SURVIVABILITY ANALYSIS OF NETWORKED SYSTEMS

Jeannette M. Wing

Computer Science Department

Carnegie Mellon University

Pittsburgh, Pennsylvania 15213

U.S.A.

wing@cs.cmu.edu

Abstract Survivability is the ability of a system to continue operating despite the presence of abnormal events such as accidental failures and malicious intrusions. Ensuring system survivability has increased in importance as critical infrastructures have become heavily dependent on computers. Examples of these infrastructures are utility, transportation, communication, and financial networks. Complicating the analysis of these networked systems is their inter-dependencies: a failure in one may trigger a failure in another.

In this talk I present a two-phase method for performing survivability analysis of networked systems. First, we inject failure and intrusion events into a system model, use model checking to verify it for fault- and service-related properties, and visually display the model's effects with respect to a given property as a *scenario graph*. Then, we annotate the graphs with symbolic or numeric probabilities to enable reliability analysis using standard Markov Decision Process policy iteration algorithms. We use similar modeling and analysis techniques to do latency and cost-benefit analyses of these networked systems. We model dependencies among events using Bayesian Networks. We applied our two-phase method to two large cases studies from the financial industry and are currently applying it to a case study on intrusion detection systems.

This work is jointly done with Somesh Jha of the University of Wisconsin and Oleg Sheyner of Carnegie Mellon University. A full paper describing this work is in *the Proceedings of the International Conference on Software Engineering*, May 2001.

Keywords: survivability, fault-tolerance, security, reliability, model checking, Markov Decision Processes, Bayesian Networks, scenario graphs.