RELIABLE DIGITAL COMMUNICATIONS SYSTEMS USING UNRELIABLE NETWORK REPEATER NODES

Paul Baran
Mathematics Division
The RAND Corporation

P-1995

May 27, 1960

Reproduced by

The RAND Corporation • Santa Monica • California

The views expressed in this paper are not necessarily those of the Corporation

SUMMARY

A communications network that utilizes a moderate degree of redundancy to provide high immunity from the deleterious effects of damage of relay centers is described. The degree of redundancy needed is shown to be determined primarily by the amount of damage expected. Curves indicating the optimum degree of redundancy are shown and the distribution of performance under different damage patterns described. The redundancy desired is shown to vary as a function of the station position in the network, the stations at the fringe of the network requiring more redundancy than the inside stations.

ACKNOWLEDGMENT

I would like to acknowledge the contribution of Miss Sharla Perrine in programming the Monte Carlo simulation. I am still amazed by the rapidity with which she wrote and debugged the program.

Although all the work in this paper has been performed at The RAND Corporation, the work described in the following two papers was done while this writer was employed by the Hughes Aircraft Co. The aid of Dr. Marvin Adelson, Mr. William Walters and Dr. A. Victor Stern of Hughes Aircraft in encouraging me to describe the work done there is acknowledged, as is the permission and encouragement received from Mr. Keith Uncapher, Dr. Willis Ware and Mr. Robert Belzer of the RAND Corporation to write this and the following two papers.

RELIABLE DIGITAL COMMUNICATIONS SYSTEMS UTILIZING UNRELIABLE NETWORK REPEATER NODES

INTRODUCTION

The cloud-of-doom attitude that nuclear war spells the end of the earth is slowly lifting from the minds of the many. Better quantitative estimates of post-attack destruction together with a less emotional discussion of the alternatives may mark the end of the "what the hell--what's the use?" era. A new view emerges: the possibility of a war exists but there is much that can be done to minimize the consequences.

If war does not mean the end of the earth in a black and white manner, then it follows that we should do those things that make the shade of grey as light as possible: to plan now to minimize potential destruction and to do all those things necessary to permit the survivors of the holocaust to shuck their ashes and reconstruct the economy swiftly.

PURPOSE

This paper and the following two papers* are directed toward the communications systems designer in the hope that he will not neglect these problems of survival in the design of his future systems. Unfortunately, no panacea can be presented.

*F. Yates and P. Baran, A Non Synchronous Digital Data Link Transmission System Using Randomly Surviving Relay Points, P-1996.

*P. Baran, A Verified Point of Origin Synchronous Digital Data Link Transmission System Using Randomly Surviving Relay Points, P-1997.

There is none. Only a single limited technique is described, that of using one form of distributed redundancy to minimize vulnerability. A detailed examination demonstrates that the problem is not an unsolvable one, but that much money and much work are necessary to provide all the elements needed for the true solution to the vulnerability problem.

The timing for such thinking is particularly appropriate now, for we are just beginning to design and lay out designs for the digital data transmission systems of the future. We are just approaching the initiation state of the designs of systems where computers speak to one another. When this day comes, the digital communications system capacity needed will be orders of magnitude greater than our chief present-day digital transmission technique; namely, teletype. For example, a 60 WPM teletype channel would take about two weeks, operating 24 hours per day without breakdown, to transmit a single standard size reel of.magnetic tape used on a digital computer. This may be compared to a writing time of about 6 minutes on the computer.

Millimicrosecond clock rate data links will be needed in the future. Our present communications plant will not suffice. As there does not seem to be any fundamental technical problem that prohibits the operation of digital communications links at the clock rate of digital computers, the view is taken that it is only a matter of time before such design requirements become hardware. The systems designs of the next few years will be the systems-in-being of the next few decades. It is hoped that these systems will be foresighted enough to include an insurance policy purchasing invulnerability.

CONTENTS

This first paper of this series describes a rationale for the use of redundancy in networks and the payoff for varying degrees of such redundancy.

The second paper, by Frank Yates and Paul Baran, describes a high speed automatic switching technique for digital messages. In this paper the time of arrival of messages is used to determine the shortest routing paths over a severely damaged network.

The third paper, by Paul Baran and Robert Hamerly, describes a lower speed digital system using a tag containing the number of times a message has been relayed to provide a method for authenticating point of origin.

These two separate systems exhibit different properties; it is possible to multiplex them together to utilize the advantages of both and devise a third system. It is thus possible to visualize a new set of systems based upon a distributed organization.

Automatic route selection is not new, but these papers seek as a common goal synthesis of systems where the intelligence required to switch signals to surviving links is at the link nodes and not at one or a few centralized switching centers. This paper thus describes what we choose to call distributed organization as compared to the more familiar centralized switching center type organization.

The problem of physical protection of the nodes and links of systems is avoided in these papers, and it is assumed that all that can be done economically to harden communications has already been done. Again it must be emphasized, this is not a cure-all.

These three papers are intended only to encourage thinking on methods for utilizing redundancy to reduce system vulnerability.

UTILIZING REDUNDANCY IN SYSTEM DESIGNS

The use of redundancy in systems design is not new.

For example, if one wanted to be more reasonably sure of not missing "Maverick" on television, he might buy a second TV set. The probability of both sets being inoperative simultaneously is p^2, where p is the probability of either statistically independent television set being inoperative at any one time. If p is about 0.001, then both sets would be inoperative only about 0.000001 of the time. With a few more television sets, one can make the probability of missing "Maverick" arbitrarily small. This form of system redundancy requires a modicum of intelligence somewhere within the system. One can only look at one television set at one time, therefore one must have some way of knowing which set has failed. With a TV set, the problem is simple; the human operator is intelligent enough to determine failure and agile enough to look at the operative set. If a designer wished to build a bank of inductance-capacitance oscillator circuits each with redundant elements, he faces a more difficult decision. He could not, for example, leave a redundant capacitor permanently connected in each circuit, for it would lower the frequency of oscillation. He must, therefore, wait until the instant of failure occurs and then replace the defective element. Again intelligence is required to determine _where_ failure has occurred. Thus, the beautifully simple concept of pure parallel redundancy is limited in its utility.

This requirement for intelligence is the bugaboo to the use of simple parallel redundancy. It takes some logic to determine what has failed, and it takes switching means to connect the new elements.

There has been some excellent work performed during the last two decades on designing networks capable of performing logical or computational functions using redundant elements where the redundant elements are permanently connected in the network. In these circuits, switching and logic are combined. Unfortunately, such networks are characterized by the requirement of horrendous redundancy before extremely reliable operation results. Examples of such systems include the work of von Neumann* who describes the use of redundancy when using fallible Sheffer Stroke logic elements to produce computational systems of any arbitrary degree of reliability (provided the degree of redundancy is sufficient).

*von Neumann, J., "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components" in _Automata Studies_, edited by C. E. Shannon and J. McCarthy, Princeton University Press, Princeton, N. J., 1956.

Shannon and Moore* describe the use of redundant relay contacts and circuits to provide arbitrary increase of system reliability to provide a desired degree of reliability from a single input to a single output.

McCulloch** describes the design of neural networks using majority logic type elements to build computational circuits that are less sensitive to variations of threshold than conventional minimum number-of-component circuits. This performance is accomplished by the utilization of redundancy of neuron-like elements.

These three foundation papers all seek the same goal--reaching desired systems reliabilities using "realistic" components.

The present paper considers a different problem: the more modest task of maintaining reliable multilateral communications within a network connecting N separate points with each other, where the failure rate of the nodes, f, is arbitrarily high. Successful system operation is defined when a certain percentage or fraction of the communicators are able to maintain conversation with one another. Such a system makes itself content with

*E. F. Moore and C. E. Shannon, "Reliable Circuits Using Less Reliable Relays," Journal of the Franklin Institute, Vol. 262, Sept., 1956, pp. 191-208; Oct., 1956, pp. 281-297.

**W. S. McCulloch, "Infallible Nets of Fallible Formal Neurons," Massachusetts Institute of Technology, Research Laboratory for Electronics, Quarterly Progress Report, No. 53, April 15, 1959.

the <u>assured</u> operation of a certain fraction of the network. Such a system will not die upon the failure of a single element, but decay to a reduced level of performance.

The use of redundancy in the system to be described will be of the form of separate failure detection logic and separate switching and is more akin to the bypassing of defective elements technique rather than those organically combining correction integrally with logic.

To better visualize the operation of the network, a hypothetical application is postulated: a congressional communications system where each congressman may vote from his home office. The success of such a network may be evaluated by examining the number of congressmen surviving an attack and comparing such number to the number of congressmen able to communicate with one another and vote via the communications network. Such an example is, of course, farfetched but not completely without utility. Such a system would do much to help preserve our democratic institutions after a possible nuclear attack.

As a model system designed to fit the application, consider a generalized system of identical digital transmission-reception stations interconnected to form a network. Of interest is the greatest number of such stations or home offices of Congressmen that are theoretically capable of being in communication with one another under different degrees of interconnection redundancy and attack levels. "Theoretically capable," implies the temporary assignment of omnipotent intelligence to each node to relay signals. Those stations interconnected by links to other intact stations are said to be theoretically capable of communicating with one another. The implementation of such required intelligence nodes is described in detail in papers number two and three.

Figure 1 shows part of an infinite matrix of nodes arranged in a network formed using a minimum number of interconnecting links, one link per node. The redundancy of such a network is unity.

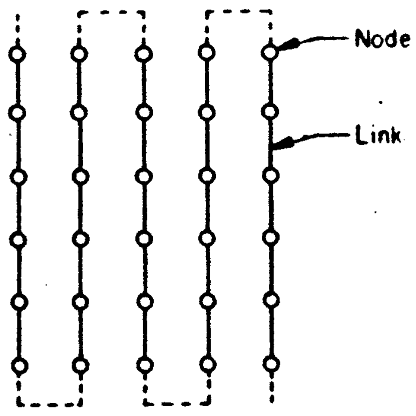
To examine the invulnerability properties of various forms of distributed networks, the system model used has the following properties:

1. Each link has the bandwidth to transmit the full traffic of the over-all system, if needed.
2. The communications link cost is a constant cost per link, (for example, microwave), as opposed to telephone cable, which exhibits a constant cost per unit length. This constant link cost assumption provides freedom

for the analyst to map all stations in a convenient matrix form.

3. Rapid human intervention to repair the system and establish emergency communications patches is assumed to be impossible.
4. Each station is fully equivalent to all others, and no station carries a higher destruction premium than any other node. Hierarchical or branched tree form communications networks do have such premium target stations and so are not examined.
5. An 18 X 18 array or a total of 324 interconnected stations is used as a digital simulation model.

Figure 1 shows an example of an absolutely minimum redundancy system where redundancy is defined to be the ratio of links, L, to nodes, N.



REDUNDANCY = 1

Figure 1

In this example, an 18 X 18 matrix is considered. An absolute minimum redundancy system is sought.

$$R = \frac{323}{324} \text{ or } \simeq 1$$

Figure 1 thus represents a minimum redundancy network, where $R \simeq 1$, and there are no premium nodes.

In this illustration, there is just a sufficient number of paths necessary to interconnect all the stations or nodes without spares. Failure of a single link breaks the network into two pieces. Failure of several links breaks the network into as many as n+1 pieces where n is the number of fractured links. Although this is the most economical configuration with perfectly reliable links, it is not a practical design because of the high probability of failure of at least one of m stations. The probability of such failure is $1-(1-p)^m$ where p is the probability of destruction of a single station, and m is the number of stations. Thus, if the value of p or m, particularly m, is high then the network is certain to be cut.

Figure 2 solves this temporary problem by adding cross links. Here the redundancy has been increased to 1.5.

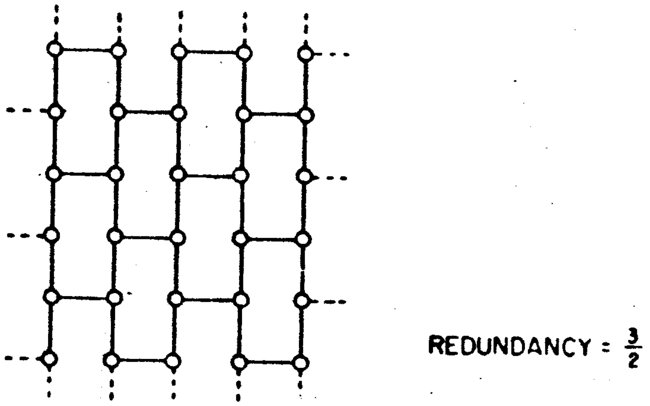


Figure 2

Figures 3, 4, and 5 show other redundant configurations with values of redundancy of 2, 3 and 4 respectively.

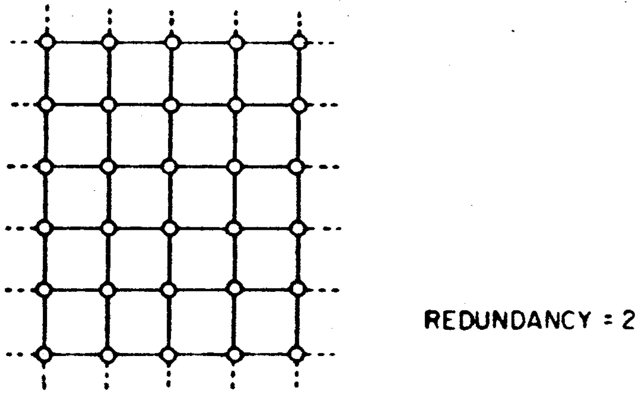


Figure 3

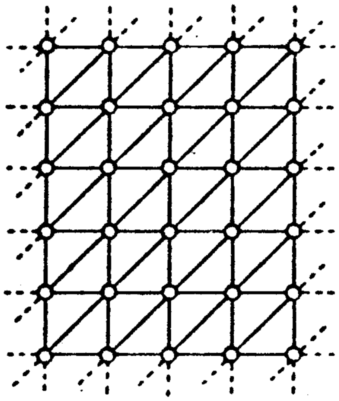


Figure 4

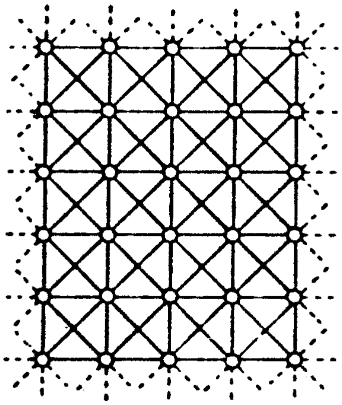


Figure 5

Figure 6 examines a small piece broken out of Figure 3, a redundancy-of-2 type network. This illustrates a central station speaking to its four adjacent stations and shows that the central station receives four potentially different messages at a time, T, while it transmits a common output message at some time later than time T.

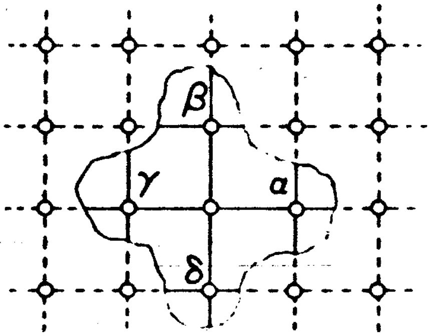


Figure 6

This may be better visualized by reference to Figure 7.

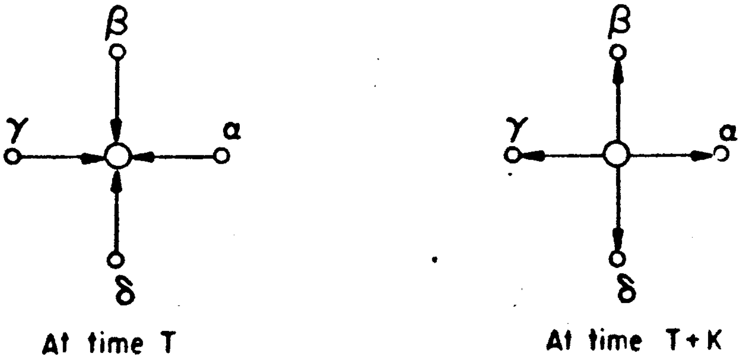


Figure 7

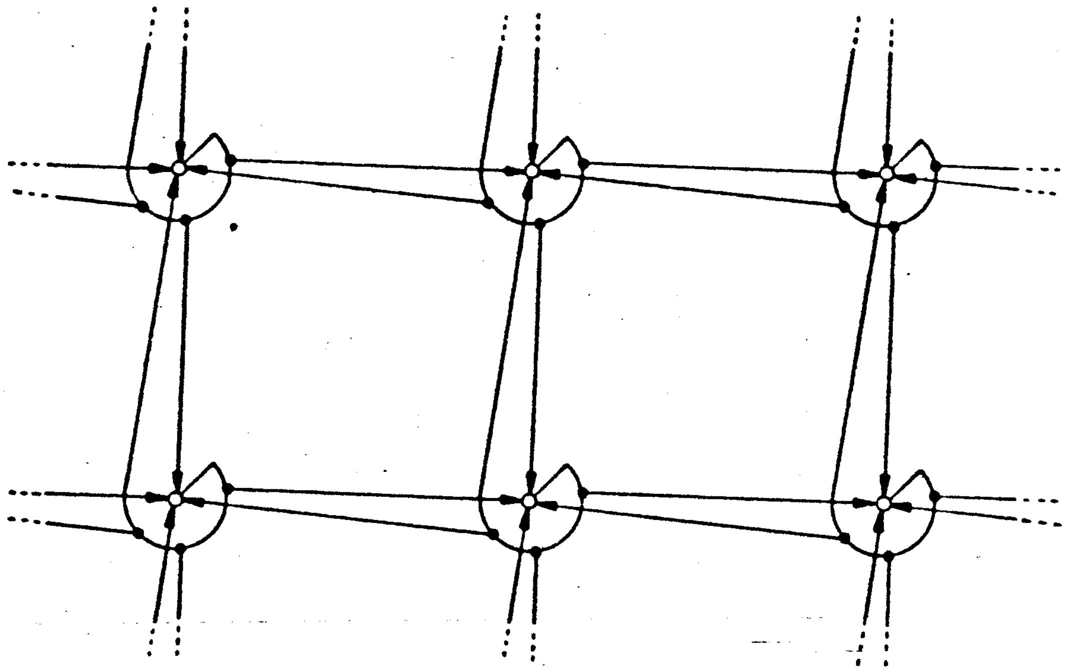


Figure 8

Figure 8 shows the identical elements connected in matrix fashion, where the input and output times are not differentiated. It is interesting to note that such a distributed interconnection, at least spatially, resembles those models often associated with neural networks. Such networks have been generated in an attempt to explain the extremely reliable behaviour of biological organisms using unreliable components.

Although such an analysis here is somewhat strained, it is interesting to note a common property of this network and a desired property of neural networks. In spite of high damage levels, the bulk of the surviving nodes are interconnected with one another, and only a small number of the surviving nodes are isolated into islands.

RESULTS OF THE DIGITAL SIMULATION

In digital simulation of the performance of this network, damage patterns were examined and found to exhibit this necessary "single long string" survival pattern. This was found to be particularly true at moderate damage levels, and as expected, is a function of the degree of redundancy of the network.

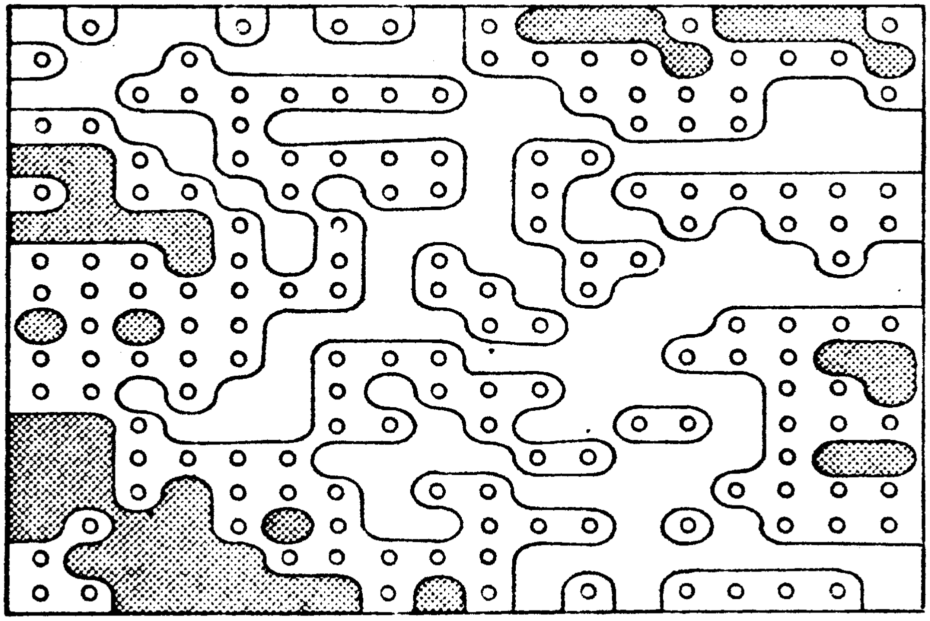
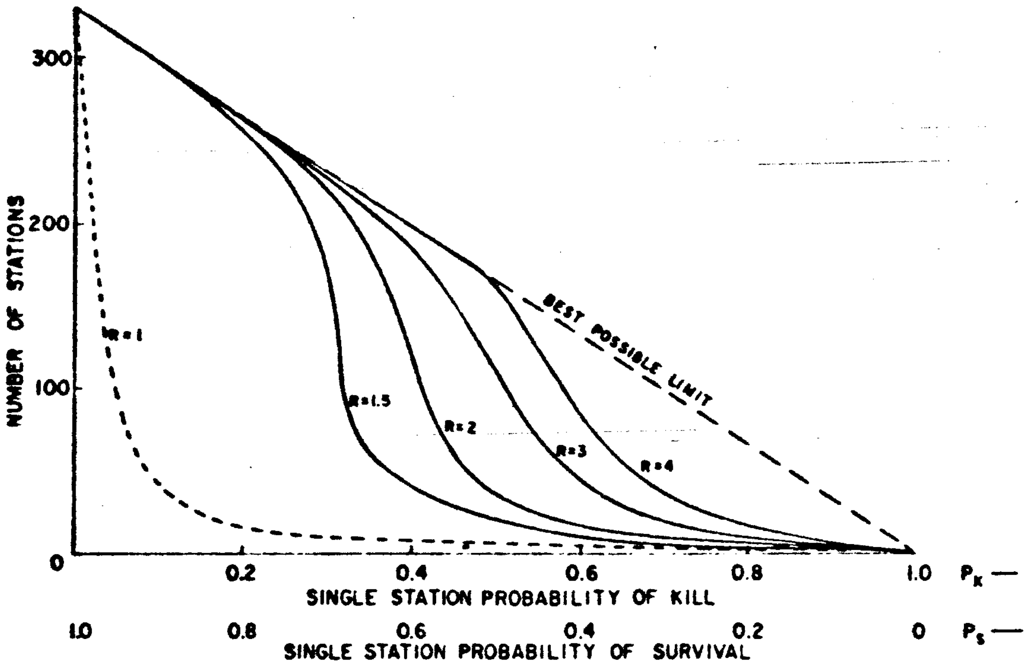


Figure 9

Figure 9 shows a matrix of 18 X 18 stations after an attack where a random 50 per cent of the stations were destroyed. The circles represent the destroyed stations, while the shaded area encloses surviving stations. The surviving stations form clusters that are capable of speaking to members of that group only. The largest such group of surviving stations is shown in single crosshatched pattern while the smaller size groups are shown by double crosshatching.

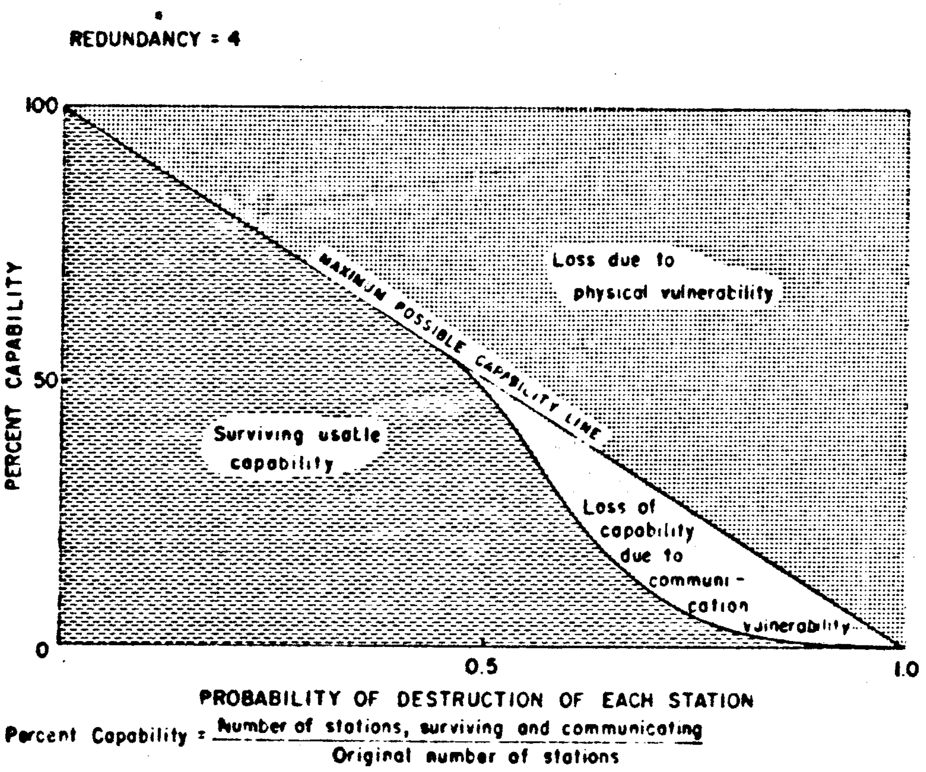
Figure 10 shows the number of stations in communications with one another as a function of the single station probability of destruction or survival. Mere physical survival is, of course, insufficient--contact must be maintained with the bulk of the other surviving stations. Figure 10 is drawn for the values of redundancy of 1, 1.5, 2, 3, and 4. The line labeled "Best Possible Limit" represents the maximum possible number of stations that can be interconnected. This line merely shows that the number of stations in contact with one another cannot exceed the number of undamaged stations.

Figures 11 and 12 should be examined together as a pair. Figure 11 shows surviving capability of a redundancy-of-one network while Figure 12 shows surviving capability of a redundancy-of-four network. The cross-shaded areas delineate the loss of capability due to communications vulnerability alone. Returning to Figure 10, it can be seen that the optimum degree of redundancy required is a function of the expected individual station probability of destruction. For example, if a probability of destruction of 0.2 is expected, a redundancy of about 1.5 is all that is required. If, on the other hand, a probability of destruction of 0.5 is expected, then a redundancy-of-



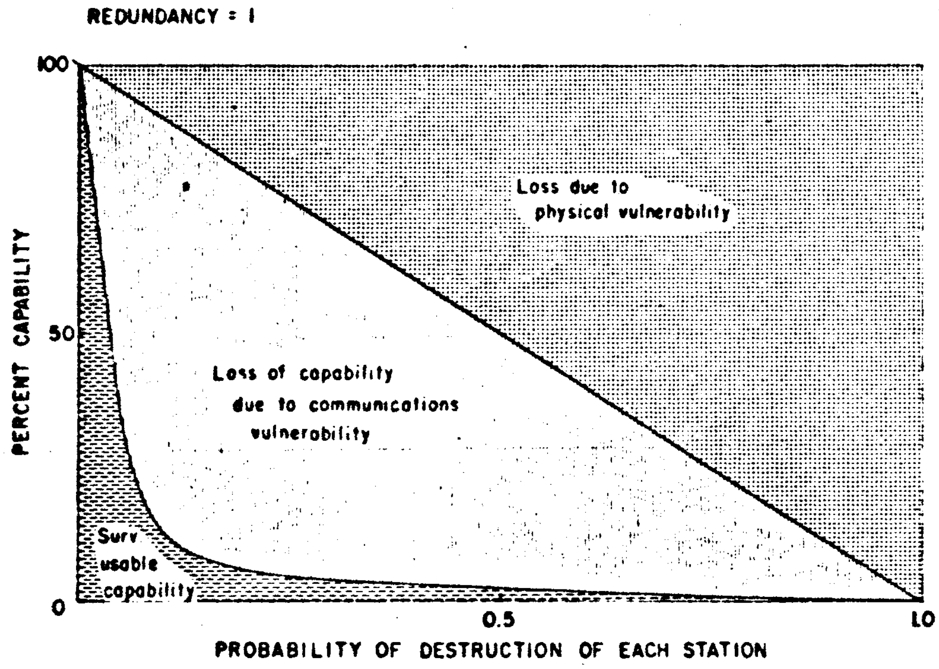
Number of stations in communication with one another as a function of individual station probability of destruction or survival.

Figure 10



Surviving capability as a function of probability of destruction, high redundancy example

Figure 11



Surviving capability as a function of probability of destruction, low redundancy example.

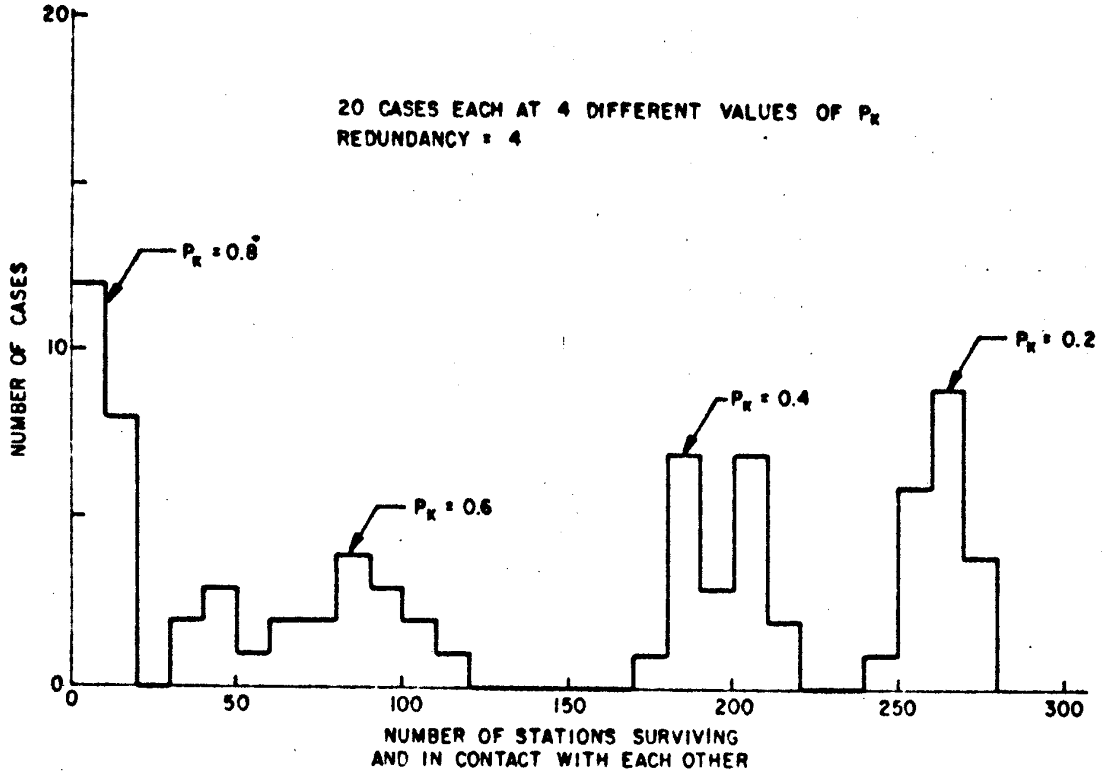
Figure 12

four is indicated. The mechanism of the payoff due to redundancy can be visualized by reference to Figure 9. Figure 9 used a network redundancy-of-three. The redundancy-of-three configurations did not include the upper left to lower right connections present when a redundancy of four is used. Adding such additional elements to change Figure 9 into a redundancy-of-four networks can be seen to link 35 of the presently isolated 41 nodes to the major portion of the system.

Expectancy alone is not a complete measure of the invulnerability of a system. For example, it is preferable to have a system retaining 50 per cent of its capability 100 per cent of time rather than a second system retaining 100 per cent of its capability 50 per cent of the time and 0 per cent of its capability 50 per cent of the time. Both systems exhibit the same expectancy, yet their performance is entirely different.

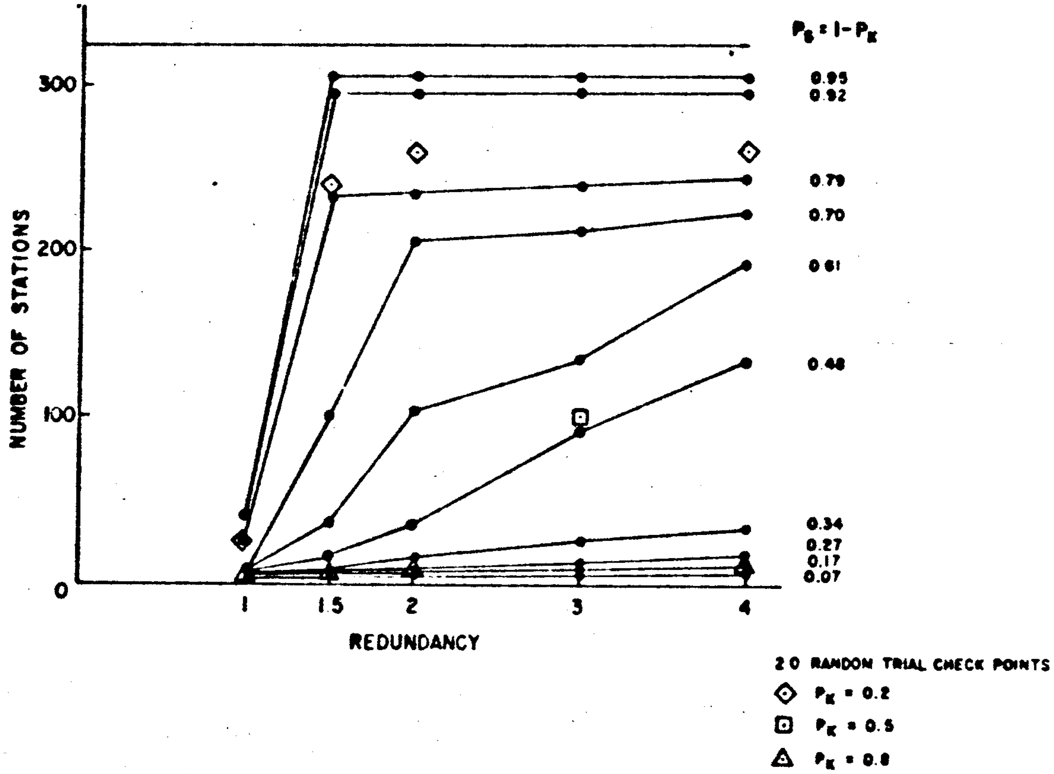
Figure 13 shows the distribution of 80 such separate trials to determine the distribution of system response under various levels of applied destruction. Twenty separate cases with a single station probabilities of kill of 0.2, 0.4, 0.6, and 0.8 were examined. These curves demonstrate that the greatest uncertainty of outcome occurs near the 0.5 probability of damage point since this damage level permits the greatest uncertainty of connection.

Figure 14 shows the number of stations in communication with one another as a function of communications redundancy. In Figure 14, the damage pattern was kept constant using several



Distribution of number of trial cases of stations surviving and in contact with one another

Figure 13

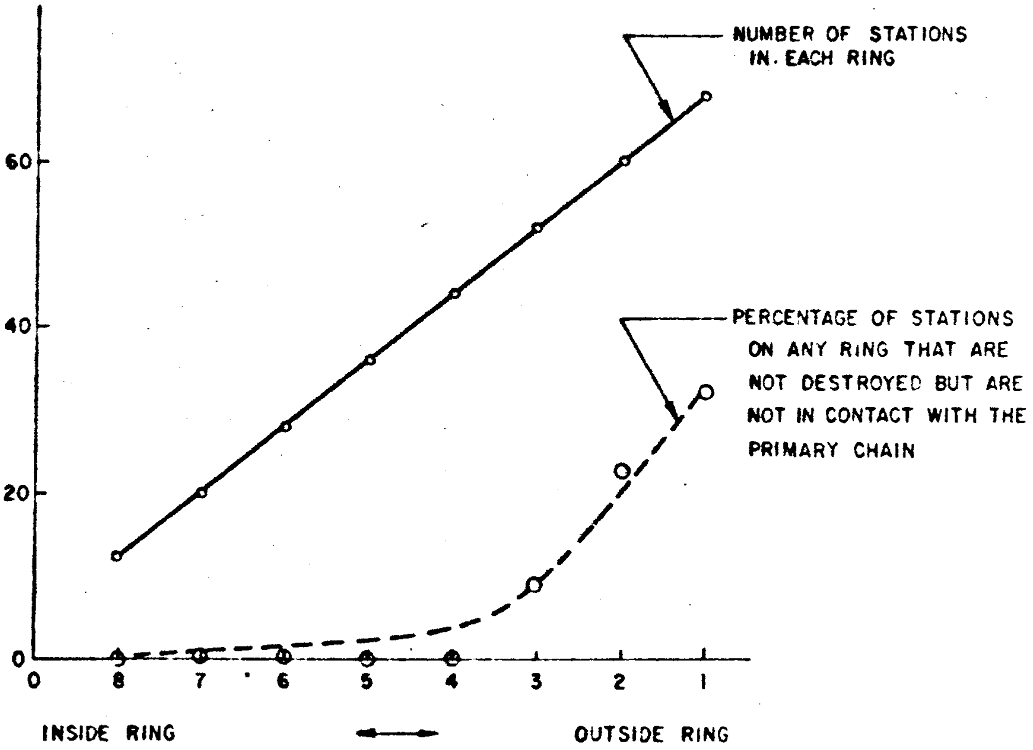


Number of stations in communication with one another as a function of communication redundancy.

Figure 14

different values of P_k, the single station probability of destruction, while the redundancy was varied. These curves provide an alternate method of viewing the optimum degree of redundancy for any given expected damage level. Several critical points on the curve were checked by a large number of runs, and these are shown as small squares and triangles. These points confirm the general validity of the limited number of cases used to generate these curves.

Figure 15 quantatively examines the phenomenon exhibited in Figure 9 in which most of the non-connected stations are found on the periphery of the matrix. This result is caused by the number of probable connections being lower for those stations on the outside fringe. The matrix of Figure 9 is decomposed into 8 concentric rings. All stations on the outside fringe are said to be on ring 1, while all those on the next inner ring are said to be on ring 2, etc. The solid line of Figure 15 indicates the number of stations in each ring, while the dotted line shows the percentage of stations that are on each that would be operable provided that they were connected to the remainder of the other operable stations. This curve demonstrates that a higher degree of redundancy is desirable at the outside edge of distributed networks than needed in the interior. Hence, even better system performance may result by a more judicious apportionment of the redundancy level.



Survivability as a function of station's distance to the outside of matrix. (Single example)

Figure 15