A Spare Capacity Planning Methodology for Wide Area Survivable Networks

by

Adel A. Al-Rumaih

ISBN: 1-58112-046-X

DISSERTATION.COM

1999

PATENT PENDING

ISBN: 1-58112-046-X

Dissertation.com
1999

www.Dissertation.com/library/112046xa.htm

A SPARE CAPACITY PLANNING METHODOLOGY FOR WIDE AREA SURVIVABLE NETWORKS

By

Adel A. Al-Rumaih

[B.S. in Computer Science and Engineering, University of Petroleum and Minerals], 1986

[M.S. in Electrical Engineering, King Saud University], 1993

Submitted to the Graduate Faculty of

Department of Information Science and Telecommunications at

School of Information Sciences

in partial fulfillment of the requirements of the degree of

Doctor of Philosophy

University of Pittsburgh

1999

University of Pittsburgh
Department of Information Science and Telecommunications

Dissertation Defense

Name of Student: ADEL AL-RUMAIH

Dissertation Title: "A Spare Capacity Planning Methodology for Wide Area Survivable Networks"

Committee:

Name	Signature	Accept	Department
Dr. Paul Munro		yes	DIST
Dr. James G. Williams		Yes	DIST
Dr. Marek Druzdzel		YES	DIST
Dr. Bryan Norman		Yes	Engineering

Major Advisor:

Dr. David Tipper		Yes	DIST

Date: January 13, 1999

DIST Chair: _____ **Date:** 1/15/99

To my parents

Dr. David Tipper
Research Advisor

A SPARE CAPACITY PLANNING METHODOLOGY FOR WIDE AREA SURVIVABLE NETWORKS

Adel A. Al-Rumaih, Ph. D.

University of Pittsburgh, 1999

ABSTRACT

In this dissertation, a new spare capacity planning methodology is proposed utilizing path restoration. The approach is based on forcing working flows/traffic which are on paths that are disjoint to share spare backup capacity. The algorithm for determining the spare capacity assignment is based on genetic algorithms and is capable of incorporating non-linear variables such as non-linear cost function and QoS variables into the objective and constraints.

The proposed methodology applies to a wider range of fault scenarios than most of the current literature. It can tolerate link-failures, node-failures, and link-and-node failures. It consists of two stages: the first stage generates a set of network topologies that maximize the sharing between backup paths by forcing them to use a subset of the original network. The second stage utilizes a genetic algorithm to optimize the set of solutions generated by the first stage to achieve an even better final solution. It can optimize the solution based on either minimizing spare capacity or minimizing the total network cost. In addition, it can incorporate QoS variables in both the objective and constraints to design a survivable network that satisfies QoS constraints.

Numerical results comparing the proposed methodology to Integer Programming techniques and heuristics from the literature are presented showing the advantages of the technique. The proposed methodology was applied on 4 different size networks based on spare capacity optimization criteria and it was found that it achieved solutions that were on average 9.3% better than the optimal solution of the IP design that is based on link-restoration. It also achieved solutions that were on average 22.2 % better than the previous heuristic SLPA.

The proposed methodology is very scalable. It was applied on networks with different sizes ranging from a 13-node network to a 70-node network. It was able to solve the 70-node network in less than one hour on a Pentium II PC. The curve-fitting of the empirical execution time of the methodology was found to be $O(n^3)$.

KEYWORDS

Survivable networks, spare capacity, capacity assignment, mesh restoration, genetic algorithm, capacity placement, network design, path restoration, quality of service, delay calculations

Acknowledgements

All thanks are due to Allah for showing his mercy and grace to me in this life. Allah gave me the chance and the means to do this work.

I would like to express my deepest gratitude to my advisor, Dr. David Tipper, for his support, encouragement, invaluable guidance throughout the course of this work, and most of all, for being a good friend. His knowledge, dedication, and work ethics have been a constant source of inspiration. Without his patience and understanding in difficult times, it would most probably not be possible to complete this work.

My thanks to Dr. Bryan Norman, a member of my Ph.D. committee, for his constructive criticism, and useful suggestions to improve the genetic algorithm implementation. I would also like to thank the other members of my Ph.D. committee, Dr. Jim Williams, Dr. Marek Druzdzel, and Dr. Paul Munro for their invaluable comments, useful suggestions and for taking the time to make sure this work was a quality one.

I gratefully acknowledge the financial support I received from the Ministry of Defense and Aviation, Saudi Arabia. I am grateful to General Saad Al-Rumaih and Dr. Ibrahim Al-Nasser for their personal support regarding this matter. There are many other people who have helped me. I apologize for not naming them all, but I would like to thank them all.

I will always be grateful to my parents, for their du'aa, love, understanding, help, and continuing support throughout the years. My brothers deserve special thanks for their encouragement, concern, and for only being a phone call away when I needed them.

I save my final, insufficient word of gratitude for my wife, Maha, for her help, patience, and for sacrificing her time throughout the course of my Ph.D. study. I am indebted to my wife and my kids, Fatmah, Albatul, Omar, and Norah for providing me with the moral support that has made it possible to accomplish the work presented in this dissertation.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Due to the widespread use of telecommunication networks and society's increasing dependence upon the exchange of information, reliable network services have become essential for societal growth and survival. Many organizations and individuals now rely heavily on voice (e.g., phone calls), data (e.g., Internet resources, facsimile transmission, electronic fund transfer), and video (e.g., video conferencing) services in their day-to-day activities. Disruption of telecommunication services may result in both short-term and long-term effects. Short-term effects would be things like the loss of emergency services (e.g., 911), or airport traffic-control. The long-term effects of such disruptions include things like a company's loss of business (e.g. an Internet service provider) to competitors due to unreliable telecommunication service.

Survivability has become a critical issue in telecommunication networks due to the growing society reliance on telecommunications, on the one hand, and the increasing importance of information exchange, on the other hand. This vital relationship between society and telecommunications reflects the importance of having stable and secure

telecommunication networks. Previous studies of network reliability identified network failures and classified them into the following categories:

- Architectural / Implementation defects
- Human errors
- Environmental hazards
- Accidents
- Sabotage
- Operational disruptions

Architectural/implementation defects: include designing and manufacturing defects, software bugs, database errors, etc. Human errors: include maintenance and procedural errors, errors during upgrades, and rearrangement of equipment. Environmental hazards: include floods, fires, lighting, earthquakes, and hurricanes. Accidents: include things like cutting of underground cable by a construction activity. Sabotage: includes things like vandalism, software break-ins, etc. Operation disruptions: include things like intentional breaking of links to carry out networks' expansion or maintenance operations [1, 2].

Because of the recent advances in the technology of computer equipment, communication devices, and software systems, telecommunication networks have become a major part of the national infrastructure of civilized countries. Thus, many structures of society including business, finance, air traffic control and reservation, education, medicine, security, and government agencies are among those who are critically dependent on reliable telecommunication networks. Hence, telecommunication networks are identified as one of the nations' most critical infrastructures. Because of its importance, telecommunication incapacity or destruction would have a debilitating

impact on the national defense or economic security of any modern country. Threats to these critical infrastructures can be classified into two categories: “physical threats” (tangible) to the telecommunication network facility, and “cyber threats” which include computer-based attacks on the information or communication components that control the critical infrastructures. In this regard, the U.S. government took three major actions to overcome these threats: first, establishing the Reliability and Vulnerability Working Group (RVWG), as part of the Information Infrastructure Task Force (IITF) of the National Information Infrastructure (NII). RVWG aims to develop a survivable and reliable national telecommunication architecture that satisfies the requirements of the national security and emergency preparedness of the nation [3]. Secondly, the establishment of the “information survivability” program by the Department of Defense (DoD), which aims to create affordable, verifiable, scalable technologies for reliable defense infrastructure [4]. Thirdly, the formation of the president’s commission on critical infrastructure protection to formulate a comprehensive national strategy for protecting the nation’s critical infrastructures. These infrastructures include: telecommunications networks, electric power systems, gas and oil production, storage and transportation, banking and finance, transportation, water supply systems, government services, and emergency services [4].

One of the main reasons for the increased focus on telecommunication network survivability is that economies of scale over the last ten years have caused network providers to deploy optical fibers (with high bandwidth capability), to provide higher throughput for the network, resulting in a higher average traffic cross-section for a given cable [5]. Deploying more optical fibers in telecommunication networks tends to make

the network topology sparser (the connectivity of the network topology graph decrease). As a result, a failure in a network link will have larger impact on network reliability since an optical transmission link can carry a significant amount of traffic.

Network survivability has recently attracted many researchers to investigate it [1, 6-14], and it recently became an area of interest by itself [15]. There is no standard definition for the term “survivability”; however, it is defined in some literature as “the capability of a network where a certain percentage of the traffic can still be carried immediately after a failure” [16]. In [17], the researchers defined it as “the ability of a network to cope with facility outages, capacity overloads, and national disasters.” Network survivability was also defined in [18] as: (1) the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and (2) the mitigation or prevention of service outages from network failures by applying preventive techniques.

Survivability procedures are essential to recover the lost service of the network that occurs due to a network component failure. To start with, survivable network design generally has three stages: physical topology configuration, path distribution between each node-pair, and spare capacity assignment. Physical topology configuration will be discussed in section 1.2.1 (Survivable Network Design, page 6), path distribution will be discussed in section 1.2.2 (Traffic Flow Management, page 15), and spare capacity assignment in survivable networks will be presented in Chapter 2 (This chapter presents a review of previous work presented in the literature for solving the spare capacity problem in survivable networks. The two approaches in solving the spare capacity problem are

discussed in details in the first section. The problem considered in this dissertation is presented in the second section).

The organization of this dissertation is as follows: in this chapter, a background of survivable network techniques will be presented which include: (1) survivable network design, and (2) traffic flow management in survivable networks. In the second chapter, (1) a survey of the spare capacity planning research in survivable networks (reviews and discussions) is presented, and (2) the problem considered in this research is identified with the research objectives. In the third chapter, the proposed new methodology for economical spare-capacity planning for a large-size survivable network with link, node, both link and node failure tolerances, and quality of service (QoS) is discussed and illustrated. Chapter 4 discusses the implementation details of the proposed methodology with its sensitivity analysis. In the fifth chapter, there is a comparison between the proposed methodology and previous approaches with numerical results and discussions. In the sixth chapter, the scalability of the proposed methodology and the incorporation of QoS constraints are illustrated. Finally, a conclusion with the main contributions of this dissertation and future work is presented in the last chapter.

1.2 Background

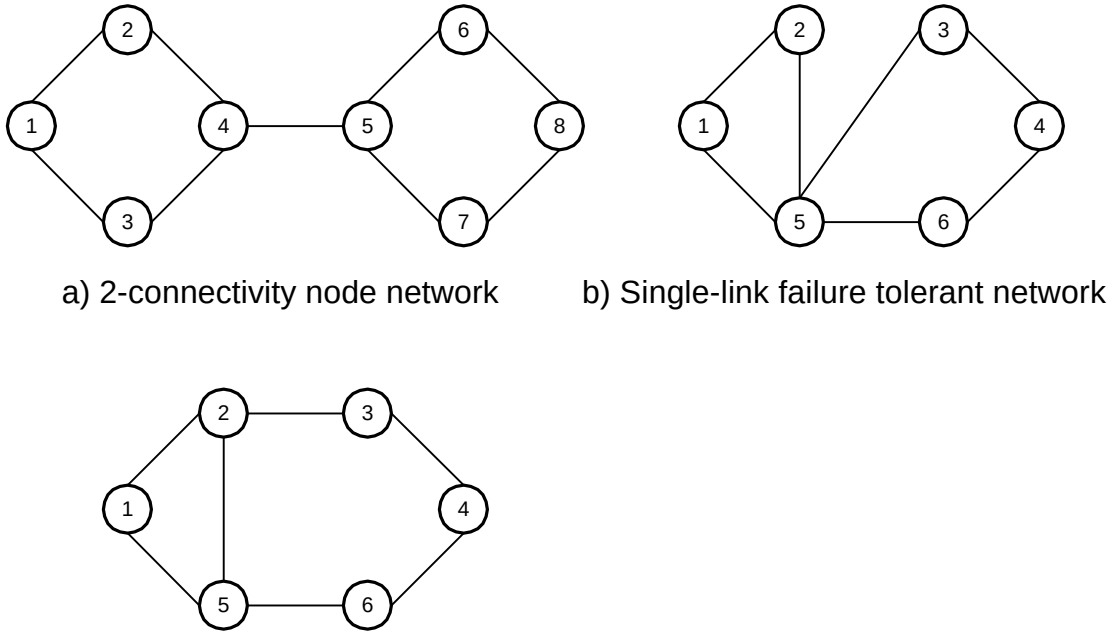
Telecommunication networks consist mainly of links and nodes. Links are the transmission media between nodes. Nodes are the processing units (e.g. switches, routers, digital cross-connect switches) of the network. Links can be of any type of transmission media such as fiber, copper, coax, microwave, and satellite [19]. Network failures can be classified into link failures, node failures, link and node failures. Link failures include

things like cable cut, and interface card failures. Node failures include things like hardware malfunctions, software bugs, and operational failures. Link and node failures include both the failures of links and nodes.

Survivable network design includes the capability of the network to tolerate network failures. In order for the network to tolerate failures, it should have many characteristics in terms of topology, link capacities, and working and backup traffic routing. In this section, survivable network design will be discussed with its different architectures, in addition to the traffic management of survivable networks.

1.2.1 Survivable Network Design

Network survivability depends mainly on the network architecture. Network architecture design determines which survivability mechanism could be used to restore the network from different failures. All network failure discovery and restoration procedures are designed to take advantage of the architecture of the network. In order to have a survivable network, we should have some kind of redundancy in network resources. The excess resources are utilized to recover the lost network service due to a failure. These extra resources can be links, bandwidth, buffers, or a combination of them. In order for the network to be survivable in case of failures, its topology should have specific characteristics. For a single-link failure tolerance, the connectivity of the nodes should be at least of degree two. However, not all networks with degree 2-connectivity nodes can mitigate single-link failures (see Figure 1.1a for an example). In Figure 1.1a, if the link between nodes 4 and 5 fails, the network will be separated into two disconnected sub-networks.



a) 2-connectivity node network b) Single-link failure tolerant network

c) Single-node failure tolerant network

Figure 1.1 Network Topologies with Different Levels of Failure Tolerance

Another way to verify if a given network is survivable for single-link failures, is by testing if there are at least two link-disjoint paths between each node-pair of the network. Figure 1.1b shows a network that is single-link failure tolerant, but not single-node failure tolerant. For the single-node failure survivability, we should have at least two node-disjoint paths between each node-pair of the network. Figure 1.1c shows a network which is both single-link and single-node failure tolerant [1]. For a simultaneous two-link failure tolerant network, we should have at least three link-disjoint paths between each node-pair of the network. Similarly, for a simultaneous three-link failure tolerant network, we should have at least four link-disjoint paths between each node-pair

[1] Any network with n-node failure tolerant is also n-link failure tolerant

of the network, and so on[2]. As a result, the number of links, the connectivity of nodes, and the capacity of links required are increased for multiple failure survivable networks.

The traffic load between each pair of nodes is the amount of traffic (voice, data, or video) that should be sent across the network per unit time. The network should have adequate capacity on its links to handle all the traffic load of each node-pair of the network according to some quality of service (QoS) constraints. The QoS constraints can be a connection blocking requirement, and/or delay constraints such as maximum link delay, average path delay, maximum path delay, average network delay, or a combination of two or more of them. In packet-based networks, one is also concerned with QoS metrics like packet loss rates and path delay jitter. In addition to providing a QoS level for a normal operation, a survivable network should have additional (spare) capacity on the links to use for rerouting traffic around any failed link/node. Since this spare capacity is redundant and may be reserved for use in case of failures, an important goal in survivability research is to minimize spare capacity as much as possible without affecting the survivability level of the network [11-13, 20, 21].

Survivable network architectures are generally classified into two categories: dedicated facility restoration and dynamic facility restoration [22]. Dedicated facility restoration uses standby resources that are dedicated for failure restoration, and not used during normal operation of the network, such as an automatic protection switch (APS) and self-healing rings (SHRs). Dynamic facility restoration uses spare resources within working facilities to restore lost services in case of failures. Dynamic facility restoration

[2] For an n node-failure tolerant network, there should be at least n+1 node-disjoint paths in the network

includes techniques such as dual homing and dynamic routing with mesh-type network architectures. We briefly illustrate these concepts.

1.2.1.1 Automatic Protection Switch (APS)

APS is a technique used in case a cable is cut between two nodes (which are connected by a link). One type of APS is 1:1 that means there is one standby cable for each working cable between any two nodes connected by a link [22, 23]. In case of a failure in the working cable, the traffic will be switched to the standby cable almost immediately (within 50 msec.[24]) and the service will be restored without any serious interruption.

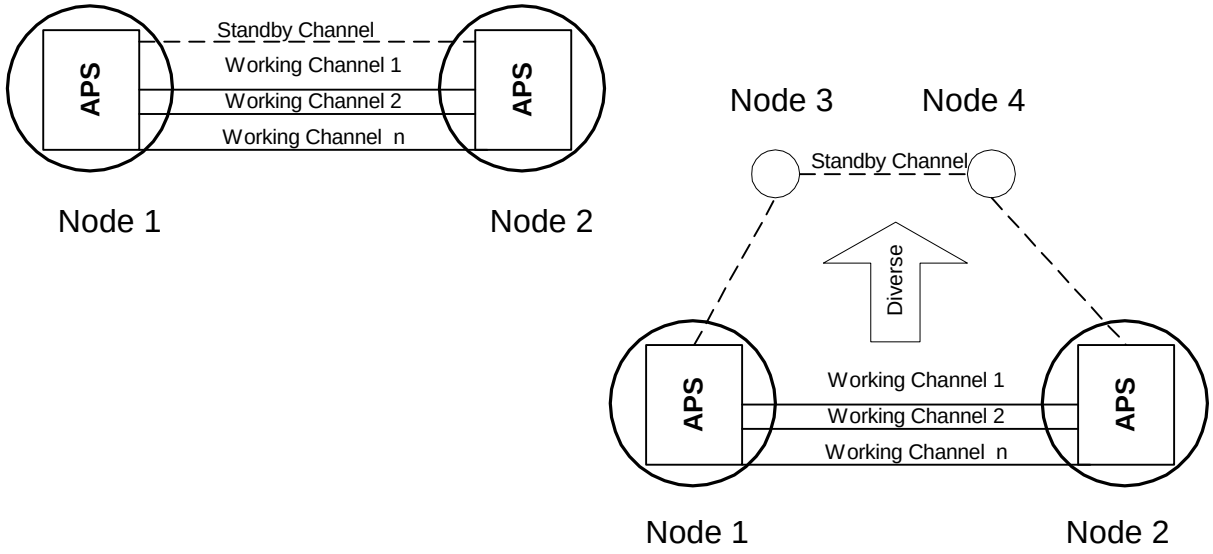


Figure 1.2 Automatic Protection Switch (APS) and APS with Diverse Protection (APS/DP)

Another type of APS is 1:N, which means that there is one standby cable for N working cables. In this case, the survivability has decreased since only one of the working cables could be recovered in case of failures; however, the standby facility has

been reduced by a factor 1/N. The standby facility could be physically on a different route than the working facility, which in this case is called APS with diverse protection (APS/DP). 1:1 APS/DP means that there is a standby cable for each working cable, but the standby cable is placed physically on a diverse route other than the working cable. 1:N APS/DP means that there is only one standby cable for each working cable in a diverse physical route. The problem with APS (without DP) is that a cable cut may result in cutting both the working and standby cables at the same time, while this does not occur in the case of diverse protection (DP). 1:1 APS/DP provides 100 % survivability level, while 1:N APS/DP provides only 100/N % survivability level. However, 1:1 APS requires more facility and equipment (cost) than 1:N [22].

A fully restorable APS/DB system requires 100% capacity redundancy (total spare to working capacity ratio) in the network. In addition, it is limited to link-failure tolerance only, it can not alone tolerate node-failures, or line card failure [25].

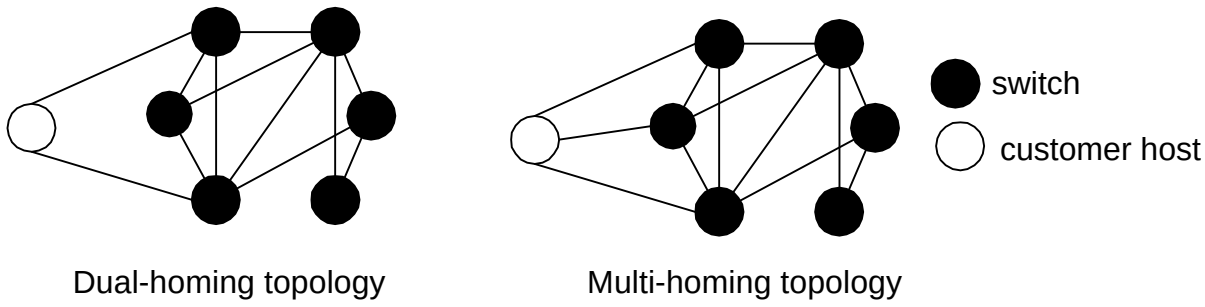


Figure 1.3 Dual-homing and Multi-homing Architectures