1. Introduction

2. Fault Models

3. Applications

4. Anomaly Detection

5. Summary
Monolithic Smart-Grid Communications Model

- PMU: Phasor Measurement Unit
- PDC: Phasor Data Concentrator
- Area: Balancing Authority running on a High Performance Computing (HPC) Cluster

A communication model for a three-area distributed smart-grid application

- PMUPeriod: 1.0/30
- SCADAPeriod: 120
Monolithic Smart-Grid Communications Model

- PMU: Phasor Measurement Unit
- PDC: Phasor Data Concentrator
- Area: Balancing Authority running on a High Performance Computing (HPC) Cluster

A communication model for a three-area distributed smart-grid application

- PMUPeriod: 1.0/30
- SCADAPeriod: 120
Aspect-Oriented Modeling: A Comparison

Introduction

Fault Models

Applications

Anomaly Detection

Summary
The Aspect-Oriented Way

For the communication architecture, the specific implementation uses four different network fabrics, each modeled as a separate aspect.
Fault Models

- Faults can be viewed as an aspect of a system, as they are often orthogonal to the application model.
- A fault model is a structured and well-defined representation of a faulty behavior of a system.
- Help identify and isolate an anomaly in a system component.
History of Fault Models

- Fault hypotheses are essential for complex system architectures
  - Aerospace
  - Automotive
  - Energy systems
  - Manufacturing, ...

- Architecture Analysis & Design Language (AADL)
  - Standardized by SAE (Society of Automotive Engineers)
  - Error-model annex: fault and fault propagation models

[www.examiner.com]

http://www.chipestimate.com/blogs/IPInsider/?p=92
Fault Models in Ptolemy: Goals

- Cyber-Physical System Design goals
  - Flexibility
  - Fault-tolerance
  - Robustness
- Modal faults: Learning and detection of faulty and normal system behavior
  - Parameter estimation
  - Maximum-Likelihood classification using Machine Learning techniques
- Refinement of the functional model
Fault Models in Ptolemy

- Goal: introduce reusable design patterns for fault modeling and detection
- Aspect-oriented models used in modeling
  - Communication/Network behavior
    - Network delays
    - Queuing behavior
    - Packet drops
  - Atomic Probabilistic Faults
    - Stuck-At Faults
    - Bit-Flip Faults
  - Modal Models extended with Probabilistic Transitions
    - Adds modeling capability of numerous stochastic models:
      - Markov Models, Markov Chains, Mixture Models, etc.
Fault Models as Aspects

Introduction

Fault Models

Application

Anomaly Detection

Summary
Transition Systems are an effective tool for modeling deterministic modal behavior.

However, the uncertainty in the nature of faults motivates use of probabilistic models.
Extending Modal Models in Ptolemy: Markov Chains

StuckAt Fault as a Probabilistic Automaton

guard: probability(0.1)
Extending Modal Models in Ptolemy: Hidden Markov Models

- An HMM is a Markov model with unobservable states (latent variables)
- $q_i$: Hidden State: evolves according to a Markov process with transition probability matrix $A$
- $y_j$: Observed state: $P(y_j|q_j = q)$ is a random variable
- $\pi$: Prior distribution of hidden states Above: arrows indicate probabilistic dependence.
Extending Modal Models in Ptolemy: Hidden Markov Models

- Fault Models
- Applications
- Anomaly Detection
- Summary

Introduction

Fault Models

Extending Modal Models in Ptolemy: Hidden Markov Models

- guard: probability(0.5)
- guard: probability(0.05)
- guard: probability(0.02)
- guard: probability(0.05)
- guard: probability(0.01)
- guard: probability(0.01)

- WiFi
- LTE
- fault

- delayStateMean: {50E-3, 150E-3, 400E-3}
- delayStateStandardDeviation3: {10E-3, 40E-3, 80E-3}
Extending Modal Models in Ptolemy: Hidden Markov Models

fault

init

guard: probability(0.5)
guard: probability(0.5)
guard: probability(0.05)
guard: probability(0.05)
guard: probability(0.02)
guard: probability(0.01)
guard: probability(0.02)
guard: probability(0.01)

WIFI
LTE

port

observation
state

- delayStateMean: {60E-3, 150E-3, 400E-3}
- delayStateStandardDeviation: {10E-3, 40E-3, 80E-3}

SDF Director

iterations: AUTO

port

Rician

observation

trigger

xMean: delayStateMean(stateIndex)
standardDeviation: delayStateStandardDeviation(stateIndex)

Const

state

stateIndex

value: stateIndex

Ilge Akkaya

Introduction
Fault Models
Applications
Anomaly Detection
Summary

UC Berkeley
Extending Modal Models in Ptolemy: Hidden Markov Models
Goal: Building a generic anomaly detection library to
- Perform *unsupervised learning* on data streams
- Notify services (and/or TerraPlane) when anomaly has been inferred
Service Channel

Aspect-Oriented Fault Modeling and Anomaly Detection in Ptolemy II

Ilge Akkaya

Introduction
Fault Models
Applications
Anomaly Detection
Summary

Latency Distribution

SDF Director

xMean: delayStateMean(stateIndex)
standardDeviation: delayStateStandardDeviation(stateIndex)

const

state

trigger

observation

value: stateIndex

port

WiFi

LTE

anomalous

guard: probability(0.5)
guard: probability(0.05)
guard: probability(0.02)
guard: probability(0.05)
guard: probability(0.01)
guard: probability(0.01)
guard: probability(0.5)

Latency Distribution

10^2

0 0.05 0.10 0.15 0.20 0.25 0.30 0.35 0.40 0.45 0.50 0.55 0.60 0.65 0.70

0 1 2 3 4 5 6

WiFi

LTE

anomalous

observation

state

trigger

const

value: stateIndex

iterations: AUTO

0

stateIndex: 2

delayStateMean: {1.5E-3, 150E-3, 400E-3}
delayStateStandardDeviation: {10E-3, 40E-3, 80E-3}
Anomaly Detection

- Goal: Building a generic anomaly detection library to
  - Perform unsupervised learning on data streams
  - Notify services (and/or TerraPlane) when anomaly has been inferred
- In the HMM setting, the best effort solution is the Maximum Likelihood estimate of
  - Underlying parameters of the stochastic models
  - Maximum-likelihood classification of hidden state sequences
Anomaly Detection: Expectation-Maximization (EM)

- EM is an iterative algorithm used for finding the Maximum-Likelihood parameter estimates of a probabilistic graphical model.
- Given the observations, finds the most likely set of parameters that explain the observations.
- Statistically-sound version of the well-known heuristic: K-Means Clustering algorithm

![EM Convergence Pattern For GMM with Two Mixture Components](EM Convergence Pattern For GMM with Two Mixture Components.png)
A Ptolemy Toolkit for HMM-Based Anomaly Detection

Parameter Estimation

Observation Classification
Introduction

Fault Models

Applications

Anomaly Detection

Summary
Smart Grid Communication Fault Injection

- **PMULink**: Dedicated single-server network for each PMU sensor
- **Middleware Network**: A common single server for processing messages from all three areas
- **Local network**: Single-server NASPINet T1 links with adjustable network capacity and packet size

**Middleware Aspect**: Aggregation and Convergence Control

---

**Aspect-Oriented Fault Modeling and Anomaly Detection in Ptolemy II**

- **Introduction**
- **Fault Models**
- **Applications**
- **Anomaly Detection**
- **Summary**
Smart Grid Communication Fault Injection

- **Introduction**
- **Fault Models**
- **Applications**
- **Anomaly Detection**
- **Summary**

**Aspect-Oriented Fault Modeling and Anomaly Detection in Ptolemy II**

**Summary**

Ilge Akkaya 24 / 26
Introduction

Fault Models

Applications

Anomaly Detection

Summary

Smart Grid Communication Fault Injection

Aspect-Oriented Fault Modeling and Anomaly Detection in Ptolemy II

Ilge Akkaya
Summary

- Aspect-oriented modeling
- Probabilistic fault models implemented in Ptolemy
- Goal: Provide a generic parameter estimation and classification library to perform generic anomaly detection on real-time data streams
- Investigating future methods to better model separation between environmental and system-imposed uncertainties
- Additional fault-detection mechanisms
- Dynamic, multi-sensor fault models
- A framework for generic anomaly detection on aggregate sensor streams
Questions?

Comments?