OnTimeDetect: Offline and Online Network Anomaly Notification Tool

Prasad Calyam, Ph.D.
pcalyam@osc.edu

Other Team Members: Jialu Pu, Weiping Mandrawa

“Network Tools Tutorial” Session, Internet2 Spring Member Meeting, April 26, 2010
Topics of Discussion

• Project Overview
• OnTimeDetect Background
• OnTimeDetect Tool Features (Work in progress)
  – Offline Mode (GUI version for Windows/Linux)
    • Drill-down analysis of a path trace (Demo)
  – Online Mode (Command-line version for Linux)
    • Real-time anomaly monitoring for multiple sites
• Tool Deployment Experiences
• Future Development Plan
• Questions and Feedback
Project Overview

• DOE ASCR Network Research Grant to OSC/OARnet
  – PI: Prasad Calyam, Ph.D.

• Goal: To develop *multi-domain* network status sampling techniques and tools to measure/analyze multi-layer performance
  – To be deployed on testbeds to support networking for DOE science
  – E.g., E-Center network performance monitoring for Tier-1 to Tier-2 LHC sites consuming data feeds from CERN (Tier-0)

• Collaborations: LBNL, FermiLab, Bucknell U., U. of Delaware, Internet2

• Expected Outcomes:
  – Enhanced scheduling algorithms and tools to sample multi-domain and multi-layer network status with active/passive measurements
  – Algorithms validation with measurement analysis tools for network weather forecasting, anomaly detection, fault-diagnosis
OnTimeDetect Overview

• Background:
  – Effort to enhance the NLANR/SLAC implementations of a network performance “plateau-detector” algorithm
  – Evaluated anomaly detection performance for both synthetic and actual perfSONAR measurement traces
  – Developed “OnTimeDetect” v0.1 tool prototype from evaluation experiences

• Significance:
  – perfSONAR web-service users need automated techniques and intuitive tools to analyze anomalies in real-time and offline manner
  – Tools should not be “noisy” when used for monitoring anomalies
    • Network anomaly detector in tool should produce minimum false alarms and detect bottleneck events quickly
Plateau-Detector

- Enhanced mean ± standard deviation (MSD) algorithm
Plateau-Detector Illustration

![Plateau-Detector Illustration](image)
OnTimeDetect Tool Features

• Offline Mode (GUI version for Windows/Linux)
  – Drill-down analysis of anomaly events in path traces at multi-resolution timescales
  – Modify plateau-detector settings to analyze anomalies
  – Zoom In/Out, Hand functions supported
  – Save annotated graph with anomalies and text report

• Online Mode (Command-line version for Linux)
  – Real-time anomaly monitoring for multiple sites
Tool Deployment Experiences

• OnTimeDetect tool has been used to analyze BWCTL measurements from perfSONAR-enabled measurement archives at 65 sites

• Anomalies analyzed on 480 network paths connecting various HPC communities (i.e., universities, labs, HPC centers) over high-speed network backbones that include ESnet, Internet2, GEANT, CENIC, KREONET, LHCOPN, ...

• Evaluation performed in terms of accuracy, agility and scalability of anomaly detection
Future Development Plan

• Integrate tool into DOE E-Center efforts for analyzing ESnet deployed perfSONAR measurement archives

• Release “OnTimeDetect” v1.0 Beta – Summer 2010

• Integrate into perfSONAR “Web-Admin” Analysis – before SC’10
“OnTimeDetect” v0.1 Screenshot

ESnet perfSONAR BWCTL Trace

GUI Tool to Analyze Anomalies (e.g., plateaus) in perfSONAR Measurements
Ideas for “OnTimeDetect” in perfSONAR

- Toolkit could extend perfSONAR “Web-Admin” Analysis capabilities
  - Add “Analyze” button in addition to existing “Graph” button
- Could enable users to perform online (on current data sets) and offline (on historic data sets) analysis of multi-domain measurements

![Current Data Set](image1.png)

![Historic Data Set](image2.png)

![Proposed Graph with anomaly events marked](image3.png)

![Proposed Interactive web-form to adjust Anomaly Detection “Analysis” settings](image4.png)
Questions and Feedback