Networks Immune to Isolated Failures*

Arthur M. Farley
University of Oregon, Eugene, Oregon 97403

The notion of isolated failure immune (IFI) networks is introduced. A network is an IFI network if and only if all message transfers between operating sites can be completed as long as all site and line failures are isolated. Failures occurring at any time are isolated if they are pairwise isolated. A pair of site failures is isolated if the down sites are not neighbors. A pair of line failures is isolated if the lines are not incident to a common site. A site and a line failure are isolated if the down line is not incident to a neighbor of the down site. We show that 2-trees are minimum IFI networks. An algorithm is described which adds lines to an arbitrary tree network to produce an IFI network (a 2-tree). The algorithm also determines routing tables which allow a simple calling protocol to complete all message transfers between operative sites under isolated failures. Specializations and generalizations of our notion of IFI networks are discussed and issues for future research are proposed.

I. INTRODUCTION

We model a communication network by a graph $G = (V, E)$ consisting of a set V of vertices, or *communication sites*, and a set E of edges, or *communication lines*. Each line (u, v) connects a pair of sites u and v. Information is disseminated within such networks in the form of *messages*. Each message has a *sender* and a *receiver* (or set of receivers). Messages are transmitted by *calls* which are placed between directly connected (i.e., *neighbor*) sites over lines of the network. We assume that a call consists of message transmission and an associated verification protocol. As such, a call may succeed or fail.

Messages are transferred between distant (i.e., nonneighboring) sites by being forwarded along a path of lines in the network which connects the sending and receiving sites (i.e, by the store and forward method). The routing of messages is an important activity in such communication networks. *Message routing* refers to the process of determining a path or part of a path between two sites of a network. We assume that message routing is based upon *routing tables*, one located at each site. A site's routing table contains entries indicating which neighbor that site is to call for each other site as message receiver.

Every effective communication network is connected. A *connected network* con-

*This work was supported in part by the National Science Foundation under grant ENG-79-02960.

CCC 0028-3045/81/030255-14$01.40

tains at least one path between every pair of distinct vertices. A *tree network* is a connected, acyclic network. It has certain advantages when selected as the architecture (or topology) for a communication network. A tree network requires only $|V| - 1$ communication lines, which is the fewest lines possible in a connected network. Furthermore, one and only one path exists between any two sites. This can simplify the construction and maintenance of routing tables within the network. Tree networks are also advantageous for routing messages during the information dissemination process known as *broadcasting*. In broadcasting, one site is sender of a message which is to be transferred to all other sites as receivers. When broadcasting in a tree network, a site receiving the message simply calls all other sites to which it is connected. This completes broadcasting after only $|V| - 1$ calls, which is the minimum number required. Such a "flooding" procedure in more general network architectures can lead to much redundant calling and the attendant degradation of network performance.

Other properties of tree networks are not advantageous for communications applications. Traffic bottlenecks can develop, with no alternate routes being available for any message transfer. The most unfortunate characteristic of tree networks is their relatively high vulnerability to network failures. We assume two types of network failure are possible—an inoperative communication line and a down (i.e., inoperative) communication site. The first will be referred to as a *line failure* and the second as a *site failure*. A call attempted over an inoperative line or to a down site fails, without indication of which type of failure is the cause. Properties and levels of *network reliability* reflect a given network's ability to overcome network failures by still completing message transfer requests between sites which are not down. A network is *immune* to a set of failures iff all message transfers between operative sites can be completed though such failures exist (i.e., the operative sites remain connected).

Tree networks are not highly immune. An inoperative line or a down site disconnects a tree network at that point. This disables all information dissemination requests requiring message transfer between the two disconnected components. To improve the reliability of a tree network, additional lines must be added. Of course, the resultant network will not be a tree. The additional lines must provide the redundancy necessary to overcome network failures. One obvious way to add redundancy would be to duplicate the lines of a given tree, as shown in Figure 1. This is a relatively cheap method, the additional number of lines required being only $|V| - 1$, which is linearly related to the number of sites. The resultant network maintains the agreeable routing characteristics of trees. Furthermore, as long as both lines of a pair do not fail simultaneously (which we may consider quite unlikely), the resultant network can overcome line failures. However, the network is still vulnerable to site failures at interior (nonleaf) sites. Thus, this solution to a tree network's reliability problem is not entirely satisfactory.

If we consider the concurrent occurrence of network failures within local neighborhoods of a network to be relatively unlikely, the following reliability property becomes attractive. A network is an *isolated failure immune* (IFI) network iff message transfers between operative sites can be completed as long as network failures are isolated. Of course, we must define what we mean by the isolation of network failures. Two line failures are isolated if the inoperative lines are not incident to a common site.

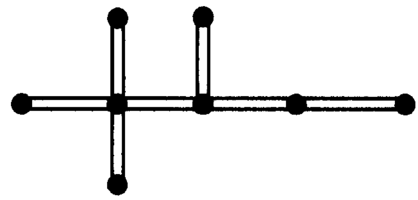

FIG. 1. A tree with redundant lines added.

Two site failures are isolated if the two down sites are not neighbors. A line failure and a site failure are isolated if the inoperative line is not incident to a neighbor of the down site. Figure 2 presents examples of nonisolated pairs of network failures.

The investigation of IFI networks represents a new direction in the study of reliable networks. Much of the research on network reliability has concentrated on issues of connectivity. A network is *K-site (line) connected* iff at least K sites (lines) must be removed (i.e., be down or inoperative) to disconnect the network. A network can be K-connected (either line or site) only if the degree of every site is at least K. Otherwise, the removal of fewer than K incident lines or neighboring sites would disconnect a site with degree less than K. Several classes of K-connected networks which require the minimum number of lines (i.e., approximately $(|V|K)/2$) have been described [2-4]. The estimation of connectivity level based upon the degrees of sites in a network has been discussed [1].

Of importance here is that, for any K, there exist K-connected networks which are not immune to isolated failures. The K-connected networks of interest have disconnecting sets of $n > K$ lines such that no pair of these lines share a common end site. For example, consider two K-connected networks having $n > K$ sites, interconnected in a matching, or one-to-one, fashion. The resultant network is $(K + 1)$-connected. The n lines interconnecting the two components constitute a set of isolated failures which disconnect the network. Therefore, such networks are not IFI networks, though they are $(K + 1)$-connected (site or line).

The study of IFI networks is well motivated from a practical point of view as well. Network maintenance could be scheduled in a straightforward manner to minimize the likelihood (or frequency) of occurrence of pairs of nonisolated network failures. Furthermore, the effects upon network performance of making a line or site inoperative for maintenance purposes could be readily determined.

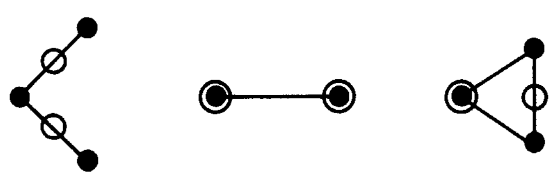

FIG. 2. Pairs of nonisolated network failures (failed elements circled).

produces routing tables for the resultant IFI network, which are sufficient to complete message transfers between operative sites under isolated failures. Following verification of the algorithm, a discussion of related notions of immunity to isolated failures is undertaken. In closing, suggested topics for future research are offered.

II. ISOLATED FAILURE IMMUNE NETWORKS

In this section we define a general class of IFI networks. We then specify a class of IFI networks which require the fewest lines. The simplest IFI network on two sites has the two sites connected by two lines. In what follows, network G is assumed to have set of sites V and set of lines E, such that $|V| \geqslant 3$.

The subnetwork *induced* by a subset V' of sites of network G is the network $G' = (V', E')$, where $(v, v') \in E'$ if $v, v' \in V'$ and $(v, v') \in E$. Given network G, let $N(v)$, $v \in V$, be the set of neighboring sites of v in G. A network G is *neighborly* iff, for every $v \in V$, the subnetwork induced by $N(v)$ is connected and contains at least two sites.

Theorem 1. If G is neighborly, then G is an IFI network.

Proof: Suppose a down site v is encountered during message transfer. Then all sites and lines in the subgraph induced by $N(v)$ will be operative, if failures are isolated. Thus, site v can be bypassed by appropriate message routing through $N(v)$, and the site failure overcome. Suppose a line failure is encountered during a message transfer. Then a neighbor of the intended recipient of the unsuccessful call can be called successfully, given that failures are isolated. That neighbor can then call the original recipient. As before, this call will be successful if network failures are isolated.

Since any message transfer between operative sites can be completed in G as long as failures are isolated, G is an IFI network. ■

By Theorem 1, *complete networks*, in which each site is directly connected to all others, are IFI networks. Fortunately, we can determine a class of IFI networks requiring considerably fewer lines. A *K-clique* of network G is a complete subnetwork of K vertices in G. A *K-tree* is either a complete network on K sites or, given any K-tree on $n \geqslant K$ sites, a K-tree on $n + 1$ sites is obtained by directly connecting a new site to each site in a K-clique of the given K-tree [6]. A 1-tree corresponds to a tree network. For $K > 1$, K-trees contain (many) cycles as the basic building block is a K-clique. Every K-tree is K-connected.

Theorem 2. If network G is a 2-tree, then G is an IFI network.

Proof: We will show that G is neighborly, by induction on the number of sites in G. For G having three sites, G is neighborly. Let us assume that G is neighborly for G having less than or equal to n sites, and consider the addition of an $(n + 1)$st site. The neighborhood of the new site contains two sites and is connected. Furthermore, the new site becomes connected to the neighborhoods of the two sites to which it is connected. Therefore, a 2-tree on $n + 1$ sites is neighborly. ■

Networks which are 2-trees have several other properties which are advantageous for communication applications. Each property can be established by a straightforward inductive argument. As such, we state them here as lemmas, without proofs.

Lemma 1. If G is a 2-tree, then G is planar.

Lemma 2. If G is a 2-tree, then G has $2|V| - 3$ lines.

Lemma 3. In a 2-tree network G, the subnetwork induced by $N(v)$ is a tree network, for any site $v \in V$.

The first two properties indicate that efficient realizations of an arbitrary 2-tree are possible. The third property indicates that 2-trees are extremal instances of neighborly networks. This suggests 2-trees may be extremal instances of IFI networks as well. An IFI network G is a ***minimal IFI network*** if, when an arbitrary line is removed from G, the resultant network is not an IFI network.

Theorem 3. If G is a 2-tree, then G is a minimal IFI network.

Proof: Let an arbitrary line (v, v') be removed from G, creating G'. The subnetwork induced by $N(v)$ in G is a tree. As such, all of the neighbors of v' in $N(v)$ (i.e., $N(v) \cap N(v')$) can be down without creating a pair of nonisolated failures in G'. When these sites are down, message transfers between v and v' can not be completed through the immediate neighborhood of v and v' in G'. By our recursive definition of 2-trees, these transfers can not be completed through longer routes either. Sites in $N(v') - N(v)$ are separated from sites in $N(v') - N(v)$ by an edge connecting v' with a vertex in $N(v) \cap N(v')$. As such, G' is not an IFI network. ■

An IFI network G is a ***minimum IFI network*** iff G has the fewest lines possible in an IFI network having $|V|$ sites. Being minimal IFI networks does not necessarily guarantee that 2-trees are minimum IFI networks. To prove that they are, several definitions and a lemma are required. A ***separator*** S of a connected network G is a set of vertices (i.e., the subnetwork induced by those vertices) such that the subnetwork of G induced by $V - S$ is not connected. A u, v ***separator*** of a connected network G for $u, v \in V$ is a separator S such that no path exists between u and v in the subnetwork of G induced by $V - S$.

Lemma 4. If G is an IFI network then the subnetwork of G induced by any u, v separator of G contains a 2-clique.

Proof: (By contradiction.) Suppose there exists a u, v separator not containing a 2-clique. All of those sites can go down without creating a pair of nonisolated failures. No message transfer can then be completed between u and v. As such, G is not an IFI network. ■

We can now establish the following theorem.

Theorem 4. If G is a minimum IFI network, then G has $2|V| - 3$ lines.

Proof: As 2-trees are IFI networks (Theorem 3), the number of lines in G is less than or equal to $2|V| - 3$ (Lemma 2). We will show by induction that the number of lines in G must be greater than or equal to $2|V| - 3$. By inspection, this conjecture is true for G where $|V| = 3$ or 4. Let us assume the conjecture is true for $K > 4$ sites.

Let G be a minimum IFI network where $|V| = K + 1$. Let v be a site of minimum degree in G. By the first part of our proof, v has degree 2 or 3. If v has degree 2, then by Lemma 4, the neighbors of v form a 2-clique. Site v offers no alternate routes bypassing a neighbor. As such the subnetwork G' induced by $V - v$ is an IFI network. By our inductive hypothesis G' has at least $2K - 3$ lines. Therefore, G has a number of lines greater than or equal to $2|V| - 3$.

If v has degree 3, several cases must be considered. Again, by Lemma 4, the subnetwork N of G induced by the neighbors of v must contain a 2-clique. Subnetwork N cannot be a 3-clique, as this contradicts our assumption that G is a minimum IFI network. If N were a 3-clique, site v would only need to be connected to 2 of its 3 neighbors to maintain immunity to isolated failures. Similarly, N cannot be a 2-clique and an isolated site v'. The edge between v and v' can be removed without destroying immunity to isolated failures. The neighbors of v' must be accessible from v through its other neighbors when v' is down and network failures are isolated.

Therefore, N must be a tree (i.e., a path) of three vertices. Let N be v_1 connected to v_2 connected to v_3. Let $G_{1,2}$ be the largest IFI subnetwork of G containing v_1 and v_2, but not v. Let $G_{2,3}$ be the corresponding subnetwork for v_2 and v_3. Clearly, the set of sites occurring in both $G_{1,2}$ and $G_{2,3}$ is either only v_2 or $V - v$. If it is $V - v$, then G is not a minimum IFI network, as v would only need to be connected to v_2 and either v_1 or v_3 to maintain immunity to isolated failures. In the other case, the union of sites in $G_{1,2}$ and $G_{2,3}$ is equal to $V - v$ as G is an IFI network. By our inductive hypothesis, the total number of lines in both $G_{1,2}$ and $G_{2,3}$ is greater than or equal to $2|V| - 6$. As such, G has number of lines greater than or equal to $2|V| - 3$. ■

The following corollary is immediate:

Corollary 1. If G is a 2-tree, then G is a minimum IFI network.

The equivalence of 2-trees and minimum IFI networks has yet to be established. The following characterization of K-trees by Rose provides support for such a conjecture:

Lemma 5. [6, Theorem 1.1, p. 318] A network $G = (V, E)$ is a K-tree iff

(i) G is connected;

(ii) G has a K-clique but no $(K + 2)$-clique;

(iii) the subnetwork of G induced by every minimal u, v separator of G is a K-clique.

The proof of Theorem 4 indicates that a 4-clique cannot appear in minimum IFI networks. Thus, to establish equivalence between 2-trees and minimum IFI networks, one need only prove that each minimal u, v separator not only contains a 2-clique (Lemma 4), but is exactly a 2-clique. A ***minimal u, v separator*** is a u, v separator S such that, for each vertex w in S, $S - w$ is not a u, v separator. An alternate approach to a proof would be to establish that every minimum IFI network includes a site of degree 2. Since each site of degree 2 can be removed without affecting immunity to isolated failures, existence of a vertex of the degree 2 would establish equivalence with our initial, recursive definition of 2-trees.

Although an arbitrary 2-tree is immune to isolated failures, we have yet to provide routing tables and a calling protocol sufficient to produce the desired communication performance in the 2-tree. Also, establishing 2-trees which cover a set of (prelocated) sites is not the normal process in designing a communication network. Networks are more often designed around minimum-weight (distance) spanning trees, which can be determined by well-known efficient algorithms. As such, we now present an algorithm which creates IFI networks and associated routing tables from arbitrary tree networks.

III. MAKING TREE NETWORKS IMMUNE TO ISOLATED FAILURES

In this section, an algorithm is described which transforms tree networks into IFI networks by the addition of new lines. Furthermore, the algorithm establishes routing tables sufficient to complete all message transfers between operative sites under isolated failures. We briefly describe the algorithm prior to its formal definition, which is followed by a proof of correctness.

The algorithm, named IMMUNIZE, accepts as input an arbitrary tree network of more than two sites and routing tables for the sites in that network. It produces as output an IFI network over sites of the three and routing tables for use in the resultant network. A routing table for a site in a tree indicates the call to be made by the site for each other site as message receiver. A routing table for a site in the new network indicates a preferred and an alternate call to be made by the site for each other site as message receiver.

The output IFI network is constructed by adding lines to an input tree network. An *interior site* of a tree network is a site with degree greater than one (i.e., not a *leaf site*). For each interior site S of the input tree, $N(S)$ can be considered to be $V_1, \ldots, V_K$, where K is the degree of site S. The algorithm adds communication lines between V_1 and V_i, for $2 \leqslant i \leqslant K$. Figure 3 illustrates the subnetwork constructed about site S. Figure 4 presents a network obtainable by this process from a given input tree. In both figures, the lines of the input tree are shown as solid, while the newly added lines are shown dotted.

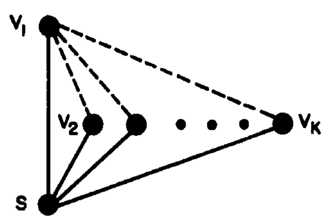

FIG. 3. The new (dotted) lines added to the neighborhood of an interior site S.

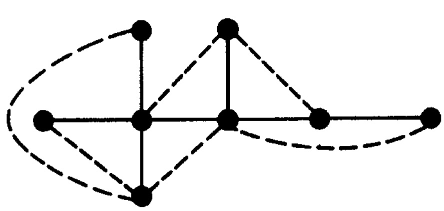

FIG. 4. The new (dotted) lines added to an input tree by IMMUNIZE.

As each interior site S is considered by the algorithm, certain entries are made in the routing tables of the sites in $N(S)$. These entries are for those receivers at each neighboring site for which the input routing tables indicate a call to S. The new entries direct calls either to S or to V_1. Which of these two calls is the preferred and which is the alternate depends upon distances in the tree network. Also, entries in the new routing table for S are determined for those neighbors which are leaf sites in T. This must be done as leaf sites are never directly considered by IMMUNIZE.

The algorithm IMMUNIZE is defined formally as follows:

Algorithm IMMUNIZE

Input: A tree network $T = (V, E)$, where $|V| \geqslant 3$; routing tables for the sites of T.

Output: An IFI network $G = (V, E')$; routing tables indicating preferred and alternate calls for sites of G.

Method: {Comments appear in brackets.}

Step 1. {Initialize.}
 1.1. Set G to T.
Step 2. {Add Lines and Establish new Routing Tables.}
 2.1. For each interior site S of T
  {Consider interior site S.}
  2.1.1. Let the neighbors of S be $V_1, \ldots, V_K$, where K is the degree of S.
   {Connect the neighbors of S into a star with V_1 as center.}
  2.1.2. Add lines (V_1, V_i) for $2 \leqslant i \leqslant K$ to G.
   {Determine entries in routing tables of G.}
   {Route $V_2, \ldots, V_K$ for S as receiver and S for leaves as receivers.}
  2.1.3. For each neighbor $V_i, 2 \leqslant i \leqslant K$
    Set the preferred call of V_i for S to S.
    Set the alternate call of V_i for S to V_1.
    If V_i is a leaf of T then
     Set the preferred call of S for V_i to V_i.
     Set the alternate call of S for V_i to V_1.
   {Route V for S as receiver.}
  2.1.4. Set the preferred call of V_1 for S to S.
  2.1.5. Set the alternate call of V_1 for S to V_2.
   {Route S for leaf V_1 as receiver.}
  2.1.6. If V_1 is a leaf of T then
    Set the preferred call of S for V_1 to V_1.
    Set the alternate call of S for V_1 to V_2.
   {Route neighbors of S for other receivers through S.}
  2.1.7. For each site V, such that $V \neq S$
    Let j be such that S calls V_j in T for V as receiver.
    For each neighbor V_i of S, $1 \leqslant i \leqslant K$
     If $j \neq i$ then {V_i would call S in T to contact V.}
   (a) If $j = 1$ then {Prefer shortcut through new neighbor V_1.}
      Set the preferred call of V_i for V to V_1.
      Set the alternate call of V_i for V to S.

(b) Else if $i = 1$ then $\{V_1$ prefers shortcut call through $V_j.\}$
Set the preferred call of V_1 for V to V_j.
Set the alternate call of V_1 for V to S.
(c) Else $\{V_i$ prefers call through $S.\}$
Set the preferred call of V_i for V to S.
Set the alternate call of V_i for V to V_1.

Theorem 5. The network G created by IMMUNIZE is an IFI network.

Proof: Lemma 5 provides three properties sufficient to define a 2-tree. G is connected, as the input tree T is connected and lines are only added to T by IMMUNIZE. G contains 2-cliques as T contains lines. G does not contain a 4-clique. Each interior site w is an u, v separator for all pairs u and v of its neighbors in T. As such, when u or v is considered by IMMUNIZE (as site S), only w can be connected into 3-cliques with other neighbors of v or u, respectively. Therefore, no 4-clique can be formed. Finally, in tree T each minimal u, v separator is a single interior site. In G, each minimal u, v separator is now an interior site S and its associated, neighbor vertex V_1, or two successive sites on the path between u and v in T. Therefore, each minimal u, v separator is a 2-clique. As such, G is a 2-tree and, by Theorem 2, is an IFI network. ∎

We now turn our attention to the routing tables produced by IMMUNIZE. We first establish that the algorithm completes the new routing tables. The routing tables are then shown to be sufficient to produce communication performance immune to isolated failures in G through use of a simple calling protocol.

Lemma 7. A routing table for each site in the resultant network is completely determined by Algorithm IMMUNIZE.

Proof: A site S in the resultant network is either a leaf or an interior site of the network T. Suppose S is a leaf in T. Then its neighbor V is an interior site of degree greater than 1 in T, as T has more than two sites. When V is considered by the algorithm, all entries of its routing table indicate calls to sites other than S, except in the case for S as receiver. Furthermore, all entries in the routing table for S in T indicate calls to V. As such, all the new routing table entries for S are determined when V is considered by IMMUNIZE.

Suppose S is not a leaf in T and has neighbors $V_1, \ldots, V_K$. If V_i is a leaf in T, then routing table entries of S for V_i are determined at the time that S is considered. Routing table entries of S for its other neighbors as well as for other sites beyond those neighbors are determined when those neighbors are considered. ∎

Now a calling protocol can be defined in terms of the newly completed routing tables. Consider the simple calling protocol P which is defined as follows:

Suppose message M with receiver R is to be transmitted by site S.

Then,

(1) Record the message identification of M; if message M has previously been processed by site S, then note (apparently) down receiver R and stop processing M;

(2) Transmit M to the site indicated by the preferred call for R in the routing table of site S;

(3) If the call placed in step (2) fails, note network failure and transmit message M to the site indicated by the alternate call for R in the routing table of site S;

(4) If the call placed in step (3) fails, note pair of nonisolated failures.

The above calling protocol is executed by a site when processing each message transfer request. The actions "note down receiver R" and "note pair of nonioslated failures" can be implemented in any of a variety of ways. These may involve attempting to return the message to the sender, informing a central site which can then initiate repairs, or in some cases, simply removing the message from active consideration. We now verify that protocol P results in immunity to isolated failures.

Theorem 6. Protocol P, using the routing tables produced by IMMUNIZE, completes all message transfers between sites which are not down as long as network failures are isolated in output network G.

Proof: Inspection of IMMUNIZE indicates that all routing table entries are made in pairs of preferred and alternate calls and that the sites in these pairs are neighbors in G. Therefore, as long as network failures are isolated, either the preferred or alternate call will be successful. This verifies the correctness of Step 4 of calling protocol P.

Now assume that network failures are isolated. Let $(s_0, s_1, \ldots, s_m)$ be the unique path of sites between sender s_0 and receiver s_m (i.e., R) in the input tree T. We first show that if the message is currently at site s_i then after one or two successful calls according to protocol P and the routing tables the message is at site s_{i+1} or s_{i+2} for $0 \leqslant i \leqslant m-2$. As such, the message transfer process makes progress and will reach the neighborhood of s_m. We then show that once reaching the neighborhood of s_m, either the message is delivered or a down receiver site s_m is discovered. As such, the message transfer process halts correctly.

If the message is at site s_i, several cases must be considered. If s_i is the site V_1 associated with s_{i+1} by IMMUNIZE, then its preferred call for s_m as receiver is s_{i+2} and its alternate call is s_{i+1} (by Step 2.1.7 (b)). Since one of these two calls must succeed, the proposition holds. If site s_{i+2} is the site V_1 associated with s_{i+1}, then the same situation occurs (by Step 2.1.7(a)). Otherwise, the preferred call of s_i is s_{i+1} and the alternate is V_1 associated with s_{i+1}, where V_1 is not part of the path $(s_0, \ldots, s_m)$. If the call to s_{i+1} succeeds; the proposition holds. If we find ourselves at V_1, its preferred call for s_m as receiver is s_{i+2} and its alternate is s_{i+1} (by Step 2.1.7(b)). If s_{i+1} is down, s_{i+2} can not be down when failures are isolated. If there had been a down line between s_i and s_{i+1}, the line between V_1 and s_{i+2} may also be down. However, a successful call can be made to s_{i+1}. Again, our proposition holds, now in all cases. In a finite number of calls, the message reaches the neighborhood of s_m.

Now we must show that the protocol and routing tables perform correctly in the neighborhood of s_m. We just demonstrated that if s_{m-1} is down, then s_m cannot be down and will be called correctly from site V_1 associated with s_{m-1}. If s_{m-2} is site V_1 associated with s_{m-1} by IMMUNIZE, then s_{m-2} will place its preferred call directly to s_m, never even attempting to call s_{m-1}. Therefore, if s_{m-1} is down, the eventual message receiver s_m always is contacted. Let us now assume that s_{m-1} is not down and that the message has reached that site. The preferred call of all neighbors of s_m for s_m as receiver is s_m (by either Step 2.1.3, 2.1.4, or 2.1.6 of IMMUNIZE). This includes s_{m-1} and site V_1 (or V_2) associated with s_{m-1}. Either s_{m-1} will succeed in calling s_m or s_{m-1} will call its alternate site which will successfully call s_m. Thus, if s_m is not down, all message transfers with s_m as receiver are completed as long as failures are isolated. ∎

To complete verification of protocol P and the routing tables produced by IMMUNIZE, the following theorem is established.

Theorem 7. Protocol P, using the tables provided by IMMUNIZE, correctly recognizes a down receiver site R when failures are isolated.

Proof: Assume that $(s_1, \ldots, s_m)$ is as in proof of Theorem 6. Furthermore, now assume s_m (i.e., R) is down. Suppose s_{m-1} is V_1 associated with s_m by IMMUNIZE. It will complete a call to V_2 (by Step 2.1.5). Site V_2 will be forced to return the message to V_1 according to its alternate call (by Step 2.1.3). Assume s_{m-1} is not V_1 or s_m. Then, its alternate call will be to V_1. If s_{m-1} is V_2, then the return call of V_1 to s_{m-1} will cause down receiver recognition. Otherwise, the above V_2's call back to V_1 will suffice, and V_1 of s_m will recognize down site s_m. If s_m were a leaf of V, a similar process (and proof) ensues. Our proof concerning the performance of P and the routing tables outside the neighborhood of s_m (Theorem 6) guarantees that the "looping" of calls can only occur within the neighborhood of s_m, when s_m is a down receiver. ∎

IV. CONCLUSION

In closing, we briefly discuss several specializations and generalizations of our notion of isolated failure immune network and suggest future research issues. One means for specializing our notion is to assume that only site or only line failures can occur. We refer to such networks as *site-only* or *line-only IFI networks*, respectively. Lemma 4 indicates that 2-trees are still minimum IFI networks when only site failures can occur, as a 2-clique in every u, v separator would still be necessary when considering only site failures. Figure 5 presents a network having six sites and only eight lines which is a line-only IFI network. Thus, 2-trees are not minimum line-only IFI networks.

The above results concerning site-only and line-only IFI networks suggest that our

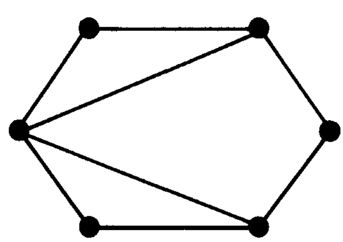

FIG. 5. A network which is a line-only IFI network requiring fewer then $2|V| - 3$ lines.

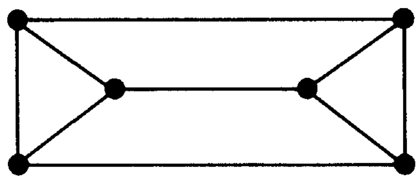

FIG. 6. A network which is a site-only (and site-line) IFI network but not a line-only IFI network.

initial definition of IFI networks may have included redundant requirements. Recall that there are three types of nonisolated pairs of failures: site-only, line-only, and site-line. One may now surmise that if a network is a site-only IFI network then it is a line-only IFI network; that is, if the removal of no set of isolated sites disconnects a network G, then no set of isolated lines will disconnect G. Figure 6 presents a network contradicting this conjecture. The network is a site-only IFI network as only one site from each triangle can be removed if failures are isolated. The network is not a line-only IFI network as the three isolated lines connecting the two triangles can be removed to disconnect the network. Note also that the network of Figure 6 has 9 lines and is a minimum site-only IFI network which is not a 2-tree. By Figure 5, we know that being a line-only IFI network does not imply being a site-only IFI network.

Similarly, we may wonder about the redundancy of site-line requirements for IFI networks. A network is a ***site-line IFI network*** if no set of isolated failures which includes at least one site and one line failure can disconnect the network. Figure 6 shows a network which is a site-line, but not a line-only, IFI network. If any site goes down, there is only one line which is isolated from that failure, and this does not disconnect the network. Figure 7 presents a network which is a site-line IFI network but not a site-only IFI network. For each site on the four-cycle there are two lines, only one of which can be removed if failures are isolated; this does not disconnect the network. However, two opposite sites of the four-cycle are isolated and their failure disconnects the network.

Finally, Figure 8 presents a network which is both a site-only and a line-only IFI network but which is not a site-line IFI network. Only one site from each 5-clique and the bottom site can be down if failures are isolated. The network is obviously a site-only IFI network as there are three lines between the 5-cliques. Only one of the four lines incident to the bottom site can be down given isolated failures. This allows

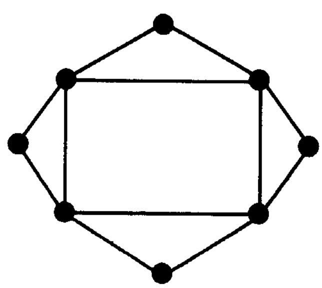

FIG. 7. A network which is a site-line IFI network but not a site-only IFI network.

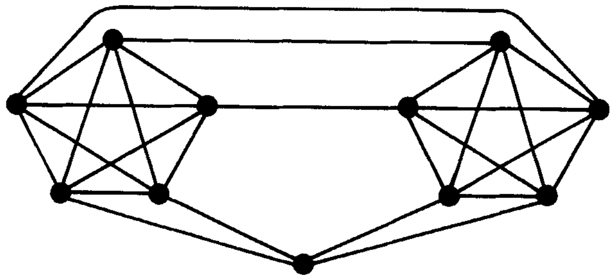

FIG. 8. A network which is a site-only and line-only IFI network but not a site-line IFI network.

communication between the two 5-cliques which are line-only IFI networks. As such, the whole network is a line-only IFI network as well. However, the bottom site and the three lines connecting the 5-cliques can be removed while failures are isolated. This disconnects the network, which is therefore not a site-line IFI network. This completes verification that our initial set of requirements for IFI networks are not redundant.

Generalizations of our notion of immunity to isolated failures can also be considered. One such is immunity to limited-size of nonisolated failures. An *ImFI network* is a network in which all message transfers between sites which are operative can be completed as long as less than m nonisolated pairs of network failures occur. By this generalization, we have been considering I1FI networks throughout this paper. It appears that K-trees where K is equal to $(m + 1)$ are ImFI networks. Whether they are minimal cases of such networks is uncertain. K-trees can complete message transfers as long as any site is not neighbor of or incident to a total of more than K network failures. Furthermore, K-trees are economical, requiring only a number of lines linearly related to the number of sites. K-trees deserve further consideration in reliable network design.

Obviously, several future research questions have been raised and/or motivated by the results we have presented. Issues which we are now pursuing include:

(i) the characterization of classes of minimal and minimum line-only, site-only, and site-line IFI networks;

(ii) the characterization of classes of ImFI networks and of other generalizations of immunity to failures;

(iii) the recognition of IFI networks (i.e., is this recognition problem NP-complete and, if not, how can it be done efficiently?);

(iv) the determination of adequate routing tables for an arbitrary IFI network;

(v) the determination of minimum-weight spanning 2-trees for a set of (prelocated) sites.

I wish to thank reviewers of an earlier draft of this paper. Their comments led to significant improvements in the presentation of these results. Dr. A. Proskurowski offered important suggestions as well.

References

[1] F. T. Boesch, "Lower Bounds on the Vulnerability of a Graph," *Networks*, 2, 329-340 (1972).
[2] F. T. Boesch and A. P. Felzer, "A General Class of Invulnerable Graphs," *Networks*, 2, 261-283 (1972).
[3] D. R. Fulkerson and L. S. Shapley, "Minimal K-Arc Connected Graphs," *Networks*, 1, 91-98 (1971).
[4] S. L. Hakimi and A. T. Amin, "On the Design of Reliable Networks," *Networks*, 3, 241-260 (1973).
[5] R. E. Pippert and L. W. Beineke, "Characterizations of 2-Dimensional Trees," in *The Many Facets of Graph Theory*, Lecture Notes in Math. No. 110, Springer-Verlag, New York, 1969.
[6] D. J. Rose, "On Simple Characterizations of K-Trees," *Discrete Math.*, 7, 317-322 (1974).

Received August 3, 1979
Accepted October 20, 1980