

HELSINKI UNIVERSITY OF TECHNOLOGY

Measuring network with packets:
delay, loss, bandwidth and other
network properties

Lecture slides for S-38.183
23.3.2006
Mika Ilvesmäki

Networking laboratory

HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ilvesmäki, Lic.Sc. (Tech.)

Timescales of different events

- This course focuses primarily on packet and flow level measurements and analysis

Networking laboratory

HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ilvesmäki, Lic.Sc. (Tech.)

Contents

- Basic network events
- Purpose of packet measurements
- Passive measurements
- Active measurements

Networking laboratory

HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ilvesmäki, Lic.Sc. (Tech.)

Goals of this lecture

- After this lecture you should be able to
 - Understand the basic phenomena to be measured in a network
 - Understand the difference between active and passive measurements
 - And the results they produce
 - Be able to explain (in detail) various active measurement types (BW, Loss, Delay)
 - List some of the applications for active and passive measurements with packets

Networking laboratory

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Packet

- (IP) packet is the basic event that all measurements (in this course) are based on
 - Packet has a header and payload
 - Measurement analysis is (usually) interested in using headers to group packets
 - Done with filters/masks
 - Interesting packet measures include:
 - #packets (per time unit, per trace, etc.)
 - Packet sizes (to determine capacity usage, to detect different types of applications)
 - Packet interarrival times (to determine arrival process characteristics)

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Purpose of packet measurements

- Develop traffic models
- Find traffic dynamics and directionality (for routing)
- Detect of various network phenomena (currently focus is on detecting malicious traffic and network anomalies)
- TCP studies (congestion detection)
- No additional traffic introduced
 - However, needs access to the measurement point
 - Choice between collecting statistics on the fly or capturing packet (or parts of it) and analyzing it later

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)


Network phenomena to measure

- Networks deliver packets (Paxson)
 - As we asked (bandwidth)
 - Not at all (packet loss)
 - Significantly late (delay), significantly meaning that a retransmission might occur
 - Out-of-order
 - Due to routing and queue management problems resulting in uneven path delays
 - Replicated
 - Due to bugs/design faults in router/L2 implementations/design
 - Corrupted
 - Neglected CRC-checks (core routers?)

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Packet data to collect

- Arrival time (absolute or relative) or lack thereof (packet loss)
- Header info
 - 5-tuple (addresses, proto, ports)
 - Remember address sanitation
 - Ports present only in protos 6 and 17 (TCP and UDP)
 - Others indicated by protocol id.
- Packet size
- Packet contents for protocol/content analysis
- Packet data collected at several points results in traffic matrices





HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ovaska, Lic.Sc. (Tech.)

Passive measurements

- Information determined
 - Bit/byte/packet rates, bandwidth
 - Packet IAT/timing information
 - Queue levels (indicating packet loss/delay)
 - Traffic/protocol mixes from packet captures





HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ovaska, Lic.Sc. (Tech.)

Passive measurement objectives

- Arrival process characterization
 - Packets, flows, applications
- Network status & traffic profiles
- General measures
 - Utilization, traffic trends etc.
- Detecting network anomalies
 - Malicious traffic characteristics





HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ovaska, Lic.Sc. (Tech.)

Passive measurements in action

- Capture data, discard unusable parts/payload
- Sanitize
 - Preserve as much information as possible
 - IP address mapping
 - IP address hierarchy
 - TCP ports
- Save and archive




HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ovaska, Lic.Sc. (Tech.)

Passive vs. Active

- Passive measurements are accurate
 - Based on historical data
 - Depend upon active users and existing traffic
- Active measurements
 - Measure the network here and now
 - May disturb the network



HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Active measurements

- Insert additional traffic, probes, into the network
 - Requires the source and the sink (monitor); these can be the same machine
- Information monitored
 - Bandwidth (current, available, bottleneck)
 - Delay and jitter
 - Packet loss

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Active measurement pitfalls

- Inserted traffic interferes and disturbs "real" traffic
 - Need to carefully determine probe insertion rate
- To get proper results the probe packets should be similarly classified in the network (and be similar to real traffic properties (IAT, packet length etc.))

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Bandwidth measurements

- Bottleneck bandwidth is the minimum of bandwidths of the links in the route
 - Also known as Path Capacity
- Available Bandwidth is the unused bandwidth in the link
 - May be unused because of bottleneck link
 - Aka as Hop Capacity
- Bandwidth Asymmetry is the relative difference of the BW within the same path to different directions

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Hop capacity

- Send probes deeper into the network step by step (utilize TTL)
 - Get echo-packets back, measure for RTT
- RTT consists of
 - Propagation delay
 - Queuing delay
 - Processing delay
 - ICMP may also be restricted

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Path capacity

- Packet pair –technique
 - Send two packets back-to-back (make note of the interval) to the other end which echoes the packets back
 - Measure the difference at the other end and determine the bandwidth based on the added transmission delay
 - Cross-traffic has a big effect
 - To get true results
 - Send several packet pairs at various times
 - Send longer back-to-back packet trains
 - Packet pairs determine bottleneck capacity
- Several tools available
 - Pathchar, pathrate, pathload, pchar etc.

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Delay in the network

- Delay is caused by
 - Bugs in router implementations.
 - Packet loss
 - Speed of EM waves in media.
 - CPU Power (e.g. routing updates).
 - Packet loss
 - Packets on the slow path.
 - Congestion (Queuing).
 - Packet loss
 - Packet sizes.
 - Noisy channels.
 - Route flapping.

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Delay variation, jitter

- No commonly accepted definitions exist for delay variation
 - PPDV – packet to packet delay variation
 - Easy to measure
 - Jitter envelope
 - Track the max and min delay compared to short term average delay
- Delay is (usually) caused by several network elements

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Timing compression

- Packets arrive earlier than they should
 - Queues usually store(delay) packets
 - Sometimes packets are earlier packets are held up in the network and later packets have time to catch up

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Delay measurement methods

- Obtain a good timing source, synchronize clocks
- Basic Active measurement
 - Send measurement probes, record send and receive times
- Basic Passive measurement
 - Payload CRC acts as a signature
 - CRC recorded at the source and checked at the receiver -> match packets and record timestamps -> off-line analysis
- Basic delay measurements may be based on RTT observations (ping)
 - Are delays(routes) symmetrical?
 - 2-point measurements are preferable
 - Synchronize site clocks, send measurement probes

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

Packet loss in the network

- Unavoidable in packet switched networks
 - With complex traffic characteristics
- TCP bases some of its congestion detection on packet loss
 - Large buffers would lead to very large delays
- Packet loss happens (usually) in just one (congested, faulted) place in the network

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)


Measuring for packet loss

- A packet lost is a packet lost
 - A packet lost in capture is not packet lost in the network!
- A packet lost might be just an acknowledgement lost!
 - Route asymmetry
- Need to keep record of sent packets and arrived packets
 - And packets dropped by the measurement device

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ovaska, Lic.Sc. (Tech.)

BW, Delay, Drops inter-related

- Available BW is depends up on transmission speed, queue status and router processor capacity
- Delay is a result of transmission speed, processing limitations and subsequent storage of packets in a buffer
- When buffers overflow packet drops occur





HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Siivola, Lic.Sc. (Tech.)

Other active measurements

- Inject packets into the network from multiple points and evaluate the delay/latency
 - Packets sent to pre-selected targets
- Network topology discovery
 - Determine path properties and status





HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Siivola, Lic.Sc. (Tech.)

The next step

- Most of the techniques presented progress towards using longer and longer packet trains
- Packet trains have the following properties
 - Length
 - Direction
- Packet trains are called flows and play an important part in understanding network and traffic characteristics



HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Siivola, Lic.Sc. (Tech.)

Packet measurement summary

- Passive packet measurements
 - To characterize traffic and obtain info on network status
 - Huge amounts of data to analyze
 - Give an accurate view on the past network status
- Active packet measurements
 - Probe the network for bandwidth, delay and loss
 - Determine network topology
 - Increases the amount of traffic in the network
 - Give an accurate view of the current network status

