Telecommunications Systems manuscript No.
(will be inserted by the editor)

Resilient Network Design: Challenges and Future Directions

David Tipper

Received: date / Accepted: date

Abstract This paper highlights the complexity and challenges of providing reliable services in the evolving communications infrastructure. The hurdles in providing end-to-end availability guarantees are discussed and research problems identified. Avenues for overcoming some of the challenges examined are presented. This includes the use of a highly available network spine embedded in a physical network together with efficient crosslayer mapping to offer survivability and differentiation of traffic into classes of resilience.

Keywords Survivable Networks · Multi-Class Resilience · High Availability

1 Introduction

Communication networks are one of the critical national infrastructures upon which society depends [8, 15, 20]. The USA government categorizes communication networks as one of the most important critical infrastructures, since many other critical infrastructures (e.g., financial/banking, transportation, emergency services, etc.) depend on communication networks in order to function [9, 20]. This cross infrastructure dependency on communication networks has led to concern about the reliability and resilience of the current infrastructure by a number of USA government agencies (e.g., DoE, FCC, DHS) [9, 40] and the research community in general. Hence it is imperative that communication networks be designed to adequately respond to failures and attacks.

A communication network failure is usually defined as a situation where the network is unable to deliver communication services. Thus a failure can be viewed as a disruption of service rather than degradation due to congestion. Typical failure events include cable cuts, hardware malfunctions, software errors, power outages, natural disasters (e.g., flood, fire, earthquake, etc.), accidents, human errors (e.g., incorrect maintenance) and malicious physical/electronic attacks. As society becomes more dependent on networks, the consequences of network failures increase and the need to make the network resilient to failures grows as well. This has led to interest in the design of resilient networks, which are able to survive failures.

Survivability techniques for improving network resilience can be classified into three categories: 1) prevention, 2) network design, and 3) traffic management and restoration. Prevention or avoidance techniques focus primarily on improving component and system reliability and security in order to reduce the occurrence of faults. Some examples are the use of physical security measures where equipment is housed and provisioning backup power supplies for network equipment. Network design techniques try to mitigate the effects of system level failures such as link or node failures by placing sufficient diversity and redundancy in the network topology. An example is the use of multi-homing nodes so that a single link failure cannot isolate a network node or an access network. Traffic management and restoration procedures seek to direct the network load such that a failure has minimum impact when it occurs and that connections affected by a failure are reconnected around the failure. The use of pre-configured backup LSP paths in MPLS networks is a widely used exam-

David Tipper
Graduate Program in Telecommunications and Networking
University of Pittsburgh, Pittsburgh, PA, 15260 USA
Tel.: +1 (412) 624-9421
Fax: +1 (412) 624-2788
E-mail: {tipper}@tele.pitt.edu

ple of traffic mangement and restoration. The combined goal of the three categories of survivability techniques is to make a network failure imperceptible to network users by providing service continuity and by minimizing congestion in the network. This may be accomplished by designing network infrastructures that are robust to malfunctions of nodes and links, and implementing network protocols and control systems that are inherently fault-tolerant and self-healing. However, cost and complexity are always an issue. The key challenge is to provide the required availability at a minimum cost and in the simplest fashion.

At first glance one would assume that providing resilience in communication networks would be easy in comparison to other fields that require high levels of availability. For example, in the aerospace/satellite industry high levels of availability are required in the face of several hurdles, such as: an adverse operating environment (i.e., radiation, temperature, vibration), weight limitations, physical space constraints, electrical power constraints and in most cases no chance for physical repair of failed components [27, 35]. Given these constraints satellite systems are designed to maximize the mean time to failure and extensive use is made of structural importance measures in determining where and how redundancy should be added to systems. The end result is often partial or full redundancy used only in the components, which are crucial from a system wide perspective for mission critical services [27].

In contrast in the communication network field, one can argue it is easy to reach availability requirements by utilizing standard redundancy techniques such as adding additional communications links, nodes, restoration techniques (e.g., preconfigured back up path with preserved resources) and services until the availability goals are met. However in this paper we show such an assumption is naive and the problem is far from simple with many challenges. Here, we discuss some of the challenges and open research problems and point out possible directions for future work. The remainder of this paper is organized as follows. Section 2, presents a sample network architecture and discusses the trends and issues in providing resilience. Next in Section 3, we sketch out potential solutions to some of the challenges identified. Finally, Section 4 summarizes the paper.

2 Trends and Issues in Resilience

We begin the discussion by briefly examining a sample network architecture. The goal is to provide an overview and context that can be referred to in explaining the challenges and framing potential solutions.

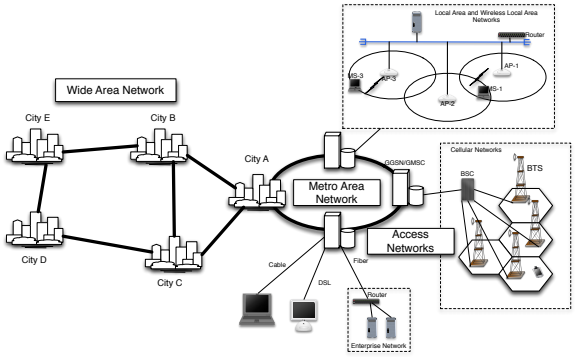


Fig. 1 Example Network Architecture

2.1 Network Structure

The current communications infrastructure consists of a set of interconnected networks which can be categorized based on their geographic size and function as either access networks (ANs), metropolitan area networks (MANs), or wide area networks (WANs) as shown in Figure 1. Access networks provide the end communication path to and from the users (i.e., the so called "last mile"). A wide variety of technologies are utilized in access networks including; cable, twisted pair, DSL, fiber to the home or office, fiber to the curb, power line communications, cellular networks, wireless LANs, WiMAX, and satellites. Access networks typically have a tree or hub and spoke type of topology with little or no redundancy provided due to cost constraints, though customers willing to pay for extra services (generally medium to large commercial customers) can be provided with dual-homed premises (i.e., two diverse links to different points on a MAN). Metropolitan area networks provide a local backbone network spanning a city or metro area. MANs typically have some fault tolerance with rings or mesh topologies used. Technologies used in MANs include WDM optical fiber, SONET, Ethernet, WiMAX, etc. WANs also known as core backbone or long haul networks, are the most uniform technology with almost all WANs now using optical communication links with WDM or DWDM technology. Furthermore, WANs are usually designed in a mesh topology with some level of fault tolerance (e.g., any single link failure) pre-planned. Given this infrastructure an end-to-end connection for a user/service/application would typically span several component networks (e.g., one AN, one MAN, one or more WANs, and then another MAN and AN). Note that, the component networks (ANs, MANs, WANs) will typically be owned and operated by multiple organizations (e.g., service providers).

The component networks (ANs, MANs, and WANs) in the communications infrastructure are multi-layer in nature, accommodating a wide variety of users and applications. Broadly speaking, each network consist of a top layer where services such as, voice, video, data, broadcast video, are provided. These services are provided over a middle or switched layer (e.g., MPLS label switching). Lastly, the middle layer is provided over a physical transport layer technology such as DWDM light paths on optical fibers. Note that, these layers may contain several sub-layers (e.g., SONET over DWDM over physical duct layer) depending on the level of detail one includes. For example, in a recent paper a group from AT&T [46] pointed out five distinct sub-layers could be identified in AT&T's DWDM transport backbone.

Here as a vehicle for discussion we consider a three-layer core backbone network, which could be composed of OVERLAY, IP, and WDM network layers as shown in Figure 2. In this architecture, overlay nodes are attached to an IP router. IP routers are associated with an optical WDM switch; the switches are then interconnected by multi-wavelength fibers capable of carrying a number of transmission channels. In the lower two network layers, IP and WDM, each IP route is established by one lightpath or more that spans across fibers and occupies one wavelength in each fiber. Overlays provide a top layer for the network that can take a role of processing and passing data between end-systems [2, 7]. In particular overlay networks can support applications when traffic runs across multiple Internet domains [38]. Recently, several commercial virtual network operators (VNOs) (e.g., [1, 44]) have constructed service overlay networks.

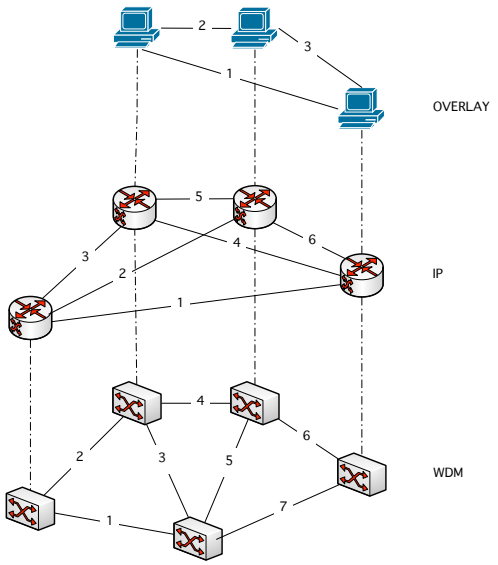


Fig. 2 Multi-layer network structure

2.2 Basic Resilient Design Concepts

Resilient network research originated with telecommunications network operators and has been a subject of study for decades. However in recent years there has been increasing interest in network resilience and survivability with journals dedicating special issues to the resilience of networks and components, specialized focused conferences being held (e.g., Reliable Network Design and Modeling (RNDM), Design of Reliable Communication Networks (DRCN)) and several excellent books published [26, 33, 42]. The current literature tends to focus on providing survivability in a particular technology at a specific layer (i.e., application overlay layer [21, 36] switched layer (IP [18], MPLS [4]), physical transport layer [25]) in a piece of the network architecture (e.g., MAN or WAN). For example, developing techniques for implementation of lightpath restoration in core DWDM optical backbone sections of the Internet (e.g., a Tier 1 ISP network) [25] or survivable SONET Ring techniques to overcome link failures in MANs. A survey of resilient network design techniques is given in [16]. While the implementation of survivability in a particular technology or protocol in a component network involves many details particular to the application, the basic techniques and principles used are largely the same in each case.

While a variety of survivability techniques (e.g., multiple homing, trunk diversity, self-healing rings, preplanned backup routes, p-cycles, etc.) have been proposed for a range of network technologies, they all work on the concept of redundancy and diversity. Consider a mesh network where traffic is routed on fixed end-to-end paths (e.g., lightpaths in a WDM network). An active path (AP) (sometimes called the working path) is the route taken by the traffic under normal operating conditions. For the network to be survivable to failures in the active path, one must be able to find a suitable backup path (BP) (i.e., an alternate path around the failure) in the topology. Obviously, the backup path and the active path must be physically diverse or disjoint so that both paths are not lost at the same time. How the active and backup paths are diverse can be defined in several ways. For example, they may be link disjoint as shown in Figure 3(a) or node disjoint which is shown in Figure 3(b). One can see in the figure that the link disjoint BP can potentially recover from any link failure in the AP, whereas the node disjoint BP can potentially recover from any link or relay node failure in the AP. Note that, for diverse AP and BP paths to exist, the physical network topology must be a ring

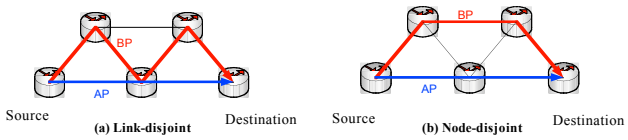


Fig. 3 Resilient network concepts

or a mesh structure with at least two disjoint end-to-end paths from every source-destination pair. However, even though a BP may exist for an AP there must be enough spare resources on the BP to carry the AP traffic at the required QoS level. This requires the allocation of redundant resources on the BP, which are typically not used except in the case of failure. The focus of resilient network design is to plan the allocation of diversity and redundancy in the network to support resilience to a set of failure scenarios (e.g., any single link failure). In order to take advantage of the redundancy and diversity in the network, appropriate fault management and traffic restoration procedures must be in place. Hence, given a specific traffic restoration scheme (e.g., p-cycles), in the current literature the resilient network design problem is to determine the network topology or virtual topology to survive a set of failure scenarios. Survivable network design, typically makes use of graph theoretic or optimization-based problem formulations with heuristic or meta heuristic solution algorithms used to provide scalability [14, 16, 33].

2.3 Issues and Trends

Given the overall infrastructure network architecture of Figure 1 and a typical multi-layer network structure like Figure 2, a number of trends and issues that affect resilience can be identified as discussed below.

Cost is the major factor affecting the amount of redundancy and fault tolerant mechanisms that can be implemented in a network. As communication networking is increasingly becoming a commodity type of business the cost constraints in improving network availability are more severe. Furthermore, only a small fraction of users are willing to pay extra for high levels of availability. The resulting cost limitations directly affect network resilience by limiting the amount of redundancy that an operator can afford to add to the network infrastructure. For example, cost may limit factors such as the connectivity of the network topology, the quality and reliability of the equipment/software used in the network, the number of sites that can employ backup battery supplies, etc. Cost limits also impose constraints on the network operations staff, both the size of the staff used to maintain and operate the network and the amount of training for the staff. This is particularly important as several studies have shown that human error is responsible for between 33-55% of network failures.

As noted above, the network infrastructure in composed of component networks, which are multi-layer in nature. Virtualization and the deployment of virtual private networks (VPNs) is possible at the various layers in the component networks (e.g., lightpath based VPNs in WDM, MPLS LSPs based VPNs, etc.) Virtualization is a well-established trend with virtual private networks being deployed within a network (e.g., VPLS within a MAN, IP/MPLS within a WAN), across multiple networks, and end-to-end at the application layer. Virtualization is appealing to customers in providing logical segregation of traffic, improved security and support for traffic engineering and QoS. However for network service providers the complexity of managing thousands of VPNs increases the likelihood of human errors and cross-layer traffic engineering and fault tolerance provisioning is increasingly difficult. This is especially true given that traffic demand occurs at each layer in the network. Furthermore, interdomain issues such as peering and domain boundaries can occur at multiple layers. Additionally, the nature of the traffic itself is changing with recent studies showing that video is now the dominant traffic type in WANs. This is exacerbated by the move towards information or content centric networking where most of the traffic is connecting customers to content rather than customers to customers. This shift to content networking has resulted in the deployment of overlay networks by content delivery network operators and the fielding of optical layer underlay networks by large content providers. Currently the traffic dynamics largely differs with the layer, as the lower layers show significant changes on a slower time scale then higher layers. However, the networking as a service (NAAS) concept where high bandwidth lightpaths can be provided on demand will add dynamic Layer 1 traffic on a faster time scale in the future. Thus, there is a potential for dynamic overlay and underlay virtual networks

In general multiple layers present a number of survivability problems. Here we illustrate the problems by considering the sample network given in Fig. 2. In the figure, the OVERLAY, IP, and WDM networks consist of 3 nodes, 3 links, 4 nodes, 6 links, and 5 nodes, 7 links, respectively. The numbers on each link indicate the link index. Let $H_i^j : \mathcal{L}^{(j)} \mapsto \mathcal{L}^{(i)}$ be a link incidence matrix or cross-layer mapping matrix showing the mapping of Layer j onto Layer i where each j-th layer link is assigned to a subset of i-th layer links. When put in matrix form, the cross-layer mapping has rows corresponding to layer j links whereas columns correspond

to layer i links. The layers are numbered in ascending order with Layer 1 corresponding to the physical WDM transport layer. For example, the OVERLAY to IP cross-layer mapping H_2^3 could be given by

$$H_2^3 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

which is the most obvious mapping as each link in the OVERLAY network uses only one link in the IP network. However, if the IP to WDM cross-layer mapping H_1^2 is given by

$$H_1^2 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

then one can see that links 5 and 4 in the IP layer have link 3 in the WDM layer in common. Thus the failure of link 3 at the WDM layer will result in two links (4 and 5) failing at the IP layer, which in turn results in two links (1 and 2) failing at the OVERLAY layer resulting in a disconnected overlay network. The cross-layer mappings given by H_2^3 and H_1^2 are illustrated in Figure 4, where the lower layer links implementing high layer virtual links are marked with the same colors. For example, link 2 in the OVERLAY layer is colored blue as is it's mapping on to links 5 in the IP layer and links 3 and 5 in the WDM layer.

This effect of a single lower layer failure resulting in multiple failures at the layer above and in turn higher layers is called *fault propagation*. A major cause of fault propagation is poor cross-layer link mapping. In [24] the authors reveal that, in a highly-meshed operational IP over WDM network, ill-chosen link mapping contributes to 12% of all unplanned failures that affect the IP traffic. The figure is likely to be higher in partial-meshed IP networks as it increases the chance of network partitioning or reduces the number of rerouting choices when a backup path is needed or failures happen in the WDM layer.

An additional cause of fault propagation is *shared risk link groups* (SRLGs) which are defined by a set of links that fail together due to physical placement of cabling in conduits/infrastructure. When a SRLG conduit fails all of the lower layer links contained in the conduit may fail simultaneously. Most the work on SRLGs has focused on a single-layer or two-layer network (e.g.,[13]). Obviously, to solve the fault propagation problem, higher layers will need information on the

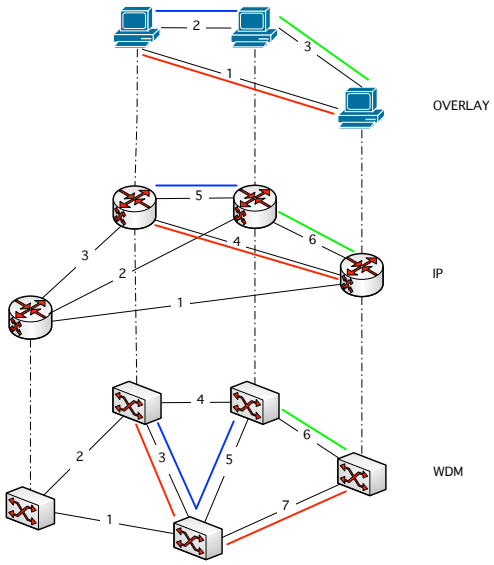


Fig. 4 Cross-layer Mapping with Fault Propagation

structure of the lower layers. Note, that this is especially true for application overlay [2, 17] and virtual private networks at layer two and above.

A second problem in multiple layer networks is capacity efficiency, since a top-layer path may require more or less total bandwidth depending on which layer determines the capacity allocation and routing assignment and how the cross-layer mapping is accomplished. In particular, *backhaul* on lower layers physical links that are shared by virtual links in higher layers [23] is a problem. Again, consider the sample network illustrated in Figure 2 with the cross-layer mappings given above. If we modify the cross-layer mapping of the OVERLAY network to IP network H_2^3 such that link 2 in the OVERLAY layer is mapped to links 2 and 3 in the IP layer then the OVERLAY network can survive any single physical WDM layer link failure. The resulting mapping is given by:

$$H_2^3 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array} .$$

However, for OVERLAY link 2 a backhaul routing loop occurs in Layer 1, because the IP links 2 and 3 use WDM links 2 and 4, and 2 respectively. Thus, the WDM link 2 is used twice. The cross-layer mappings given by H_2^3 and H_1^2 are illustrated in Figure 5, where the lower layer links implementing high layer virtual links are marked with the same colors. While this routing is survivable, it is not resource efficient.

This backhaul problem can arise when higher layer routes are mapped through an intermediary node in the layer below. Therefore, a survivable link mapping alone

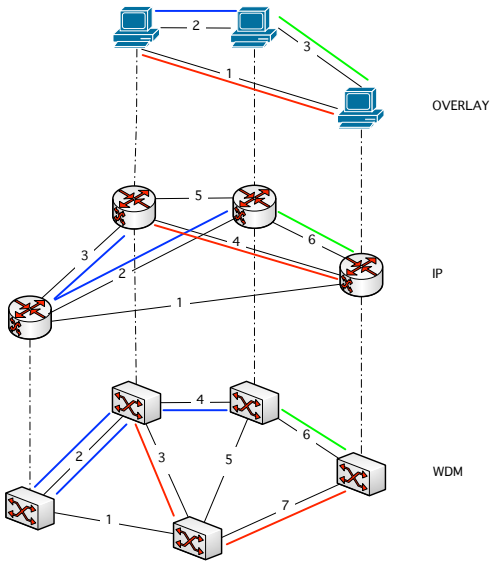


Fig. 5 Cross-layer Mapping with Backhaul

is not sufficient to guarantee capacity efficiency when backup paths using more than a single hop are considered in a multi-layer network. In general, each layer of a network will need to employ some type of self-healing capabilities to address faults occurring in that layer and possibly lower layers. In such a multi-layer scheme, coordination between layers is required to provide an efficient network design and recovery process upon a failure. Specifically, coordination of alarms and resilience mechanisms at the layers and prioritization of traffic for fault recovery within and among the layers is needed. Note, that without proper coordination of the resilience mechanisms oscillatory behavior and instability can occur.

As mentioned previously an end-to-end connection will typically traverse several component networks. These component networks will typically have multiple owners and operators making end-to-end availability guarantees hard to provide. This is due to the need for coordination across component networks (e.g., MAN and WAN, between two WANs, etc.), which may include harmonizing survivability techniques at various network layers. Note, that this requires policy coordination to share information (e.g., cross-layer mapping, fault alarms, details of restoration schemes, etc.) among possibly competing companies. Only a small a amount of literature exists on this topic [6, 38] with many open problems, such as coordination of different restoration techniques across networks and the development of trusted third party mechanisms for the exchange of information.

An additional policy concern is government regulations, which often specify what network operators can and can't do. Consider the critical infrastructure protection plans of the USA government, which focus on the reliability, and security of critical infrastructures [9]. This can lead to cross regulation issues where the needs of one infrastructure impose requirements on the communications infrastructure. For example, in contrast to the current power grid, the smart electrical grid requires significantly more communications. In fact, one of the key requirements is the use of two-way communications between customers and the grid, which is necessary to implement demand response techniques, balance generation with consumption and enable the integration of distributed generation sources. The US Department of Energy (DoE) recently put forth a set of requirements for the communications infrastructure to support the smart grid [40]. Table 1 lists typical values given by the DoE, illustrating the wide range of availability requirements to be met. In particular, the wide area situational awareness function which is implemented by the installation of synchrophasors at substations to closely monitor and adaptively stabilize the power grid requires very high levels of end-to-end availability in connecting to regional power grid control centers. Obviously, these availability requirements will impact feasible implementations and resilient network design choices in ANs, MANs and WANs. In particular, the US Federal Communications Commission (FCC) [12] noted that the lack of a mission-critical WAN meeting the requirements of the Smart Grid threatens to delay its implementation and points to this as an area for research and development.

Another little-studied issue in the literature is the design of networks for resilience taking into account the variations in failure impacts and likelihood of failures. Several, studies have observed that the rates of failure and repair rates are geographically correlated due to a number of factors. Examples of factors are variations in: weather, workforce capabilities, exposure to natural disasters (e.g., earthquakes, hurricanes, ice storms, etc.), local regulations (e.g., call before dig penalties), population density, power supply reliability and targeted malicious attacks [28]. The end result of these factors is that failures often happen in a correlated fashion with multiple near simultaneous failures. In addition, not all failures of the same type (e.g., single link failures) have the same societal impact or magnitude. For example, the failure of an optical fiber carrying critical supervisory control and data acquisition (SCADA) traffic for the electrical power grid can result in more societal damage than a fiber carrying web traffic. Determining the potential societal impact of various failures would require knowledge of traffic content/service

Table 1 Sample requirements for smart grid communications

Function	Bandwidth	Latency	Availability
Smart Meter (AMI)	10-100 Kbps	2-15 sec	99-99.99%
Demand Response	14-100 Kbps	500 msec - several minutes	99-99.999%
Wide Area Situational Awareness	600 Kbps - 1.5 Mbps	20-200 msec	99.999-99.9999%

level agreements and how they are mapped onto physical networks.

Lastly, it is worth noting that green networking is a rapidly emerging set of efforts by standards bodies (e.g., ITU, TIA, ETSI, IEEE), governments, corporations, foundations and academics aimed at improving the sustainability of ICT devices and infrastructure. One aspect of these efforts is a focus on improving the energy efficiency of ICT devices and their operation. This includes initiatives pushing for rapid power up/down methods and energy efficient sleep/idle modes for networking equipment (from access equipment to core equipment). Furthermore, noting the diurnal nature of communication network traffic, proposals for powering down parts of a network infrastructure during low load periods to save power and OPEX costs have appeared in the literature [3]. This literature has focused on saving energy without regard for the effects on resilience, which will be longer restoration times, less fault tolerance and lower levels of availability. The interaction of resilience and green networking is an area ripe for research.

3 Future Directions

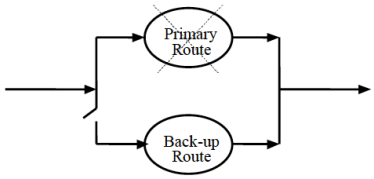
Given the network architecture and the trends discussed above one can see that providing end-to-end availability guarantees for mission critical services (e.g., power grid supervisory control and data acquisition, emergency services) is a difficult challenge with many complex issues to be addressed. A number of research directions that have promise in meeting this challenge are briefly discussed in the following.

3.1 Classes of Resilience and the Spine Concept

Only a small number of users and services (e.g., financial institutions, VoIP emergency calls, power grid wide area situational awareness) need very high levels of availability. Furthermore, the users/services requiring high levels of resilience produce only a small fraction of the total network traffic. Also, several studies have shown that the majority of customers are unwilling to pay extra for high levels of availability. For example, consumers are happy with residential Internet access if the availability is in the range of 93 -95%, which is well below the 99 - 99.99% range given for smart metering at homes in Table 1.

Unfortunately, the small amount of high availability traffic derives the network design giving rise to a free rider scenario where the majority of customers get a higher level of availability then they need or are willing to pay for. Hence there is a need to support classes of resilience in a fashion similar to quality of service classes. The basic concept is to categorize traffic into classes and provide different levels of availability and fault protection for each class. The goal is to just meet availability requirements without over-engineering. Providing quality of resilience classes has been mentioned in the current literature [5] in a qualitative fashion or quantitatively examined within a single layer. The current approach to resilience service differentiation is to support multiple classes of resilience by using different restoration mechanisms per traffic type in a particular network layer (e.g., WDM). For example, providing gold, silver and bronze service classes by giving the gold traffic 1+1 (node and link) disjoint path restoration, silver class shared backup restoration and the bronze class no protection relying on rerouting after failure. Typical simulation-based numerical results for this type of approach [43] for a sample European network topology show average availabilities of gold 99.89%, silver 99.73%, and bronze 97.74% classes respectively. While this approach can provide differentiated quality of resilience service classes, it is not designed around end-to-end availability guarantees. Notice that the availability value for the gold class is too low for mission critical services (i.e., 99.999% or higher), the spread between gold and silver classes is small and the bronze class availability may be higher than needed.

In order to improve the end-to-end availability to mission critical levels across a single network (e.g., WAN) the traditional resilient design method is increase the network connectivity and add redundancy (e.g., more than one backup path). This can be thought of as using many components in parallel type of design. However, such an approach would be difficult and expensive to implement in an existing network. Here we propose an alternative approach based on the adoption of



Scenario	Primary Route Availability	Backup Route Availability	Availability with Redundancy
1	0.95	.90	0.995
2	0.95	.91	0.9955
3	0.96	.9 0	0.996

Fig. 6 Improving Parallel Component Availability

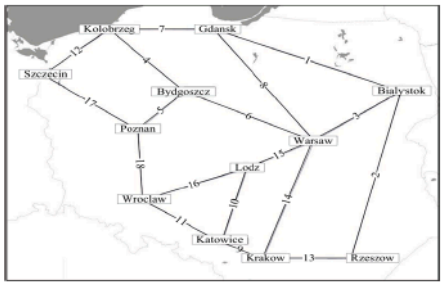
ideas from the aerospace reliability area. Given the constraints in mission critical aerospace systems, extensive use is made of Birnbaum's importance measure to guide efforts to improve the availability [34]. Specifically, the derivative of the system availability per component as determined from a reliability block diagram or fault tree analysis is used to determine where to increase the availability. In general, one can show that for series components the availability of the weakest component should be improved to increase the system availability, whereas for parallel components one should improve the availability of the strongest component. This concept is illustrated in Figure 6 where two communication paths are in parallel. As shown in the table in Figure 6 for the baseline scenario 1 the primary route has availability 95%, the backup route 90% and the parallel combination 99.5% respectively. For scenarios 2 and 3 in the table we increase the availability of one of the routes by 1% (e.g., deploying a 24 hour battery backup power supply along the route). In scenario 2, the increased availability is applied to the backup route whereas in scenario 3 the increased availability is applied to the primary or working route. One can see from the table that scenario 3 results in the largest increase in the overall availability of the parallel configuration.

Here we apply the concept of improving the availability of the strongest component in parallel systems, by constructing a highly available section of the network at the physical layer. We term the high availability portion of the network the network *spine*. The spine would connect those nodes with traffic needing a high level of availability and the highest quality of resilience class traffic would be routed on the spine or use the spine as a backup path. The nodes, link interfaces and links on the network spine would have higher availability then the equipment that is not part of the spine. This provides levels of availability differentiation at the physical component level. The spine could be determined in a number of ways such as using a capacitated minimum spanning tree algorithm, although the spine need not be a tree.

We illustrate the potential of the spine approach by a simple example. In Figure 7, the top figure (a) shows the topology of the 12-node, 18-link Polska network taken from the SNDlib repository. In the base line scenario, for the sake of simplicity we assume all links and nodes have availability 99.9% and failure independent backup paths are used which are node and link disjoint with the working path. Consider a traffic stream between Szczecin and Katowice that needs availability 99.999%. If the working path takes the route Szczecin - Poznan - Wroclaw - Katowice then four nodes and three links are utilized with a resulting availability of 99.3%. Letting the backup path take the route Szczecin - Kolobrzeg - Bydgoszcz - Warsaw - Lodz - Katowice then six nodes and five links are used which results in an availability of 98.9%. The subsequent end-to-end availability from the working and parallel backup path combination is 99.9236%, which is below the desired 99.999%. In the traditional survivable network design method to meet the desired availability goa,l one could add an additional link to the network from Szczecin to Gdansk so that a second backup path could be provided along Szczecin - Gdansk - Bialystok-Rzeszow-Krakow-Katowice. In contrast for the spine approach a tree with higher available components is embedded in the network as shown by the red links in Figure 7(b). Assuming the components along the spine have been selected to have availability 99.99%, then the availability of the working path between Szczecin and Katowic increases to 99.93% while the backup path availability will stay the same. The resulting overall end-to-end availability from the working and backup path combination increases to 99.99923%, thereby meeting the desired availability goal.

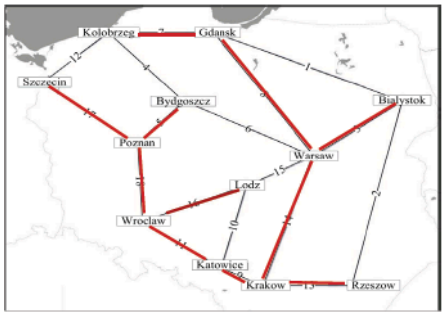
The higher availability of the spine, in comparison to the non-spine part of the network can be accomplished using a variety of techniques. For the spine more expensive equipment can be utilized that is arranged and configured to provide high availability (e.g. hot standby line card, redundant fans, redundant backplane, etc.) with redundant equipment deployed locally in parallel as needed (e.g., hot standby OXC). Also, the equipment along the spine can be situated to increase the mean time to failure (MTTF) using a number of techniques such as longer back up power supplies, better heating/cooling, stronger outside cabinets, underground links instead of above ground, etc.

In a similar vein methods can be employed to reduce the mean time to repair (MTTR) along the spine. For instance, one can follow best practices and training procedures as determined by several government and



Scenario	Working Path Availability	Backup Path Availability	End-to-End Availability
All equipment 99.9% availability	99.9%	99.9%	99.99236%

(a) Polska Network



Scenario	Working Path Availability	Backup Path Availability	End-to-End Availability
Spine Equipment 99.99% Other Equipment 99.9%	99.93%	98.9%	99.99923%

(b) Polska Network with Spine in Red

Fig. 7 Spine Example

trade organizations (e.g., NRIC, FCC, TIA) and standards bodies (e.g., ITU). The operator can pre-position spare parts, equipment, software and test equipment along the spine. Similarly, the network operations center (NOC) can more closely monitor the spine portion of the network. Furthermore, the operator can assign the most experienced staff to the operations, administration and management (OAM) of the spine portion of the network. Many of the methods above are employed in other critical infrastructures (e.g., the power grid) and industries and studies show that the average MTTR can be reduced by 5 - 25% resulting in a significant improvement in the availability.

In general the spine based approach has the potential to provide larger differences in the availability provided to quality of resilience classes resulting in less over engineering of the network to meet the most stringent availability requirements. Furthermore, it can naturally support the green networking concept by potentially allowing one to power down some of the equipment that is not part of spine during low load periods. Obviously, much additional work needs to be done to fully flesh out the spine concept, including: detailed design algorithms; comparative analysis contrasting with current survivable design techniques; and integration with classes of resilience in a multi-layer network design.

3.2 Cross-layer Mapping

As noted in Section 2.3, cross-layer mapping must be both survivable and efficient. Over a series of papers we have examined various aspects of cross-layer mapping. In [22] an optimization model to find a cross-layer mapping in a two-layer network context (i.e., IP - WDM) that is free of fault propagation due to any single lower layer failure was given. This model was extended in [30] to allow for traffic and survivability techniques at both layers and numerical results showed the advantages of providing survivability of two-layer traffic at the bottom layer when sharing spare capacity among all backup paths is allowed. In [29] sufficient conditions for elimination of backhaul in multi-layer network cross-layer survivable mapping were given and the model of [22] was extended to a three-layer context. In [32] we extended the cross-layer survivable mapping optimization problem to maximize the overlay network availability given the physical layer link and node availability information. It was shown that survivable mappings of higher layer virtual links can result in much different network availabilities even for the same cost. Lastly, the idea of using differentiated cross-layer mapping to provide quality of resilience classes in part by topological masking was presented in [31]. The basic concept is that at any layer different quality of resilience classes see a different topology. For instance, the most reliable class (e.g., gold class) would see the entire topology and can route working and protection paths on the full topology, but lower resilience classes may have links, nodes, or capacity (e.g., wavelengths) hidden from them. A unified optimization model was formulated to provide differentiated cross-layer survivable mapping for a multi-layer network with multiple quality of resilience classes.

This work plus other recent work in the literature [19, 37, 39] can be viewed as pieces of preliminary work towards a unified view of cross-layer survivable mapping in support of developing quality of resilience classes that provide availability guarantees. However, much work needs to be done in terms of developing optimization based model formulations that incorporate all the required features and the development of scalable solution algorithms. Scalability is particularly important due the large number of virtual networks that are concurrently deployed in networks and typically the current literature focuses on designing a single or small number of overlays.

3.3 Risk Based Design

As noted in Section 2.3, there are large variations in the location and rate of failures in a network and their societal impact. A possible line of research to incorporate this variation is the systematic consideration of risk factors into the resilient network design. Risk management has been advocated for critical infrastructure protection as the method of choice in allocating scarce/spare resources for guarding against failure, accidents and attacks [9, 10, 11, 20]. Risk analysis is widely used in aerospace and civil engineering, IT security and economics. In engineering fields, the term risk accounts not only for the likelihood of failure but also for a degree of damage resulting from the failure. The risk of a failure is commonly defined as the product of the failure probability and the magnitude of damage caused by the failure, where the damage can be measured in various dimensions (e.g., financial, reputation, human impact, etc. [9]). Typically, different customers are willing to live with different levels of risk that a service level agreement is violated [45]. Consequently, not all need to have the same level of resilience from physical layer networks. Incorporation of risk factors can result in different resilience classes in terms of design and different real-time restoration policies when a failure occurs.

For the design problem, the basic approach is to use risk analysis information in formulating optimization based survivable network design investment strategies to reduce the network risk. The baseline design problem considered is that given a working network and a fixed budget, how best to allocate the budget for deploying a survivability technique in different parts of the network based on managing the risk. Preliminary work along these lines was given in [41] where designing a survivable single layer WDM network was studied. The design approach consisted of two parts: a risk assessment and a risk reduction investment strategy. Fault tree models, which depict causal relationships among failure events in the network were used for the risk assessment. A risk-reduction investment strategy was used to determine an allocation of budget for implementing a survivability technique (e.g., link protection, path protection) in different parts of the network to minimize the network risk. A Mixed Integer Linear Programming (MILP) formulation and greedy-based heuristic were developed for solving the minimum-risk design problem. Additionally, various models with different risk-based design objectives were considered, for example, minimizing the expected damage, minimizing the maximum damage, and minimizing a measure of the variability of damage that could occur in the network. Numerical results and analysis illustrating the different risk based designs and the tradeoffs among the schemes were presented. This preliminary work needs to be extended to include a multi-layer network architecture and different classes of resilience.

3.4 Resilient Access

A potential bottleneck to providing end-to-end availability guarantees is the access network portion of an end-to-end path. For example, connecting smart grid synchrophasors at substations to regional network control centers. The fundamental challenge in access networks is lack of diversity and redundancy in the network topology. In order to provide resilience services, access networks must adhere to the same architectural guidelines as MAN and WAN networks. However, given the economic cost limitations of the so called "last mile", a basic question is how much resilience can be added at minimal cost and in an incremental risk mitigation-based fashion. Specifically, we advocated the adoption of the integration of risk based analysis techniques (e.g., fault trees, apportioned risk reduction, and ranked order risk reduction) and incremental resilient network design to access networks. Another line of research here is setting up a mechanism such that competing access network technologies be used to provide redundancy. For example, utilizing a 4G cellular network as a backup resource/path for synchrophasors at substations with a wired connection for a primary working path.

4 Conclusions

In this paper a number of challenges to providing reliability in current networks were examined, namely: cost constraints; virtualization and traffic trends; multi-layer technology and cross-layer mapping; multiple networks and operators, regulatory issues and ultra high availability traffic; variation and correlation of failure rates; and green networking. Promising paths for future research to solve some of the identified challenges were examined including: providing differentiated classes of resilience in multi-layer networks, use of a highly available spine embedded in a network to enhance availability differentiation and support high availability traffic; the need for cross-layer mapping algorithms that are scalable and that provide classes of resilience; incorporation of risk into resilient network design and increasing access network reliability. In conclusion, resilient networking is an area rich in open research problems with much work to be done.

References

1. Adapt: (2011). URL http://www.adaptplc.com/
2. Andersen, D., Balakrishnan, H., Kaashoek, F., Morris, R.: Resilient overlay networks. In: SOSP '01: Proceedings of the eighteenth ACM symposium on Operating systems principles, pp. 131–145. ACM, New York, NY, USA (2001)
3. Bianzino, A.P., Chaudet, C., Rossi, D., Rougier, J.L.: A survey of green networking research. IEEE Communications Surveys and Tutorials **14**(1), 3–20 (2012)
4. Bigos, W., Gosselin, S., Cousin, B., Le Foll, M., Nakajima, H.: Optimized design of survivable MPLS over optical transport networks. Optical Switching and Networking **3**(3–4), 202–218 (2006)
5. Cholda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J., Jajszczyk, A.: A survey of resilience differentiation frameworks in communication networks. IEEE Communications Surveys & Tutorials **9**(4), 32–55 (2007)
6. Cinkler, T.: Some more aspects of resilience multidomain, multi-cast, physical impairments. Telecomunication Systems **to appear** (2012)
7. Clark, D., Lehr, B., Bauer, S., Faratin, P., Sami, R., Wroclawski, J.: Overlay networks and the future of the internet. Communications & Strategies **63**, 1–21 (2006)
8. Department of Homeland Security: The National Strategy For the Physical Protection of Critical Infrastructure and Key Assets (2003)
9. Department of Homeland Security: National Infrastructure Protection Plan (2009)
10. Department of Homeland Security: Communications Sector Specific Plan (2010)
11. Department of Homeland Security: Information Technology Sector Specific Plan (2010)
12. Federal Communications Commission: National Broadband Plan (2010)
13. Gomes, T., Simoes, C., Fernandes, L.: Resilient routing in optical networks using srlg-disjoint path pairs of min-sum cost. Telecomunication Systems **to appear** (2012)
14. Grosan, C., Abraham, A., Hassainen, A.E.: Designing resilient networks using multicriteria metaheuristics. Telecomunication Systems **40**(1-2), 755–88 (2009)
15. Homeland Security Presidential Directive: Critical Infrastructure Identification, Prioritization, and Protection, hspd-7 edn. (2003)
16. Jager, B., Doucette, J., Tipper, D.: Network Survivability. in Information Assurance: Dependability and Security in Networked Systems, Eds.Y. Qian, J. Joshi, D. Tipper, and P. Krishnamurthy, Morgan Kaufmann (2008)
17. Koizumi, Y., Miyamura, T., Arakawa, S., Oki, E., Shiomoto, K., Murata, M.: Stability of virtual network topology control for overlay routing services. Journal of Optical Networks **7**(7), 704–719 (2008)
18. Kvalbein, A., Hansen, A., Cicic, T., Gjessing, S., Lysne, O.: Multiple routing configurations for fast IP network recovery. IEEE/ACM Trans. Networking **17**(2), 473 –486 (2009)
19. Lee, K., Lee, H.W., Modiano, E.: Reliability in layered networks with random link failures. IEEE/ACM Transactions on Networking **19** (2011)
20. Lewis, T.G.: Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience (2006)
21. Li, Z., Mohapatra, P.: On investigating overlay service topologies. Computer Networks **51**(1), 54 – 68 (2007)
22. Liu, Y., Tipper, D., Vajanapoom, K.: Spare capacity allocation in two-layer networks. IEEE Journal on Selected Areas in Communications **25**(5), 974–986 (2007)
23. Madhu Kumar, S.D., Bellur, U.: Availability models for underlay aware overlay networks. In: DEBS '08: Proceedings of the second international conference on Distributed event-based systems, pp. 169–180. ACM, New York, NY, USA (2008)
24. Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C.N., Ganjali, Y., Diot, C.: Characterization of failures in an operational IP backbone network. IEEE/ACM Trans. Netw. **16**(4), 749–762 (2008)
25. Modiano, E., Narula-Tam, A.: Survivable routing of logical topologies in WDM networks. In: *Proc.* IEEE INFOCOM 2001., vol. 1, pp. 348–357. Anchorage, AK (2001)
26. Mouftah, H., Ho, P.H.: Optical Networks: Architecture and Survivability. Kluwer Academic Publisher (2003)
27. NASA: Safety and mission assurance (2012). URL http://kscsma.ksc.nasa.gov
28. Neumayer, S., Zussman, G., Cohen, R., Modiano, E.: Assessing the vulnerability of the fiber infrastructure to disasters. In: *Proc.* IEEE INFOCOM 2009, pp. 1566 –1574 (2009)
29. Pacharintanakul, P., Tipper, D.: Crosslayer survivable mapping in Overlay-IP-WDM networks. In: Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on, pp. 168–174. Washington, D.C. (2009)
30. Pacharintanakul, P., Tipper, D.: The effects of Multi-Layer traffic on the survivability of IP-over-

WDM networks. In: *Proc.* IEEE ICC 2009., vol. 1, pp. 1–6. Dresden, Germany (2009)
31. Pacharintanakul, P., Tipper, D.: Differentiated crosslayer network mapping in multilayered network architectures. In: 14th International Telecommunications Network Strategy and Planning Symposium (NETWORKS 2010). Warsaw, Poland (2010)
32. Pacharintanakul, P., Tipper, D.: Link availability mapping in infrastructure based overlay networks. In: Reliable Networks Design and Modeling (RNDM), 2nd Intl. Workshop on (2010)
33. Pioro, M., Medhi, D.: Routing, Flow, and Capacity Design in Communication and Computer Networks. Morgan Kaufmann (2004)
34. Rausand, M., Hoyland, A.: System Reliability Theory: Models, Statistical Methods and Applications, 2nd Edition. Wiley Interscience (2003)
35. Saleh, J., Castet, J.: Spacecraft Reliability and Multi-State Failures: A Statistical Approach, 1 edn. John Wiley & Sons (2011)
36. Shamsi, J., Brockmeyer, M.: QoSMap: Achieving quality and resilience through overlay construction. IEEE International Conference on Internet and Web Applications and Services pp. 58–67 (2009)
37. Song, L., Zhang, J., Mukherjee, B.: Dynamic provisioning with availability guarantee for differentiated services in survivable mesh networks. IEEE Journal on Selected Areas in Communications **25**, 35–43 (2007)
38. Staessens, D., Colle, D., Pickavet, M., Demeester, P.: Computation of high availability connections in multidomain IP-over-WDM networks. In: Reliable Networks Design and Modeling (RNDM), 1st Intl. Workshop on, pp. 1 –6. St. Petersburg, Russia (2009)
39. Tornatore, M., Lucerna, D., Mukherjee, B., Pattavina, A.: Multilayer protection with availability guarantees in optical wdm mesh networks. Journal of Network and Systems Management **20**, 34–55 (2012)
40. US Department of Energy: Communications Requirements of Smart Grid Technologies
41. Vajanapoom, K., Tipper, D., Akavipat, S.: Risk based resilient network design. Telecomunication Systems **to appear** (2012)
42. Vasseur, J.P., Pickavet, M., Demeester, P.: Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS. Morgan Kaufmann (2004)
43. Verbrugge, S., Colle, D., Demeester, P., Huelsermann, R., Jaeger, M.: General avialability model for multilayer transport networks. In: Design of Reliable Communication Networks, 2005. DRCN 2005. 5th IEEE International Workshop on (2005)
44. Virtela: (2011). URL http://www.virtela.net/
45. Xia, M., Tornatore, M., Martel, C., Mukherjee, B.: Risk-aware provisioning for optical wdm mesh networks. IEEE/ACM Transactions on Networking **19**, 921–932 (2011)
46. Xu, D., Li, G., Ramamurthy, B., Chiu, A., Wang, D., Doverspike, R.: Srlg-diverse routing of multiple circuits in a heterogeneous optical transport network. In: Design of Reliable Communication Networks, 2011. DRCN 2011. 8th International Workshop on, pp. 1–8 (2011)

David Tipper received the B.S.E.E. degree from Virginia Tech, Blacksburg, VA and the M.S. Systems Engineering and Ph.D. Electrical Engineering degrees from the University of Arizona, Tucson, AZ. He is an Associate Professor and Director of the Graduate Telecommunications and Networking Program at the University of Pittsburgh. Prior to joining Pitt in 1994, he was an Associate Professor of Electrical and Computer Engineering at Clemson University, Clemson, SC. He is the co-author of the textbook The Physical Layer of Communication Systems, which was published by Artech House in March, 2006. Also, he is the co-editor and a contributor to Information Assurance: Dependability and Security in Networked Systems which was published by Morgan Kaufman in 2008. His current research interests are survivable networks, information assurance techniques, performance analysis, wireless and wired network design. His research has been supported by grants from various government and corporate sources such as NSF, DARPA, NIST, IBM, and AT&T.