Diagnosing Performance Problems in Wide Area Providers

Partha Kanuparthry, Constantine Dovrolis

USENIX ATC 2014
Wide Area Providers

- Internet providers: residential, enterprise, transit
- Content and cloud providers
Wide Area Providers
Wide Area Providers

- Contain inter-domain paths
Wide Area Providers

- Contain inter-domain paths
- Unknown changes: network upgrades, traffic matrix
Wide Area Providers

- Contain inter-domain paths
- Unknown changes: network upgrades, traffic matrix
- Unknown performance problems: new, short-lived, …
Wide Area Providers

- Use monitoring deployments
  - troubleshooting long-term problems (offline)
  - e.g., perfSONAR: 1,000+ monitors
  - `ping, traceroute`: delay, loss, reordering, paths

---

**Figure 1:** System architecture. "DB" and "FE" refer to the database and front end, respectively.

The system overview includes:

- **Measurement paths**:
  - Between each other, potentially covering long-term problems.
  - Advantage points on the Internet so that the paths between probes can easily plug into an existing monitoring infrastructure.

- **Database**:
  - Contains historical data, routing tables or trouble tickets/alerts.
  - Designed to operate in a distributed manner.
  - Can be scalable to handle large amounts of data.

- **Front end**:
  - Provides a user interface for monitoring network health.
  - Helps with troubleshooting and diagnosis.
  - May use domain knowledge on pre-defined sets of features.

- **Probe**:
  - Active measurements to detect Ethernet issues.
  - Does not require network-specific data such as syslogs, SNMP traps, router syslogs.
  - Work on end-to-end active measurements, and it does not need network-specific data such as syslogs, SNMP traps, router syslogs.

- **Netalyzr** probes to help a user with troubleshooting information.
  - Capable of diagnosing root causes of TCP performance problems using distributed monitoring tools.
  - Can easily plug into an existing monitoring infrastructure.
  - Works on end-to-end active measurements and can use a combination of domain knowledge and network data.

- **Tulip** diagnoises and localizes reordering, loss, and congestion using domain knowledge.
  - Ensures troubleshooting long-term problems.

- **Other tools**:
  - **Planet Seer** uses a combination of domain knowledge and network data to diagnose problems.
  - **G-RCA** works on data sources that use a significant amount of data sources usually available.
  - **META** probes to help with diagnosis by mining dependencies from historic data.

- **NICE** diagnoses faults in an enterprise by profiling end-host variables and user activities.
  - Provides the choice of carefully crafting probing structures based on domain knowledge.

- **Pythia** infrastructure is designed to operate in a distributed manner.
  - Works in an inter-domain setting, since it does not use significant network data sources.
What is Pythia?

• One system, three goals:
  • Detection: is there a performance problem?
  • Diagnosis: root cause of the problem?
  • Localization: where is the problem?

![Diagram of network with cloud symbols and server icons connected by lines]
Pythia and Wide Area Providers

Impact: Enable quick troubleshooting
Pythia and Wide Area Providers

Impact: Enable quick troubleshooting

- Near real time detection, diagnosis, localization
Pythia and Wide Area Providers

Impact: Enable quick troubleshooting

- Near real time detection, diagnosis, localization
- Works with data from existing monitoring deployments
Pythia and Wide Area Providers

Impact: Enable quick troubleshooting

- Near real time detection, diagnosis, localization
- Works with data from existing monitoring deployments
- Diagnose short-lived performance problems
Pythia and Wide Area Providers

Impact: Enable quick troubleshooting

- Near real time detection, diagnosis, localization
- Works with data from existing monitoring deployments
- Diagnose short-lived performance problems
- Tackle unknown problems (e.g., inter-domain)
Typical Deployment

- **Lightweight** agents at ISP monitors
- read measurement data in real time
- detect and diagnose problems

![Diagram of Typical Deployment](image)

One-way delays, loss, reordering

Detection ➔ Diagnosis
Typical Deployment

- **Lightweight** agents at ISP monitors
- read measurement data in real time
- detect and diagnose problems
Handling Inter-domain: Pathology Specifications

Specification language: operators can input problem definitions via domain/operational knowledge

<table>
<thead>
<tr>
<th>Pathologies</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATHOLOGY ContextSwitch DEF delay-exist AND large-triangle</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY EndHostNoise DEF delay-exist AND unipoint-peaks</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY RandomLoss DEF loss-exist AND NOT delay-loss-corr</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY DelayCorrelatedLoss DEF loss-exist AND delay-loss-corr</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY ShortOutage DEF loss-exist AND lossevent-small-dur</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY LargeBuffer DEF delay-exist AND high-delayIQR AND NOT large-triangle AND NOT unipoint-peaks AND NOT delay-levelshift AND NOT loss-exist OR delay-loss-corr</td>
<td></td>
</tr>
<tr>
<td>PATHOLOGY RouteNTPChange DEF delay-exist AND NOT large-triangle AND NOT unipoint-peaks AND delay-levelshift</td>
<td></td>
</tr>
</tbody>
</table>
Handling Inter-domain: Pathology Specifications

Specification language: operators can input problem definitions via domain/operational knowledge

### Pathologies

- **ContextSwitch**
  
 \[
  \text{PATHOLOGY } \text{ContextSwitch} \text{ DEF } \text{delay-exist AND large-triangle}
  \]

- **EndHostNoise**
  
 \[
  \text{PATHOLOGY } \text{EndHostNoise} \text{ DEF delay-exist AND unipoint-peaks}
  \]

- **RandomLoss**
  
 \[
  \text{PATHOLOGY } \text{RandomLoss} \text{ DEF loss-exist AND NOT delay-loss-corr}
  \]

- **DelayCorrelatedLoss**
  
 \[
  \text{PATHOLOGY } \text{DelayCorrelatedLoss} \text{ DEF loss-exist AND delay-loss-corr}
  \]

- **ShortOutage**
  
 \[
  \text{PATHOLOGY } \text{ShortOutage} \text{ DEF loss-exist AND lossevent-small-dur}
  \]

- **LargeBuffer**
  
 \[
  \text{PATHOLOGY } \text{LargeBuffer} \text{ DEF delay-exist AND high-delayIQR AND NOT large-triangle AND NOT unipoint-peaks AND NOT delay-levelshift AND NOT loss-exist OR delay-loss-corr}
  \]

- **RouteNTPChange**
  
 \[
  \text{PATHOLOGY } \text{RouteNTPChange} \text{ DEF delay-exist AND NOT large-triangle AND NOT unipoint-peaks AND delay-levelshift}
  \]

### Symptoms

- **Specifiers**

  Allows incremental diagnosis deployment
Processing Pathology Specifications

- Create a forest of decision trees
  - different trees contain disjoint symptoms
- Prune “unused” symptoms
- Generate diagnosis code

PATHOLOGY `ContextSwitch` DEF delay-exist
AND large-triangle

PATHOLOGY `EndHostNoise` DEF delay-exist
AND unipoint-peaks

PATHOLOGY `RandomLoss` DEF loss-exist
AND NOT delay-loss-corr

Symptoms

Pathologies

Efficient diagnosis code
Process

Pathologies

- ContextSwitch
- EndHostNoise
- RandomLoss

Symptoms

- large-triangle
- unipoint
- loss-exist

Efficient diagnosis code

Create a forest of decision trees
- different trees contain disjoint symptoms
- prune "unused" symptoms
- generate diagnosis code
Live Deployment

- 3 domains, 260+ inter-domain paths
- 11 pathologies diagnosed
- 100,000+ events/day (at highest sensitivity)

http://pythia.cc.gatech.edu
Live Deployment

- 3 domains, 260+ inter-domain paths
- 11 pathologies diagnosed
- 100,000+ events/day (at highest sensitivity)

http://pythia.cc.gatech.edu

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:25:32
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ac744b06000d689276f4968d8.owp

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:20:25
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ad744b06000d689276f4968d8.owp

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:15:24
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ad744b06000d689276f4968d8.owp

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:10:23
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ad744b06000d689276f4968d8.owp
C-S rate: 32521 Kbps

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:05:22
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ad744b06000d689276f4968d8.owp

Path: gammon.washington.k12.ga.us -> gammon.oconeeschools.org
Send timestamp: Thu, 12 Jun 2014 21:00:17
Diagnosis: ContextSwitch
File: /var/lib/owamp/hierarchy/root/regular/a609263ad744b06000d689276f4968d8.owp
C-S rate: 21657 Kbps
Detecting a Problem

- **Input:** one-way delays, loss, reordering
- **Output:** Is there a problem?
- **Solution:** find significant deviations from baseline.

<table>
<thead>
<tr>
<th>Type</th>
<th>Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay</td>
<td>Propagation + TX delay + noise</td>
</tr>
<tr>
<td>Loss</td>
<td>No loss</td>
</tr>
<tr>
<td>Reordering</td>
<td>No reordering</td>
</tr>
</tbody>
</table>

One-way meas.
Default Pathology Specifications

- Monitor effects
- Congestion & buffering
- Loss events
- Routing changes
- Reordering events
Default Pathology Specifications

- Monitor effects
- Congestion & buffering
- Loss events
- Routing changes
- Reordering events

### Monitor effects

<table>
<thead>
<tr>
<th>Network</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet2</td>
<td>4%</td>
</tr>
<tr>
<td>PlanetLab</td>
<td>72%</td>
</tr>
<tr>
<td>Residential</td>
<td>63%</td>
</tr>
<tr>
<td>ESnet</td>
<td>95%</td>
</tr>
</tbody>
</table>

Matters for short-lived problems!

Depends on monitor activity
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods
Monitor Effects

Busy OS environments => vacation periods

“large triangles”
inter-packet gap < vacation

600ms rise!
Monitor Effects

Busy OS environments => vacation periods

“large triangles”
inter-packet gap < vacation

“single point peaks”
inter-packet gap > vacation

600ms rise!

< 100ms peaks
Congestion and Buffers

- **Congestion**: significant backlog for long periods (> seconds)
  - overload?
  - bursty?
- Bottleneck buffer:
  - over-provisioned?
  - under-provisioned?
Loss events

Delay-correlated losses

Random losses
Unkowns

- Events that do not match any known signatures
- Rule out “unknown” end-host events by correlating paths to/from monitor
- Typically <10%
Perf. Problems in Networks

Data: 10Hz 40-byte probing:

- ESnet
- Internet2
- ShaperProbe (residential)
- PlanetLab

- Academic networks are similar
- Residential: more loss and congestion events
Residential Networks

Cable: more upstream events
DSL: more downstream events

DSL has more loss-based events than cable
Takeaways from Study

Domain and operational knowledge-based models give detailed diagnosis in wide area

Nature of pathologies varies with the wide area network

Configurable, real time, diagnosis systems can help!