Model-Driven Recovery in Distributed Systems

Kaustubh R. Joshi, Matti A. Hiltunen (AT&T), William H. Sanders, and Richard D. Sclichting (AT&T)

Probabilistic Diagnosis

One failure results in many alarms:

- Restoring health of distributed systems using adaptive recovery
  - Minimize disruptions, downtime, and lost capacity
  - Use feedback control to drive system to good states
  - When the precise cause of failure is unknown
  - Multi-tier systems, may span administrative domains
  - Monitoring in one layer, fault in another
  - Poor localization, false positives and negatives
  - Result: uncertainty about true system state

- and when several recovery options are available
  - Restart of component, host, subsystem, entire system
  - More diagnostic information
  - Each has different costs, benefits

A Model Driven Recovery Controller:
- Uses path based monitors to detect failures
- Uses probabilistic Bayesian diagnosis to estimate cause of failure
- Uses stochastic planning to choose recovery/diagnostic action sequences
- Always terminates, probabilistically succeeds, upper bounds recovery cost

Solutions: Probabilistic Model-based Bayesian Diagnosis

Recovery Action Selection

Model recovery actions and their effects

- Visible system states: state variables: Boolean, integer
  - e.g., Boolean: server1.enabled
- Partially visible system states: Boolean fault hypotheses
  - e.g., Boolean: server1.valuefault, null fault hypothesis
- Uncertainty: path monitors, log monitors
  - Coverage models, probability of false positives
- Recovery actions: preconditions, probabilistic state change
  - Change both visible state and fault hypotheses
  - e.g., restart, enable/disable
- Cost model:
  - Unit impulse costs as function of state, fault, action
  - e.g. fraction of lost requests (rate cost)

... and utilize sequential nature of recovery

... to choose good action sequences: optimize multi-step recovery trajectory tree

Use optimization bounds to provide guarantees

- How to decide when to stop recovery?
  - Include cost of stopping in wrong states in decision making
  - Stop when it is optimal action

- Looking beyond finite horizon
  - Formulate undiscounted partially observable Markov Decision Process
  - We develop new bounds on undiscounted optimal value beyond horizon
  - Step 1: Compute bound on underlying MDP
  - Step 2: Form POMDP bound by combining MDP bounds

- Cheaper computation for up to millions of states

- Bounds allow recovery controller to guarantee
  - Probabilistically guaranteed recovery: recovery does not terminate until recovery is successful (with probability p)
  - Finite termination: recovery always terminates in finite time
  - Performance guarantee: average cost lower than promised value

www.iti.uiuc.edu
University of Illinois at Urbana-Champaign