Introduction to Performance Measurements and Monitoring

Vinayak Hegde
vinayakh@gmail.com
@vinayakh

Structure

- Part 1 – Basics of Measurement (40 min)
- Part 2 – Basic Statistics primer (40 min)
- Part 3 – Measurement Case Studies (10 min)
- Part 4 – Overview of Tools (10 min)
- Q&A – (10 min)

Act I - Basics of Measurement

- Covers
  - Types of measurements
  - Challenges and considerations
  - IETF related WGs

Why are measurement needed ?

- Capacity planning and network design
- Finding anomalies and fault detection
- Defining a baseline for policy / pricing
- Measuring adoptions of technology
- Mapping the Internet
- Academic research
- Measuring QoS and SLAs

What can you measure ?

- Latency
- Throughput
- Connectivity
- Periodicity
- Adoption
- Packet Loss

What can you measure ?

- Delay Variation (Jitter)
- Packet reordering
- Buffering
- Counters (such as hop-count)

RFC 6792 Terminology

- Transport-level metrics
- Application-level metrics
- End System Metrics
- Direct Metrics
- Interval Metrics
- Cumulative Metrics
- Sampled Metrics

Types of Measurements

- Active Measurements
- Passive Measurements
- Hybrid Measurements

Active Measurements

- Active Measurements

  The active approach relies on the capability to inject test packets into the network and follow them and measuring service obtained from the network/application.

- Alternative Definition (from draft-morton-ippm-active-passive-01)

  An Active metric or method depends on a dedicated measurement packet stream.

Passive Measurements

- Passive Measurements

  The passive approach uses devices to watch the traffic as it passes by and collect data.

  Often they do not collect every data point. It maybe not be possible to collect / observe every data point so sampling is often used.

Passive Measurement

- Alternative definition (from draft-morton-ippm-active-passive-01)

  A Passive metric or method depends solely on observation of one or more packet streams. The streams only serve measurement when they are observed for that purpose, and are present whether measurements take place or not.

Hybrid Measurements

- Uses elements of both passive and active monitoring.

  eg. One such approach is proposed in http://datatracker.ietf.org/doc/draft-ietf-ippm-6man-pdm-option/
- In reality a lot of metrics fall in between the two extremes of active and passive.

Active Measurements

- Pros
  - More “objective” since you can control some parts the measurement environment
  - Easier to emulate scenarios by scheduling, mimicking traffic patterns
  - Better control over sampling
- Cons
  - Measurement could modify the test environment
  - Increases network traffic

Passive Measurements

- Pros
  - Measures real traffic
  - Extremely valuable in network-debugging
  - Does not create extra traffic (not strictly true)
- Cons
  - Full line speed data collection is often impossible.
  - Can lead to processing lot of data. Proper sampling is crucial.
  - Can add extra devices to monitor live network
  - Privacy & Security issues
  - E2E encryption can hinder data collection

Software & Hardware

- Software
  - Remote monitoring (RMON)
  - SNMP
  - Netflow
  - RIPE Atlas
  - M-lab
- Hardware
  - DAG Cards

Challenges and Considerations

- Setting up the test environment
- Understanding Traffic patterns
- Removing “white noise”
- Understanding layers underneath
- Sampling correctly

Challenges and Considerations

- Some questions
  - Is the test “controlled” ?
  - Are there other random factors that can affect the test ?
  - Do you control the middleboxes ?
  - Do you understand the algorithms and software quirks ?
  - Do understand the underlying layers ? Eg delayed ack, cwnd and slow start for bulk transfer.

Challenges and Considerations

- Some more questions
  - If the test is being conducted on live network, are there any underlying patterns that you should take care of ? Seasonality ? Diurnal patterns ? Spikes ?
  - Are you sampling the data properly ? Is the sample representative of the population

IETF WGs

- IPPM (Transport Area)
  - The IP Performance Metrics (IPPM) Working Group develops and maintains standard metrics that can be applied to the quality, performance, and reliability of Internet data delivery services and applications running over transport layer protocols (e.g. TCP, UDP) over IP.

IETF WGs

- BMWG (Ops Area)
  - The Benchmarking Methodology Working Group (BMWG) will continue to produce a series of recommendations concerning the key performance characteristics of internetworking technologies, or benchmarks for network devices, systems, and services. Taking a view of networking divided into planes, the scope of work includes benchmarks for the management, control, and forwarding planes.

IETF WGs

- LMAP (Ops area)
  - Standardizes the LMAP measurement system for performance measurements of broadband access devices such as home and enterprise edge routers, personal computers, mobile devices, set top box, whether wired or wireless.
  - Measuring portions of the Internet on a large scale is essential for accurate characterizations of performance over time and geography, for network diagnostic investigations by providers and their users, and for collecting information to support public policy development.

IETF WGs

- Performance Metrics Directorate (Ops Area)
  - A directorate now (ML currently inactive)
  - Looks at other areas such as RAI and APPs

Act II – Statistics Primer

- Statistics Terminology
- Sampling
- Distributions
- Gotchas and Common fallacies

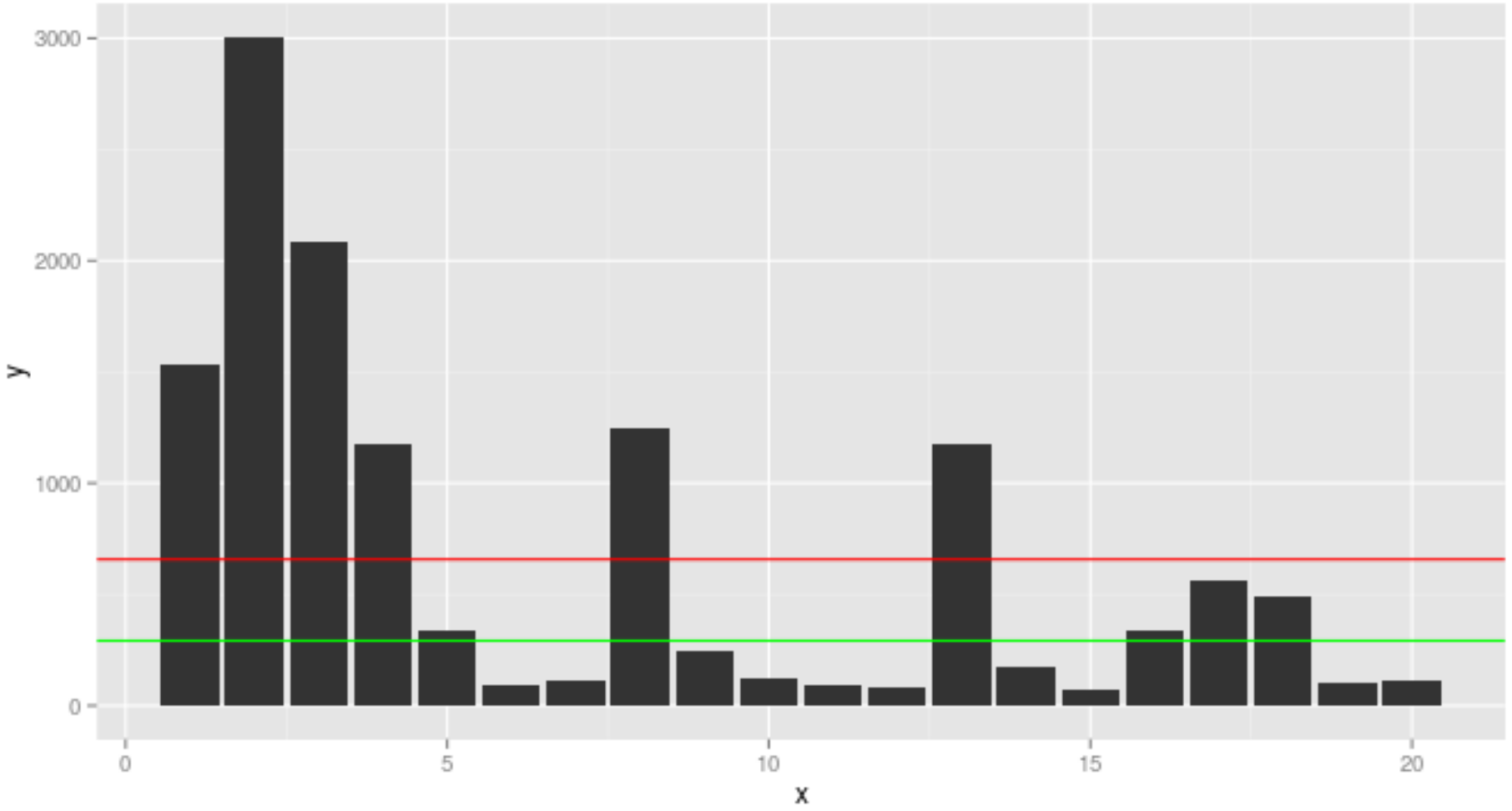
Basic terminology - I

- Distribution
- Mean
- Mode
- Median

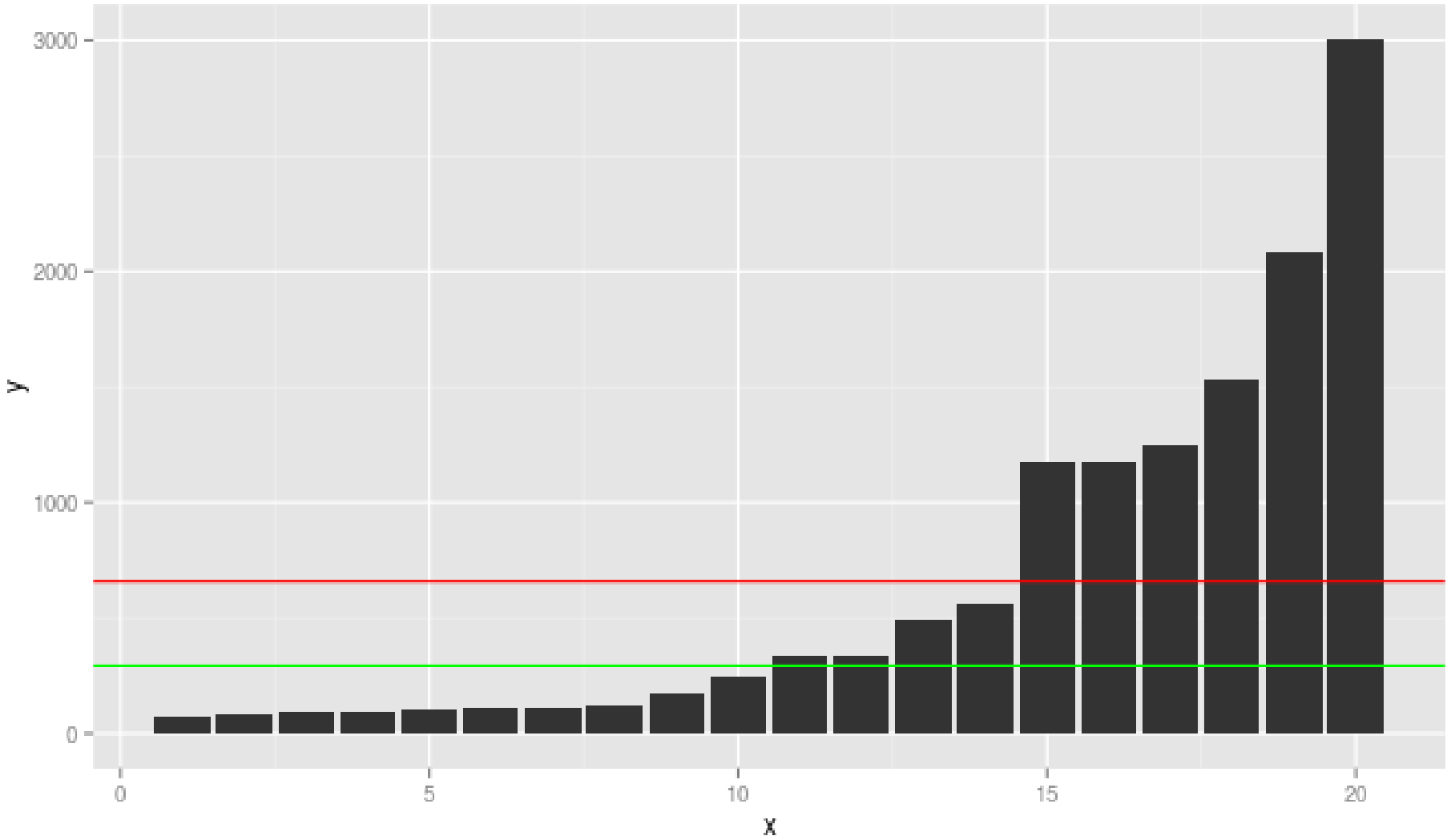
Ping

```
vinayak@vivi64:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=1534 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=3006 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=2083 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=1178 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=57 time=339 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=57 time=90.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=57 time=113 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=57 time=1248 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=57 time=248 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=57 time=120 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=57 time=87.8 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=57 time=82.4 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=57 time=1171 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=57 time=171 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=57 time=71.7 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=57 time=335 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=57 time=562 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=57 time=486 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=57 time=107 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=57 time=108 ms
^C
--- 8.8.8.8 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19047ms
rtt min/avg/max/mdev = 71.794/657.416/3006.095/786.019 ms, pipe 3
vinayak@vivi64:~$
```

Histogram



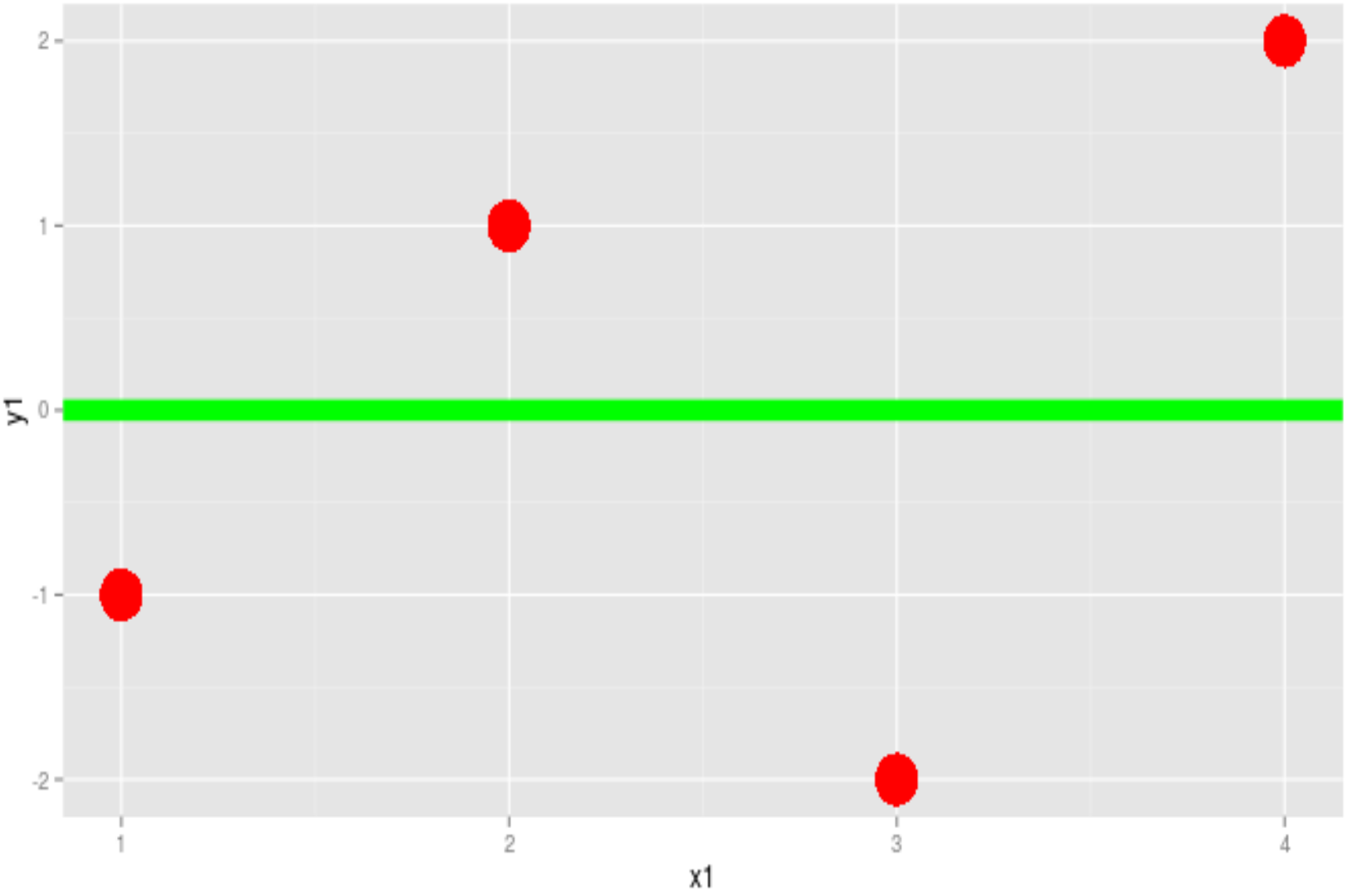
Sorted



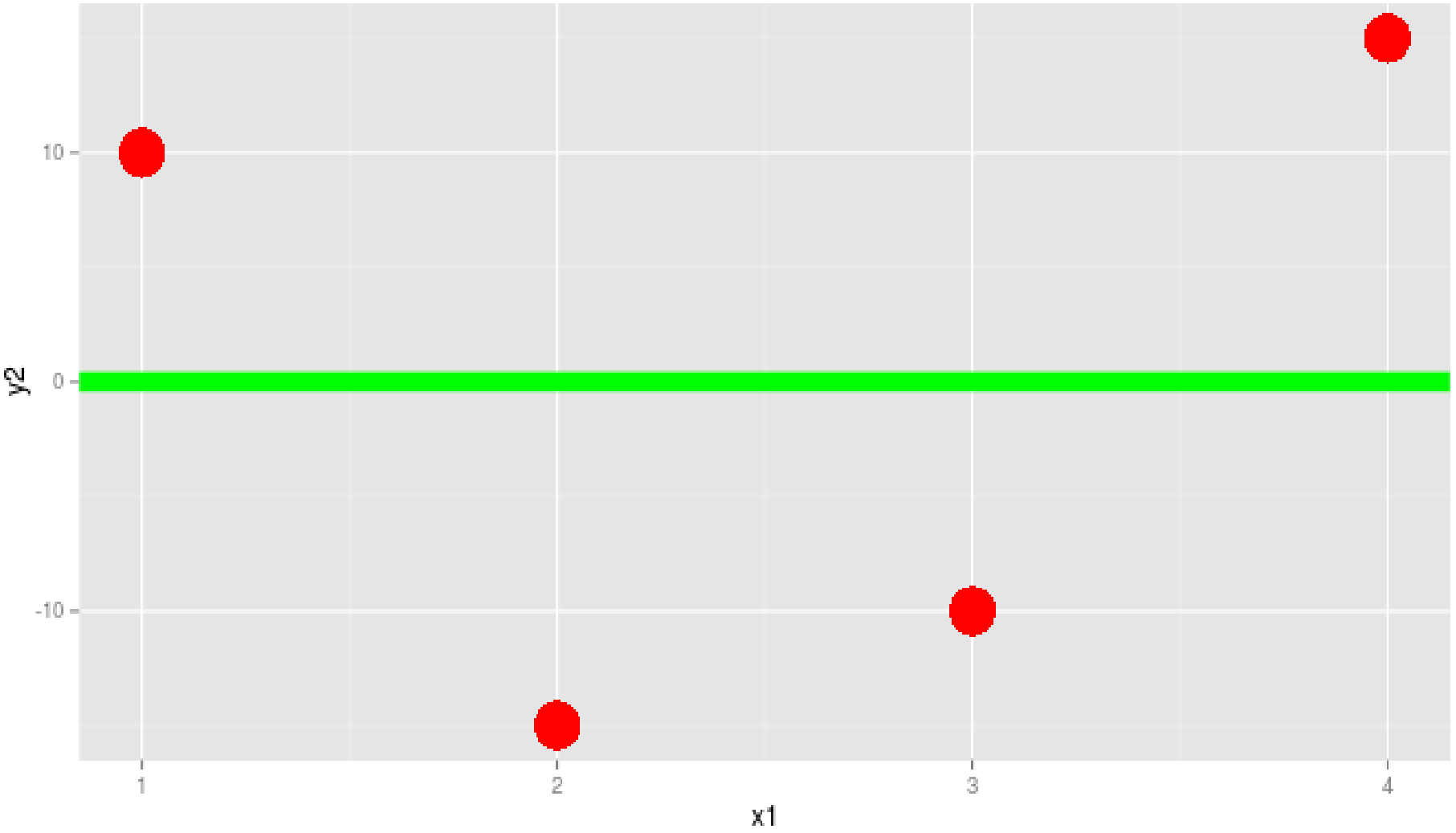
Basic terminology - II

- Variance
- Standard Deviation
- Population
- Sampling

Y1 = [-1,1,-2,2]



Y2 = [10,-15,-10,15]

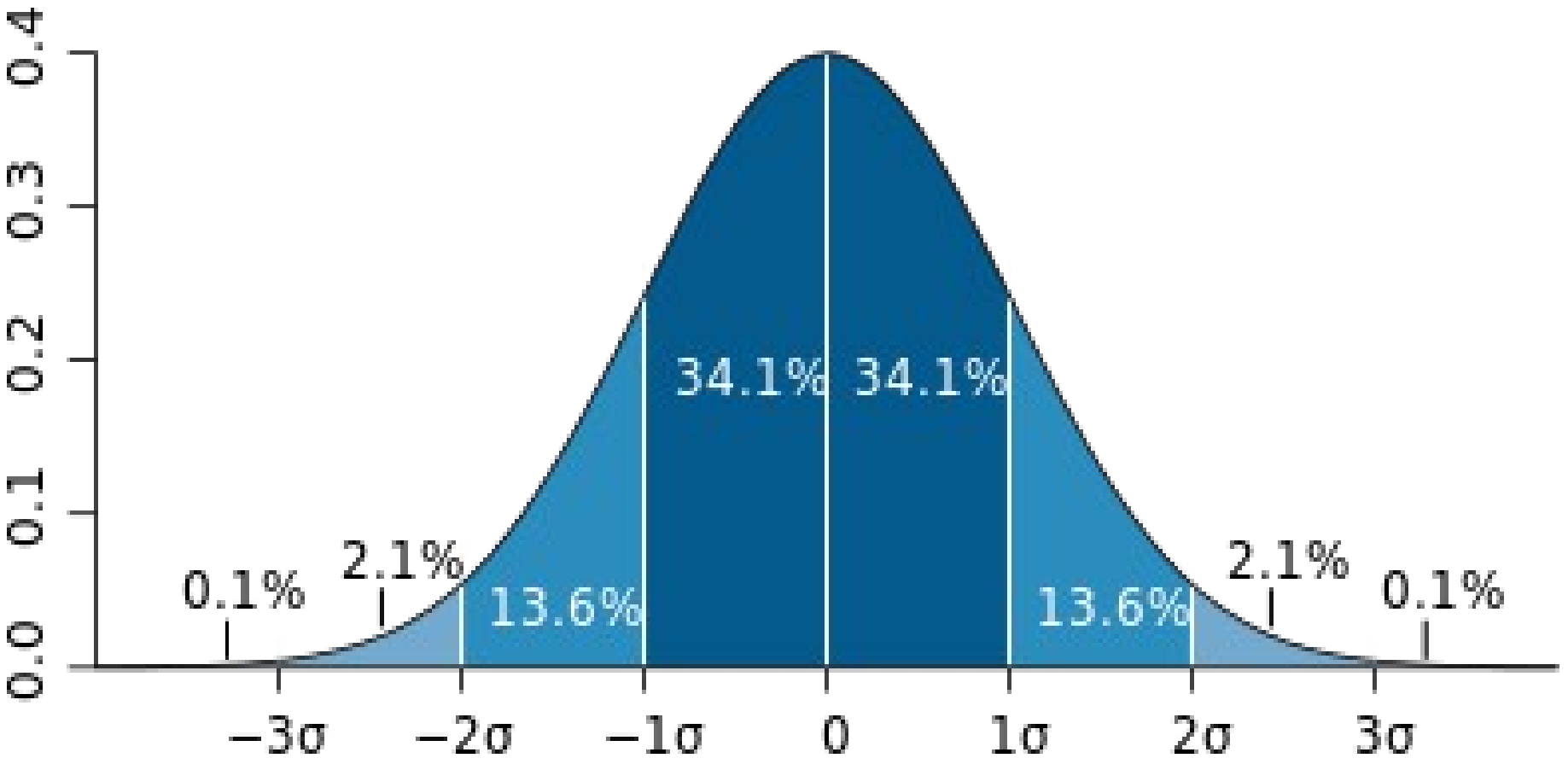


What is the difference ?

- For Y1
  - Median = Mean = 0
- For Y2
  - Median = Mean = 0

- RMS (proxy for Variance)
  - sqrt(sum(value - mean)^2)
  - RMS(Y1) = 1.224
  - RMS(Y2) = 18.37

Standard Deviation for Normal Distribution

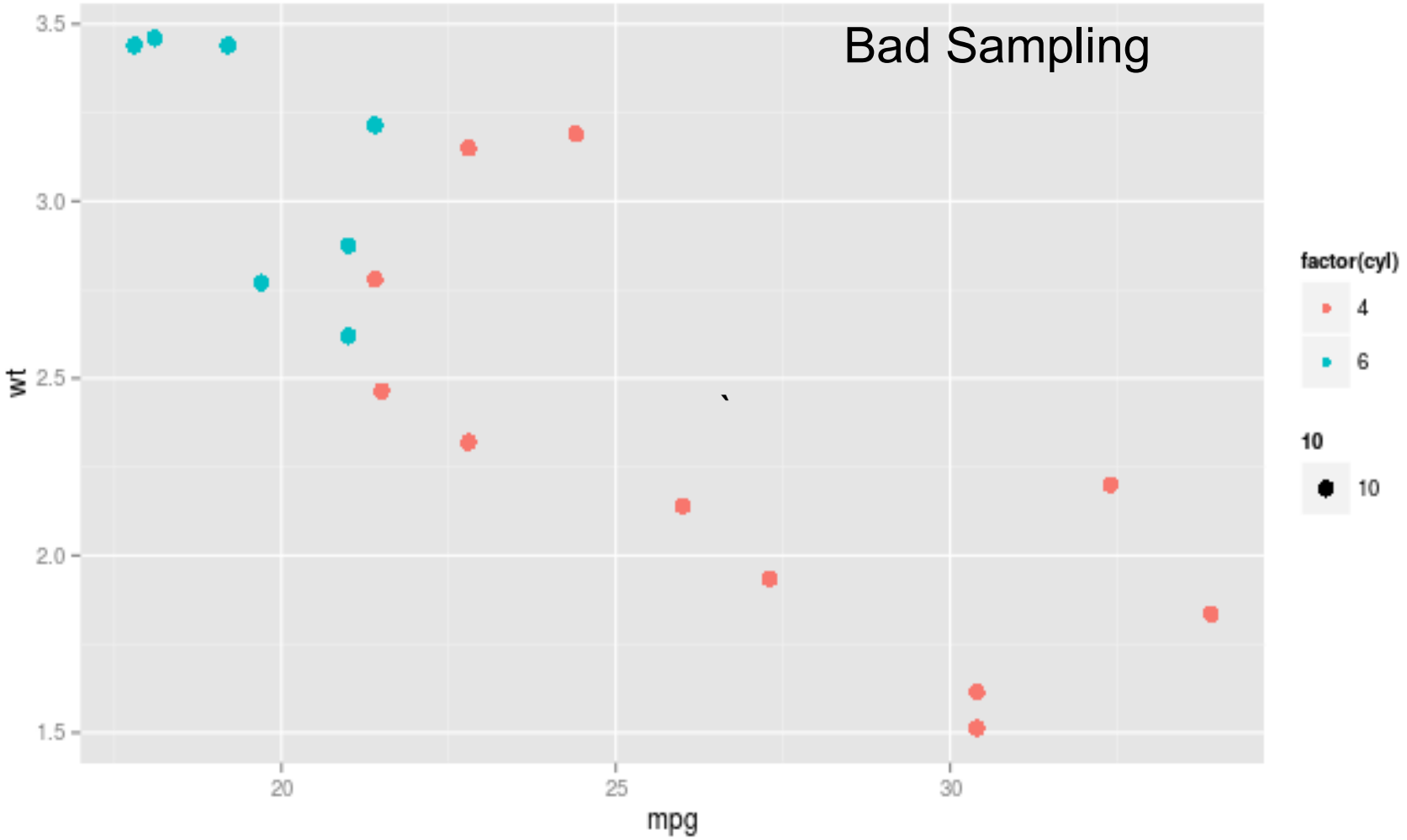


Population & Sampling

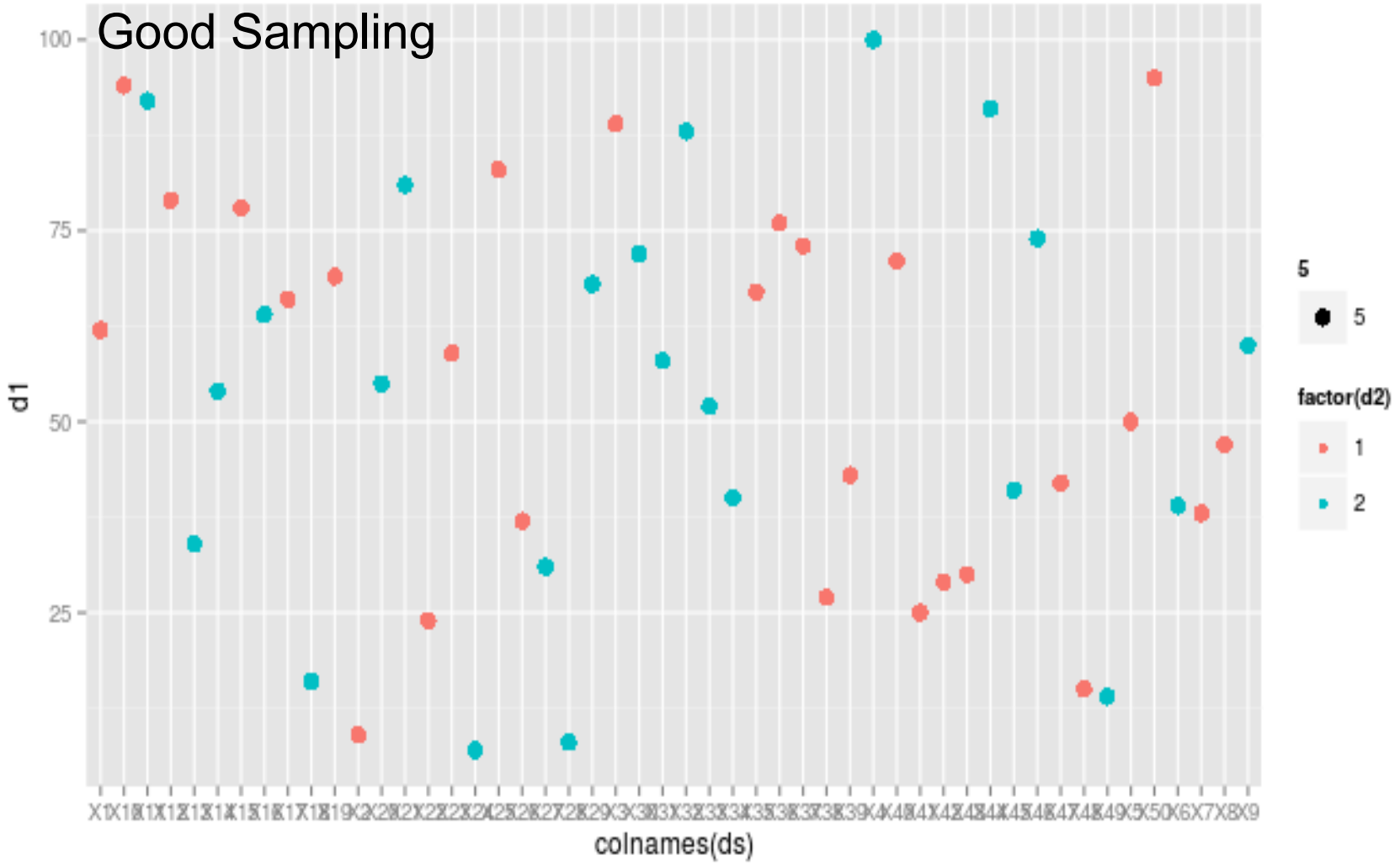
- Population
  - A population is a complete set of items that share at least one property in common that is the subject of a statistical analysis.

- Sample
  - A data sample is a set of data (subset of population) collected and/or selected from a statistical population by a defined procedure.

Population & Sampling



Population & Sampling

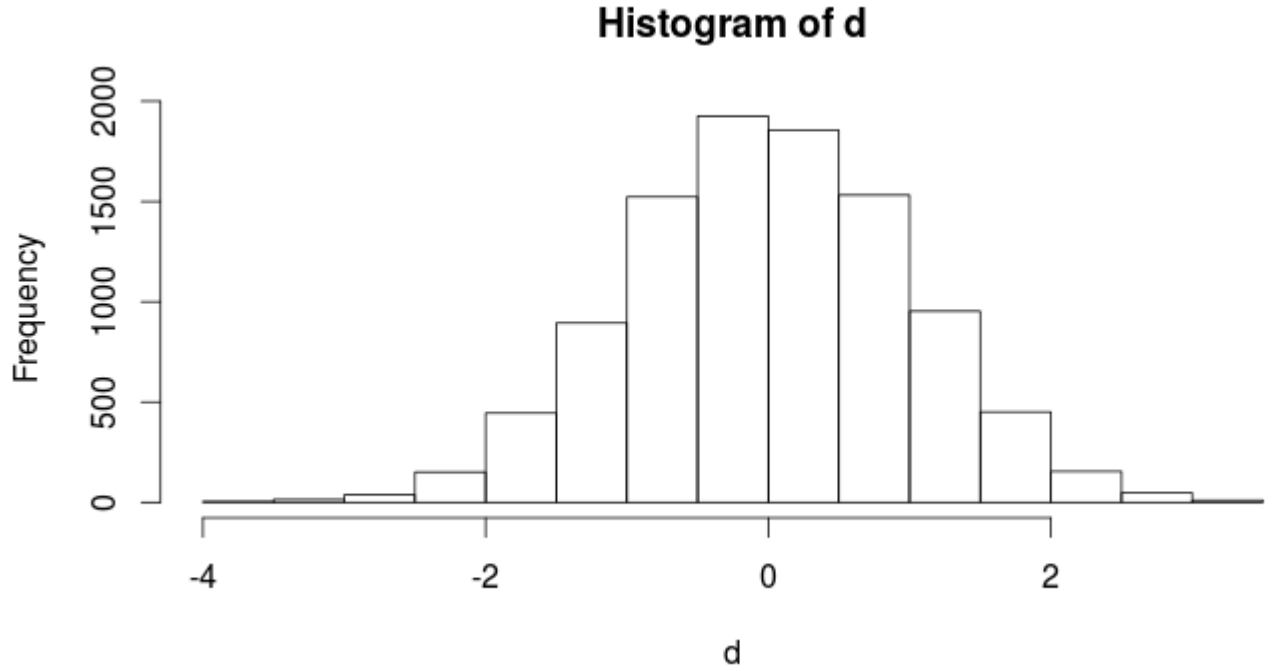


Sampling

- Process of Sampling
- Types of Sampling
  - Simple Sampling
  - Stratified Sampling
  - Systematic Sampling
  - Cluster Sampling
  - Opportunity Sampling

Distributions

- In statistics, a frequency distribution is a table that displays the frequency of various outcomes in a sample.



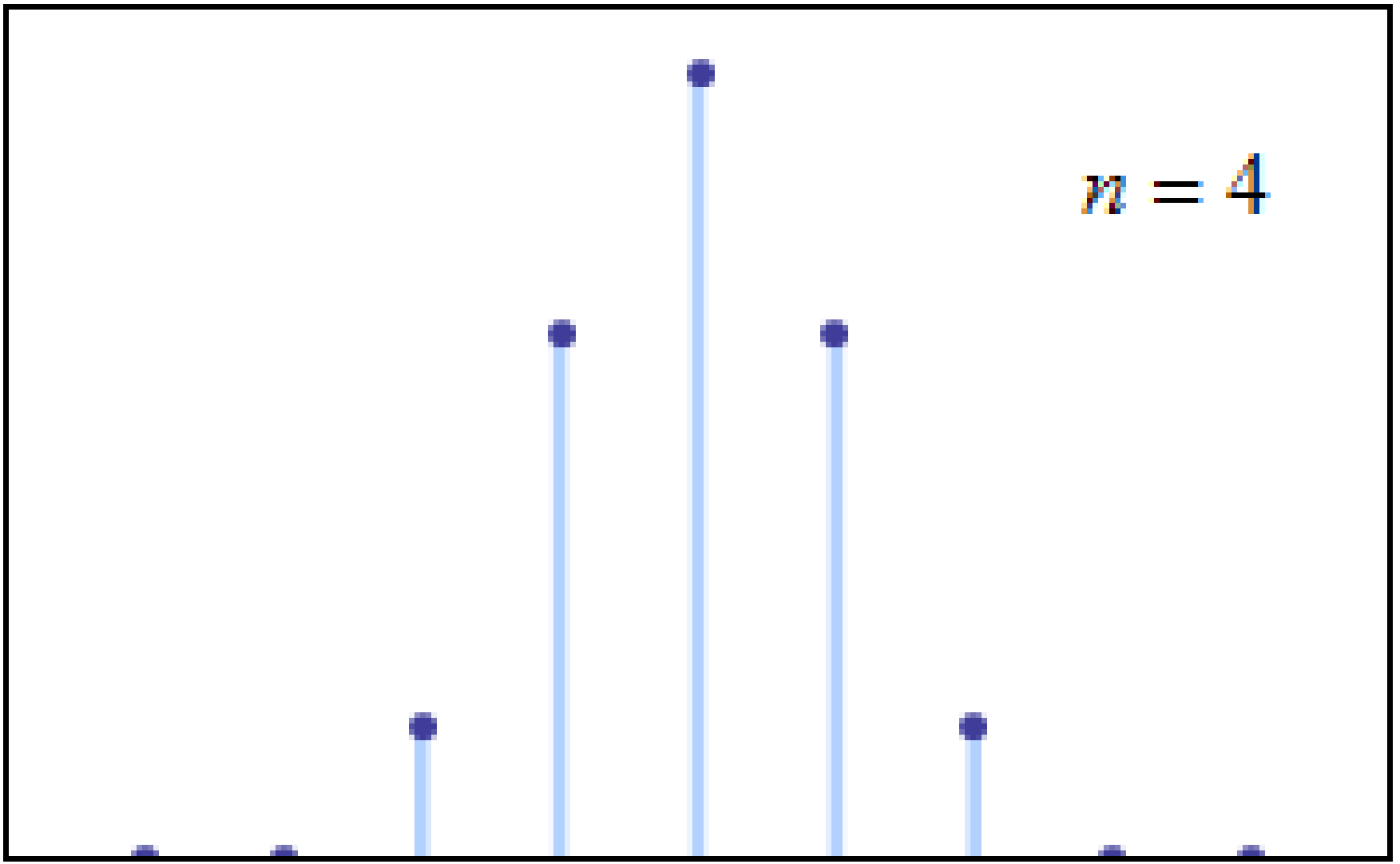
Distributions

- Normal Distributions
- Bimodal Distribution
- Lognormal Distribution

Normal Distribution

- Normal (or Gaussian) distribution is a very common continuous probability distribution.
- Often used in the natural and social sciences to represent real-valued random variables whose distributions are not known.
- It is symmetric around the point $x = \mu$, which is at the same time the mode, the median and the mean of the distribution.

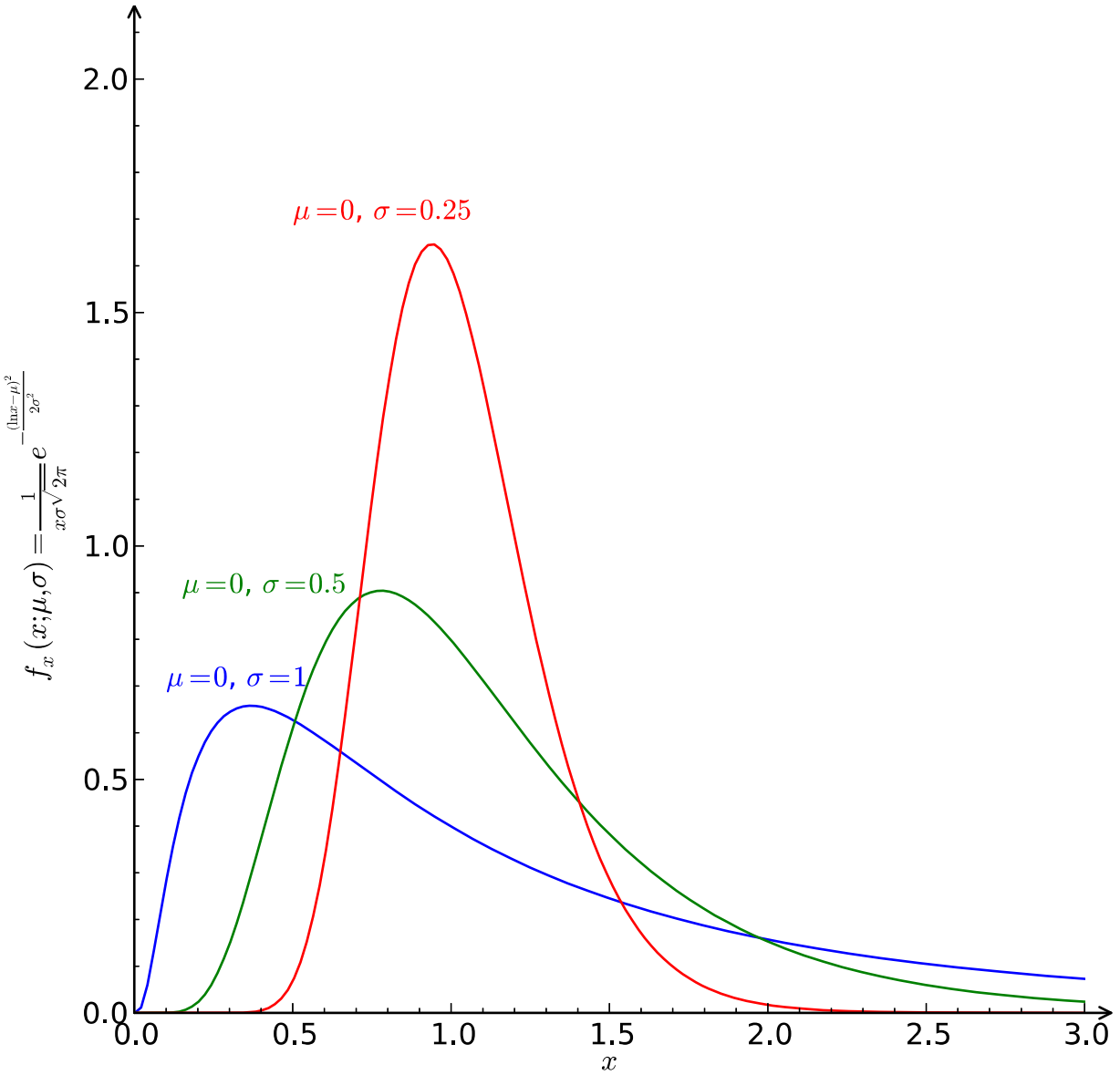
Normal Distribution



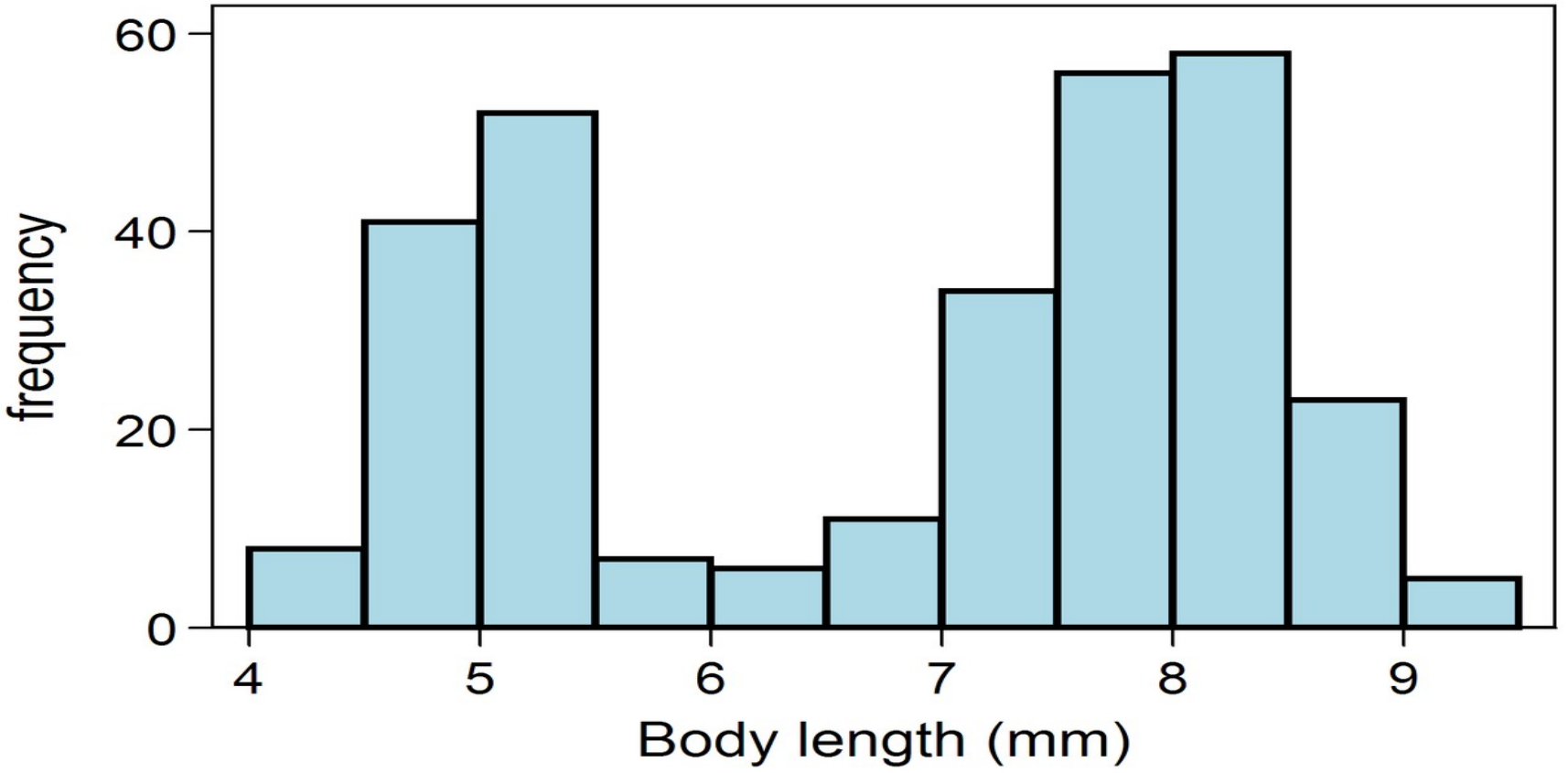
Lognormal Distribution

- A log-normal (or lognormal) distribution is a continuous probability distribution of a random variable whose logarithm is normally distributed.
- Example
  - The random obstruction of radio signals due to large buildings and hills, called shadowing, is often modeled as a lognormal distribution
  - Often used to model times to repair a maintainable system.
  - To model file size distribution of publicly available audio and video data files

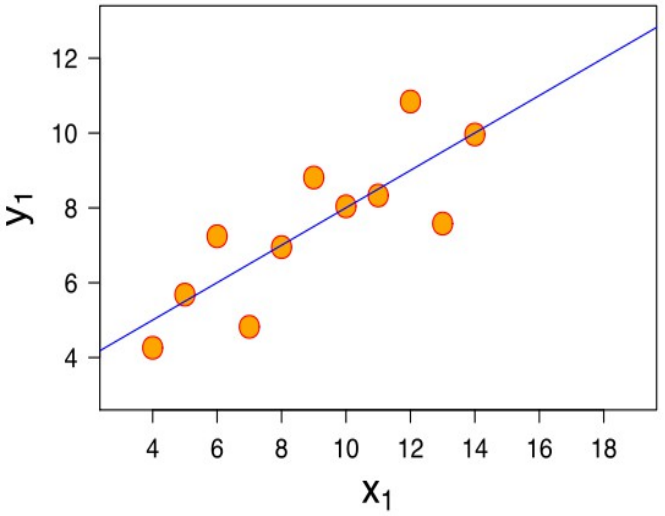
Log Normal Distribution

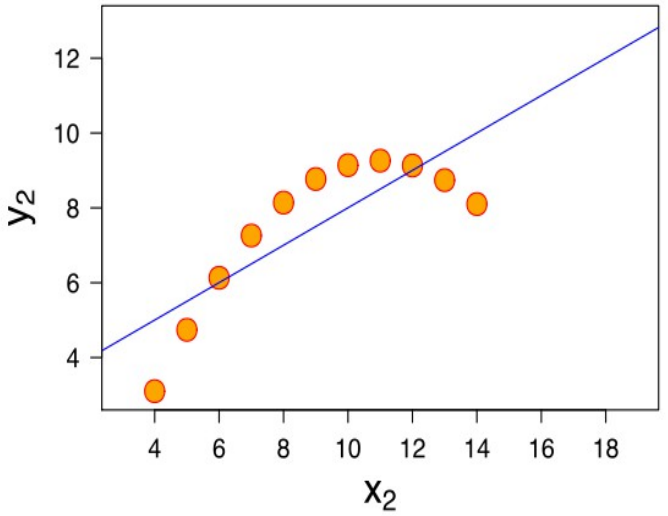


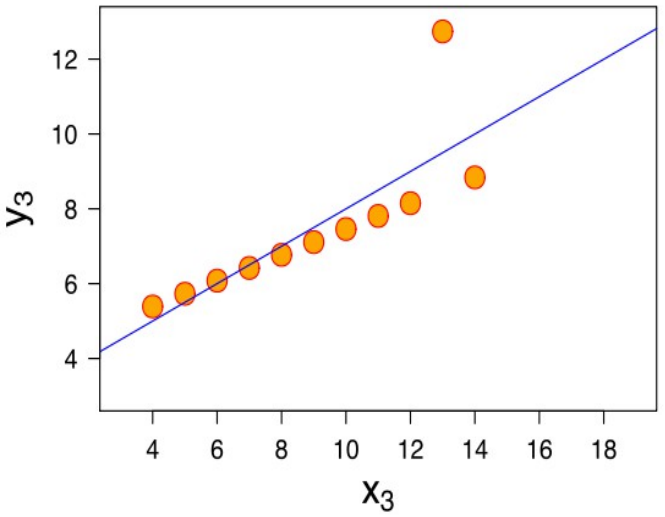
Bimodal & Multimodal Distributions

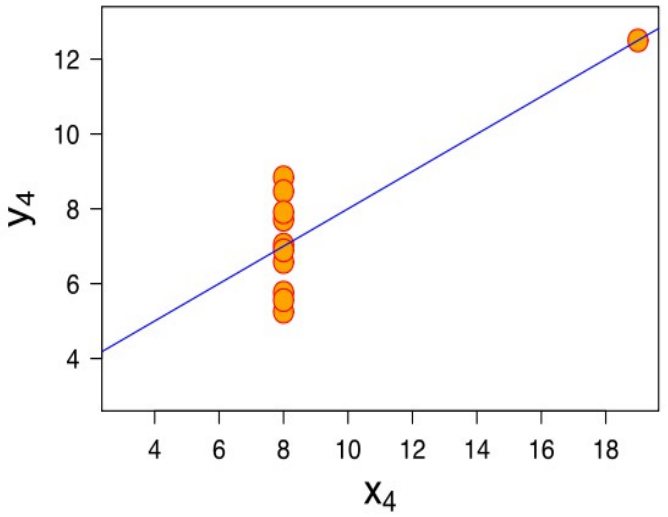


Anscombe's Quartet









More concepts

- Sampling Bias
- Outliers
- Margin of Error
- Sample Size
- Statistical significance
- A/B Testing
- Correlation
- Percentiles

Gotchas & Traps

- Correlation is not causation
- Visualise your distribution (Anscombse Quartet)
- Confounding Variables

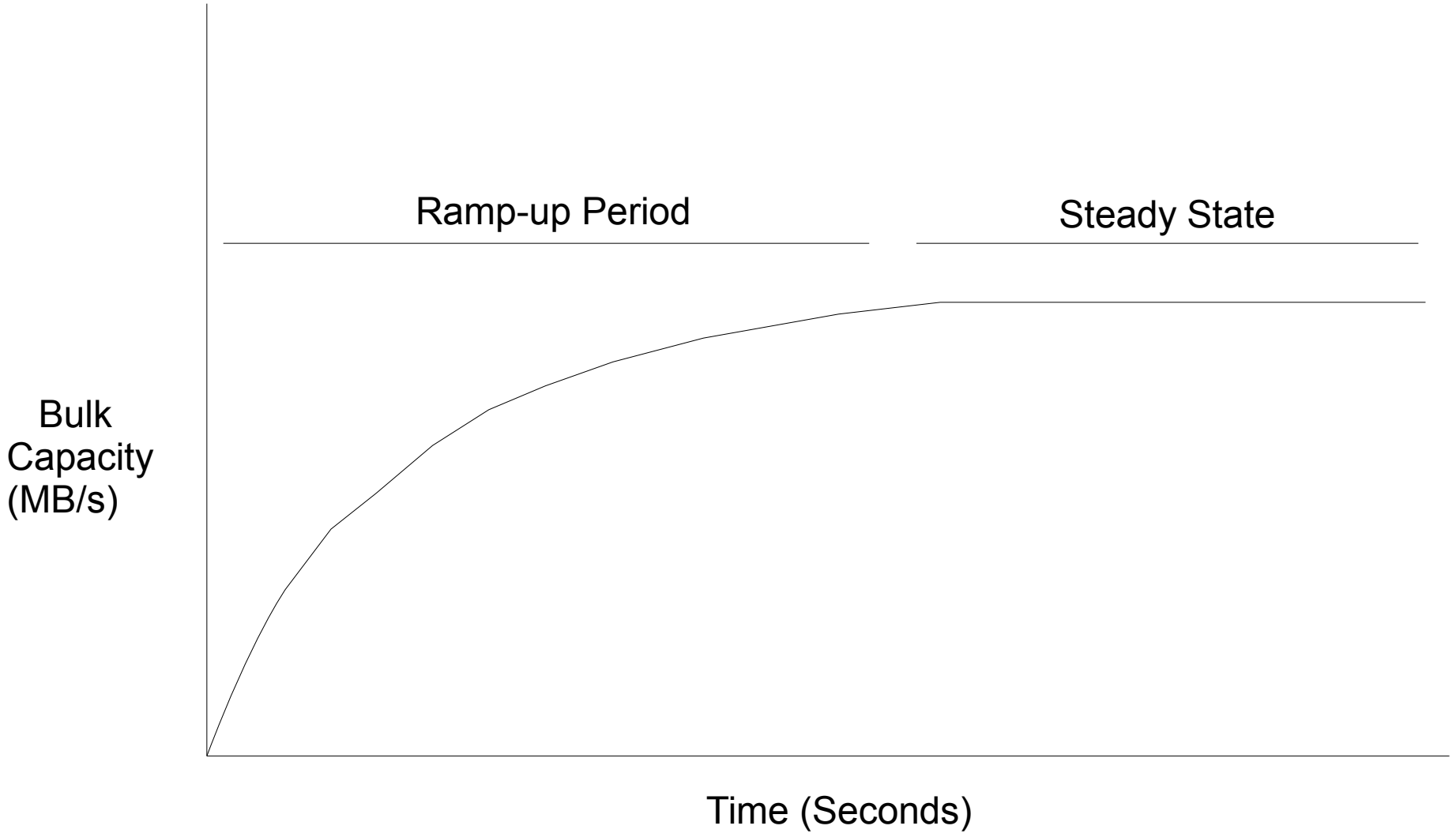
Case Studies and Tools

- Bulk Data Transfer
- Burstable Billing
- Reachability of Root Server
- Latency of Root Servers
- Network Outages
- Internet censorship and detection

Case Studies

- Bulk Data Transfer (RFC 3148)
  - Bulk Transport Capacity (BTC) is a measure of a network's ability to transfer significant quantities of data with a single congestion-aware transport connection (e.g., TCP)

Bulk Transfer Capacity



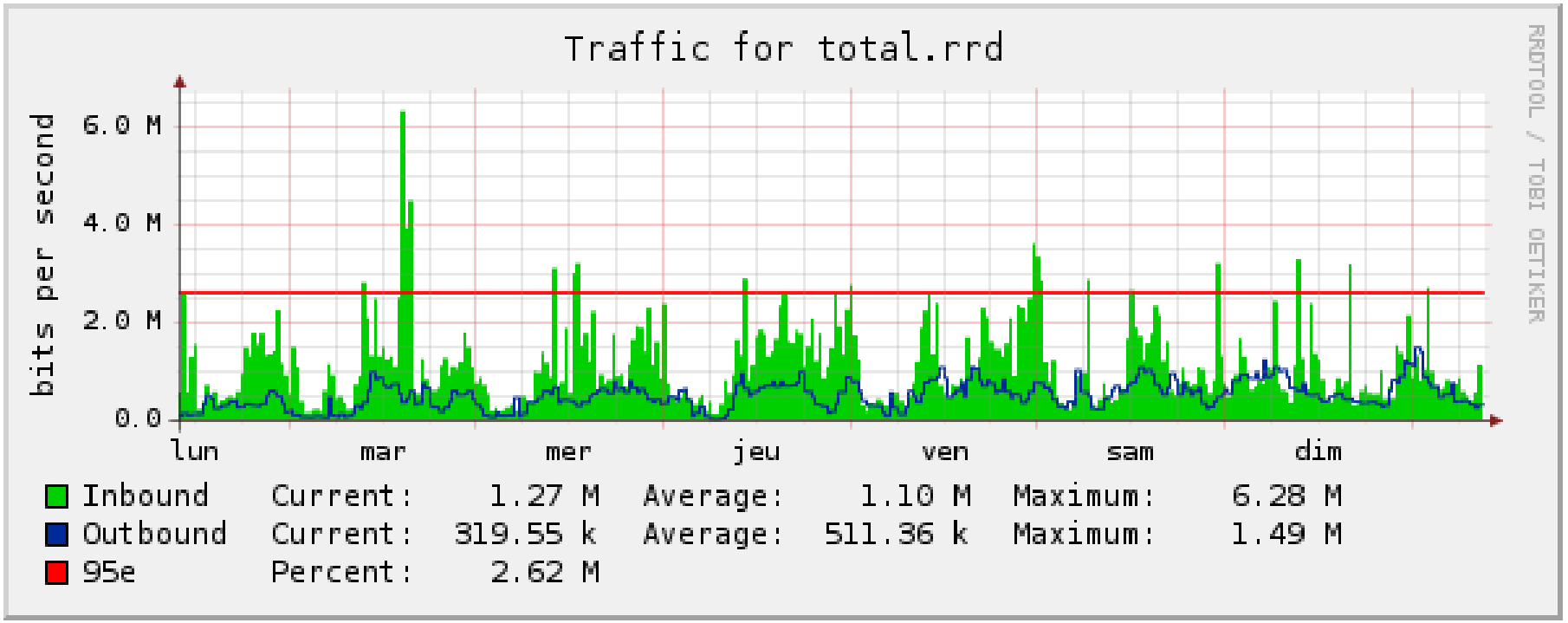
How to measure ?

- Make the time period of the experiment longer to reduce the impact of slow start
- Detect and measure only steady state part (true measure of stable capacity)

Issues to be aware of

- TCP algorithms
  - Slow Start Algorithm
  - Congestion control algorithms
  - Interaction between delayed ACKs & SS
- Retransmits and packet loss
- May need multiple connections to saturate network bandwidth

Burstable Billing (95th Percentile)



Sampling (every 5min) + 95th Percentile

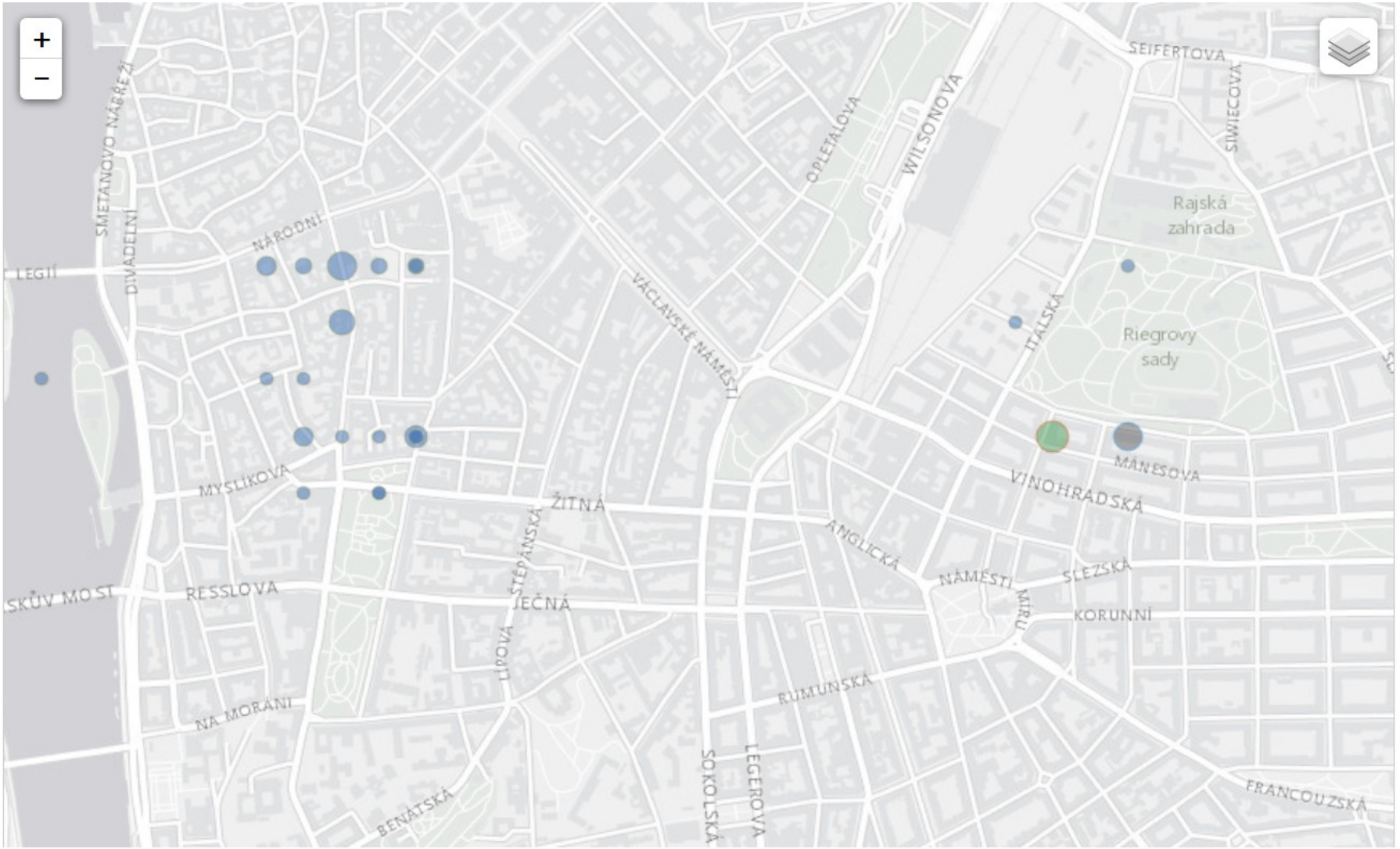
A short note on RIPE Atlas

- Ripe Atlas probes
- Ripe Atlas Anchor probes
- Distributed around the world (though unevenly)
- Can use pre-defined measurements
- Can setup user-defined measurements
- Streaming event API

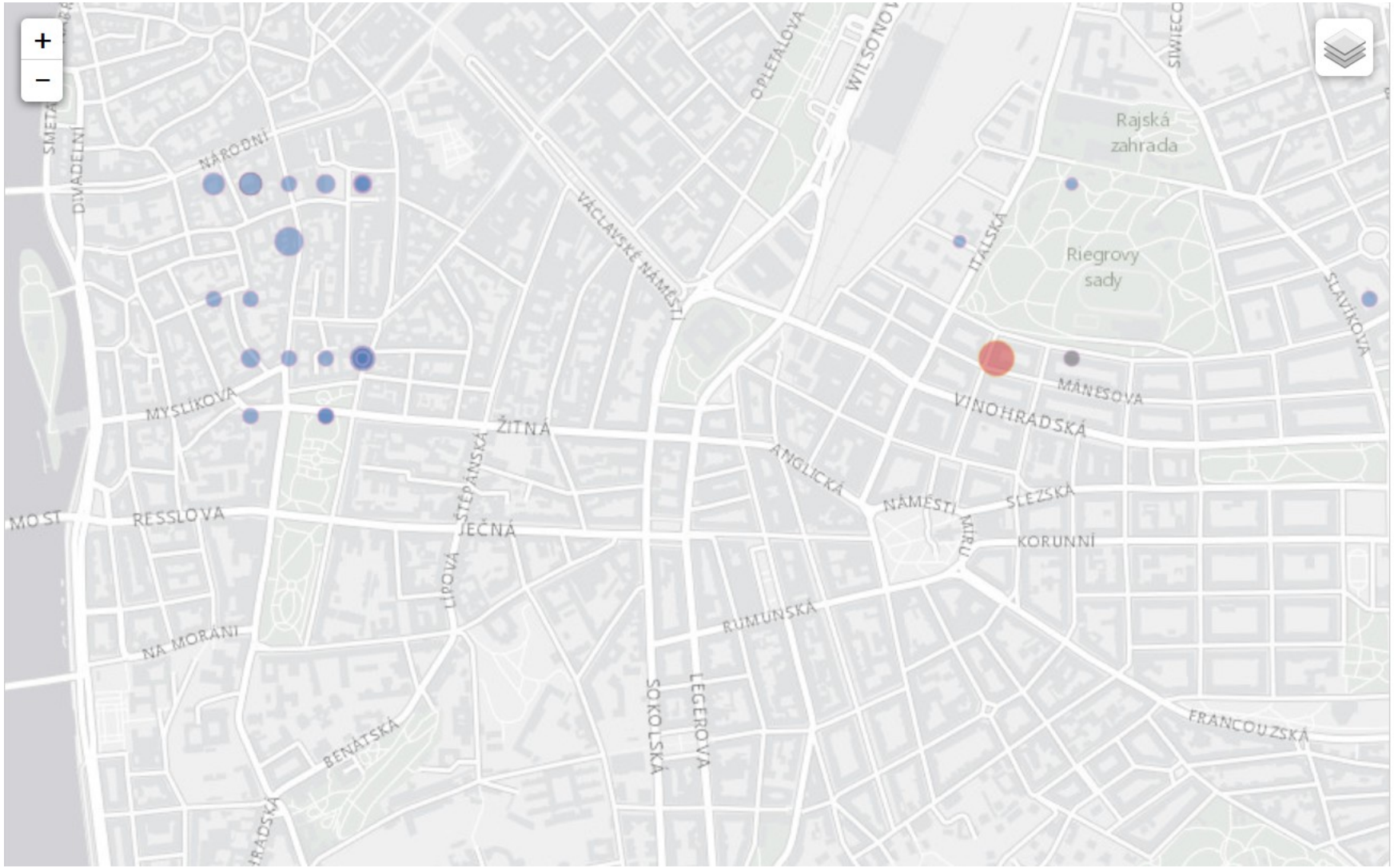
Reachability of anycast Root servers

- Look at the reachability of servers
- Look at the latency and “best” root server

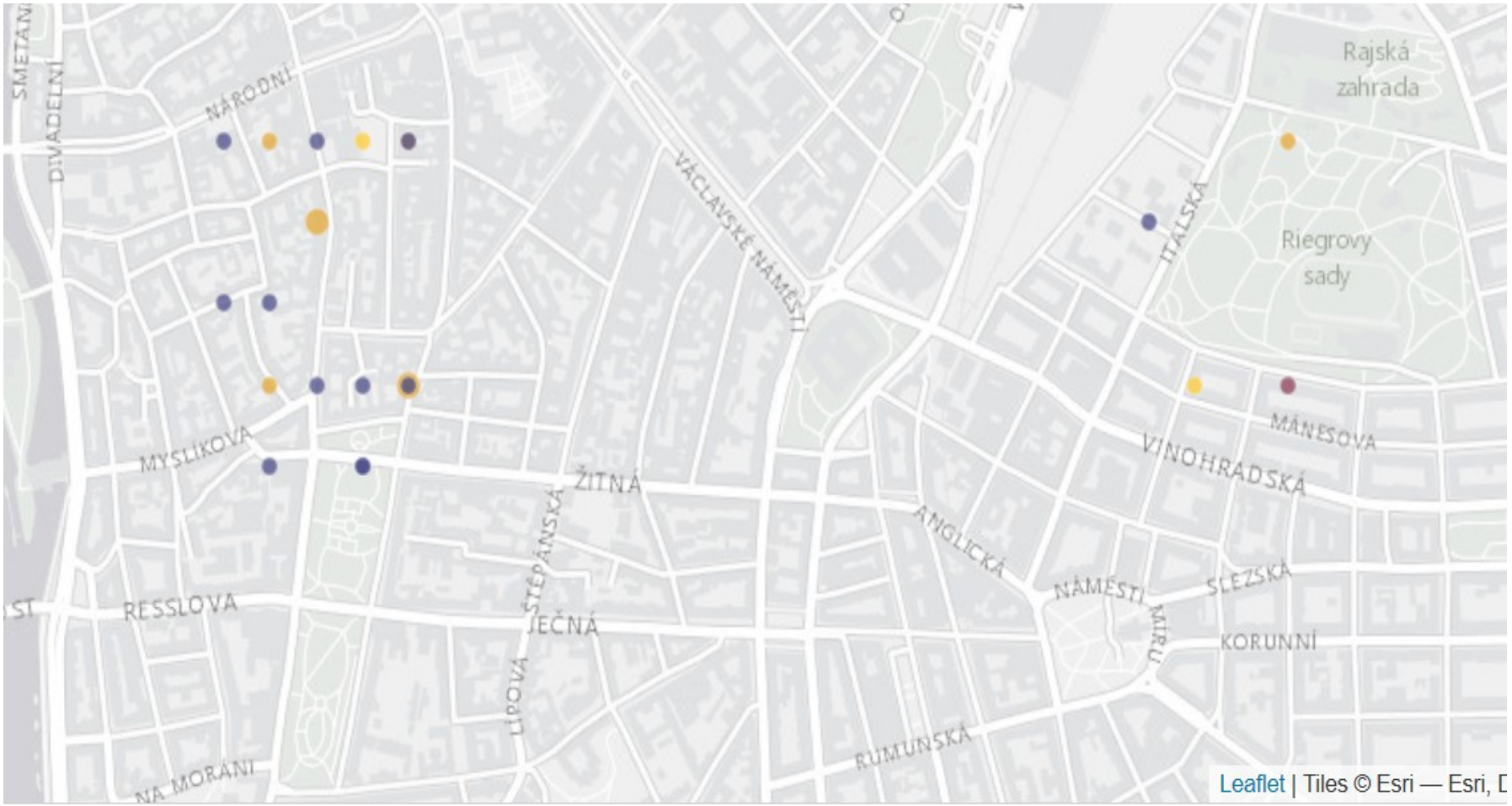
F-root server



L-root server

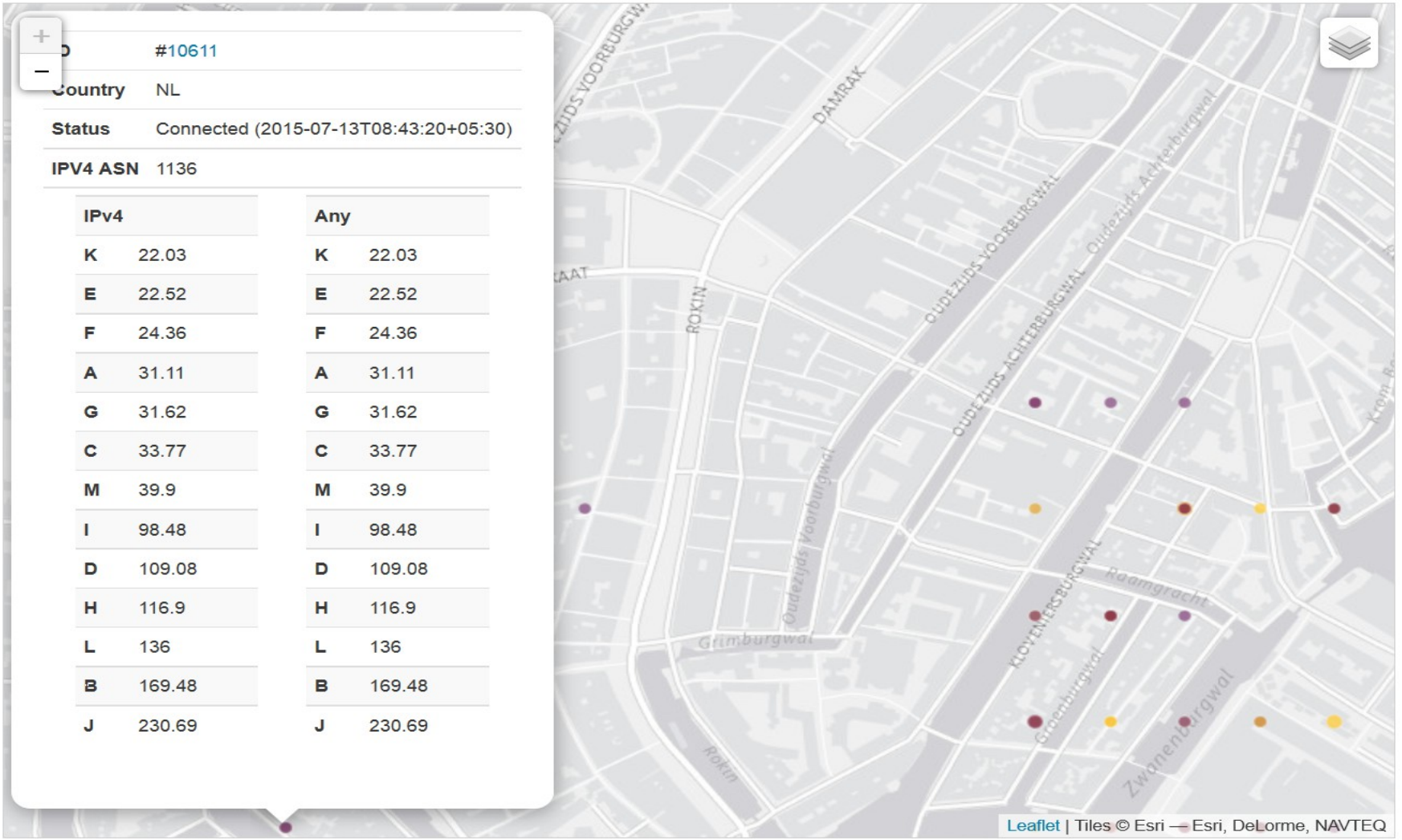


Best Root Server - PRG

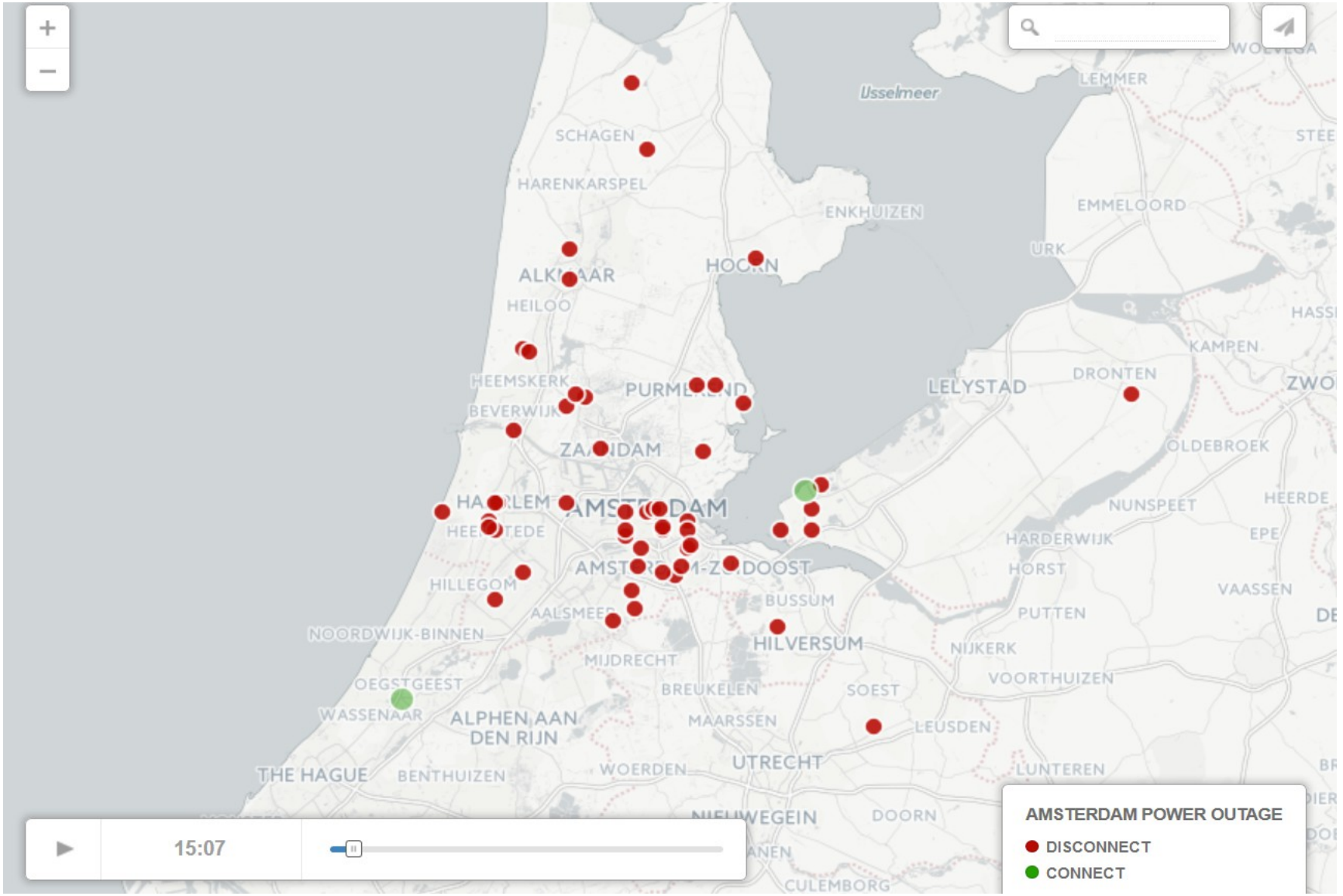


A: 0 | B: 0 | C: 2 | D: 2 | E: 17 | F: 95 | G: 1 | H: 0 | I: 5 | J: 2 | K: 2 | L: 112 | M: 1 | No Data: 8

“Best” root server - AMS



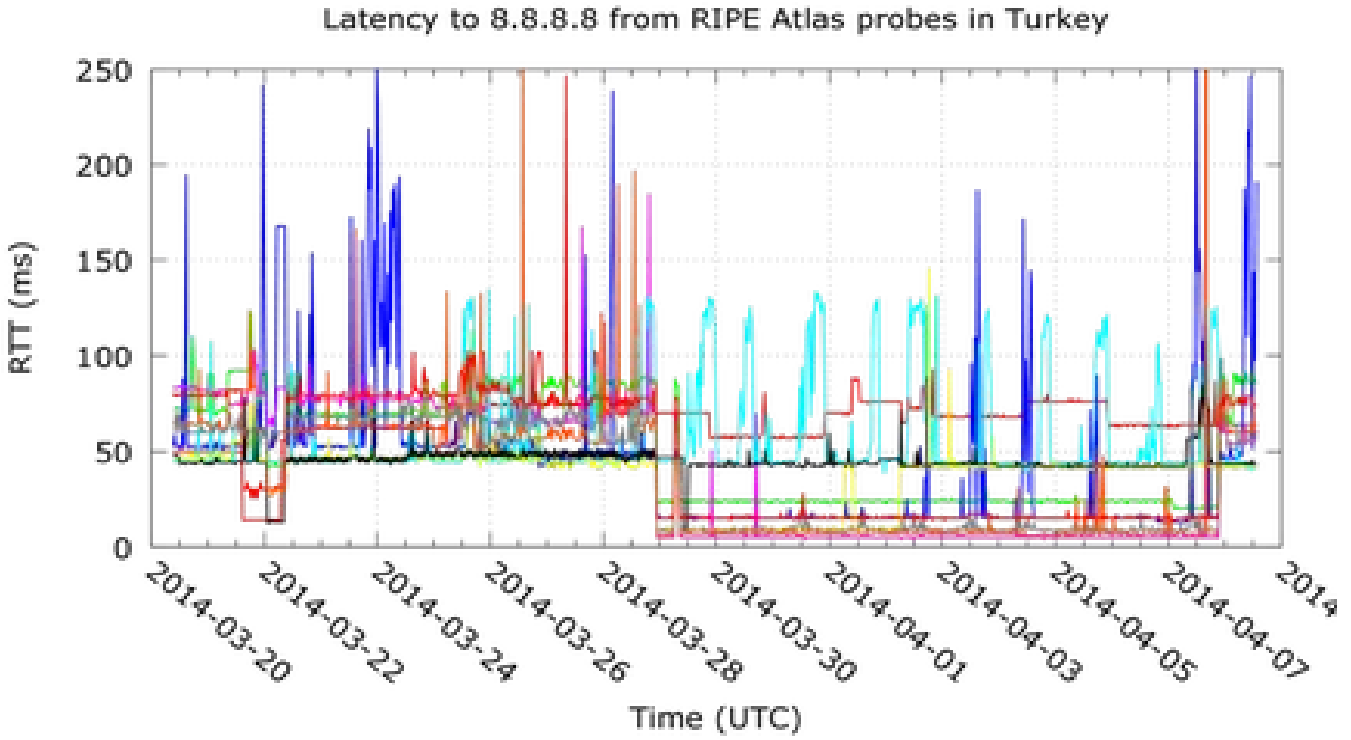
Electricity & Network outage



Internet Meddling in Turkey

- Turk Telecom uses DNS poisioning to block twitter
- People use 8.8.8.8 and 4.4.2.2 for resolution
- Turk Telecom does BGP hijacking and answers for Google DNS and Level 4 DNS

Internet Meddling in Turkey



Each line is a Atlas Probe – See the sudden latency drop

RIPE Stats

- Has statistics from Atlas probes around the world
- Prepackaged and easy to search
- Information about ASNs, IP address space, hostnames, countries
- Accessible via API
- Best of all – available for free (might need free registration for some features)

Resources

- Guidelines for Use of the RTP Monitoring Framework - RFC 6792
- Active & passive monitoring – https://tools.ietf.org/html/draft-morton-ippm-active-passive-01
- Hybrid Measurements – https://datatracker.ietf.org/doc/draft-ietf-ippm-6man-pdm-option/
- One-way Measurements (OWAMP) - RFC 4656
- Two-way Measurements (TWAMP) - RFC 5357, 6038
- TCP Throughput Testing - RFC 6349
- Loss Episode Metrics - RFC 6534
- Bulk Transfer Capacity – RFC 3148
- Passive Frame work - http://datatracker.ietf.org/doc/draft-zheng-ippm-framework-passive/

Resources

- Anscombe's Quartet – https://en.wikipedia.org/wiki/Anscombe%27s_quartet
- TCP and The Lower Bound of Web Performance - https://www.youtube.com/watch?v=C8orjQLacTo
- Outliers – https://en.wikipedia.org/wiki/Outlier
- Confounding - https://en.wikipedia.org/wiki/Confounding
- Slow Start - https://en.wikipedia.org/wiki/Slow-start – RFC 5681
- TCP Congestion Avoidance - https://en.wikipedia.org/wiki/TCP_congestion-avoidance_algorithm
- Statistical Significance - https://en.wikipedia.org/wiki/Statistical_significance
- Margin of Error - https://en.wikipedia.org/wiki/Statistical_significance

Resources

- Burstable billing – https://en.wikipedia.org/wiki/Burstable_billing
- RIPE Atlas – https://atlas.ripe.net/
- RIPE Stats – https://stat.ripe.net/
- RIPE Internet Maps – https://atlas.ripe.net/results/maps/
- Internet Meddling in Turkey - https://labs.ripe.net/Members/emileaben/a-ripe-atlas-view-of-internet-meddling-in-turkey
- RIPE NCC Analyses - https://labs.ripe.net/atlas/user-experiences/ripe-ncc-analyses
- Amsterdam Power Outage – https://labs.ripe.net/Members/andreas_strikos/amsterdam-power-outage-as-seen-by-ripe-atlas
- Anaysis of Turkey BGP hijacking - http://www.bortzmeyer.org/files/bortzmeyer-google-dns-turkey.pdf