Measuring Network Traffic

Remco van de Meent
r.vandemeent@utwente.nl

University of Twente
Outline

- Introduction
- Contribution and Approach
- Measurement Setup
- Measurements
- Selection of Results
- Conclusions Future Plans
Introduction

**Background** Ph.D study combining telematics and mathematics; industry-funded Internet-NG and M2C projects; supervisors: Aiko Pras, Michel Mandjes, Hans van den Berg, Bart Nieuwenhuis
Introduction

**Background** Ph.D study combining telematics and mathematics; industry-funded Internet-NG and M2C projects; supervisors: Aiko Pras, Michel Mandjes, Hans van den Berg, Bart Nieuwenhuis

**Rationale** QoS in networks may be achieved by means of overprovisioning → need to understand traffic characteristics
Introduction

Background Ph.D study combining telematics and mathematics; industry-funded Internet-NG and M2C projects; supervisors: Aiko Pras, Michel Mandjes, Hans van den Berg, Bart Nieuwenhuis

Rationale QoS in networks may be achieved by means of overprovisioning → need to understand traffic characteristics

Goal Intelligent overprovisioning of network links
Introduction — Related Work

Numerous measurement “projects”, e.g.:

**Research**  IRTF (imrg, e2e, aaaarch, nmrg?), COST (242, 257, 279), IST-SCAMPI
Introduction — Related Work

Numerous measurement “projects”, e.g.

Research  IRTF (imrg, e2e, aaaarch, nmrg?), COST (242, 257, 279), IST-SCAMPI

Operations  RIPE (ttm), CAIDA, NLANR, MCI-Worldcom, Sprint ATL
Introduction — Related Work

Numerous measurement “projects”, e.g.:

**Research**  IRTF (imrg, e2e, aaaarch, nmrg?), COST (242, 257, 279), IST-SCAMPI

**Operations**  RIPE (ttm), CAIDA, NLANR, MCI-Worldcom, Sprint ATL

**Standardization**  IETF (aaa, rtfm, ipfix, psamp, rmonmib, ippm, bmwg), not so much ISO/ITU
Introduction — Related Work

Numerous measurement “projects”, e.g.:

**Research**  IRTF (imrg, e2e, aaaarch, nmrg?), COST (242, 257, 279), IST-SCAMPI

**Operations**  RIPE (ttm), CAIDA, NLANR, MCI-Worldcom, Sprint ATL

**Standardization**  IETF (aaa, rtfm, ipfix, psamp, rmonmib, ippm, bmwg), not so much ISO/ITU

**European NoEs**  MAUI → E-NEXT
Contribution

intelligent overprovisioning
Contribution

intelligent overprovisioning

- course measurements
- what must be measured
Our Approach

course measurements (e.g. MRTG)
fine-grained measurements (tcpdump + custom analysis tools)
Our Approach

- course measurements (e.g. MRTG)
- fine-grained measurements (tcpdump + custom analysis tools)
- find relations between course- and fine-grained measurements
Our Approach

- course measurements (e.g. MRTG)
- fine-grained measurements (tcpdump + custom analysis tools)
- find relations between course- and fine-grained measurements
- verification using measurements on other networks
Our Approach

- course measurements (e.g. MRTG)
- fine-grained measurements (tcpdump + custom analysis tools)
- find relations between course- and fine-grained measurements
- verification using measurements on other networks
- mathematical models
Our Approach

- course measurements (e.g. MRTG)
- fine-grained measurements (tcpdump + custom analysis tools)
- find relations between course- and fine-grained measurements
- verification using measurements on other networks
- mathematical models
- “go back to Start”
Measurement Setup

access network

Internet

switch

measurement pc
Measurement Setup

**Measurement PC:**

- Pentium-III, 1 GHz
- 512MB RAM
- 64-bit PCI
- standard Linux 2.4 kernel
- Gigabit networking.
Measurement Setup

**Measurement PC:**

- Pentium-III, 1 GHz
- 512MB RAM
- 64-bit PCI
- standard Linux 2.4 kernel
- Gigabit networking.

captures packet headers using tcpdump, anonymization through tcpdpriv
Measurements (1)

- store packet header traces (first 64 octets, includes everything up to tcp/udp layer)
  - 15 minutes each
  - multiple times a day
  - 7 days per week
  - since 2002, different locations, SURFnet “backbone”
Measurements (2)

- ~ 2000 users $\times$ 100 Mbit/s, 300 Mbit/s uplink
- ~ 200 users $\times$ 100 Mbit/s, 1 Gbit/s uplink
- ~ 1000 users $\times$ 10–100 Mbit/s, 1 Gbit/s uplink
- (not SURFnet) ADSL: hundreds of users, 0.5 – 1 Mbit/s, 155 Mbit/s uplink, multiple locations
Measurements (2)

- 10 – 500 packets per 10 milliseconds
- up to 4 GB of disk space per 15 minutes
So... what did we do?

Packet traces give detailed information on, e.g.,
- throughput on arbitrary time scales (tomorrow)
- burstiness and dimensioning (peak / mean) (submitted, sneak preview here)
- other characteristics that help to understand traffic (visualization tools)
- application recognition
- arrival process
- multi-level view on traffic (packets, flows, sessions)
What did we not do

In our research we do not perform measurements based on multiple, correlated metering points, so:

- no end-to-end information
- no available bandwidth estimation
- no information on delay
- no packet-loss information
- ...

Dimensioning Rules
Dimensioning Rules

- 5 minute average throughput $m$
- 99th percentile of 1 second average $p$
- $\rightarrow$ hundreds of $(m, p)$-tuples
Dimensioning Rules
Dimensioning Rules

![Graph showing data points and a trend line for dimensioning rules.](image-url)
Dimensioning Rules

- we tried multiple rules (lines, curves), all give better (tens of percents) results than original “50% overprovisioning required guideline”

- based on course-grained measurements; fine-grained measurements every now and then, to finetune parameter settings
Visualisation Tools

- works on flow-level 5-tuple: ip src/dst, proto, tp src/dst
- supports different types of statistics (extendible)
- [http://m2c-a.cs.utwente.nl/bsc-visual/](http://m2c-a.cs.utwente.nl/bsc-visual/)
# Visualisation Tools

## Statistic type

<table>
<thead>
<tr>
<th>burstiness of various splits</th>
</tr>
</thead>
<tbody>
<tr>
<td>cumulative flow size</td>
</tr>
<tr>
<td>distribution: active flows</td>
</tr>
<tr>
<td>distribution: flow arrival rate</td>
</tr>
<tr>
<td>distribution: flow duration</td>
</tr>
<tr>
<td>scatterdiagram</td>
</tr>
<tr>
<td>throughput: 10 second average rates</td>
</tr>
<tr>
<td>throughput: mice / elephants</td>
</tr>
</tbody>
</table>
### Visualisation Tools

**Statistic parameters**

<table>
<thead>
<tr>
<th>x-axis</th>
<th>src-port</th>
<th>dst-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>any</td>
<td>img-width 650</td>
</tr>
<tr>
<td></td>
<td></td>
<td>img-height 650</td>
</tr>
</tbody>
</table>

[Diagram showing statistic parameters]
Visualisation Tools

Statistic dataset

Select location:
Institution 0

Select dataset:
i0_20020526_1115

generate »
Visualisation Tools

Timing: Image creation took 6.639 seconds...
Showing: src_port vs dst_port
Dataset: i0_20020526_1115
Condition: protocol any
Application Recognition

- port lists (IANA, other...
Application Recognition

- port lists (IANA, other...)
- relating flows
Application Recognition

- port lists (IANA, other...)
- relating flows
- no payload inspection
Application Recognition

- port lists (IANA, other...)
- relating flows
- no payload inspection

Campusnet:
- > 90% of local traffic is windows networking, little email or web, hardly any p2p
- traffic from/to Internet: still tens of percents unknown
Packets / Flows

Throughput for dataset campusnet-20020523-1835 (short/long flows)

- 10 second average for short flows (duration < 10 sec)
- 10 second average for long flows
Conclusions

- detailed measurements with moderate hardware are feasible
Conclusions

- Detailed measurements with moderate hardware are feasible.

- Course measurements together with occasional detailed measurements seem to give reasonable idea of peak load.
Conclusions

- detailed measurements with moderate hardware are feasible

- course measurements together with occasional detailed measurements seem to give reasonable idea of peak load

- (increasing) amount of unidentified traffic is worrying
Conclusions

- Detailed measurements with moderate hardware are feasible.

- Course measurements together with occasional detailed measurements seem to give a reasonable idea of peak load.

- Increasing amount of unidentified traffic is worrying.

- Data and tools available for public use soon.
Future plans

- more measurements, other networks
Future plans

- more measurements, other networks
- repository of measurement data
  - anonymous
  - possibly distributed
  - easy access via web
Future plans

- more measurements, other networks
- repository of measurement data
  - anonymous
  - possibly distributed
  - easy access via web
- network dimensioning rules based on course measurements and “out-of-band” information
Future plans

- more measurements, other networks

- repository of measurement data
  - anonymous
  - possibly distributed
  - easy access via web

- network dimensioning rules based on course measurements and “out-of-band” information

- simulations, mathematical foundations