Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks [1]

T. H. Shake†, B. Hazzard‡, D. Marquis†

†Distributed Systems Group, ‡Advanced Networks Group
Lincoln Laboratory, Massachusetts Institute of Technology
Lexington, Massachusetts

Abstract

Wide-area fiber-based communication networks pose several unique security challenges. They usually rely on large expanses of minimally to moderately protected fiber infrastructure. They are subject to surreptitious signal monitoring and/or insertion at many points in this infrastructure, which may include optical repeater nodes, switching nodes, operation and management nodes, and fiber itself. They typically carry large volumes of data, making even short duration outages potentially very costly.

The trend toward increasing reliance on relatively high data rate applications involving high-resolution imagery, real-time video, and multi-media data streams is increasing the criticality of the high-rate backbones that are capable of moving this information across long distances. Thus the impacts of outages or congestion in high-rate fiber backbone infrastructures may become increasingly serious, especially for users passing critical information (e.g., time sensitive information requiring fast delivery and/or confirmation of receipt) through them.

This paper examines the problem of assessing the vulnerabilities of long haul fiber infrastructures to calculated attacks, particularly denial-of-service attacks at the physical layer. It discusses why physical layer attacks are significant threats in high-rate fiber networks, and examines the degree of disruption that can be produced by such attacks. Appropriate measures of network infrastructure vulnerability to such threats are discussed, and a conceptually simple new method of quantifying these types of vulnerabilities is proposed and briefly illustrated.

Keywords: Network Survivability, Infrastructure Protection, Network Security, Denial-of-Service

Introduction

The degree of vulnerability of the nation's critical infrastructures to deliberate attacks is currently a matter of some controversy. Some authorities maintain that the electric power grids, communications networks, air traffic control systems, and water distribution systems are quite vulnerable to computer-based attacks from the Internet and to various other forms of sabotage (see, for example, [1, 2]). Others hold that these vulnerabilities are overrated and that there is little evidence to back up the supposed threats to these infrastructures [3]. A very recent book sponsored by the US National Research Council Computer Science and Telecommunications Board gives an interesting overall summary of potential communication network security vulnerabilities in the national information infrastructure [4]. It is neither dismissive of the potential threats nor alarmist about them, but finds a sufficient number of vulnerabilities to cause concern. Clearly there is reason to work to improve the security of the nation's infrastructure, even if the exact degree of the threat is still unclear.

The potential vulnerabilities to information attack are numerous, and may be categorized in many ways. Attacks may be categorized by the goal of the attack, such as intercepting private information, altering database records, or denying service to authorized users of an information system. They may be classified by the method of attack, or the OSI layer at which the attack is targeted or promulgated.

[1] This work was sponsored by the Defense Advance Research Projects Agency under Air Force Contract F19628-95-C-0002

Network security publications are filled with information concerning prevention of attacks against network protocols and computer operating systems. Computer user behavior and network security policy is another area where much information has been published, and there is a large amount of literature and discussion concerning cryptographic algorithms for confidentiality, authentication, integrity, and non-repudiation. Physical layer attacks on communication infrastructure, however, seem to have received little attention in recent literature on network security.[2]

This paper is primarily concerned with physical layer attacks on high-rate communication infrastructure aimed at service denial. A major motivation for this focus is that we consider the vulnerability to this type of attack to be among the greatest vulnerabilities facing high-rate, long haul fiber systems. This is for the following reasons.

Degree of Network Disruption

As mentioned in the introduction, a successful denial-of-service attack on a high-rate backbone link or links can cause serious disruptions to network users. Through technologies such as SONET transmission and wavelength division multiplexing (WDM), huge amounts of data can be aggregated into a single fiber bundle or even a single fiber. Jamming, cutting, or otherwise disrupting traffic on a single fiber for any appreciable period of time can thus cause the loss or delay of large amounts of data.

If the fiber is carrying stream data, that data may all be lost until the network can be reconfigured to switch around the failed link. Automatic Protection Switching (APS), which is typically used in commercial telephony, can quickly reconfigure around single points of failure, except when the protection channels use the same physical channels (e.g., fiber or conduit) as the failed circuit, which is all to often the case. Self-healing rings are widely used for high-rate fiber transmission, and these often use physically diverse paths for backup transmission. This type of topology is very effective for backing up random failures. However, an intelligent attacker is likely to be able to disable or disrupt communications on two or more separate paths simultaneously, thereby subverting the extra protection of self-healing rings.

If the fiber is carrying packetized data, routers will detect a failed path and attempt to reroute around it. However, when a high-rate backbone link fails, other network links are very likely to become severely congested as routers attempt to reroute large numbers of packets over lower rate links, or over the remaining high-rate links that may already be heavily loaded. In this case, disrupting a high-rate backbone link can cause serious disruptions for a whole network of users, even those who were not using the link in question.

Ease of Attack

While many types of network attacks require either a high degree of technical expertise or significant financial or personnel resources to mount successfully, some physical layer attacks may be accomplished with few resources, little expertise, and, in some cases, a high degree of covertness. Consider the ease of severing a fiber or conduit that is part of a high-rate backbone. Most of the fiber infrastructure in the United States is buried in the ground within a few feet of the surface. What is not buried is usually mounted on utility towers. The difficulty of digging up and severing such fibers is not very great, and it happens regularly by accident. (By far the most common cause of telephony outages is the accidental severing of fiber infrastructure, typically by backhoes digging for construction projects. This happened an average of 59 times per year in the United States over the five year period between 7/92 and 7/97 [5].)

One person with a backhoe, or even a determined person or two with a shovel and cutting equipment can quite feasibly dig up and sever a fiber carrying SONET class data rates (currently

[2] The literature on survivable network topologies is extensive in both the graph theoretic literature and the literature on system reliability, but this work is almost entirely neglected in today's literature, which typically focuses on higher layer issues of protocols or operating systems.

hundreds of Mbps to tens of Gbps). Since wide-area fiber backbones tend to be relatively sparse topologically, coordinated attacks severing fibers in just a few geographic locations could completely disconnect significant segments of a typical high-rate backbone network. Still worse, the large geographic extent of many fiber backbones gives attackers a relatively high probability of mounting such an attack covertly (until the fibers are severed) and escaping immediately after the attack. Additional attacks could be mounted in sections of fiber that have been disconnected by a primary attack to prolong the duration of the outage.

These types of attacks require that the attacker can locate the fibers they wish to cut. This may take a little research, but an attacker with more than a casual interest has several resources that should help locate them. The general locations of high-rate fibers can be obtained for a fee from published maps of the national telecommunication infrastructure. Furthermore, many cable locations are well known in the industry, and there are databases available to help construction contractors avoid accidentally digging them up. It is not hard to imagine that a few individuals might be able to locate vulnerable fibers and choose attacks to maximize network disruption.

Durations of Typical Outages

The duration of outages due to typical fiber dig-ups depends on how long it takes to locate the fiber break, how long it takes to get repair crews to the location of the break, and how long it takes to effect repairs once the crew is onsite. Fiber breaks can usually be located fairly quickly via Optical Time Domain Reflectometry. The other two factors are more variable. For the five year period between 7/92 and 7/97, a telecommunications industry group has found that the mean outage duration for "facility outages" (mostly fiber cuts/damage) was 435 minutes, with the median being 275 minutes and the 95^{th} percentile being 1048 minutes [5]. An intelligent attacker could be expected to cut fibers requiring a long drive time to reach the location of the attack. (This might also minimize the probability of the attacker being caught.) Since the statistics referred to above include fiber dig-ups in urban areas, one can expect that the mean outage duration due to an intelligently chosen attack would be somewhat greater than 435 minutes.

A disruption of several hours may represent little more than an inconvenience to a telephone user who wants to make a social call, but for users relying on such infrastructures for sending time sensitive information it could be quite serious. It could be expected that attacks of this sort might be timed by the attackers to disrupt communications during events of geo-political significance. Since military users in most nations are relying increasingly on both public and private high-rate fiber infrastructures, such attacks could be mounted in scenarios with military significance.

For these reasons we believe that physical layer attacks on high-rate communication backbones represent a threat that must be taken seriously. A few people with limited resources and expertise can mount a credible attack that disrupts many users and/or large amounts of data for at least several hours. The threats posed by these attacks cannot be addressed through cryptography (which is often treated as a panacea for network security problems).

It is worth mentioning at this point that, while our analysis above has focused on attacks that attempt to deny or disrupt service via fiber cuts, large expanses of fiber infrastructure also have vulnerabilities to other types of attacks such as tapping for eavesdropping or signal insertion for jamming [6]. Such attacks may require more resources or expertise of the attacker, but are well within the realm of credible threats. And while it is true that buried fibers are much more resistant to eavesdropping and jamming attacks than most wireless channels, this does not mean that they are invulnerable, or even "safe enough".

Assessing Network Vulnerabilities

In this and the next section we focus on assessing and quantifying network vulnerabilities to intelligently chosen denial-of-service attacks at the physical layer. (The most obvious example is a coordinated

multiple fiber cut attack.) We will narrow our focus still further to address attacks specifically chosen to disconnect specific pairs of nodes, or all connectivity to a particular node. This scenario is most applicable to situations where the attackers have specific objectives in mind, such as disruption of military communications to a key command center, or disconnection of a particular network server or database from a network. We propose a new measure that allows different parts of the network infrastructure to have varying degrees of vulnerability, and that can also take into account the degree of opportunity for an attacker to disrupt the network.

We first briefly survey the literature concerning network survivability. There have typically been two major approaches to evaluating the vulnerability or survivability of communication networks—the statistical approach (e.g., reliability calculations) and the deterministic approach (e.g., graph theoretic calculations). The literature on network reliability is quite extensive, and typically attempts to model such quantities as mean time between failures (MTBF) and mean time to repair (MTTR). The graph theoretic literature is also extensive, offering various ways of quantifying network vulnerability, such as minimum cutset cardinality or minimum connectivity. (An in-depth survey of graph theoretic results can be found in [8].) Companies supplying long haul telephony infrastructure have developed sophisticated simulation and analysis capabilities for design and evaluation of these infrastructures (e.g., [7]) which draw on both types of techniques. However, these design and evaluation techniques (at least the ones published in the open literature) seem generally aimed at making systems robust to random or accidental failures, and focus much less on calculated, malicious attacks.

A primary difficulty with statistical approaches is assigning plausible random processes to model intelligent, calculated attacks. If probabilities of link or node failures are not accurately modeled, even basic comparisons between simple topologies can yield dramatically varying results. Also, statistical approaches are usually simplified by assuming that component failures (such as link or node failures) are independent of each other, and this is clearly not the case for intelligent attacks.

Many results from graph theory are more applicable to assessment of vulnerabilities to calculated attacks. For example, an attacker might examine a network topology and assess the most efficient denial-of-service attacks available to meet their objective. This might involve evaluating the minimum set of fibers or switching nodes that could be cut to disconnect certain nodes (a “minimum cutset” in graph theoretic terminology). Developing efficient algorithms for finding such minimum cutsets has been a significant area of graph theoretic research (e.g., [9]). The cardinality of such cutsets (i.e., the minimum number of links or nodes whose removal disconnects a part of the network) is one commonly proposed measure of network vulnerability. The minimum number of link-disjoint and/or node-disjoint paths from one node to another is also a commonly used vulnerability measure. Other graph theoretic approaches quantify the size and/or number of disconnected fragments due to link cuts, or quantify the minimum connectedness of a network. There are many more specific measures of vulnerability proposed in the literature, some of which also combine probabilistic measures with deterministic measures.

This paper seeks to extend the applicability of these concepts, while introducing a method for assessing attack vulnerabilities that is conceptually simple and intuitively appealing. We start by proposing that, for reasons discussed in the previous section, links (fibers) are easier to attack than nodes (e.g., switching or routing centers), and hence are more vulnerable. Note that this is in contrast to many reliability scenarios, where complicated equipment and complex software control algorithms are concentrated at network nodes and may represent the most likely points of failure. Nodes are easier to protect from physical attacks than fiber links, since they can be enclosed in attack-resistant physical structures and guarded more easily. Furthermore, a physical attack on a node is likely to have a much higher profile than a fiber cut, and the legal or geopolitical consequences of node attacks are thus likely to be greater. This may make attacks on nodes less likely than attacks on fiber, except perhaps in times of war. For the purposes of this analysis we treat minor nodes such as optical repeaters as part of the fiber infrastructure and hence as part of the “links” of the network.

Quantitative Methods

We now wish to examine methods for quantifying the vulnerability of the fiber links of a given network. One useful construct is Boesch's concept of the "edge-cut frequency vector" [10]. This is a vector of integer elements, whose i^{th} element is equal to the number of i^{th} order edge cuts (link or fiber cuts, in our terminology) that create a disconnected, trivial, or empty graph. In other words, the i^{th} element corresponds to the number of different ways that a network can be disconnected by cutting exactly i links.[3] This concept can also be applied in the context of connectivity between two specific nodes. Boesch's original paper gave each link a probability of failure, but as noted above, it is difficult to assign meaningful failure probabilities in the context of intelligent attacks. Two possible solutions to this problem are to simply count the number of cutsets of a given order as a measure of vulnerability, or to assign a specific vulnerability metric to each link reflecting its vulnerability to attack.

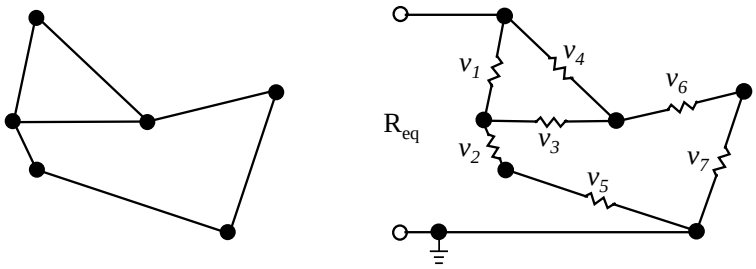
Using the first solution, one can get a simple idea of network vulnerability to intelligent attack by examining the individual elements of the cut frequency vector, (i.e., the number of ways to disconnect a network by removing exactly i links). This can be done for each value of i that represents a plausible attack. Networks that can be disconnected by cutting a very small number of links are obviously more vulnerable to disconnection than networks where a larger number of links must be severed to disconnect any part of the network. Furthermore, consider two networks, ***A*** and ***B***, that have identical edge-cut frequency vectors for $i < k$. If the k^{th} element of the frequency vector for Network ***A*** is less than the k^{th} element for Network ***B***, Network ***A*** may be considered less vulnerable than Network ***B***.

The second solution allows for incorporating factors that may make some links more or less vulnerable to attack than others. For example, a 200-mile link through isolated and minimally monitored countryside is probably easier and more attractive to attack than a 2-mile link in an urban environment. Some fiber links might be buried much more deeply than others, or encased in more attack resistant conduit, or have a larger number of minimally protected repeater huts, and so on. (This vulnerability differentiation could be used with wireless links, which might have differing degrees of jamming resistance, etc.) If each link l_j is assigned a vulnerability metric v_j, the edge-cut frequency vector elements can be modified to become sums of the cutset elements that are weighted according to their individual vulnerability metrics. This effectively weights the vulnerability of each link in the calculation of the modified elements of the cut frequency vector. However, assigning an appropriate mathematical function for combining these modified vector elements to obtain an overall vulnerability value for the network is not straightforward.

Assigning a vulnerability metric to each link in a network suggests another intuitively appealing approach for characterizing infrastructure vulnerabilities. Consider a network, as above, where each link has an associated vulnerability, v_j. We wish to calculate a path vulnerability between any two nodes, s and t, in the network. Suppose we redraw a graph of the network as a network of resistors, where each resistor corresponds to a link and the value of each resistor is set to the corresponding link vulnerability metric, v_j. This is illustrated in Figure 1. To calculate the path vulnerability between any two nodes, we simply define the nodes of interest as terminals of a "one-port" device. The path vulnerability may then be calculated as the driving point impedance of the one-port device. Such calculations are quite standard in circuit theory (see any text in basic circuit theory such as [11]) and can be programmed very easily.

Figure 2 illustrates some basic properties of this path vulnerability metric. If a signal must cross two links, l_j and l_k, in series to reach its destination, the vulnerability of the end-to-end path is $v_j + v_k$. If a signal may cross either of two links in parallel to reach its destination, the vulnerability of the end-to-end path is $(v_j v_k)/(v_j + v_k)$. Thus if two paths of equal vulnerability are placed in parallel, the equivalent path vulnerability is half of the vulnerability of either link alone. If a very vulnerable link is placed in parallel with a much less vulnerable link, the equivalent vulnerability is only slightly less than that of the less vulnerable link. Parallel links are obviously allowed in this formula (as opposed to some graph theoretic formulations, which explicitly prohibit them). However, parallel links that have no geographic diversity

[3] A graph is disconnected if there are two or more nodes in the graph between which there exists no path, or connection.



(a) (b)

Network Topology Equivalent Resistor Network

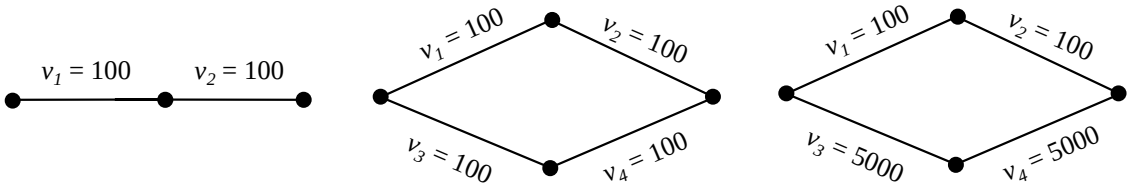
Figure 1: Redrawing network topology as resistive circuit

(e.g., are bundled in the same conduit) do not decrease the path vulnerability to fiber cutting attacks and should be combined into a single link for the purposes of this calculation. Alternatively, the independence or diversity of parallel links could be quantified along a continuous range of values, and the two links combined according to the degree of vulnerability reduction appropriate to that amount of independence.

Note that this characterization does not measure the likelihood of any event, nor the probability of path failure given a certain type of attack. Rather it quantifies the overall vulnerability of a network topology between two nodes, taking into account the equivalent vulnerability of the whole ensemble of possible paths between them. Overall characterizations of a network may, of course, be obtained by averaging over all node pairs in the network.

There are many different ways to consider assigning the individual link vulnerabilities. Depending on the particulars of a network, assignments of absolute link vulnerabilities may or may not be feasible, but vulnerabilities normalized to an arbitrary value may be used to compare different topologies, as long as the normalization is consistent across the different topologies. Unlike probabilistic formulations, such comparisons are not sensitive to the absolute vulnerabilities assigned to each link.

One possible assignment is to consider each link in a network to be equally vulnerable, with unit vulnerability for example. This assignment might be useful in applications where the number of links in a path is of particular concern, as in certain routing algorithms. Other assignments may take real world hardening techniques into account. Another interesting assignment strategy could be to make link vulnerability a function of link length. This may prove to be a useful assignment for long-haul fiber topologies, since longer links 1) are harder to protect or even monitor than shorter links; 2) allow attackers greater flexibility in choosing attack points on targeted links and greater ability to get away after the attack without being caught; and 3) allow attackers greater chances of successfully mounting additional concealed



Equivalent vulnerability = 200 Equivalent vulnerability = 100 Equivalent vulnerability = 196

(a) (b) (c)

Figure 2: Illustrations of vulnerability metric

attacks in disconnected portions of the network while the primary attack is still under repair. These factors should make attacks significantly more probable on longer links. Perhaps the most natural function of link length (and the one that corresponds most precisely to the resistive circuit analogy) would be to make the link vulnerabilities linearly proportional to link length. A physical interpretation of the resulting metric could be that having longer link lengths increases the "defense perimeter" of the network. In other words, if one link is twice as long as another one, there is twice the fiber to protect, and twice the area over which an attacker could mount an attack. This particular metric is not expected to be appropriate for all networks, but may be useful as one interpretation of an infrastructure's vulnerability.

Some intuitive feeling for this vulnerability metric can be gained from using it to compare some simple, standard topologies. Figure 3 shows four basic topologies connecting the same set of nodes—a star, a ring, two interconnected rings, and a fully connected mesh. Nodes are numbered from one to six for reference. For simplicity, let us assign unit vulnerability to each link in each topology. Consider a scenario where an important server is located at node 4. Figure 4 shows the vulnerabilities of the paths from every other node to node 4 in each topology. Note that the star does relatively well in this case since it connects each node to the server with a single link of unit vulnerability.

The single ring provides redundant paths, but for some nodes, each path contains multiple links in series, which increase the vulnerability. The double ring and mesh add enough redundancy to produce lower vulnerabilities than the star from every node. If traffic patterns are not all client to server, however, the star topology is poorer from a vulnerability perspective. This is shown in Figure 5, which shows the overall average vulnerability (averaged across all node pairs) for all paths connecting two nodes in each of the topologies in Figure 3. Calculations such as those illustrated in Figure 4 can also be interpreted as showing how "securely connected" two nodes are. These calculations are practical for use in assessing existing long-haul topologies and comparing alternative new ones. Since long-haul topologies tend to be relatively sparse, the total number of nodes and links is not so large as to make these calculations computationally unfeasible. To benchmark the practicality of these calculations, path vulnerabilities for paths from all nodes to a single reference node in a fully connected reference network of 50 nodes and 1225 links were made with a several line program in the MATLAB programming environment. The 49 path vulnerabilities were calculated in less than 3 minutes on a desktop computer (266 MHz Pentium II processor and 128 Mbytes of RAM).

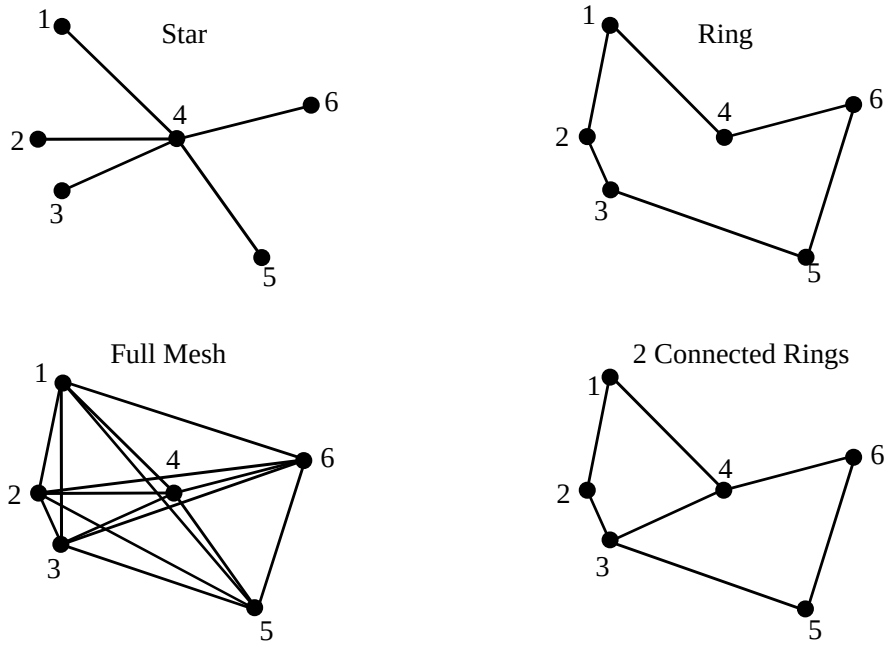


Figure 3: Topologies for comparison

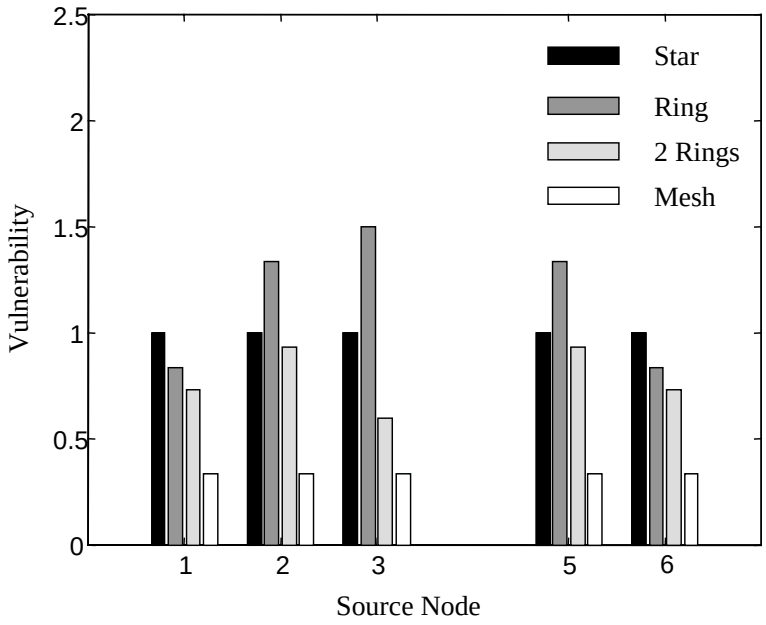


Figure 4: Vulnerabilities from source nodes to node 4

Summary and Conclusions

We have argued in this paper that physical layer denial-of-service attacks are a significant and credible threat to users of wide-area fiber networks who require timely transfer of important information. We have also presented a new evaluation tool that can be used to assess the degree of vulnerability of various network topologies to such attacks.

There are, of course, many important considerations concerning network topology design and evaluation that our path vulnerability metric does not take into account. These include traffic loadings, path delays, reconfiguration and switching delays, or the complexities of re-routing algorithms necessary to take advantage of multiple redundant paths. Depending on the user's needs and scenarios of interest, various such things may need to be taken into account for a full evaluation of a network's vulnerability to denial-of-service attacks at the physical layer. The approach we have outlined here gives a relatively intuitive starting point for evaluation and comparison of topological vulnerabilities.

The focus of this paper has been on assessment of physical, topological vulnerabilities in high-rate, wide-area networks. This is a logical first step toward improving security in such networks, but it is only a first step. We want to briefly mention some potential countermeasures in closing, if mainly as a motivation for future work.

Wide-area fiber backbones are expensive to deploy and maintain. It is unlikely that large amounts of path redundancy will be added to most such networks to ameliorate the vulnerabilities described and assessed in this paper.[4] However, users who depend on such networks for timely transmission of critical data should make their own assessments of the degree of threat posed by the types of outages that may be caused by intelligent physical attacks. Such users need to have contingency plans to deal with possible outages. One strategy could be to maintain backup channels on separate networks that could be brought up quickly and reliably. Such channel redundancy is expensive to maintain, especially at high data rates. Lower bandwidth channels, however, could serve as effective backups for a user's most critical data if this planned for in advance. This would require having lower bandwidth backup channels available immediately, and it would also require defining a core set of data for critical operations that could be trans-

[4] Indeed, reference [4] concludes that even the reliability problem of construction crews accidentally severing fibers is probably not amenable to a technological solution. (See p. 37, "Link Failures")

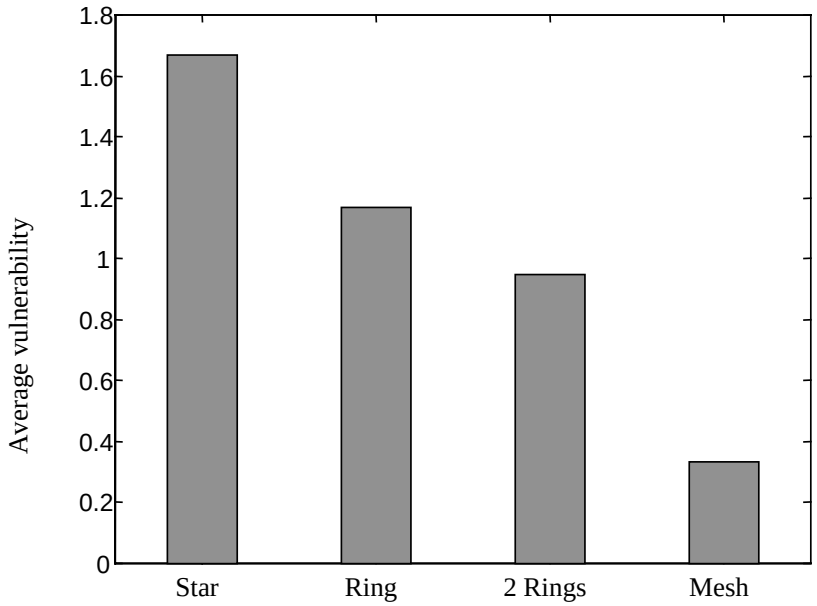


Figure 5: Average vulnerability for 4 standard topologies

mitted over lower rate channels in the event of an attack. Evaluating various backup channel options is beyond the scope of this paper, but there are a number of possible options, including dial-up T1 links, satellite communication channels, or ISDN lines.

Detection, localization, and reaction strategies for this type of attack are also needed. These strategies need to allow fast network reconfigurations to minimize network disruption. Reaction strategies can be considered at both the user and the network level, and should aim for both fast service restoral and minimum impact on user traffic in other parts of the network.

Various users of high-rate fiber backbone networks may have greatly varying concerns about the type of attack analyzed in this paper. However, there is a large scale trend, both in commercial and military organizations, toward increasing reliance on large volumes of data. This increases our overall reliance on the networks that carry this data and will translate into an increased vulnerability of our society at large to network disruptions of all kinds. The physical infrastructure of our data networks is the foundation upon which all other network functions rest. We must take care to insure its robustness and reliability.

References

[1] Office of Science and Technology Policy, National Security and International Affairs Division: *Cybernation: The American Infrastructure in the Information Age*, January 1, 1998. See http://www.whitehouse.gov/WH/EOP/OSTP/html/cyber2.html

[2] General Accounting Office (GAO): *GAO Executive Report B-266140*, Report to the Committee on Governmental Affairs, U.S. Senate, May 22, 1996. See http://epic.org/security/GAO_DOD_security.html

[3] Smith, G.: *An Electronic Pearl Harbor? Not Likely.*, Issues in Science and Technology, vol. 15 no. 1 (Fall 1998) 68-73

[4] F. B. Schneider, ed.: *Trust in Cyberspace*, National Research Council Computer Science and Telecommunication Board, National Academy Press, 1999

[5] Network Reliability Steering Committee: *Annual Report 1997*, Sponsored by the Alliance for Telecommunications Industry Solutions, see http://www.atis.org/atis/nrsc/nrschome.htm

[6] Medard, M., Marquis, D., Barry, R. A., Finn, S. G.: *Security Issues in All-Optical Networks*, IEEE Network Magazine, May/June 1997, 42-48

[7] Cardwell, R. H., Monma, C. L., Wu, T. H.: *Computer-aided Design Procedures for Survivable Fiber Optic Networks*, IEEE Journal on Selected Areas in Communications, vol. 7, no. 8, October 1989

[8] Stoer, M.: *Design of Survivable Networks*, Lecture Notes in Mathematics #1531, Springer-Verlag, 1991

[9] Nagamochi, H., Sun, Z., Ibaraki, T.: *Counting the Number of Minimum Cuts in Undirected Multigraphs*, IEEE Transactions on Reliability, vol. 40, no. 5, December 1991

[10] Boesch, F. T.: *The Cut Frequency Vector*, in Graph Theory with Applications to Algorithms and Computer Science, Alavi et. al., eds., Wiley, 1985

[11] Balabanian, N., Bickart, T.: *Linear Network Theory*, Matrix Publishers, 1981