

Adaptive Multi-Layer Network Survivability: A Unified Framework for Countering Cyber-Terrorism

William Yurcik
{yurcik@tele.pitt.edu}
Telecommunications Program
University of Pittsburgh

Speaking publicly about infrastructure threats for the first time, Director of the CIA, George Tenet, testified before Congress that several foreign governments have "information warfare" programs targeting the USA. {testimony before the Senate Committee on Governmental Affairs June 1998} This, in itself, may be reason to improve protection of computer systems and telecommunications infrastructures. However, given the fragility of the U.S. infrastructure to small random failures (such as hardware failures, bad software design, innocent human errors, and environmental events) an already serious situation becomes even worse. If small random failures have resulted in the drastic effects of many large-scale regional and national outages at an increasing rate over the last two decades, what is the vulnerability of U.S. infrastructure to a malicious, intelligent, well-funded, and determined attack?

Previous research in the application of reliability theory to large complex systems has focused on characterizing failure distributions to answer questions such as why systems fail, are systems failing more or less often, and what can be done to make systems fail less. Reliability analysis assumes failure events are independent (for mathematical analysis) and emphasizes preventing the most probable failure events from occurring.

Survivability research builds upon reliability research to focus on recovery after a failure has left part of a system unavailable. Survivability analysis allows failure events to be correlated (as in an intelligent attack) and emphasizes recovery from failure events to the most critical system components (not necessarily the most probable failure events). The goal of survivability research is to maintain continuous service performance to users despite underlying system failures. The best examples of implemented survivability research are combat aircraft that can still fly despite extensive underlying system damage. While reliability research assumes that failures may be eliminated, survivability assumes failures will continue to occur but mission functionality can be maintained despite underlying system degradation. I submit that survivability is the appropriate risk-avoidance approach given an unbounded failure set and the potential a failure could occur which causes a large-scale outage to a critical national infrastructure if no recovery procedures exist.

Survivability is an especially appropriate concept in the context of computer / telecommunications infrastructure, because, as most network managers will attest, under normal operating conditions some part of a network is almost always broken during any given time period. Thus providing survivability to computer networks can serve as a illustrative model for all computer system and telecommunications infrastructure. Another reason for choosing a network model is that while emphasis on end-user computer system security is vital, a network model can exhibit the dynamics of system interconnectivity where a failure in one system can affect many other systems due to

interdependencies and multiplier effects. While it can be argued that end-user computer system security encompasses network components (i.e., routers, switches), the reality is that network components have additional vulnerabilities due to more stringent time-based coordination.

A Multi-Layer Network Framework

A multi-layer framework is an unified approach to address both the reliability of a fragile infrastructure as well as defend against malicious attacks. In a generalized case I define three network layers as shown in Figure 1.

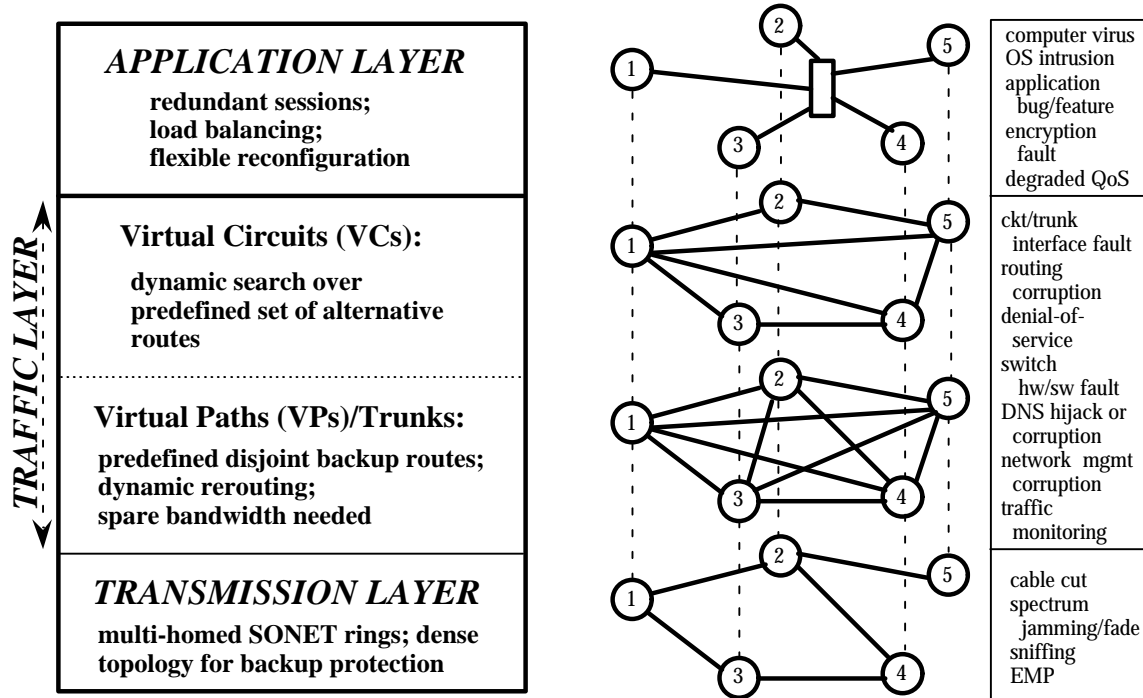


Figure 1: Multi-Layer Survivability Model with Corresponding Faults/Attacks (1) *physical layer* -transmission medium and signals, (2) *traffic layer* - provides routing and congestion control for connections across a network, and (3) *application layer* - uses network services for end-system processes and provides interface to user; and representative faults/attacks classified by the layer at which they may originate.

Different restoration techniques can occur independently at each of these network layers. For instance: at the application layer a wireless telephone handset may automatically switch from a call over an analog infrastructure to a call over a digital infrastructure or vice versa given a fault event; at the traffic layer connections may be transparently routed around link or switch failure using disjoint paths; at the physical layer 1:N trunk protection switching can provide a hot-standby for back hoe cable cuts. I expect results from this multi-layer framework will extend from conventional attacks which kinetically destroy links and nodes at the physical layer to virtual attacks which destroy or corrupt computer operating systems, application software, and databases at the application layer.

What is lacking is a coherent and integrated approach for end-to-end survivability. This proposal is to coordinate between different restoration techniques at different layers. There has been little or no research or implementation in this area due to the inertia of reliance on established restoration techniques at independent layers with no coordination but the potential benefits of coordination are enormous. While AT&T with its more dense switch connectivity has relied predominantly on restoration at the traffic layer via their proprietary FASTAR system, Sprint is relying predominantly on restoration at the physical layer via SONET self-healing rings [2,7]. Note that established techniques have not prevented large-scale outages from continuing to occur.

The main issues are the interaction between restoration mechanisms applied at different layers, defining which layer the restoration process should start independent or dependent to the specific fault type and location, when to escalate restoration to a higher layer, and which layer to escalate. To understand the benefits of coordinating different layers I must point out the tradeoffs between restoration at the different layers: the physical layer has the fastest restoration (50ms); higher layers can restore failures at lower layers; lower layers cannot restore failures at higher layers; layers in combination can provide the same restoration as a single layer; and different layer(s) can provide the same restoration as another layer for a lower cost (in terms of resources).

There has been a singular focus on restoration at each layer independent of other layers, for example computer virus protection at the application layer. While a computer virus will immediately affect systems at the application layer, traffic/physical layers can still perform useful functions such as quarantine, network partitioning, and alert mechanisms. There is also a danger in focusing protection on a particular type of attack at a single layer since cyber-attacks can easily adapt to a different vulnerability at another layer. A physical layer attack with a strategically-placed kinetic weapon or a traffic level denial-of-service attack may prove unrecoverable at the application layer despite impenetrable operating system defenses. A combined attack at different layers simultaneously is an open question. A unified approach is needed over all layers.

There is an interrelationship between restoration at the different layers in terms of flexibility, speed, and cost. Coordination between restoration at the different layers will provide effective survivability to networks by optimizing flexibility, speed, and cost. Current networks invest in restoration techniques at a single layer and this has resulted in (1) lack of flexibility since lower layers cannot recover from faults at higher layers; (2) outages due to exceeding service time thresholds since higher layer restoration is slower; and (3) survivability that is either not provided due to excessive implementation cost and/or restoration techniques whose cost is comparable to the cost of a projected outage. In contrast, a multi-layer approach provides a flexible, fast, and cost-effective solution to providing network survivability by allowing the best attributes of restoration at each layer to be shared by the entire network.

Another attraction to this multi-layer framework is feasibility. There is no need to overlay separate hardened core components or develop a separate centralized control structure. Each of these layers map to defined functionality in existing networks (i.e., circuit-switched, packet/cell-switched networks) and can be deployed via periodic software upgrades in an incremental distributed manner ensuring interoperability with existing technology.

Adaptive Restoration at Each Layer

The restoration algorithms at each layer will be suitable for automatic invocation by network components, resulting in a self-configuring system that adapts to the changing fault environment.

Since fault recovery is possible at various layers, one aspect is determining what combinations of traffic restoration should be used at each layer and how this is related to the overall network topological design.

At an individual layer, adaptive tradeoffs include end-to-end restoration versus local restoration adjacent to a failure; priority restoration for different services; and methods for identifying backup restoration routes around a failure. As a detailed example of adaptive restoration tradeoffs at the traffic layer, there are two basic methods of identifying a backup route for restoration: (1) a backup route can be computed in advance or (2) a dynamic search for a backup route can be computed in real-time. In the preplanned method restoration is guaranteed, each connection has a prearranged backup when originally assigned. In the dynamic search method, signaling messages are sent after being notified of a network failure and backup routes are chosen via processing of these signals. In the preplanned method, backup connections remain reserved for restoration purposes. In dynamic search, backup connections are not reserved and thus not guaranteed. The preplanned method is faster and dependent on the number of connections to be rerouted while the dynamic search method is slower due to signaling and dependent on network conditions in addition to the number of connections to be rerouted.

An important algorithm constraint for a restoration technique is ensuring that the failure of a any set of network components (at any layer) remains localized affecting only those network sessions directly associated with that set of components. Established sessions not directly affected by a fault should not be reconfigured unless it can be transparently accomplished. This is in direct contrast to massive reconfiguration strategies which re-optimize the entire network by interrupting all sessions and then attempting to reestablish. It is felt that massive reconfiguration strategies help to achieve malicious attacker goals of denial-of-service (by triggering massive reconfigurations) and disrupting communications (sessions not directly associated with a network fault).

In conclusion, I am proposing a unified model (an adaptive multi-layer network model) such that survivability can be provided against the complete range of potential cyber-attacks. Multiple layers reduce complexity and are a rich conceptual tool for intuitive discussion. I believe this unified framework is useful, feasible, and effective and welcome the opportunity to briefly present details, respond to questions, and receive constructive criticism.

References:

- [1] R.S.K. Chng, et. al., "A Multi-Layer Restoration Strategy For Reconfigurable Networks," in *Proc. of IEEE INFOCOM'94*, pp. 1872- 1878.
- [2] C-W Chao, "FASTAR - A Robust System for Fast DS3 Restoration," in *Proc. of IEEE Globecom'91*.
- [3] K.R. Krishnan et. al., "Improved Survivability with Multi-Layer Dynamic Routing," *IEEE Comm. Magazine*, July 1995, pp. 62-68.
- [4] K.R. Krishnan et. al., "Unified Models of Survivability for Multi-Technology Networks," *Intl. Teletraffic Congress (ITC 14)*, pp. 655- 666.
- [5] D. Medhi, "A Unified Approach to Network Survivability for Teletraffic Networks: Models, Algorithms, and Analysis," *IEEE Trans. on Comm.*, Vol. 42, No. 2/3/4, pp. 534-548.
- [6] L. Nederlof, et. al., "End-to-End Survivable Broadband Networks," *IEEE Comm. Magazine*, Sept. 1995.
- [7] T-H. Wu, *Fiber Network Service Survivability*. Artech House, 1992.
- [8] T-H Wu, et. al., "Integrity of Public Telecommunications Networks," *IEEE J. of Sel. Areas in Comm.*, Vol. 12, No. 1, pp. 1-4.