SURVIVABLE NETWORK SYSTEMS: ITS ACHIEVEMENTS AND FUTURE DIRECTIONS

M. Keshtgary, Ph.D.
Department of Computer Engineering
Shiraz University of Technology, Shiraz, Iran
Corresponding Author: email: keshtgari@sutech.ac.ir

A. H. Jahangir, Ph.D.
Department of Computer Engineering
Sharif University of Technology, Tehran, Iran
jahangir@sina.sharif.ac.ir

ABSTRACT - Society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded open network environments. Unless safeguards are incorporated in the system, a failure of even a single component, e.g. a link or a node, can significantly impact the network performance and can cause highly expensive damages. The discipline of survivability attempts to ensure that network systems can deliver essential services and maintains inherent properties such as integrity, confidentiality, and performance, in the presence of attacks, failures or accidents. Optical networks based on Wavelength-Division Multiplexing (WDM) technology can potentially transfer hundreds of gigabits of data per second in the network. WDM networks are believed to be a promising candidate to meet the explosive increase of bandwidth demand in the Internet. However, the high capacity of a link has the drawback that a failure can potentially lead to the loss of a large amount of data. This is why the survivability performance of networks is an important research issue. The objective of this paper is to answer questions like "What does survivability mean?", "Why is it important?", "How does it differ from fault tolerance?" and "How is it being measured?" by surveying the concepts of information and network survivability, its relation to and its distinction from dependability, fault tolerance and security. The survivability of optical networks and protection techniques in WDM networks are reviewed as an example of techniques to improve the network survivability. The problem of survivability measures from network analysis and design point of view is also presented in the paper.

Keywords: Information and Network Survivability, Fault Tolerance, Dependability, Optical Network, WDM.

INTRODUCTION

Since failure of information systems can cause a major loss of service, their dependability is a major concern. Current facets of dependability, such as reliability and availability, do not address the needs of critical information systems adequately as they do not include the notion of degraded service as an explicit requirement. What we need is a precise notion of what forms of degraded service are acceptable, under what circumstances each form

is most useful, and the fraction of time that such degraded service levels are acceptable. This concept is termed as survivability [20].

Survivability is a new field of research, and is viewed by many as distinct from the traditional areas of security and fault-tolerance. Information system survivability is defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [31]. The term system is used in the broadest sense, including networks and large-scale systems of systems. The term mission refers to a set of very high-level requirements or goals of the system and not limited to military settings. The best example of implemented survivability research is combat aircraft that can still fly despite extensive system damage.

Timeliness is a critical factor that is typically included in the very high-level requirements that define a mission [31]. Actually it is such an important factor that it is included explicitly in the definition of information system survivability.

Survivability addresses three main kinds of events, attacks, failures, and accidents. Attacks are potentially damaging events orchestrated by an intelligent adversary. Attacks include intrusions and denials of service. Failures are potentially damaging events caused by deficiencies in the system or in an external element on which the system depends. Failures may be due to software design errors, hardware degradation, human errors, or corrupted data [10]. The term accidents comprise a broad range of randomly occurring and potentially damaging events such as natural disasters.

The notion of survivability has been used in several engineering disciplines outside the critical information systems. The objective of this paper is to answer questions like "What does survivability mean?", "Why is it important?", "Is it the same as fault tolerance?" and "How is it being measured?". Wavelength-Division Multiplexing (WDM) networks are a promising candidate to meet the explosive increase of bandwidth demand in the Internet. Therefore, its survivability is an important issue. Thus, we will review the survivability and protection techniques in WDM networks as an example of techniques to improve the network survivability. We also discuss the problem of survivability measures from network analysis and design point of view.

This paper is organized as follows: The next section discusses the need for survivability. After that a brief summary of current definitions of information and network survivability is presented. This is followed by comparison between survivability concept and dependability, fault tolerance and security. The next part introduces characteristics of survivable systems. Survivable Network Analysis (SNA) steps are presented later, which is followed by a discussion of some strategies to improve network survivability. The last three parts will deal with survivability techniques in optical networks, the problem of survivability measures from network analysis and design point of view and finally conclusions and future trends conclude the paper.

THE NEED FOR SURVIVABILITY

The growth of the Internet and the increasing number of "mission critical" business functions that rely on communication networks make survivability an essential aspect of network design. Up to 100 terabits per second of data flowing through a single fiber with DWDM, failure can cause a major loss of service. Failure events, specially cable cuts, are surprisingly frequent. A fiber cut in the AT&T network, which occurred at Newark in January 1991, interrupted 60 percent of voice and data coming in and going out of New York City, including three major commercial airports, for about 10 hours [44]. In the first eight months of 2002, the FCC logged 116 network outages in the United States [15]. On February 13 in Yadkinville, NC, town workers severed a Sprint cable while repairing a water line, cutting 52 trunk groups and 13 DS-3 links for over 5 hours. A week later, a fire in a Maryland power transformer melted a Verizon fiber cable affecting 5000 customers for over 9 hours. On March 14, a contractor accidentally cut functional fiber during removal of retired cable, cutting 911 services to a part of San Diego for over 4 hours. Therefore, network survivability, especially in the context of optical networks, is an important research area. The steady growth in the use of the Internet for business-critical applications is the primary driver behind this increased interest in network protection and restoration. The turbulent political environment following the events of September 11, 2001 has also helped drive the issue of disaster recovery to the mainstream [30].

There are several reasons why service providers deploy some measure of survivability in their networks. First and foremost, it is the issue of customer satisfaction. The dependability of telephony networks is that everyone expects when he/she picks up the telephone, he/she will get a dial tone and be able to place a call right away. And now, people expect "always on" dependability from the Internet and Internet based services such as VOIP as well.

Second, in today's networked world, network failure can cause losses to businesses and consequent negative publicity from outages. For regulated carriers, an outage that lasts for 30 or more minutes and affects 30,000 or more subscribers must be reported to the FCC. In some failure cases, service providers may have to provide rebates to customers based on the number or duration of outages. Availability of networks is so important to some customers such as those in financial or medical services and many carriers have developed survivable services specifically for this market segment.

Third, survivable networks are essential for reliable network operations. In fact, the first applications of network survivability were developed specifically for network operations in telephony networks [30]. Call processors in telephone switches are typically designed to handle a certain incoming call rate. In the event of a failure in the network impacting a large number of customers on the same switch, everyone attempts to redial at the same time. This overwhelms the call processor and causes it to crash. So, telephony engineers

set developing survivability architectures to prevent voice calls from being dropped. This engineering exercise ultimately led to the famous 50 ms restoration standard in survivable SONET/SDH networks.

CURRENT DEFINITIONS OF SURVIVABILITY

The notion of survivability has been used in several engineering disciplines outside critical information systems. For example, it is a common concept in weapons systems engineering [2]. The survivability of combat aircraft is the capability of an aircraft to avoid and/or withstand a man-made hostile environment. In the context of software engineering [9], survivability is the degree to which essential functions are still available even though some part of the system is down. Here, we focus on the information and network survivability. Information survivability system is defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [31]. Network survivability is (i) the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and (ii) the mitigation or prevention of service outages from network failures by applying preventative techniques [40]. A summary of definitions for information and network survivability systems is illustrated in Tables 1 and 2, respectively.

There are different definitions presented for information and network survivability in the literatures. Therefore, we need a precise and adequately comprehensive engineering definition of survivability, analogous to those that have been framed for the dependability characteristics described by Avizienis [1] such as reliability, availability, and security. The definition must be precise and unambiguous enough to support an engineering approach to the specification, design, and analysis of critical information systems. A precise definition of survivability requires a precise definition of the system, the expectations of the users, the minimum level of service and the threats to the system. If these are specified, then survivability is the ability of a given system to provide a specified minimum level of service in the presence of specified threats and a system is survivable if it complies with its survivability specifications.

SURVIVABILITY, DEPENDABILITY, FAULT TOLERANCE, AVAILABILITY AND SECURITY

Survivability may be better explained with an example. Consider the case of a village farmer with the mission of supplying food to a village [28]. The farmer may have a fence around the crops to keep out deer, rabbits, and other intruders (traditional security). The farmer may have an irrigation system to be used in the event of insufficient rainfall (redundancy). The farmer may plant different kinds of crops so that if environmental

conditions adversely affect one crop, others will survive (diversity). These strategies are good. If the crops fail, the farmer may turn to hunting or fishing to provide food for villagers. Hunting is not a security, reliability, or fault tolerance strategy. It is outside the system for growing food. This is a risk-management strategy that can only be formulated with an intimate understanding of the mission that must survive as we mentioned before.

In this section, we will compare survivability concept with other concepts such as dependability, fault tolerance, availability and security. We will discuss their relation and distinction.

- SURVIVABILITY AND DEPENDABILITY

Failure of the information systems can cause a major loss of service, and so their dependability is a major concern. Current facets of dependability, such as reliability and availability, do not address the needs of critical information systems adequately because they do not include the notion of degraded service as an explicit requirement. What is needed is a precise notion of what forms of degraded service are acceptable to users, under what circumstances each form is most useful, and the fraction of time in which such degraded service levels are acceptable. This concept is termed as survivability [20].

Dependability and survivability are actually very close to each other [1,8], especially when looking at three R's, Resistance relates to fault prevention in dependability terms; Recognition together with Recovery have much in common with fault tolerance. However, dependability focuses on random faults but survivability focuses on coordinated attacks by intelligent adversaries too. Language of survivability is particularly applicable to open systems operating in hostile environments [8]. The concepts of "graceful degradation" or "failing soft" are embedded in the notion of survivability.

Lipson and Fisher argue that survivability concentrates more on the trade off between functional and non-functional requirements of a system. Survivability does not concentrate on components as suggested in the case of dependability [28].

Table 1: Summary of Information survivability definitions in current literature.

Reference (s)	Definition
[3,4,11,12, 28,31,44]	Capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents
[46]	The ability of a system to continue the adequate performance of its critical services and functions even after (unforeseen) successful attacks has taken place.
[43]	The ability of an information system to continue to operate in the presence of faults, anomalous system behavior, or malicious attack
[23]	Robustness under conditions of intrusion, failure, or accident."
[39]	Defined in terms of a survivable system where it "must be adaptable, able to respond to attacks and achieve its goals."

Table 2: Summary of Definitions of survivability for telecommunication systems.

Reference(s)	Definition
[40]	Network survivability as: (i) the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and (ii) the mitigation or prevention of service outages from network failures by applying preventative techniques.
[42]	A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance. For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive the minimum acceptable level or post-disturbance functionality and the maximum acceptable outage duration.
[35]	Ability of a computer-communication system application to satisfy certain critical requirements in the face of adverse conditions. These requirements are: a) security b) reliability c) availability and d) performance.
[29]	Network survivability gauges the ability of the network to support the committed Quality of Services (QoS) continuously in the presence of various failure scenarios.
[16]	Survivable network must achieve an acceptable level of performance under demanding conditions.
[25]	Ability of a network to cope with facility outages, capacity overloads, and natural disasters.

- SURVIVABILITY AND FAULT TOLERANCE

Some documents [24] define survivability in terms of intrusion tolerance. They believe that if the fault is malicious, then the fault detection techniques are usually termed as intrusion detection and the fault tolerance techniques are termed either as intrusion tolerance or survivability. The basic goal of fault-tolerance and survivability are essentially the same [21].

One main goal of fault-tolerant system design is to mask hardware faults, such that failure of a component does not affect the ability of the system to perform its specifications. So, many solutions found in fault tolerant system designs are suitable for adaptation in order to increase survivability. Examples of such solutions are the introduction of time and information redundancy as well as space redundancy. However, in fault-tolerant systems, malicious faults are the least likely and in network security/survivability, the attacker is expected to behave maliciously. In some documents, survivability is used to express intrusion tolerance [24,45]. One large class of fault tolerant techniques uses a set of redundant components to determine the "correct" information; for example TMR (triple modular redundancy) and N-version programming. Such techniques implicitly assume that some distinguished elements of the power set of the redundant components are trustworthy. But, if an attack occurs, this assumption fails.

Survivability is a dependability property and is a measurable system characteristic; it is not synonymous with fault tolerance. Fault tolerance is a mechanism that can be used to achieve certain dependability properties. In terms of dependability, it makes sense to

refer to a system as reliable, available, secure, safe, and survivable, or some combination using the appropriate definitions(s). Describing a system as fault tolerant is really a statement about the system's design that can be used to improve its dependability and survivability.

- SURVIVABILITY AND AVAILABILITY

System survivability typically depends on two types of properties: availability and functional safety (implying functional correctness) [35]. The network survivability performance evaluation can be done by: the measurement of frequency of failure events, the duration of the outages and the impact of failures on the system [6]. The first two items may be resolved by availability analysis. Therefore, availability is an important aspect of survivability.

- SURVIVABILITY AND SECURITY

Survivability as applied to the U.S. Health Care and the U.S. Electric Power Industry is addressed in [4] and [3] respectively. They show that traditional computer security is not adequate to protect the mission critical requirements and that a survivability approach is required.

Security attacks are a major concern for critical information systems, and in some discussions, survivability is viewed as synonymous with secure operation. While traditional computer security tends to focus on keeping the "bad guys" out of the system [19], survivability goes beyond this in its concern for ensuring that the overall system can still operate even when the "bad guys" are already in the system. Thus, survivability involves dealing with situations in which security has proved to be inadequate. Although things like erroneous software upgrades operator mistakes, common-mode software faults have caused most significant service failures of critical information systems, however, the damage that can result from a security attack can, of course, be tremendous. This is not making the security less important; clearly security attacks (i.e., deliberate faults) are a serious concern.

Current security approaches to protect information systems have focused on preventing attacks from being successful by hardening defenses with authentication, encryption, and a variety of layer-violating network devices (i.e., firewalls, network address translators, intrusion detection systems) [48]. What is not being captured is the survivability of an entire system to failures or attack. Robustness under attack and recoverability are the essential characteristics that distinguish survivability from traditional computer security [22]. There is a research group called Survivability-Over-Security (SOS) [48]; their goal is to increase the survivability of information systems using innovative techniques, which simultaneously reduce net vulnerabilities and increase restoration flexibility. While security

is one technique to protect system components, they conclude that survivability is a higher goal over security since survivability encompasses the functionality of an entire information system and not individual components.

CHARACTERISTICS OF SURVIVABLE SYSTEMS

A key characteristic of survivable systems is their capability to deliver essential services in the face of attack, failure, or accident [10,26]. It is important to define minimum levels of such quality attributes that must be associated with essential services. For example, a launch of a missile by a defensive system is no longer effective if the system performance is slowed to the point that the target is out of range before the system can launch. These quality attributes are so important that definitions of survivability are often expressed in terms of maintaining a balance among multiple qualities attributes, such as performance, security, reliability, availability, modifiability, and affordability.

Key to the concept of survivability, then, is identifying the essential services and non-essential services within an operational system. Essential services are defined as the functions of the system that must be maintained when the environment is hostile or failures or accidents occur that threatens the system [31]. Non-essential services are to be recovered after intrusions have been dealt with. This can be seen as graceful degradation. To maintain their capabilities to deliver essential services, survivable systems must exhibit the four key properties illustrated in Figure 1, namely Resistance to, Recognition of, Recovery from intrusion (the three R's) and adaptation.

Resistance to attack: Resistance refers to the capability of a system to deter attacks [10,26]. Current strategies for resistances include the use of firewalls, authentication, message filtering and encryption. Diversification is an example of a strategy that will likely become important in future unbounded networks. Diversification requirements must define a planned variation in survivable system function, structure, and organization, together with a means for achieving it.

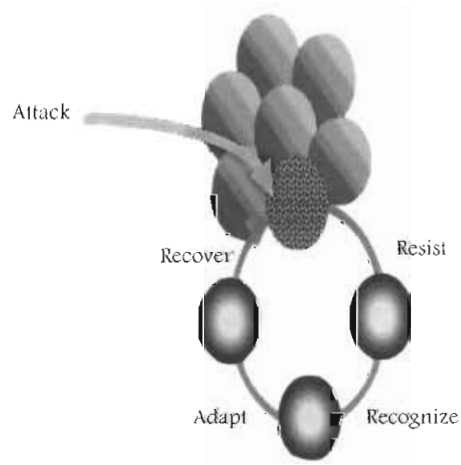

Figure 1: Survivable system with three R's [27].

Recognition of attacks and the extent of damage: Recognition refers to the capability to recognize attacks. Reaction or adaptation is impossible without some form of recognition. Some example strategies could be Intrusion detection and Integrity checking.

Recovery after attack: Recovery refers to a system's ability to restore services after an intrusion has occurred and to improve its capability to resist or recognize future intrusion attempts. Recovery also contributes to a system's ability to maintain essential services during intrusion. Today, recovery strategies in use include the replication of critical information and services, the use of fault-tolerant designs, and a variety of backup systems for hardware and software, including maintaining master copies of critical software in isolation from the network [26]. Future recovery strategies will most certainly include dynamic system adaptation, which will not only help a system recover from a current attack, but also permanently improve a system's ability to resist, recognize, and recover from future intrusion attempts. Figure 1 shows three R's concept in survivable system [27].

Adaptation and evolution to reduce effectiveness of future attack: Perhaps the hardest part of survivability is adapting a system to make it more robust in the hope that it will resist never-before-seen attacks or intrusions.

SURVIVABLE NETWORK ANALYSIS (SNA) PROCESS

The Survivable Network Analysis (SNA) method was developed by the SEI CERT Coordination Center of Carnegie Mellon University [31]. SNA is a practical engineering process that permits systematic assessment of the survivability properties of proposed systems, existing systems, and modifications to existing systems. The SNA method provides a means for organizations to understand survivability in the context of their operating environments. SNA reveals the risks and leads to strategies to increase the likelihood of a survivable system. The SNA method for assessing and improving the survivability of network architectures is depicted in Figure 2 [13]. Steps in the SNA method include system mission and architecture definition, essential capability definition, compromisable capability definition, and survivability analysis of architectural areas that are both essential and compromisable. SNA results are summarized in a survivability map which links recommended survivability strategies for resistance, recognition, and recovery to the system architecture and requirements. The process is adaptable to a variety of development processes and applies to infrastructure and applications. SNA objectives include identification of the following:

- Survivability risks to a system or infrastructure
- Effects of intrusions or incidents on the mission
- Processes, requirements, or architecture changes that can improve survivability

The analysis is carried out at the architecture level and is done in four steps [31].

Step 1: **System Mission and Architecture Definition**: Mission objectives and requirements for a current or proposed system are reviewed, and the structure and its primary functional requirements are elicited. The system architecture is elicited in terms of hardware components and connections, software configurations, and information residency. For example, the Fictional Company's (FC) primary function is to act as a payment brokering system for several on-line shopping websites. The mission objective is to provide flawless brokering of transactions between on-line shopping and credit card companies. Its architecture requires extranet connectivity, certificate authentication, firewall protection (unix based) on the front-end connectivity to the Internet and back-end firewall controls to credit companies and customers.

Step 2: **Essential Capability Definition:** Essential services are identified. Essential services and assets are those capabilities critical to fulfill the business mission. For example,

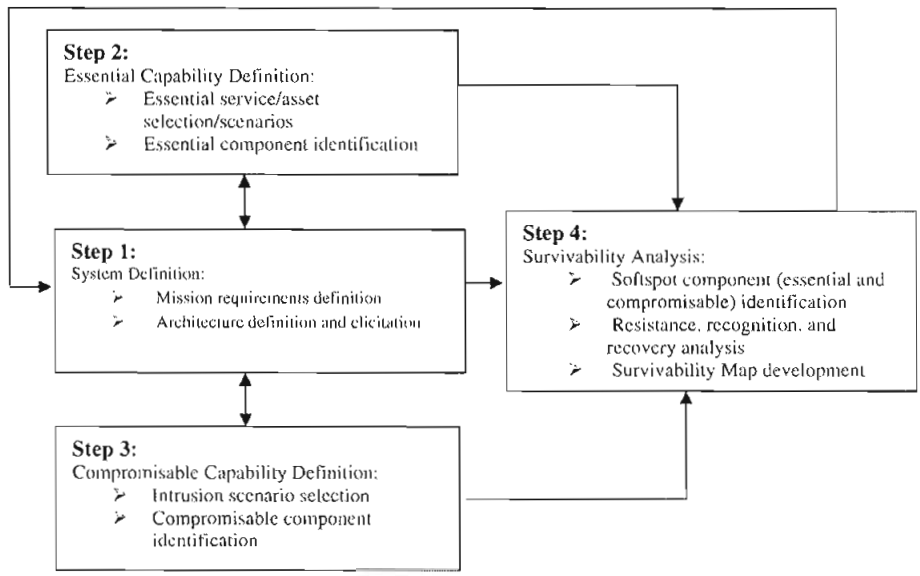

Figure 2: The survivable network analysis method

a Fictional Company (FC) would be required to provide services to keep extranet customers such as the credit card companies and online stores connected at all times for transactions to be occurred. Assets required for the transactions are the back-end firewall, database systems for record lookup, and application servers. Front-end systems are less essential being which are not involved in the actual transaction.

Step 3: Compromisable Capability Definition: A set of representative intrusions is selected based on the system's operating environment. Intrusion usage scenarios are defined and traced through the architecture to identify compromisable components that the intrusions could successfully access and damage. Steps 1-3 provide information to develop recommendations for architecture modifications, requirements changes, policy

revisions, and operational improvements. The goal is to identify survivability strategies for backup, configuration management and the three "R's" (resistance, recognition, recovery) by getting input from users, management, and system administrators. In the FC example, identification of scenarios dealing with failure/recovery of components such as a rudder, pilot must be aware of possible problems that may occur, recognize attack via radar, be aware of ground communication and visual scope, and be able to recover from attack by activating or using redundant systems.

Step 4: **Survivability Analysis:** Components that are both essential and compromisable are identified. The architecture is then analyzed for these components protection, in terms of its capability to resist, recognize, and recover from intrusions. Architectural recommendations are then formulated and summarized [27]. In the bomber example, the bomber would mitigate resistance by flying higher, flying at night, using tactics that draw less attention and use features on aircraft that hide presence. Implementation of recognition would be rear-facing cameras on the plane so the pilot can see behind or use an outside spotter for trouble. Another example is having infrared sensors to detect enemy fire. Recovery mitigation, in a worse case scenario, would be an ejection seat and recovers the pilot and crew from the sea/ground.

STRATEGIES TO IMPROVE NETWORK SURVIVABILITY

Techniques to improve network survivability can be classified into three categories [41]:

1. Prevention: improving component and system reliability (fault tolerant hardware)
2. Network design and capacity allocation: placing sufficient diversity and capacity in the network topology
3. Traffic management and restoration: direct the network load such that a failure has the minimum impact on network

The "ideal" survivability goal is to make a network failure imperceptible to the network user by providing service continuity and minimizing network congestion [41].

We will discuss each of these techniques.

- PREVENTION TECHNIQUE

Prevention techniques focus primarily on improving component and system reliabilities. Some examples are the use of fault-tolerant hardware architectures in switch design, provision for backup power supplies, use of frequency hopped spread spectrum techniques to prevent jamming in military radio networks and so on.

- NETWORK DESIGN AND CAPACITY ALLOCATION

Network design techniques try to use survivability strategies in the design phase to eliminate

the effects of system level failures such as link or node failures on the network. Placing sufficient capacity in the network topology can reduce traffic loss effect on the network in the presence of failure. Spare capacity allocation (SCA) [29] ensures enough spare capacity for the physical network or the virtual network to recover from a failure via traffic rerouting. The problem can be stated as how much spare capacity should be provisioned and where it should be located in order to minimize the impact of link or node failure on the network. We will discuss capacity design problem using an example for circuit switched networks [32].

Consider a circuit switched network with three nodes and three links as shown in Figure 3. We assume that the network has symmetric offered load and capacity. Offered load between any pair of nodes is assumed to be 10 erlangs, and the link capacity on each link is given to be 21 trunks. Assume that the traffic between each pair of nodes is routed on the direct link that connects the end nodes of the pair and call arrival follows a Poisson process. Using Erlang-B loss formula, the blocking probability [32] on each link is 0.001. Now, suppose that the link 2–3 fails. In this case, node 1 is still connected to node 3 via

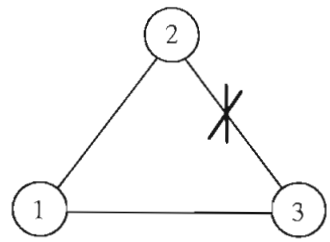

Figure 3: Three node network [32].

node 2. Assuming that the network still has the same amount of offered load, the load between node 2 and node 3 is now routed through node 1; thus, the offered load to each link is 20 erlangs now and the capacity on each link is still 21 trunks. Blocking probability for this case is 0.13144. This means blocking of traffic on each link is 0.13144, and the blocking seen by pair 2–3 traffic going through node 1 is even higher. Assuming b is the blocking probability of each link and also links are independent, the blocking on a path consisting of two links is $1-(1-b)^2$. Therefore, the blocking of traffic between 2-3 that goes through node 1 is 0.24558. In case of link failure, the blocking probability jumps to 0.24556, which may not be acceptable in some networks. If we want the network still provide a 0.1% blocking grade even under a single failure for every traffic pair, then to accommodate for the worst path blocking, we need link blocking on each of the remaining links to be 0.0005, which means each link capacity needs to be at least 36 trunks. This means that in order to cover each link failure, the network needs 80% more capacity. As we can see in this example, network capacity plays an important role in survivable network design. If the network is *not* provided with additional capacity, then the traffic blocking can be very high. In some circumstances, the network capacity needs to be 80% to 100% more to

provide the same level of service under a single link failure.

Based on when spare resources for backup paths are reserved, spare capacity allocation can be done in two ways:

1. **Pre-planned:** In this case, resources are reserved for any predicted failure. One of the choices for this design technique is 1+1 DP. DP stands for diverse protection. 1+1 denotes a dedicated standby arrangement: one working system and a completely reserved backup system which the transmit signal is copied on both systems. The receivers monitor both receive signal copies and switch from one to the other if either fails. This method's advantages are that it can guarantee survivability upon predicted failures and the restoration process is very fast. However, preplanned resources will be wasted if none of predicted failures happens. Another technique which can be used is 1:1 DP. It is like 1+1 DP, but the signal is not copied on the backup system and it can be used for other uses when not needed by the working system.

2. Dynamic: Dynamic methods try to allocate the spare resources when the failure happens. One of the examples for this method is 1:N DP. N working systems share one standby protection system. In 1:N DP, the receiver end of a failed system detects the failure and checks if the spare system is available. If so, the spare system is used. In this way, it can achieve better resource utilization but will risk the survivability assurance because the requested resource might not be available when it is requested upon failures.

- TRAFFIC MANAGEMENT AND RESTORATION

Restoration strategy specifies the responding action when a failure happens in a network. The restoration steps are shown in Figure 4.

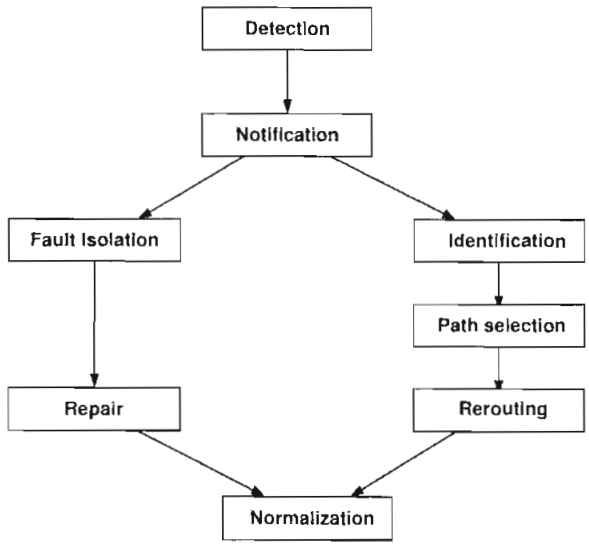

Figure 4: Restoration steps [29].

First, failure detection is responsible for deciding whether a failure exists or not. The

notification function advertises the failure information to all parties in the network, which are affected by the failure and those responsible for the restoration process. After that, the restoration process splits into two parallel processes. One is the repair process where the failure is isolated and repaired. The other is the reconfiguration process where the affected traffic flows are identified in the network nodes. The backup paths for these affected traffic flows are selected and rerouted. When the repair process is finished, the restoration process will go back to its normal state. It is also responsible to reroute the affected traffic from backup paths back to primary working paths.

According to the initialization locations of the rerouting process, restoration schemes are classified as

1- Link restoration:

2- Path restoration

In link restoration, the nodes adjacent to a failed link are responsible for rerouting the affected traffic flows. For example, consider a stream of packets from node 1 to node 4, as shown in Figure 5. If link 2-3 fails, nodes 2 and 3 are responsible to reroute the traffic to other available paths (2-5-6-7-3).

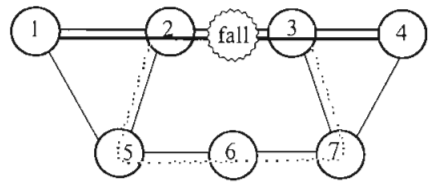

Figure 5: Link restoration schemes.

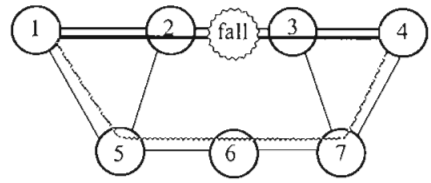

Figure 6: Path restoration schemes.

In path restoration, source and destination nodes initiate the rerouting process in case of any link failure. In Figure 6, node 1 and node 4 are responsible to reroute the traffic to other available paths (1-5-6-7-4) when link 2-3 fails. In general, path restoration requires less spare capacity reservation than link restoration [29]. However, path restoration is more complex to implement as many more nodes are involved in the restoration process. It is also slower in the speed of restoration as compared to link restoration.

In the next section, survivability of optical networks and protection techniques in WDM networks are reviewed as an example of techniques to improve the network survivability.

CASE STUDY: SURVIVABILITY TECHNIQUES IN OPTICAL NETWORKS

Wavelength-Division Multiplexing (WDM) networks are a promising candidate to meet the increase of bandwidth demand in the Internet. Optical networks based on WDM technology can potentially transfer hundreds of gigabits of data per second in the network. However, the high capacity of a link has the drawback that a failure can potentially lead to the loss of a large amount of data. This is why the survivability performance of WDM networks is an important research issue. The survivability techniques in optical networks can be classified under two general categories: predesigned protection and dynamic restoration [49], as shown in Figure 7. Predesigned protection refers to the fact that recovery from network failures is based on preplanned schemes. Usually, it relies on resources (fibers, wavelengths, switches, etc.) dedicated to protection purposes. In predesigned protection, some resources are reserved for recovery from failures at either connection setup or network design time, and kept idle when there is no failure. From this point of view, the use of capacity is not very efficient, but on the other hand, the level and speed of recovery from a failure can be guaranteed. Automatic Protection Switching (APS) and Self-Healing Ring (SHR) are the most common predesigned protection schemes used in non-WDM optical networks.

APS is typically used to handle link failures. It has three main architectures:

- 1+1
- 1:1
- 1:N

In 1+1 APS (Figure 8a), a protection link is provided for every working link. The source node transmits the information signal on both the working and protection links. The receiver at the destination node compares the two signals and chooses the less noisy one. If one link fails, the destination node is still able to receive the signal on the operational link.

In 1:1 APS (Figure 8b), every working link has a protection link, but the source and destination nodes switch to the protection link only when a failure on the working link is detected. Under normal conditions, the protection link is either idle or used to carry low priority traffic.

In 1:*N* **APS** (Figure 8c), *N* working links share a single protection link, thereby providing protection against the failure of any one of the *N* working links. But, unlike in 1:1 APS, the traffic switched to the protection link must be switched back to the working link after it is repaired so that the protection link is available for any future working link failures. In general, *m*:*n* protection refers to an APS scheme in which *m* protection links are shared among *n* working links.

SONET SHR is a very successful technique for survivable optical networks. Here,

networks are designed to have ring architectures. SHR can handle both link and node failures. Two types of SHR are: Unidirectional SHR (USHR) and Bi-directional SHR (BSHR). The difference between these two categories is the direction of the traffic flow under normal operation. In USHR, the normal traffic flow goes around the ring in one direction. Traffic is routed to the protection ring in opposite direction if failure happens. In BSHR, working traffic flows in both directions. These techniques are shown in Figure 9.

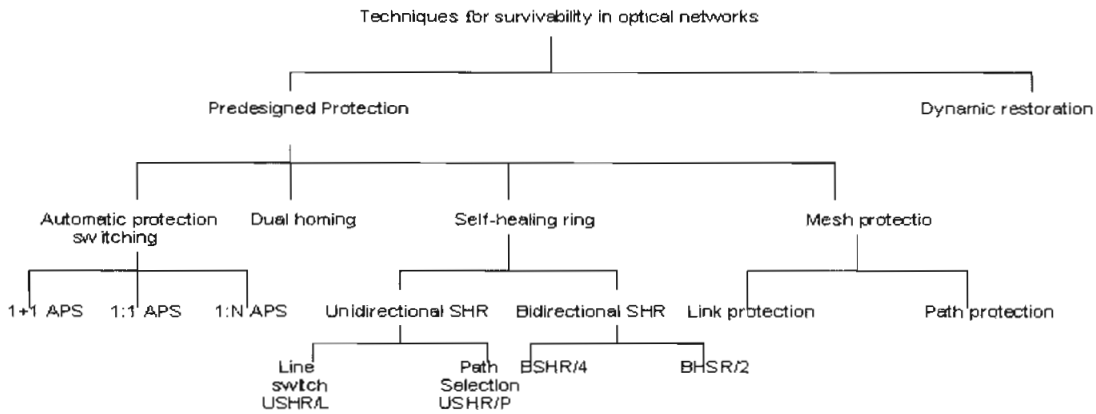

Figure 7: Survivability techniques in optical networks [49].

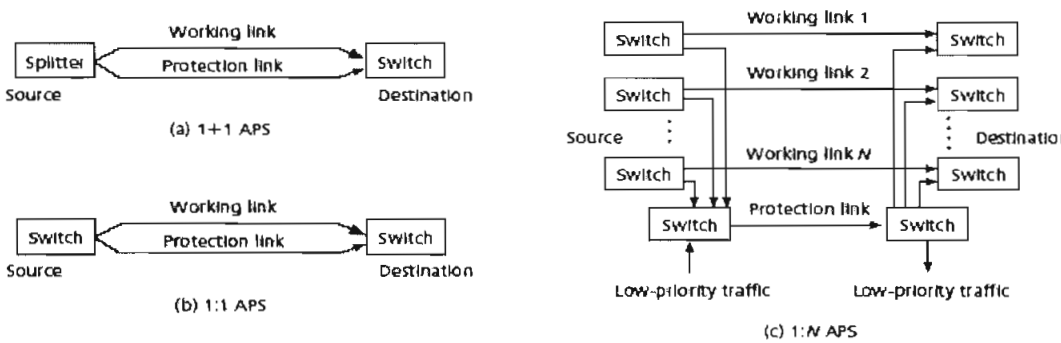

Figure 8 (a-c): Automatic protection switching (APS) [49].

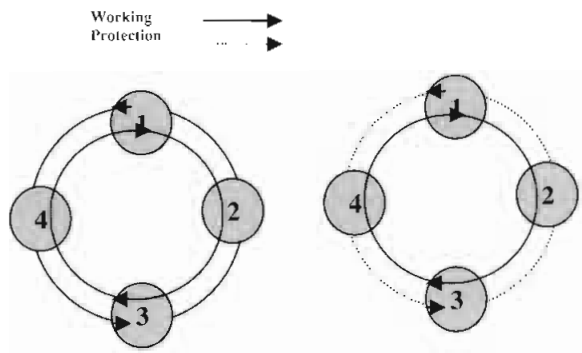

Figure 9: USHR and BSHR.

- SURVIVABILITY OF WDM

WDM systems are being widely deployed in the backbone network [49]. The use of optical

switches and all-optical components introduces a new network layer, called the *optical layer* or *WDM layer*, into the layered architecture. The WDM layer supports different higher-layer services, such as SONET connections, asynchronous transfer mode (ATM) virtual circuits, and IP-switched datagram traffic. The ideas used in WDM-layer protection are very similar to those in SONET systems, as described above [5,49]. For example, in point-to-point WDM systems, 1 + 1, 1:1, and 1:*N* optical protection are used in a way similar to APS in SONET systems, except that switching is done in the optical domain. Path or link restorations can be used in case of node or link failure. Dedicated or shared backup can be considered when designing network. In shared protection ring with two fibers, the working wavelengths on one fiber are from 1 to W/2 and the others are for restoration. On other fiber, working wavelengths are from W/2 to W and the others are for protection. 2x2 fast switches perform recovery (as shown in Figure 10). In case of failure, the working paths are routed in the opposite fiber with the same wavelengths.

In shared protection ring with four fibers, one fiber pair is used for working and the other pair for protection (as shown in Figure 11). No traffic is routed on protection fiber unless there is failure.

SURVIVABILITY ANALYSIS AND MODELING

Now, we will introduce various quantitative measures of failure impact, given a failure occurs, and of intrinsic survivability performance in terms of the ability to resist failures in the first place. Given the impact of failures, there is growing regulatory interest in attempts to quantify the magnitude of the impact of various failures that occur. Network operators are also interested in such standardized measures for quality improvement and

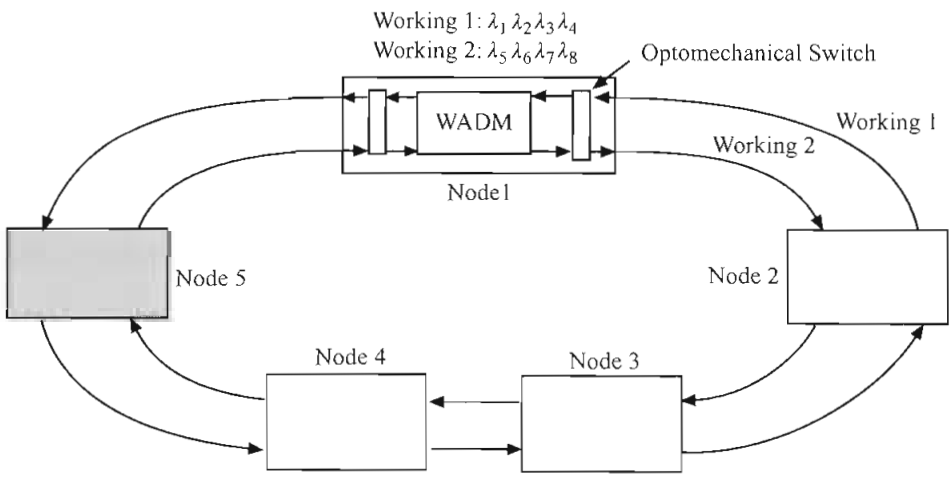

Figure 10: Two fiber WDM ring [34].

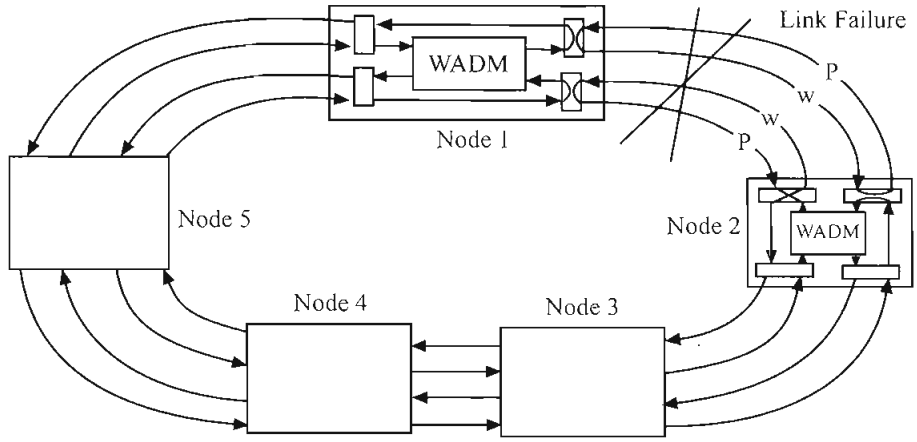

Figure 11: Four fiber WDM ring after link failure [34].

competitive processes. A second sense of "measuring survivability" is to ask about those intrinsic properties of a network that by design make it less likely to sustain an outage in the face of failures within itself. The term survivability itself is not usually given quantitative meaning but is used in general to refer to the quality of being able to keep on functioning in the face of either internal failures or externally imposed damage. The quantitative measures of survivability are necessarily more specific. One class of such measures is called conditional or Given Occurrence of Failure (GOF) models [50]. In these measures, each relevant failure scenario is first postulated to have occurred, and then an assessment of survivability is made. These tend to be design-oriented measures since they reflect the merit of a survivable design over a pre-specified set of failure scenarios against which coverage is to be ensured but do not depend on knowledge or assumptions about how often such failures may actually occur. They deal with questions such as "If failure x occurs, how well are network services protected from it?" A simple GOF-type measure, which is widely used in design and characterization of transport networks, is the restorability, also sometimes called the restoration ratio. As most commonly used, the restorability is defined as the fraction of working signal units that are subsequently restored, or that are topologically capable of being restored by replacement routes through the network. Survivability is calculated as a percentage of remaining network traffic flow to the original traffic after the network failure [17]. For example, In the case of link failure [33], network survivability degree (or restoration ratio) is defined as the ratio of traffic that restores after failure to total traffic along the link and in case of the node failure [14], routing performance is defined as the ratio of incoming requests and the demand routed successfully when the node is operating in degraded mode. When the node is operating in a degraded mode, it is incapable of creating and maintaining reservations for flows requiring guarantees, but continues to process routing and other control messages.

The other general class of survivability measures aims to take into account the probability of failure onset as well as the survivability response or capability of the network

[50]. These are called Random Occurrence of Failure (ROF) models. In contrast to the GOF orientation, ROF measures typically ask questions such as: "How likely is it that a path between nodes has an outage over x minutes in any given year?" ROF models are usually based on the assumption that failures can be characterized by random variables with given probability distribution functions. One of the most commonly used ROF-type measures of survivability is the expected annual loss of traffic (ELT) [15]. ELT is like traffic-weighted path availability. It is path-oriented measure in that it pertains to a transport signal path between a pair of nodes. For a given pair of nodes exchanging demand over possibly several paths through a network, ELT asks what the expected number of lost demand-minutes will be over a year. ELT reflects the size and number of demand units affected, diversity routing and/or restoration techniques.

A quantitative approach that considers both availability and failure impacts on the network is proposed in [6]. System availability analysis is used to find out the cost due to system downtime and system failure impact analysis is carried to find out the transient performance degradation when failure occurs. They analyzed wireless ad-hoc networks as an example for network survivability performance evaluation.

Placing sufficient diversity and capacity in the network topology can improve network survivability. An expression to find the variation of flow over the non-failed links in the case of link failure is proposed which can be used to compute the link capacity of survivable network [37].

We perceive that both performance and availability are integral components of survivability. Therefore, we propose a composite model for survivability that consists of performance and availability analysis [18]. An analytical technique is presented to find the excess loss due to failure (ELF) when the system is operating in gracefully degraded states. An algorithm is proposed to carry out the availability analysis of the network even when the available paths between nodes are non-disjoint. These two models are combined to construct a hierarchical model to evaluate the network survivability performance. We consider single and multiple link and node failures. A WDM network with wavelength conversion is used as an example for this evaluation. A summary of survivability measure models is illustrated in Table 3.

Table 3: Summary of survivability measure models in current literature.

References	Model
[33]	Network survivability is defined as the traffic that can be saved in the case of link failure. Now survivability degree (or restoration ratio) is defined as the ratio of traffic that restores after failure to total traffic along the link.
[14]	Routing performance is defined as the ratio of incoming requests and the demand routed successfully in case of node failure. The effect of availability on routing performance is also studied by using simulation.
[6]	A quantitative approach to evaluate network survivability is proposed. Their model consists of two parts: System availability analysis to find out the cost due to system downtime and system failure impact analysis to find out the transient performance degradation when failure occurs. Wireless ad-hoc networks is analyzed as an example for network survivability performance evaluation.
[37]	An expression to find the variation of flow over the non-failed links in the case of link failure is proposed. This expression can be used to compute the link capacity of survivable network.
[18]	A composite model for survivability that consists of performance and availability analysis is proposed. An analytical technique is presented to find the excess loss due to failure (ELF) when the system is operating in gracefully degraded states. An algorithm is proposed to carry out the availability analysis of the network even when the available paths between nodes are non-disjoint. These two models are combined to construct a hierarchical model to evaluate the network survivability performance.
[38]	The performance of the network is used as the analysis of survivability. Networks are evaluated with and without restorations. Two types of survivability measures have been proposed: deterministic and probabilistic. A deterministic survivability measure depends on the topology of the network and probabilistic survivability measure depends on the probability of failures and also reliability of each component in the network. Network is defined as an undirected graph with finite number of nodes and links. They find: 1) Terminal survivability which is the fraction of traffic between a specific pair of nodes that can be carried by the network. 2) Network survivability is the fraction of traffic that can be carried by the network.
[50]	Two basic approaches to survivability analysis are proposed. 1) Probability of network failures and repair rates are used to calculate network availability or unservability. 2) After a given failure events, restored traffic is calculated.
[41]	Survivability is used to describe the available performance of a network after a failure. A survivability analysis measures the degree of functionality remaining in a system after a failure.
[17]	Survivability is calculated as a percentage of remaining network traffic flow to the original traffic after the network failure.

CONCLUSIONS AND FUTURE TRENDS

Survivability is a new approach to the design and protection of the systems. Here, current literature on the information and network survivability has been thoroughly reviewed. We discussed the information and network survivability concepts and its relation to and distinction from dependability, fault tolerance and security. Researchers can use the results of this paper as a baseline from which they build subsequent efforts while recognizing the need to move the study of computation of survivability from theory to practice. The findings of this paper also support the need for a standardization of the definition of survivability that may facilitate subsequent research into computational quality attributes.

We reviewed the survivability of optical networks and protection techniques in WDM networks. We also summarized some survivability measures from network analysis and design point of view.

REFERENCES

[1] Avizienis, A., et al., "Fundamental Concepts of Dependability." *3rd Information Survivability Workshop*, (ISW-2000), Boston, Massachusetts, Available: at <www.cert.org/research/isw/isw2000/papers/table_of_contents.html>, October, 2000.

[2] Ball, R. E. *The Fundamentals of Aircraft Combat Survivability Analysis and Design.* American Institute of Aeronautics and Astronautics (AIAA), 2003.

[3] Byon, I., *Survivability of the U.S. Electric Power Industry*. Master thesis, Carnegie Mellon University Pittsburgh, Pennsylvania, 2000.

[4] Caldera, J. *Survivability Requirements for the U.S. Healthcare Industry*. Master thesis, Carnegie Mellon University Pittsburgh, Pennsylvania, 2000.

[5] Chalasani, S. and Rajaravivarma, V., "Survivability in Optical Networks." *Proceedings of the 35th Southeastern Symposium on System Theory*, pp. 6 –10, 2003.

[6] Chen, D. et al., "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks." *The Fifth ACM International Workshop on Modeling*, Analysis and Simulation of Wireless and Mobile Systems, Available: at <http://www.ee.duke.edu/~dc/publications/p77-chen.pdf>, September 2002.

[7] CMU SEI Survivability, Available: at <http://www.sei.cmu.edu/organization/programs/nss /surv-net-tech.html>.

[8] DDSI (Dependability Development Support Initiative), IST-2000-29202, Work Package 1, Conceptual Framework DRAFT, King's College London (UK), Available: at <http://www.cript.gov.au/cript/Docs/DDSI%20WP1-1%20V1.0_final_draft_version.pdf>, 2002.

[9] Deutsch, M. S. and Willis, R. R., *Software Quality Engineering: A total Technical and Management Approach*. Englewood Cliffs, NJ, Prentice-Hall, 1988.

[10] Ellison, B., et al., *Survivable Network Systems: An Emerging Discipline*. Technical Report CMU/SEI-97-TR-013 ESC-TR-97-013, 1999.

[11] Ellison, R. J., et al., "An Approach to Survivable Systems." *NATO IST Symposium on Protecting Information Systems in the 21st Century*, Washington, DC, October 1999.

[12] Ellison, R. J., et al., *A Case study in Requirements for Survivable Systems*. SEI, 2002.

[13] Ellison, R. J. et al., "A Case Study in Survivable Network System Analysis." *Technical Report CMU/SEI-98-TR-014 ESC-TR-98-014*, 1998.

[14] Gokhale, S. and Tripathi, S., "*Effect of Unreliable Nodes on QoS Routing.*" *Seventh Annual International Conference on Network Protocols*, Toronto, Canada, Available: at <http://www.nmsl.cs.ucsb.edu/~ksarac/icnp/1999/papers/1999-19.pdf>, October-November 1999.

[15] Grover, W. *Mesh-Based Survivable Transport Networks: Options and Strategies for Optical. MPLS, SONET and ATM Networking*. Prentice Hall PTR, 2003.

[16] Huffman, S., et al., "Issues for Proliferated Survivable Network Design." *Global Telecommunications Conference*, IEEE, pp. 489-492, 1988.

[17] Jiang, T. Z., "A New Definition of Survivability of Communication Networks." *Military Communications Conference*, IEEE, pp. 2007-2012, 1991.

[18] Keshtgary, M., et al., "Network Survivability Performance Evaluation with Applications in WDM Networks with Wavelength Conversion." *29th Annual IEEE Conference on Local Computer Networks*, Tampa, Florida, USA, November 2004.

[19] Kihlstrom, K. P., "Survivable Distributed Systems: Design and Implementation." *Ph.D. Dissertation*, Tech. Rep. 99-19, Dept. of Electrical and Computer Engineering, University of California, Santa Barbara., Available: at <http://www3.westmont.edu /kimkihls/thesis. pdf>, 1999.

[20] Knight, J. C., et. al., "Towards a Rigorous Definition of Information System urvivability." *Darpa Information survivability conference and exposition*, Washington DC, Vol. 1, Avaolable: at <www.cs.virginia.edu/~jck/publications/discex.2003.pdf>, 2003.

[21] Krings, A., et al., "Survivability of Computers and Networks Based on Attack." *3rd Information Survivability Workshop*, (ISW-2000), Boston, Massachusetts, Available: at <www.cert.org/research/isw/isw2000/papers/table_of_contents.html>, October 2000.

[22] Krings, A. "Survivable Systems & Networks Course." Available: at <http://www.cs. uidaho.edu/~krings/CS404/>.

[23] Kyamakya, K. et al., "Security and Survivability of Distributed Systems: An Overview." *21st Century Military Communications Conference Proceedings*, IEEE, Vol. 1, pp. 1204-1208, 2000.

[24] Lala, J. H., "Intrusion Tolerant Systems." *Pacific Rim International Symposium on Dependable Computing (PRDC'00)*, Los Angeles, California, pp. 3-6, Available: at <http://www.computer.org/proceedings/prdc/0975/09750003.pdf>, December 2000.

[25] Laretto, K. G., "Sprint Network Survivability." *Military Communications Conference*, IEEE, pp. 587-597, 1994.

[26] Linger, R. C. et al., "Requirement Definition for Survivable Network Systems." *Requirements Engineering, Proceedings, Third International Conference on*, pp. 14-23, 1998.

[27] Lipson, H. F., "Survivability - A New Security Paradigm for Protecting Highly Distributed Missin Critical Systems" *38th Meeting of IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance*, Kerhonkson, NY, Available: at<http://www. cert.org/archive/pdf/surviv-paradigm.pdf>, June-July 2000.

[28] Lipson, H. F. and Fisher, D. A., "." *Proceedings of the 1999 ACM New Security Paradigms Workshop*, Caledon Hills, Ontario, Canada, pp. 33 - 39, September 1999.

[29] Liu, Y., "Spare Capacity Allocation: Model, Analysis and Algorithm." *Ph.D. Dissertation*, University of Pittsburgh, 2001.

[30] Manchester, J. et al., "Protection, Restoration, and Disaster Recovery." *IEEE Network*, Vol. 18, No. 2, pp. 3-4, 2004.

[31] Mead, N. R., et al., *Survivable Network Analysis Method.* CMU/SEI-2000-TR-013 ESC-TR-2000-013. Available: at <www.cert.org/archive/pdf/00tr013.pdf>, 2000.

[32] Medhi, D., " *(invited paper) Wiley Encyclopedia of Electrical and Electronics Engineering*, Webster, J. G., (Ed.), Vol. 14, pp. 213-218, Available: at <http://www.cstp. umkc.edu/public/papers/dmedhi/m_jweee99. pdf>, 1999.

[33] Moitra, S. D. et al., "Some New Survivability Measures for Network Analysis and Design." *IEICE Trans. Communication*, Vol. E80-B, No. 4, pp. 625-631, 1997.

[34] Nair, S. "Protection and Restoration of Optical Network." *Advanced Network & Systems Security Course*, CSE 8394, Available: at <http://www.engr.smu.edu/~nair /courses/ 8344/wdm_protection.ppt>, 2002.

[35] Neumann, P. G., "Practical Architectures for Survivable Systems and Networks." (Phase-Two Final Report), SRI International, Available: at <http://www.csl.sri.com /neumann/ survivability.pdf>, 2000.

[36] Nikolopoulos, S. D., et al., "Addressing Network Survivability Issues by Finding the K-Best Paths Through a Trellis Graph." *INFOCOM '97*, Proceedings IEEE, Vol. 1, pp. 370-377, 1997.

[37] Pierre, S. and Beaubrun, R., "Integrating Routing and Survivability in Fault-Tolerant Computer Network Design." *Computer Communications,* Vol. 23, pp. 317-327, 2000.

[38] Shi, J., and Fonseka, J. P., "Traffic-Based Survivability Analysis of Telecommunications Networks." *Global Telecommunications Conference*, IEEE, Vol. 2, pp. 79-87, 1995.

[39] Shrobe, H., "Model-Based Troubleshooting for Information Survivability." *DARPA Information Survivability Conference and Exposition*, IEEE, Vol. 2, pp. 231-240, 1999.

[40] T1A1.2 Working Group, Available: at <http://www.tl.org/tlal/_A12-HOM.HTM>.

[41] Tipper, D. "PCS Network Survivability." *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'99)*, New Orleans, LA, pp. 1028-1032, 1999.

[42] U. S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Services, Federal Standard 1037C, Available: at <http://www.its.bldrdoc.gov/fs-1037/>.

[43] Voas, J. M. and Ghosh, A. K., "Software Fault Injection for Survivability." *DARPA Information Survivability Conference and Exposition*, IEEE, Vol. 2, pp. 256-270, 1999.

[44] Wang, C. et al., "Protection of Software-Based Survivability Mechanisms." *The International Conference on Dependable Systems and Networks*, IEEE, pp. 1413-1420, 2001.

[44] Wu, T., *Fiber Network Service Survivability*. Artech House, Inc, 1992.

[45] Wang, F., "Vulnerability Analysis, Intrusion Prevention and Detection for Link State Routing Protocols." *Ph.D. Dissertation, North Carolina State University*, Electrical and Computer Eng., Raleigh, 2000.

[46] Wilikens, M. and Jackson, T. "Survivability of Networked Information Systems and Infrastructures." European Commission Directorate, Available: at <http://dsa-isis.jrc.it/EDI-Hub/pdf/survivability.pdf>.

[48] Yurick, W. et al., "Survivability-Over-Security: Providing Whole System Assurance." *3rd Information Survivability Workshop*, (ISW-2000), Boston, Massachusetts, Available: at <www.cert.org/research/isw/isw2000/papers/table_of_contents.html>, October 2000.

[49] Zohu, D. and Subramaniam, S., "Survivability in Optical Networks." *IEEE Network*, pp. 16-23, November-December 2000.

[50] Zolfaghari, A. and Kaudel, F. J., "Framework for Network Survivability Performance." *Journal on Selected Area in Communications*, IEEE, Vol. 12, No. 1, pp. 1615-1616, 1994.