Network Resilience, Survivability, and Disruption Tolerance: Architectural Framework, Strategy, Analysis, Simulation, Tools, and Experimentation

James P.G. Sterbenz and Egemen Çetinkaya

Abstract:
As the Internet becomes increasingly important to all aspects of society, the consequences of disruption are increasingly severe. Thus it is critical to increase the resilience and survivability of the future networks in general, and the Internet in particular. We define resilience as the ability of the network to provide desired service even when the network is challenged by attacks, large-scale disasters, and other failures. Resilience subsumes the disciplines of survivability, fault-tolerance, disruption-tolerance, traffic-tolerance, dependability, performability, and security. After an introduction to the disciplines and challenges to network resilience, this presentation will first present the ResiliNets framework developed in the NSF FIND (Future Internet Design) PoMo and EU FIRE (Future Internet Research and Experimentation) ResumeNet projects. We then discuss analytical, simulation, and experimental emulation techniques for understanding, evaluating, and improving the resilience of the Future Internet. This includes a multilevel state-space based approach that plots network service delivery against operational state that is the basis for both mathematical- and simulation-based analysis, and approaches that embed fundamental properties such as redundancy and diversity into all aspects of network structure, mechanism, and protocols. A set of tools to help in this analysis has been developed: KU-LoCGen (Location and Cost-Constrained Topology Generation), KU-TopViwe (Topology Viewer), and KU-CSM (Challenge Simulation Module). Plans to experimentally evaluate resilience include using the international programmable testbed GpENI: Great Plains Environment for Network Innovation.