | │ |
| 12 | 16 | 30421755 | 30421755 | │ |
| 13 | 15 | 37442160 | 37442160 | │ |
| 14 | 14 | 40116600 | 40116600 | │ |
| 15 | 13 | 37442160 | 37442160 | │ |
| 16 | 12 | 30421755 | 30421755 | │ |
| 17 | 11 | 21474180 | 21474180 | │ |
| 18 | 10 | 13123110 | 13123110 | │ |
| 19 | 9 | 6906900 | 6906900 | │ |
| 20 | 8 | 3108105 | 3108105 | ↓ |
| 21 | 7 | 1184040 | 1184040 | a |
| 22 | 6 | 376740 | 349618 | b |
| 23 | 5 | 98280 | ? | |
| 24 | 4 | 20475 | ? | |
| 25 | 3 | 3276 | 827 | c |
| 26 | 2 | 378 | 30 | c |
| 27 | 1 | 28 | 0 | d |
| 28 | 0 | 1 | 0 | d |

Notes:
- a: not enough links to connect 23 nodes
- b: number of trees calculated by formula[3]
- c: enumerated
- d: less failed links than minimum cut set

TABLE 3.2

BOUNDS FOR C(k)

| Links Operating | Links Failed | Lower Bound[1] 1 Exact Term | Lower Bound[2] 2 Exact Terms | Upper Bound[3] |
|---|---|---|---|---|
| 22 | 6 | 112861 | 192737 | [349618] |
| 23 | 5 | 23645 | 42484 | 94404 |
| 24 | 4 | 3754 | 7067 | 19506 |
| 25 | 3 | 423 | [827] | 3105 |
| 26 | 2 | [30][4] | [30] | |

Notes: 1: Bounds obtained by projection using the value C(26) as known.

2: Bounds obtained by projection using the values C(26) and C(25) as known.

3: Bounds obtained using the number of trees as known.

4: Boxes indicate exact values obtained by enumeration or formula.

TABLE 3.3

RESULTS OF SAMPLING STRATA

| # Links Failed | Number of Nets | NSAMP | $\mu$ | $\sigma^2$ | $\sigma$ | Est. No. of Disc. Nets |
|---|---|---|---|---|---|---|
| 3 | 3276 | 440 | .22954 | .976 | .987 | 751.97 |
| 4 | 20475 | 145 | .45517 | 8.14 | 2.85 | 9319.60 |
| 5 | 98280 | 37 | .64864 | 44.27 | 6.65 | 63748.33 |
| 4 | 20475 | 798 | .48120 | 1.605 | 1.267 | 9852.57 |
| 5 | 98280 | 202 | .717821 | 8.64 | 2.9406 | 70547.44 |

## TABLE 3.4

### PROBABILITY FOR NETWORK BEING DISCONNECTED

### AS A FUNCTION OF THE PROBABILITY OF LINK FAILURE

| Link Failure probability | Lower Bound[1] | Lower Bound[2] | Upper Bound[1] | Estimate[3] By Sampling | Standard Deviation | Estimate[4] by Sampling | Standard Deviation |
|---|---|---|---|---|---|---|---|
| .01 | .00267 | .00301 | .00311 | .00297 | .00005 | .00303 | .0 |
| .02 | .00957 | .01188 | .01321 | .01178 | .00032 | .01221 | .00003 |
| .03 | .01945 | .02607 | .03154 | .02625 | .00089 | .02749 | .00014 |
| .04 | .03159 | .04485 | .05888 | .04613 | .00174 | .04865 | .00036 |
| .05 | .04568 | .06754 | .09523 | .07109 | .00285 | .07532 | .00072 |
| .06 | .06177 | .09361 | .13985 | .10075 | .00417 | .10704 | .00121 |
| .07 | .08160 | .12264 | .19141 | .13466 | .00566 | .14325 | .00181 |
| .08 | .10123 | .15436 | .24824 | .17230 | .00729 | .18330 | .00250 |
| .09 | .12539 | .18858 | .30848 | .21312 | .00899 | .22652 | .00324 |
| .1 | .15298 | .22511 | .37035 | .25654 | .01392 | .27220 | .00517 |
| .2 | .57609 | .64892 | .84098 | .70384 | .01603 | .72298 | .00648 |
| .3 | .90281 | .92194 | .97578 | .93931 | .00530 | .94493 | .00214 |
| .4 | .98984 | .99184 | .99755 | .99382 | .00063 | .99445 | .00025 |
| .5 | .99954 | .99963 | .99987 | .99971 | .00002 | .99974 | .00001 |
| .6 | .99999 | .99999 | .99999 | .99999 | .0 | .99999 | .0 |

Notes:
1: Projections were used for 3, 4, and 5 links failing.
2: Projections were used for 4 and 5 links failing.
3: Estimates used for 3, 4, and 5 links failing.
4: Estimates used for 4 and 5 links failing.

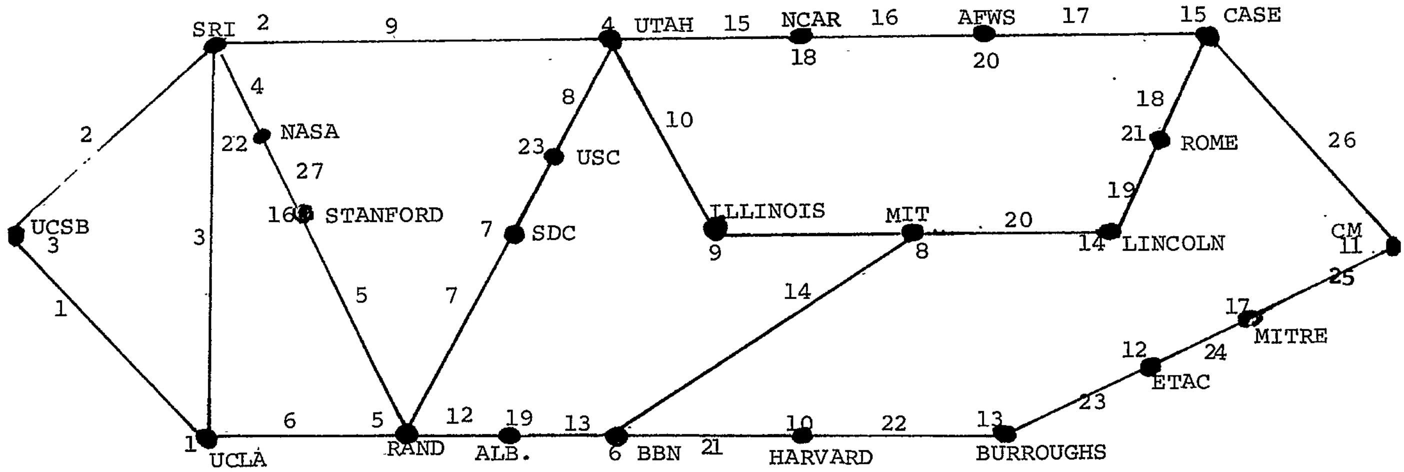
## TABLE 3.5.

### COMPARISON OF TWO DIFFERENT SIMULATION METHODS

### Sample Size 1000

| Link Failure Probability | Probability of Disconnected Net: Stratified Sampling | Probability of Disconnected Net: Straightforward Sampling | Standard Deviation: Stratified | Standard Deviation: Straightforward |
|---|---|---|---|---|
| .01 | .00297 | .004 | $5.15 \times 10^{-5}$ | $1.99 \times 10^{-3}$ |
| .02 | .01178 | .012 | $3.28 \times 10^{-4}$ | $3.44 \times 10^{-3}$ |
| .03 | .02625 | .027 | $8.96 \times 10^{-4}$ | $5.12 \times 10^{-3}$ |
| .04 | .04613 | .042 | $1.74 \times 10^{-3}$ | $6.34 \times 10^{-3}$ |
| .05 | .07109 | .070 | $2.85 \times 10^{-3}$ | $8.06 \times 10^{-3}$ |
| .06 | .10075 | .097 | $4.17 \times 10^{-3}$ | $9.35 \times 10^{-3}$ |
| .07 | .13466 | .135 | $5.66 \times 10^{-3}$ | $1.08 \times 10^{-2}$ |
| .08 | .17230 | .178 | $7.29 \times 10^{-3}$ | $1.20 \times 10^{-2}$ |
| .09 | .21312 | .224 | $8.99 \times 10^{-3}$ | $1.31 \times 10^{-2}$ |
| .1 | .25654 | .276 | $1.07 \times 10^{-2}$ | $1.41 \times 10^{-2}$ |
| .2 | .70384 | .743 | $1.60 \times 10^{-2}$ | $1.38 \times 10^{-2}$ |
| .3 | .93931 | .954 | $5.30 \times 10^{-3}$ | $6.62 \times 10^{-3}$ |
| .4 | .99382 | .995 | $6.32 \times 10^{-4}$ | $2.23 \times 10^{-3}$ |
| .5 | .99971 | .999 | $2.89 \times 10^{-5}$ | $1. \times 10^{-3}$ |
| .6 | .99999 | 1.000 | $4.23 \times 10^{-7}$ | 0 |

23 Node Net




BASE NETWORK FOR RELIABILITY ANALYSIS

FIGURE 1.1

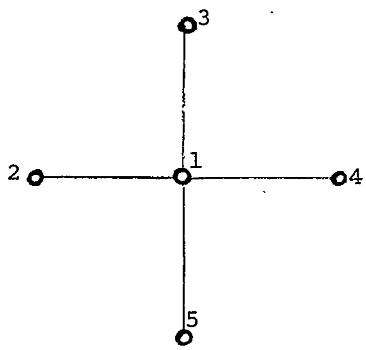



FIGURE 2.1

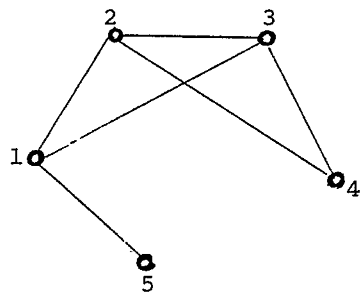
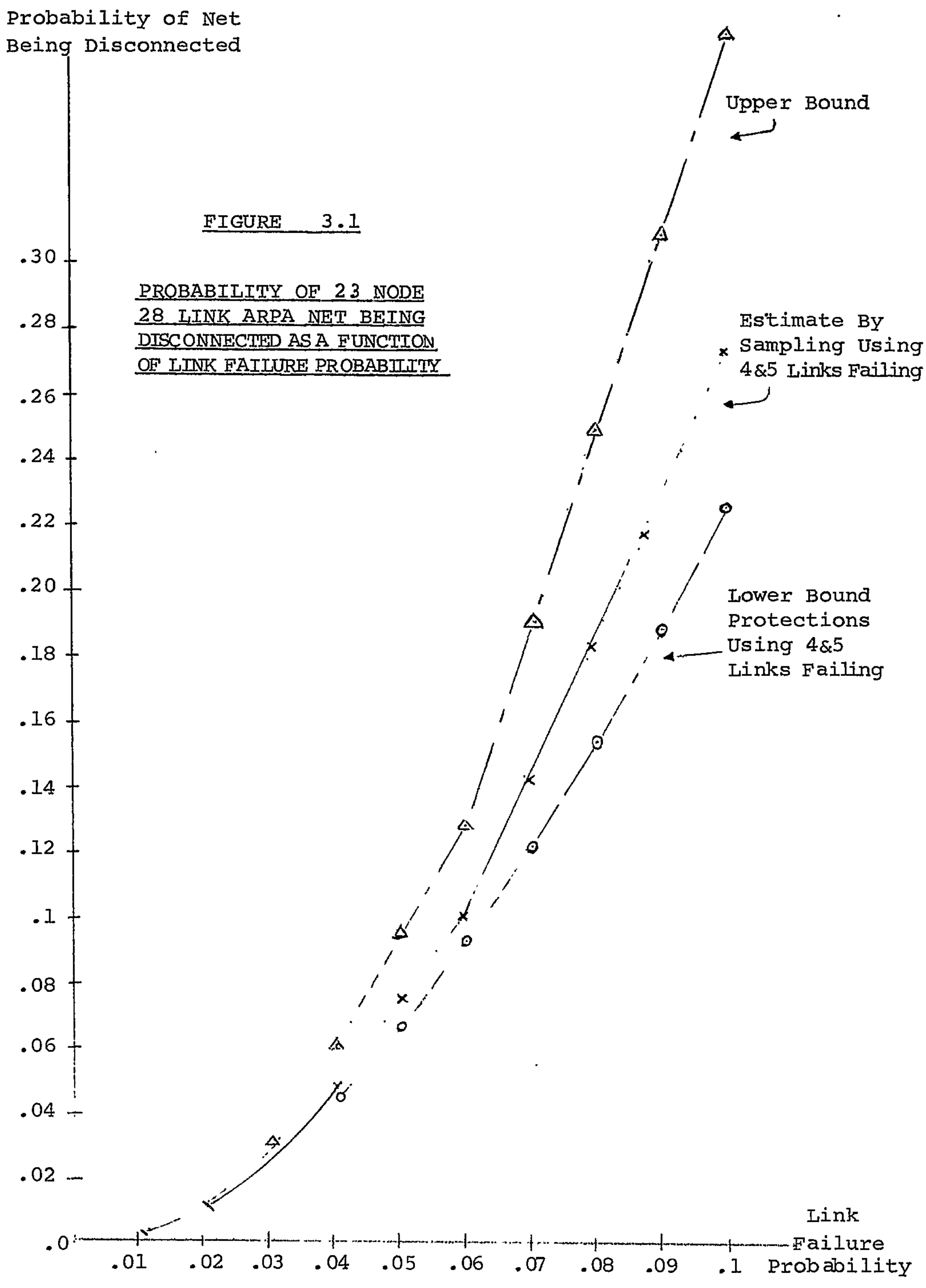



FIGURE 2.2



Probability of Net
Being Disconnected
FIGURE 3.1
PROBABILITY OF 23 NODE
28 LINK ARPA NET BEING
DISCONNECTED AS A FUNCTION
OF LINK FAILURE PROBABILITY
Upper Bound
Estimate By
Sampling Using
4&5 Links Failing
Lower Bound
Protections
Using 4&5
Links Failing
.30
.28
.26
.24
.22
.20
.18
.16
.14
.12
.1
.08
.06
.04
.02
.0
.01
.02
.03
.04
.05
.06
.07
.08
.09
.1
Link
Failure
Probability

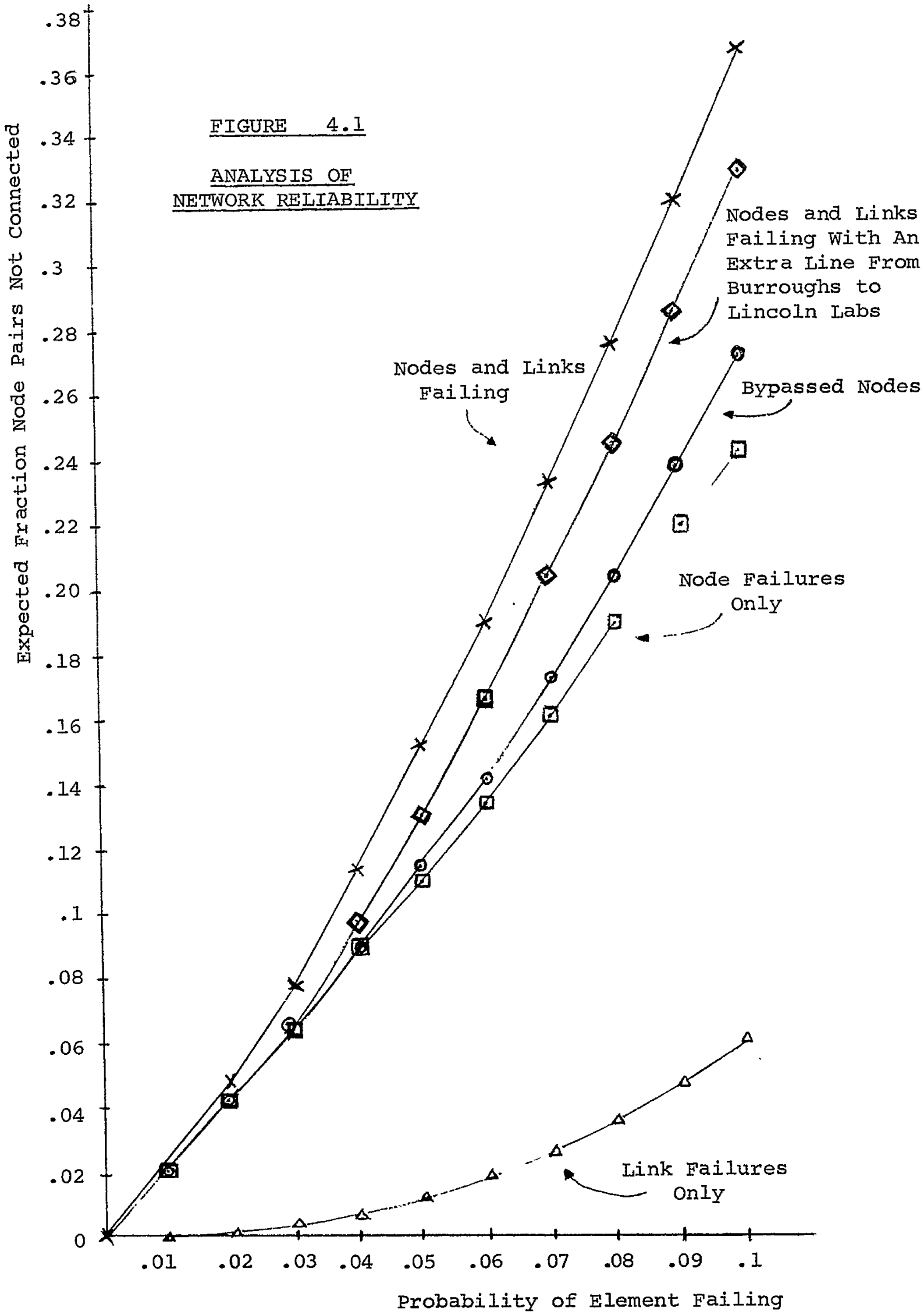
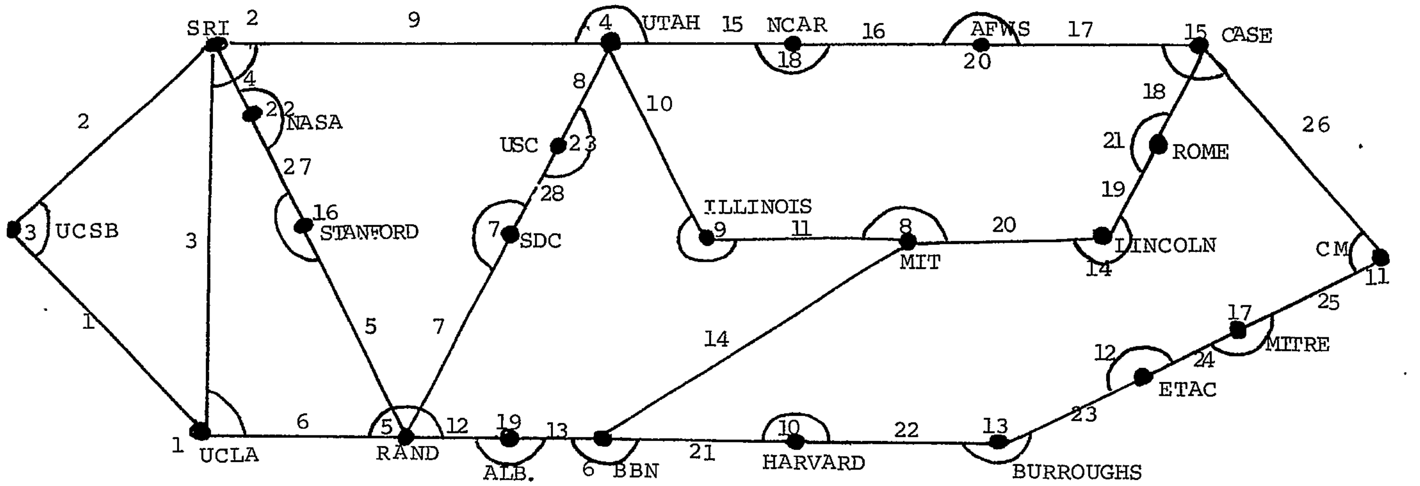


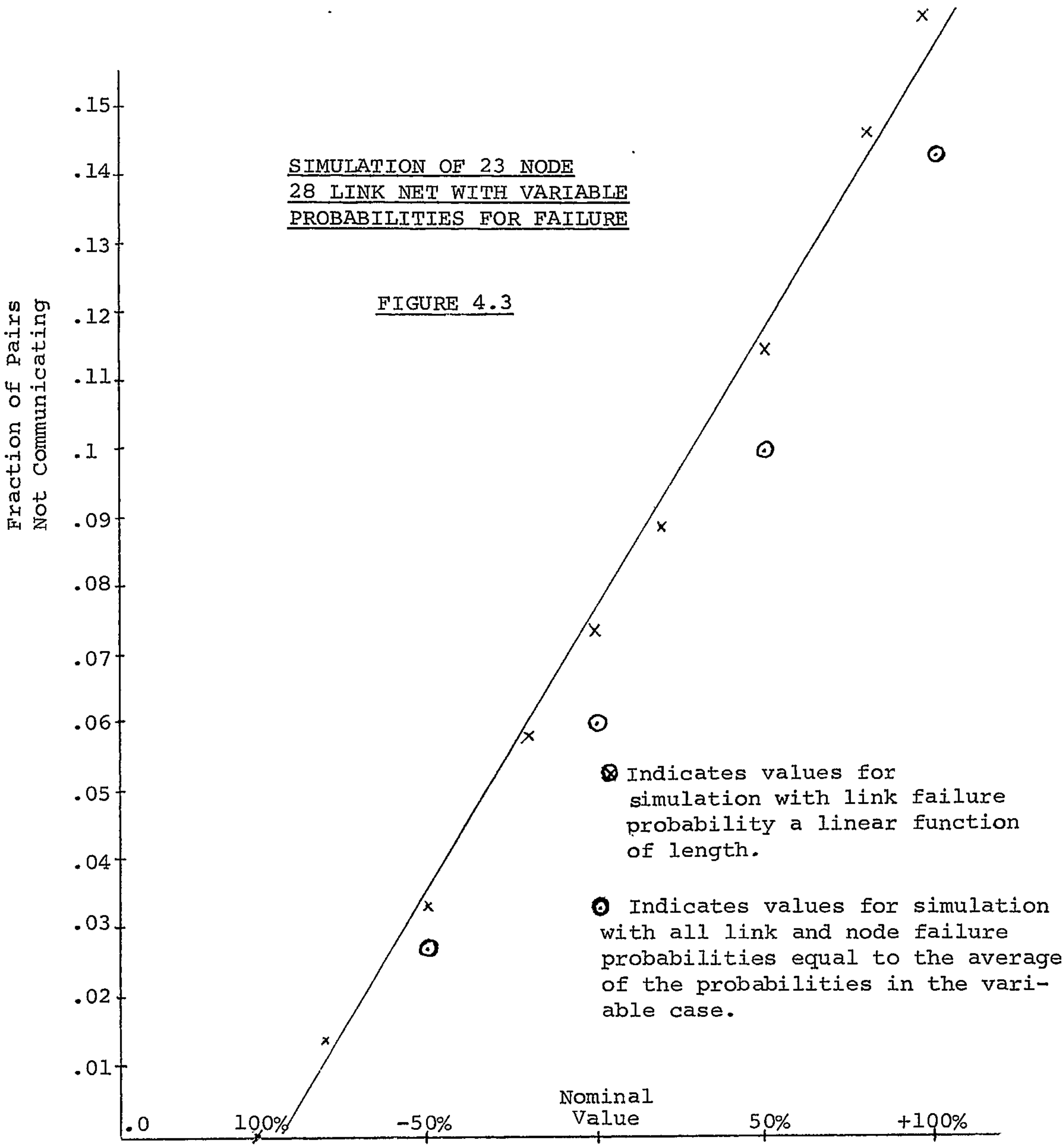
FIGURE 4.1
ANALYSIS OF
NETWORK RELIABILITY
Expected Fraction Node Pairs Not Connected
.38
.36
.34
.32
.3
.28
.26
.24
.22
.20
.18
.16
.14
.12
.1
.08
.06
.04
.02
0
.01
.02
.03
.04
.05
.06
.07
.08
.09
.1
Probability of Element Failing
Nodes and Links Failing With An Extra Line From Burroughs to Lincoln Labs
Nodes and Links Failing
Bypassed Nodes
Node Failures Only
Link Failures Only




Note: = Bypass

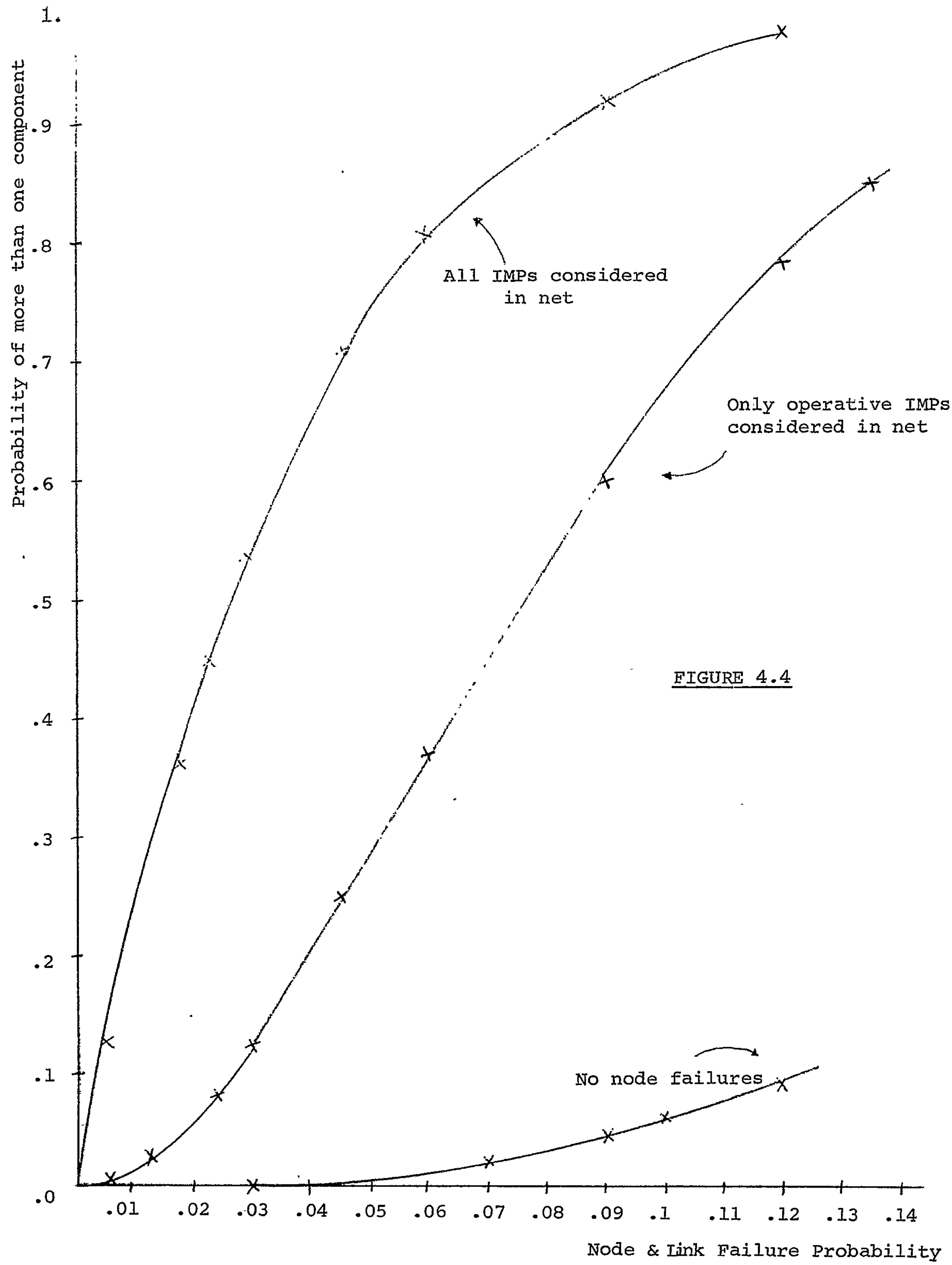
23 NODE NETWORK WITH BYPASSES

FIGURE 4.2




SIMULATION OF 23 NODE
28 LINK NET WITH VARIABLE
PROBABILITIES FOR FAILURE

FIGURE 4.3



1.
.9
.8
.7
.6
.5
.4
.3
.2
.1
.0
Probability of more than one component
All IMPs considered in net
Only operative IMPs considered in net
No node failures
.01 .02 .03 .04 .05 .06 .07 .08 .09 .1 .11 .12 .13 .14
Node & Link Failure Probability


FIGURE 4.4