Network Measurement

Brighten Godfrey

CS 538 November 14 2013
Measurement goes back to the inception of the Internet.

By the mid-1990s: Internet and its protocols were big, wild, organic.

- **Complex system:** hard to predict global effects of interacting components.
- **Distributed multi-party system:** can’t see everything that’s happening.

Network measurement moves from “just” monitoring to a science.
Challenge #1: Emergent behavior

Example: Model packet arrivals over time at a link

Simplest common model: Poisson process

- Parameter: rate $\lambda$  (mean arrivals per unit time)
- $\Pr[\text{time till next arrival} > t] = e^{-\lambda t}$  (exponential dist.)

Properties

- Memoryless: Even knowing entire history gives no clue as to next arrival time
- Number of arrivals in a given time interval concentrates around expected value
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993

Packets/Time Unit

Time Units, Unit = 0.01 Second (e)
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”  
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993

Time Units, Unit = 1 Second (c)
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993

```
Levels are used to identify the same segments of traffic
'89 trace) on 5 different time scales. (Different gray
Ethernet traffic (packets per time unit for the August
Figure 1 (a)—(e).
```

```
10
15
20
25
```

```
40
50
60
70
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993

Time Units, Unit = 100 Seconds (a)
Temporal patterns of traffic

“On the Self-Similar Nature of Ethernet Traffic”
Leland, Taqqu, Willinger, Wilson, SIGCOMM 1993

Bursty at all resolutions; Not captured by simple Poisson traffic model!
Challenge #2: Lack of visibility

Only a fraction of the system is visible

- For what we can observe, the cause is not obvious

Foundational work by Vern Paxson in the mid 1990s

- “End-to-End Routing Behavior in the Internet”, SIGCOMM 1996
- Loops, asymmetry, instability
- Established Internet measurement methodology: “looking inside the black box” via end-to-end measurements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adv</td>
<td>Advanced Network &amp; Services, Armonk, NY</td>
</tr>
<tr>
<td>austr</td>
<td>University of Melbourne, Australia</td>
</tr>
<tr>
<td>austr2</td>
<td>University of Newcastle, Australia</td>
</tr>
<tr>
<td>batman</td>
<td>National Center for Atmospheric Research, Boulder, CO</td>
</tr>
<tr>
<td>bnl</td>
<td>Brookhaven National Lab, NY</td>
</tr>
<tr>
<td>bsdi</td>
<td>Berkeley Software Design, Colorado Springs, CO</td>
</tr>
<tr>
<td>connix</td>
<td>Caravela Software, Middletown, CT</td>
</tr>
<tr>
<td>harv</td>
<td>Harvard University, Cambridge, MA</td>
</tr>
<tr>
<td>inria</td>
<td>INRIA, Sophia, France</td>
</tr>
<tr>
<td>korea</td>
<td>Pohang Institute of Science and Technology, South Korea</td>
</tr>
<tr>
<td>lbl</td>
<td>Lawrence Berkeley Lab, CA</td>
</tr>
<tr>
<td>lbli</td>
<td>LBL computer connected via ISDN, CA</td>
</tr>
<tr>
<td>mid</td>
<td>MIDnet, Lincoln, NE</td>
</tr>
<tr>
<td>mit</td>
<td>Massachusetts Institute of Technology, Cambridge, MA</td>
</tr>
<tr>
<td>ncar</td>
<td>National Center for Atmospheric Research, Boulder, CO</td>
</tr>
<tr>
<td>near</td>
<td>NearNet, Cambridge, Massachusetts</td>
</tr>
<tr>
<td>nrao</td>
<td>National Radio Astronomy Observatory, Charlottesville, VA</td>
</tr>
<tr>
<td>oce</td>
<td>Oce-van der Grinen, Venlo, the Netherlands</td>
</tr>
<tr>
<td>panix</td>
<td>Public Access Networks Corporation, New York, NY</td>
</tr>
<tr>
<td>pubnix</td>
<td>Pix Technologies Corp., Fairfax, VA</td>
</tr>
<tr>
<td>rain</td>
<td>RAINet, Portland, Oregon</td>
</tr>
<tr>
<td>sandia</td>
<td>Sandia National Lab, Livermore, CA</td>
</tr>
<tr>
<td>sdsc</td>
<td>San Diego Supercomputer Center, CA</td>
</tr>
<tr>
<td>sintef1</td>
<td>University of Trondheim, Norway</td>
</tr>
<tr>
<td>sintef2</td>
<td>University of Trondheim, Norway</td>
</tr>
<tr>
<td>sri</td>
<td>SRI International, Menlo Park, CA</td>
</tr>
<tr>
<td>ucl</td>
<td>University College, London, UK</td>
</tr>
<tr>
<td>ucla</td>
<td>University of California, Los Angeles</td>
</tr>
<tr>
<td>ucol</td>
<td>University of Colorado, Boulder</td>
</tr>
<tr>
<td>ukc</td>
<td>University of Kent, Canterbury, U.K.</td>
</tr>
<tr>
<td>unibw</td>
<td>University of Mannheim, Germany</td>
</tr>
<tr>
<td>umont</td>
<td>University of Montreal, Canada</td>
</tr>
<tr>
<td>uninl</td>
<td>University of Nijmegen, The Netherlands</td>
</tr>
<tr>
<td>usc</td>
<td>University of Southern California, Los Angeles</td>
</tr>
<tr>
<td>uscatt</td>
<td>University of Stuttgart, Germany</td>
</tr>
<tr>
<td>wustl</td>
<td>Washington University, St. Louis, MO</td>
</tr>
<tr>
<td>xor</td>
<td>XOR Network Engineering, East Boulder, CO</td>
</tr>
</tbody>
</table>

[Paxson's vantage points]
“The Collateral Damage of Internet Censorship by DNS Injection” [Anonymous, CCR 2011]

Several moving parts; let’s look in detail…
What are the main take-away conclusions?

- DNS injection censorship causes collateral damage, censoring outside its jurisdiction

![Topology of ASes neighboring CNNIC](Image)

**Figure 5:** Topology of ASes neighboring CNNIC
We typically use many vantage points in order to “see inside the black box” of the Internet. Where were their vantage points?

Figure 1: DNS query process and DNS injection

43,842 of these in 173 countries!
Discussion

How could you counteract this censorship?

How could service providers offer protection?

How could an individual client protect itself?
Discussion

How could you counteract this censorship?

How could service providers offer protection?

- Censor avoids polluting transit queries
- Threat of depeering
- DNSSEC
  - signed DNS responses
  - requires

How could an individual client protect itself?

- DNSSEC
- Query multiple servers, wait for all responses [Ruisheng]
- Tunnel queries through a friend in another country
A word of caution

The most important difference between computer science and other scientific fields is that: **We build what we measure.** Hence, we are never quite sure whether the behavior we observe, the bounds we encounter, the principles we teach, are truly principles from which we can build a body of theory, or merely artifacts of our creations. ... this is a difference that should, to use the vernacular, ‘scare the bloody hell out of us!’

– John Day
Announcements

Midterm presentations done

- Big thanks to those of you who stayed late on Tue
- Each of you will get feedback in email

Office hours

- **Brighten**: Today 5:30 - 6:30 pm, in 3211 SC and Hangout
- **Chi-Yao**: Friday 4:00 - 5:00 pm, in 207 SC and Hangout

A2

- Deadline shifted to Monday 5pm
- Post questions in thread on Piazza
- Questions now?