Resilient Optical Networks[1]

Vincent W.S. Chan, *Life Fellow, IEEE and Fellow OSA*
Claude E. Shannon Communication and Network Group
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Tel: (01)617-258-8222 e-mail: chan@mit.edu

ABSTRACT
Networking resilience is the ability to provide and maintain an acceptable level of service, albeit potentially degraded from nominal, in the face of faults and challenges to normal, including adversarial attacks. This paper explores the concept of resilient optical networks and scopes the important issues to be addressed in a sensible architecture. The solution includes monitoring and probing to determine the states of potentially unreliable network substrates, assessment of resilient network operating regimes, isolation of compromised assets, deployment of mitigation measures that may require communication over unreliable substrates and suggestions for resilient architecture design and improvement. The architecture construct evolves around a robust control plane that uses cognitive techniques to assess network states and automatically reacts to the on-set of impairments and attacks involving all the network layers from the Physical Layer to the Application Layer.
Keywords: optical network architecture, resilient networks, network security, network reconstitution.

1. INTRODUCTION

With the increasing huge number of user nodes and network elements connected via the Internet, it is unrealistic to assume a fraction of nodes, network elements and even entire subnets are not compromised. Thus, a new paradigm for resilient networking is to use a network construct that allows ***reliable networking over unreliable substrates.*** There have been research efforts in focussed areas on this front but less on the broad architecture concepts, especially in the optical network area. Recent efforts on "Orchestration" focus on improving network efficiencies but not resiliency. We address optical network resiliency from a multi-layer viewpoint and highlight necessary network characteristics and building blocks towards a resilient optical network architecture. Optical network impairments/attacks can propagate long distances due to long optical reach causing widespread damage far from the source of injection of impairments/attacks, and making localization a big challenge due to lack of mid-point sensing by repeaters. A robust and well protected network management and control system should be the center-piece of a resilient architecture and provides fast, agile and adaptive responses in sensing, assessment, protection and mitigation deployment with the following functions, Fig.1:

1. Monitoring and probing – new all optical transport systems make sensing difficult; architecture must deal with the fluid connectivities, long reach optical network state sensing without benefit of electronic mid-span sensing points and decides on the small fraction of vital network states to be sensed/probed.
2. Assessment - analytics to assess network states based on under-sampled and sometimes stale state information; cross-layer failures must be considered as well as subtle performance degradations other than clear-cut failures.
3. Mitigation and isolation – repair malfunctioning hardware/software; isolate compromised network elements with rerouting including diversity routing of all forms and defend against cloud-scale analytics by adversaries that can detect and adapt to the mitigation measures.

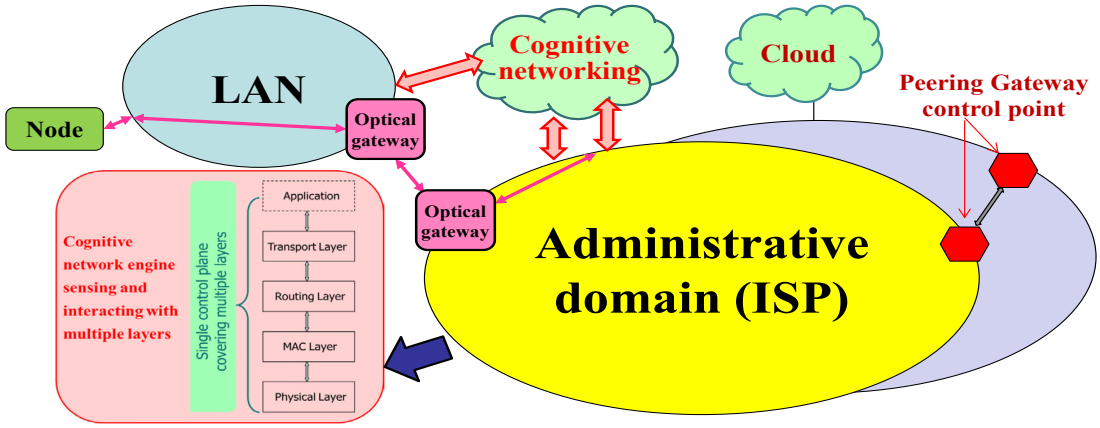

Figure 1. Resilient optical network concept with optical gateways between hierarchical subnet, peering gateway control points and cognitive engine sensing and interacting with multiple layers for network control.

[1] Research supported by NSF, the Irwin Jacobs, the Claude E. Shannon and the Rick Barry Endowment Funds.

2. RESILIENT OPTICAL NETWORK ARCHITECTURE FRAMEWORK

The first ingredient of a resilient network architecture is monitoring and sensing of network states and anomalies. This situation awareness is vital to the accurate assessment of network states and triggering of appropriate responses. Future networks will have a huge state space, [6], and complete information gathering is impossible and thus network health must be inferred using sparse and sometimes stale data, [3]. Sensing techniques should be layered and redundant for cross checking, followed by assessment and mitigations as given below, Fig.2:

1. Application performance monitoring and probing, inference on health of underlying substrates including user performance prediction, maintenance and proactive probing trials and negotiations with lower layers on sensing to achieve desired performance.
2. Transport Layer performance assessment for inference on internal state of network, e.g. TCP window state history, other parameters such as drop-out rate and error syndromes necessary for switching to more robust protocol from TCP and path and media diversity transmission.
3. Congestion and traffic monitoring, decisions on nominal or unusual traffic patterns that lead to performance degradations with sufficient information for possible rerouting, force-routing (e.g. segment routing), isolation of subnets, path diversity, path hopping, deployment of new assets for interconnection, repair of bad network elements or sectors, and network reconstitution.
4. MAC history and analytics monitoring to distinguish nominal operations from network under stress such as under DoS attack, using strong authentication, spread spectrum, multiple off-band MAC and secure Operating Systems.
5. Monitoring of hardware/software integrity with secure monitoring protocol (e.g. NOT SNMP), improving information integrity and element robustness for the purpose of isolating, switching-out, repair and routing around compromised elements.
6. Decisions on load balancing, reconfiguration, restoration using the most forefront, including cognitive, techniques.
7. Predict intentions of users and take or recommend appropriate actions.
8. Detect reliability and security related anomalies in the network (especially the control plane) and react automatically including reconstitution, re-optimization and insertion of key new interconnects.

While sensing at every network element is ideal but it is too costly to be feasible, using a fraction of major nodes as sensing centers can work if judiciously deployed, [1,2], Fig.2. A rough estimate of the fraction of nodes to be equipped with diagnostics is given in Fig. 2. Most of the isolation mechanisms are already built into optical networks. They are the optical switches and fail-over mechanisms already in place. Where necessary, additional shut-off valves can be strategically placed to isolate subnets or sectors of a subnet when deemed necessary [1,2].

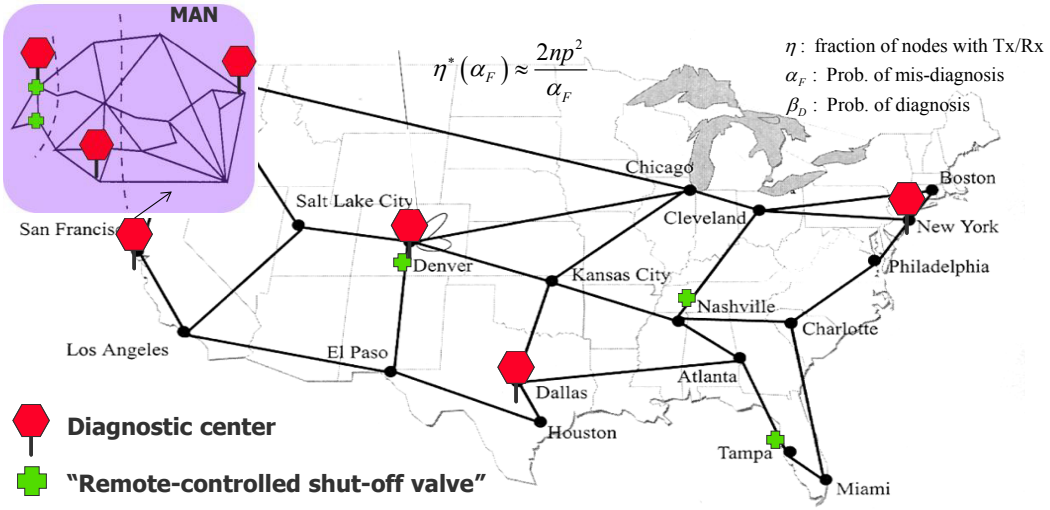

Figure 2. Optical network sensing and probing with probing centers and shut-off valves for mitigation.

2.1 Types of Impairments/Attacks and Sensing/Localization Techniques

Most research on network resilience focus on single layer considerations. However, optical networks impairments/attacks can permeate across layers to affect Application Layer performance. An example is when a transmitter laser is abruptly (<1mS) turned on or off, transients are created by cross gain coupling of the amplifiers to other wavelengths in the same fiber, Fig.3, [6]. The peaks and valleys after several amplifiers can be as long as several mS and ~10db, rendering most error correction codes and Transport Layer Protocols (such as TCP closing its window to a very low rate), ineffective. Fig.4 provides some examples of impairment/attacks and sensing methods over single and multiple layers, [4]. It is noteworthy that the sensing methods range from the Physical Layer to the Transport Layer. Most of these sensing techniques though known are not usually deployed in present day optical networks. Moreover, cross-layer sensing and assessment is seldom done. The

primary reason is optical network today typically do not pass detailed link states through layers. Thus, these phenomena are extremely difficult to detect and identify. With the advent of multi-layer network management, such as Orchestration, there are better possibilities for implementing such sensing and assessment mechanisms.

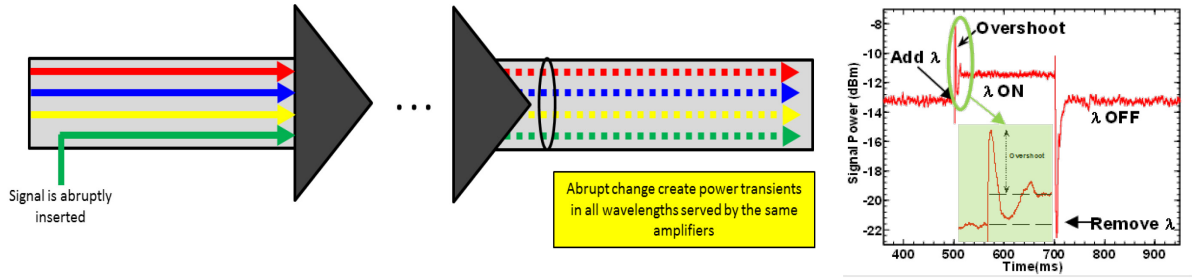

Figure 3. Impairment due to laser turn-on turn-off transients propagating over the reach of the lightpath,[6].

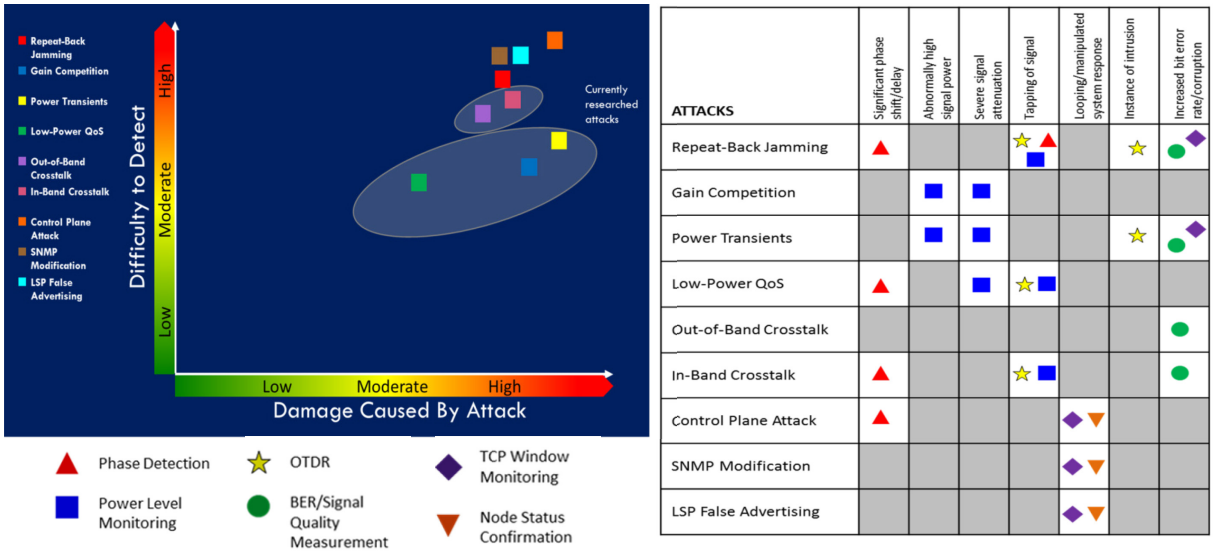

Figure 4.Examples of impairment/attacks and sensing methods over multiple layers, [4].

2.2 Active Network Probing and Enforcement

Sensing and monitoring of the states of a wide area optical network involves a large number of elements. Fresh samples of states must be available to the network management system for every coherence time of the states which can be as short as 100mS, [6]. Fig.5, [2], describe an optimum probing scheme that can be used to verify the state of the links and nodes of an optical network. This scheme is effective for both failed links or nodes but must be modified for subtle impairments short of clear-cut failuresthat can degrade network performance without disabling connectivity. In this scheme, the network uses long reach probes on un-used paths to ascertain availability. When a failure is detected, the algorithm will enter the localization phase where the location of the fault/s is/are located with the optimum number of steps as indicated by an Information Theoretic consideration.

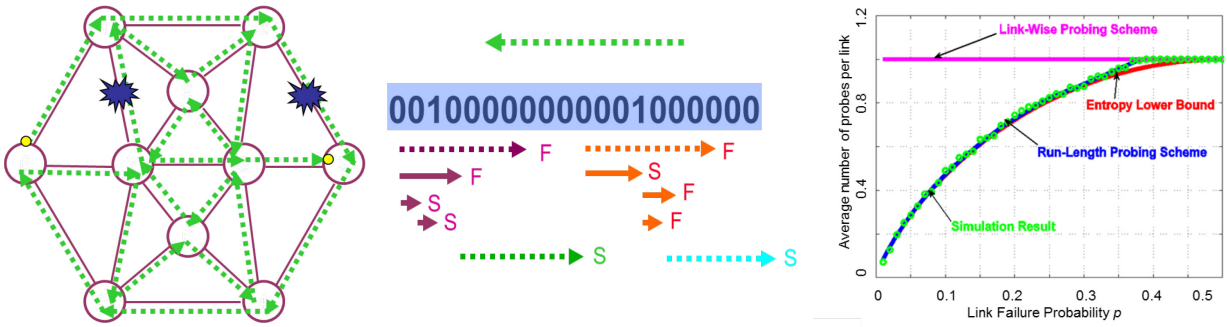

Figure 5.Optimum Euler trail probing scheme to determine integrity of optical network links and nodes, [2].

2.3 Lightpath diversity at Layers 1, 2 and 3.

To improve resiliency (at the expense of capacity), lightpath diversity at Layers 1, 2, 3 and 4 can be used. A typical method used is simultaneous communication over multiple disjoint lightpaths. This allows multiple

failures of links and nodes and response time to failures can be as short as one symbol, [2]. With a transmitter energy constraint, there is a trade-off between combating noise and providing diversity to add resiliency. An optimum diversity for the minimization of symbol error rate can be found analytically, and is illustrated in Fig. 6, [2]. Another form of path diversity is hopping between independent paths over time. With coding and enough diversity the sessions can be received successfully. However, both cases presuppose some prior knowledge of the path states albeit somewhat stale. Fig 7, [6], shows the need for network state updates approximately every ½ coherence time and how the blocking probability performance degrades if the updates are too stale.

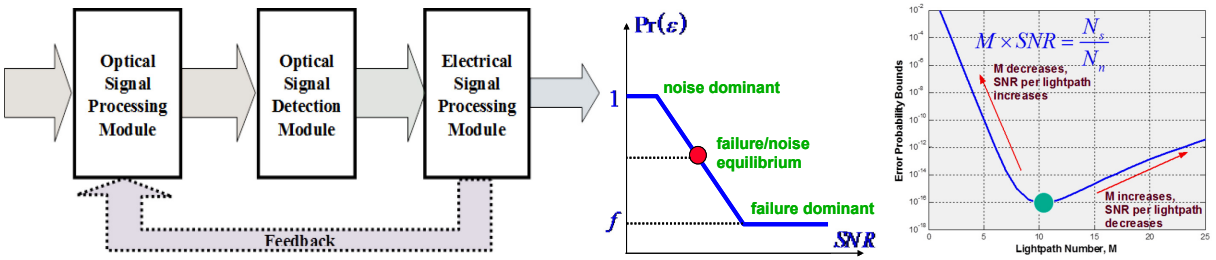

Figure 6. Lightpath diversity at L1-2 with a transmitter power constraint and optimized performance, [2].

The use of path diversity presents new challenges at the Application Layer, especially when using the time hopping version. The non-stationary behaviour of the dynamics will cause window closing even session termination by TCP, [4]. A new transport Layer protocol design suitable for bursty link performance such as that given in [8], is needed.

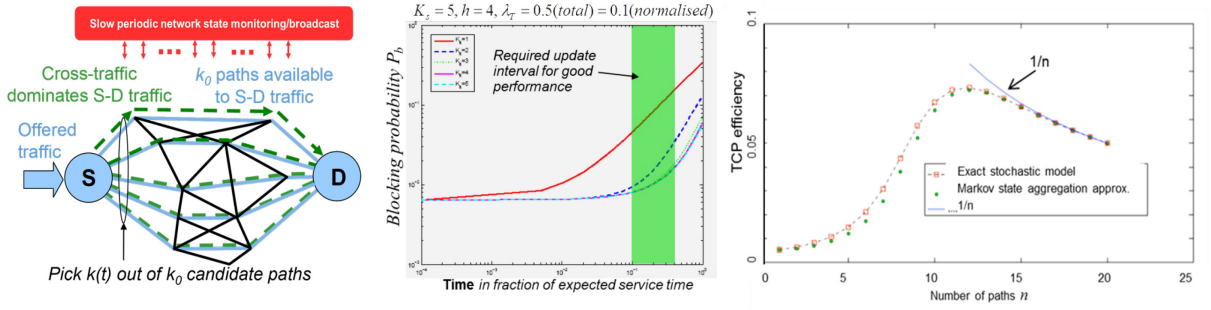

Figure 7. Optical reconfiguration with very fast setups and necessity for updates every coherence time, [3-6], and performance of optimized multi-path Transport Layer Protocol TCP designs.

3. SUMMARY AND DISCUSSIONS

A resilient optical network architecture must involve the coordination of multiple layers of the network from the Physical Layer to the Application Layer. Attacks in one layer can cause serious performance degradations in other layers and ultimately the Application Layer. Such cross layer effects have not been subjected to extensive characterisations and coupling between layers are not fully underrstood. A resilient architecture starts with a robust network management and control system's sensing of anomalies. The volume of the entirety of detailed network states will overwhelm the transport network and network management and control processors. Thus, efficient and judicious under-sampling of states and accurate assessments and decisions on mitigation actions must be made by automated cognitive systems that adaptively isolate faults, reconfigure surviving assets and reconstitute broken down domains to maintain connections and provide adequate capacities.

REFERENCES

[1] Antonia Feffer, "Comprehensive Security Strategy for All-Optical Networks," MIT EECS MS Thesis 2015

[2] Y. Wen, V.W.S. Chan, L. Zheng, "Efficient fault-diagnosis algorithms for all-optical WDM networks with probabilistic link failures," Journal of Lightwave Technology, Oct. 2005

[3] Zhang Lei and Vincent Chan, "Scalable Fast Scheduling for Optical Flow Switching Using Sampled Entropy and Mutual Information Broadcast," IEEE/OSA JOCN, April 2014

[4] Mia Qian, "Effects of Diversity Routing on TCP Performance in Networks with Stochastic Channels," MS Thesis MIT 2012.

[5] Jason Zhang, John M. Chapin, Vincent W.S. Chan, "Failure of TCP Congestion Control under Diversity Routing," IEEE WCNC, March, 2011.

[6] Lei Zhang and Vincent W. S. Chan, "Optical Flow Switching with Physical Layer Impairments - Modeling, Algorithm, and Control," IEEE Communication Society Globecom, 2015.

[7] Vincent Chan, "Cognitive Optical Networks," ICC May 2018.

[8] Henna Huang and Vincent W.S. Chan, “Optical Flow-Switched Transport Layer Protocol Design and Performance Analysis,” Journal of Optical Communications and Networks,” July 2014.