Wrinkles in Time: Detecting Internet-wide Events via NTP

Meenakshi Syamkumar[*], Sathiya Kumaran Mani[*], Ramakrishnan Durairajan[+], Paul Barford[*] and Joel Sommers[$]

[*] University of Wisconsin-Madison

[+] University of Oregon

[$] Colgate University

What causes Internet events?

- Route changes & misconfigurations
- Hardware problems e.g., faults, electricity interruptions, overheating
- Security threats e.g., BGP hijacks, Denial-of-Service (DoS) attacks
- Natural disasters e.g., hurricanes, earthquakes, tornados
- Accidents e.g., cable cuts, fires
- Controlled outages
- Political issues, censorship

Source: *www.google.com*

Our definition: A sudden change in latency experienced by a cluster of clients

Impact of Internet events

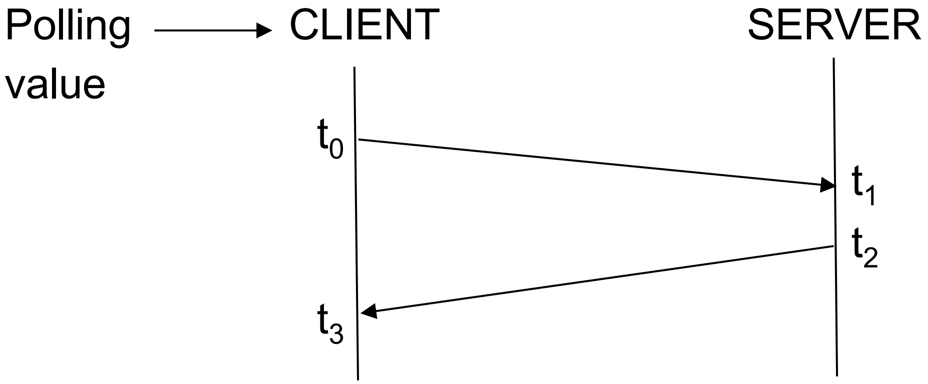
- Who does it affect?
  - End users
  - Internet Service Providers (ISPs)
- Why is it important?
  - Effective network monitoring and management
- What are the effects?
  - Increased delay in connectivity ← *Our Focus*
  - Complete loss of connectivity

Motivation

- Broad and detailed perspective on Internet Events
- Utilize existing infrastructure for passive measurements
- Traditional datasets for event detection
    - BGP datasets: provide coarse grained insight
    - Traceroutes & pings: limited by management policies and operational objectives
- Introducing new dataset for event detection
    - *NTP trace datasets collected at servers*
        - On-by-default service
        - Ubiquitously deployed
        - Fine grained insight on impact to individual clients

NTP basics

- NTP synchronizes clocks between communicating hosts

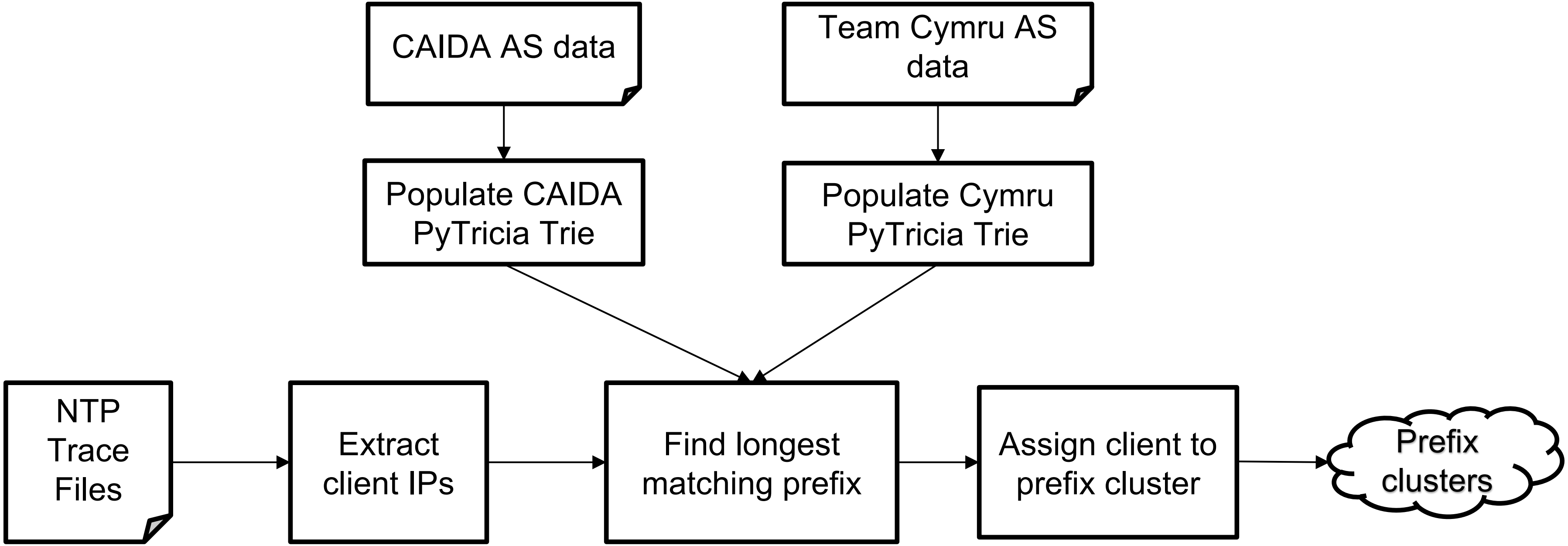


- Server to Client (s2c) delay: $t_1 – t_0$
- Client to Server (c2s) delay: $t_3 – t_2$
- NTP traces provide broad perspective on Internet clients [HotNets 2015]

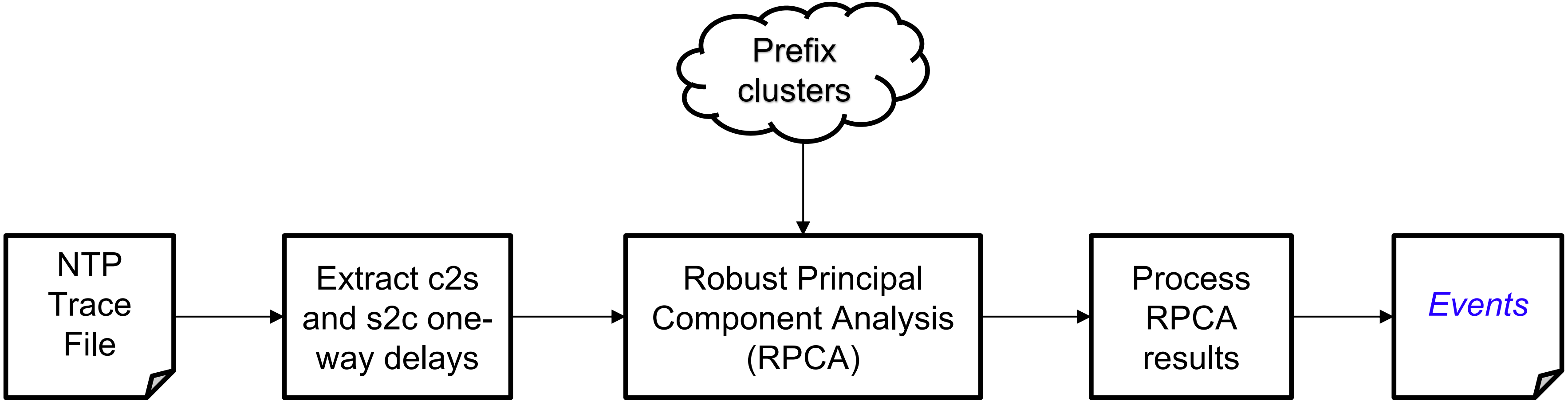
Our event detector: Tezzeract

1. Cluster Generator
    - Cluster NTP clients by longest prefix matching
2. Event Detector
    - Offline processing of NTP traces
    - Extract one-way delays (OWD) [TimeWeaver arXiv 2018]
    - For each cluster:
        - Identify time window for OWD analysis
        - Identify windows with *sudden change in OWD*
        - Combine successive time windows with change in OWD ← *Event of interest*

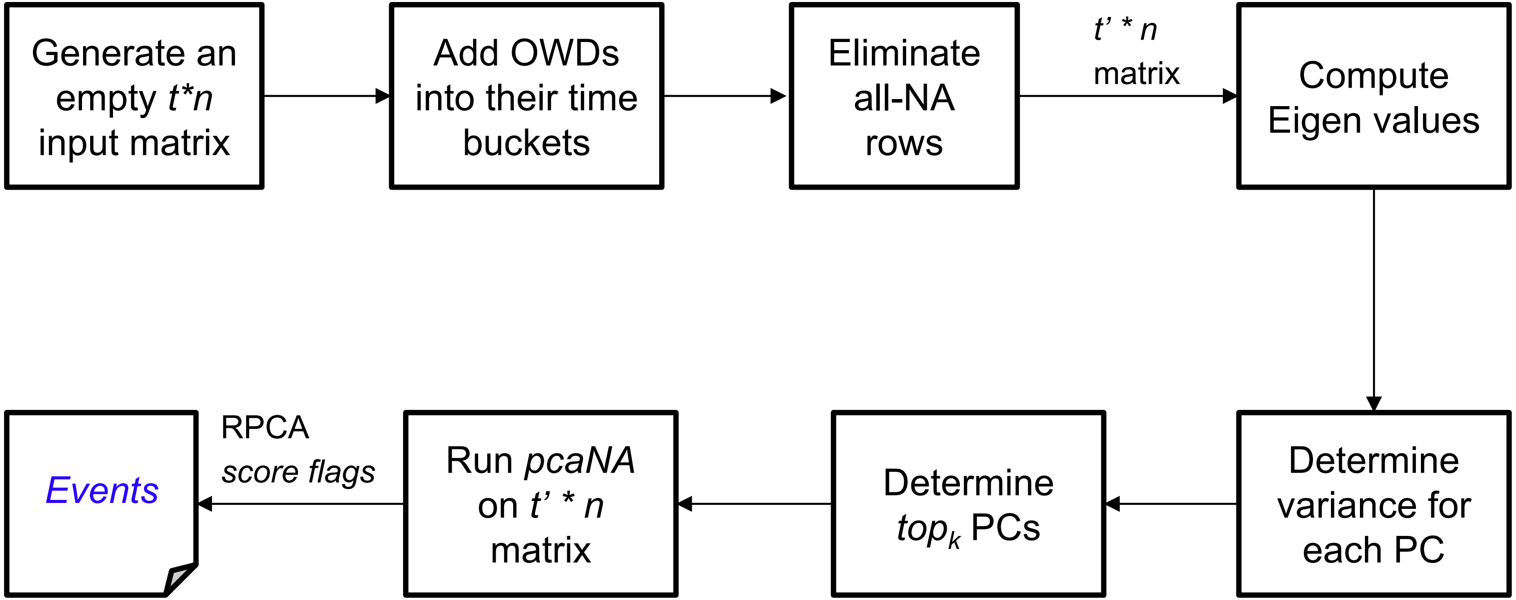
Tezzeract cluster generator


CAIDA AS data
Team Cymru AS data
Populate CAIDA PyTricia Trie
Populate Cymru PyTricia Trie
NTP Trace Files
Extract client IPs
Find longest matching prefix
Assign client to prefix cluster
Prefix clusters

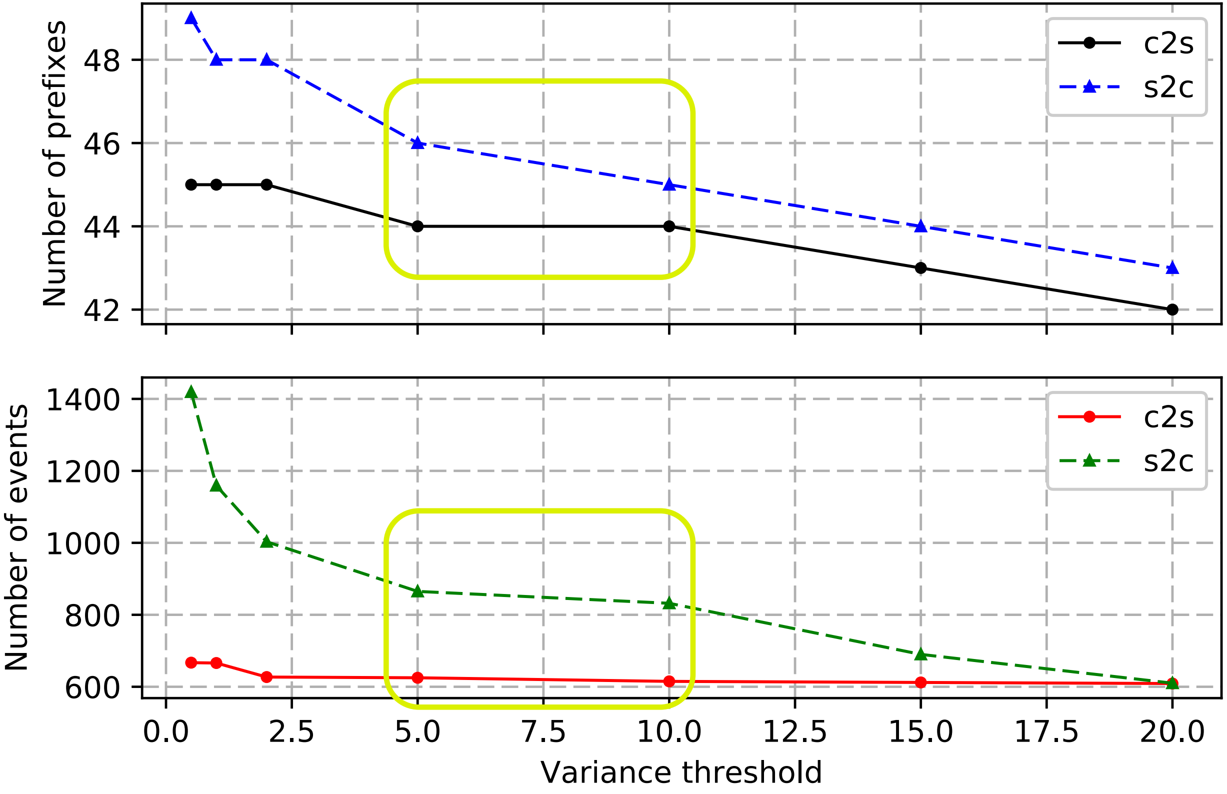
Tezzeract event detector


Prefix clusters
NTP Trace File
Extract c2s and s2c one-way delays
Robust Principal Component Analysis (RPCA)
Process RPCA results
Events

Tezzeract RPCA

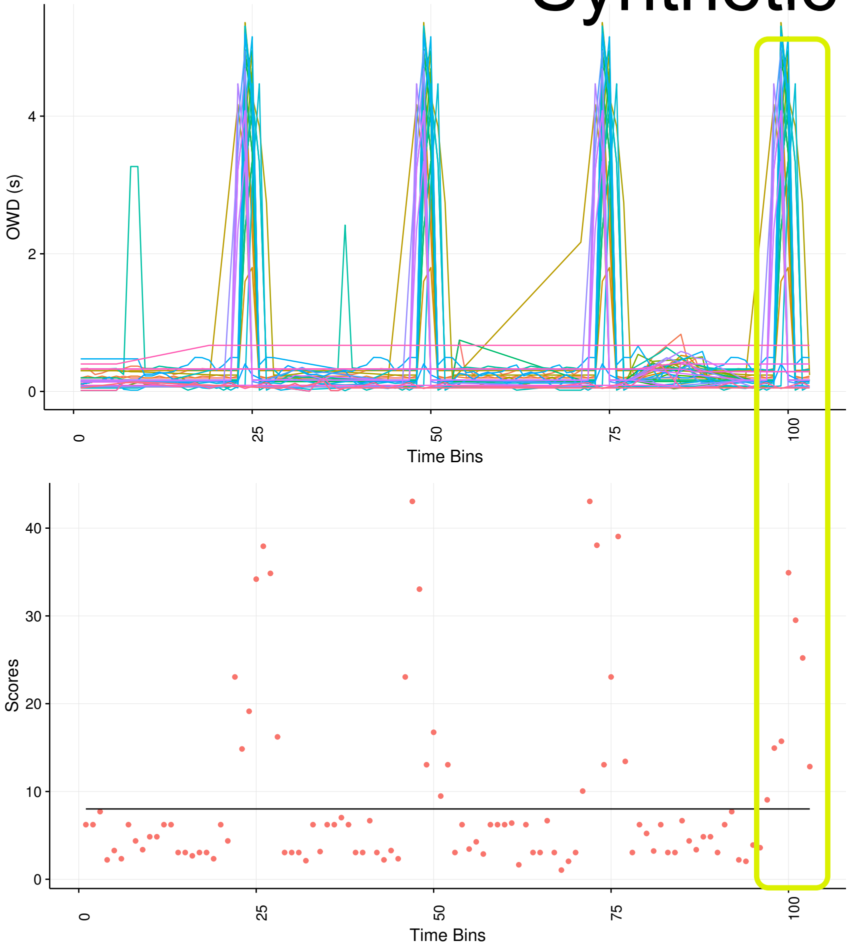

Generate an empty *t*n* input matrix
Add OWDs into their time buckets
Eliminate all-NA rows
*t’ * n* matrix
Compute Eigen values
Determine variance for each PC
Determine *top$_k$* PCs
Run *pcaNA* on *t’ * n* matrix
RPCA *score flags*
Events

Top$_k$ PCs



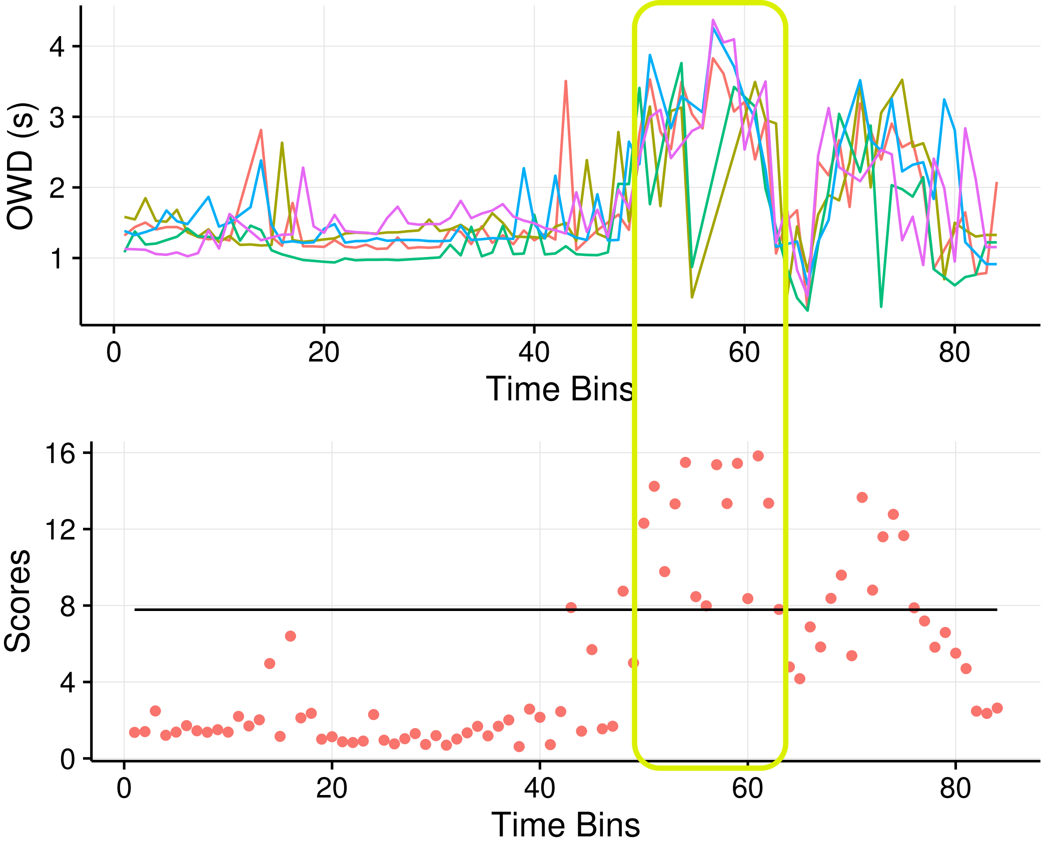
Changes in the number of events detected (bottom) and affected prefix clusters (top) with variation of variance threshold to select *top$_k$* PCs

Synthetic event



Changes in client OWDs (top) and the RPCA scores (bottom) with injection of a synthetic event once in every 25-minutes

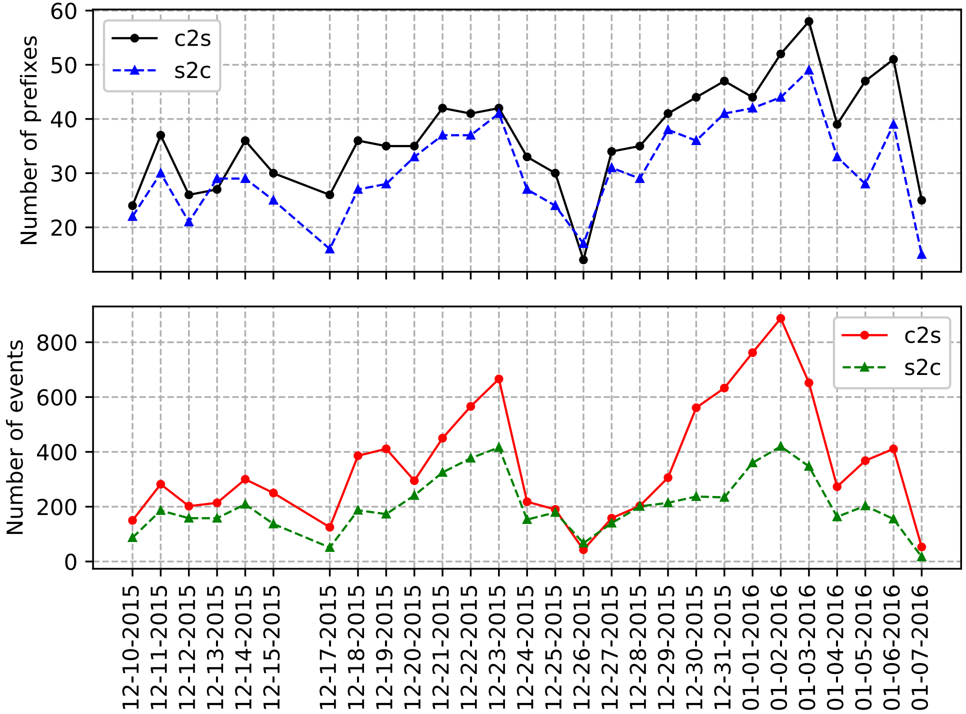
Tezzeract event example



Level3 outage identified by Tezzeract, affecting AS 20141 on December 15, 2015.

Tezzeract Evaluation

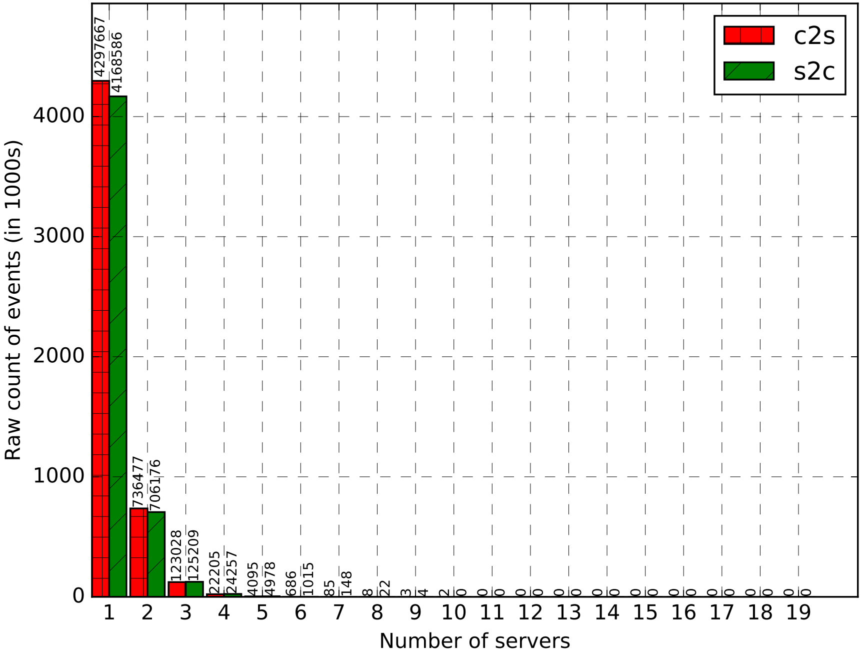
- 3 months NTP trace data from 19 servers
- Median of event duration across servers is approximately 20 minutes



Daily changes in the number of events detected (bottom) and affected prefix clusters (top)

Tezzeract Evaluation

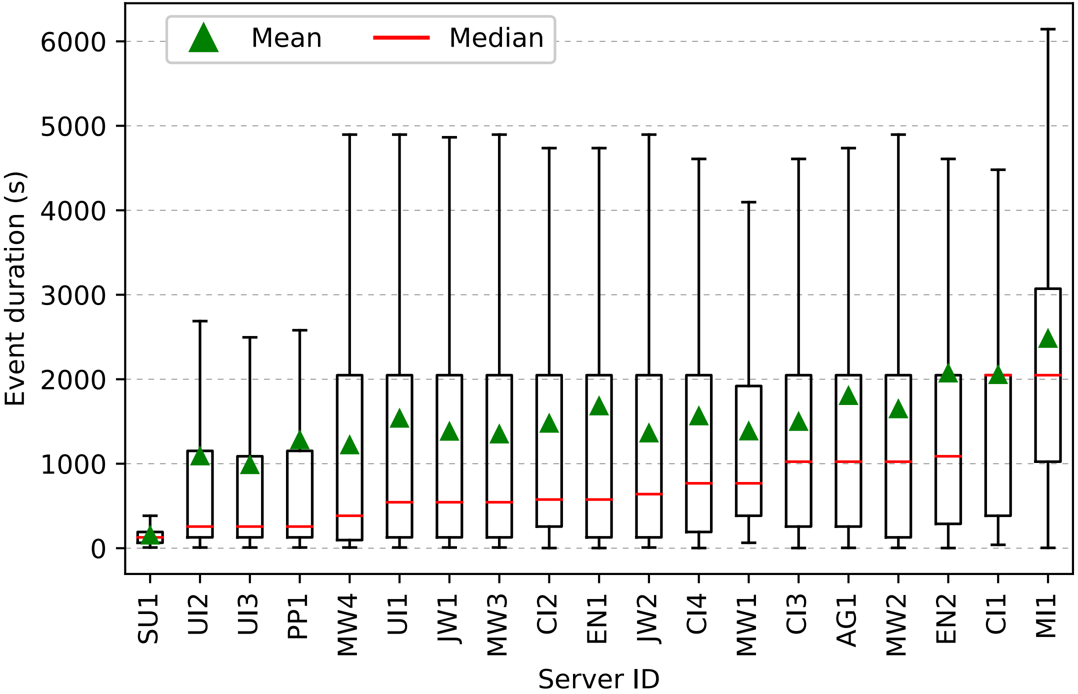
- 3 months NTP trace data from 19 servers
- Median of event duration across servers is approximately 20 minutes



Unique number of events observed across the different NTP servers

Tezzeract Evaluation

- 3 months NTP trace data from 19 servers
- Median of event duration across servers is approximately 20 minutes



Box-and-whiskers plot showing event duration characteristics of c2s events

Top 3 ISPs

- Majority of the events affect Tier-1 ISP clients and a major cloud service provider

November 2015	December 2015	January 2015	Full dataset
701, Verizon, 91933	701, Verizon, 129531	22394, Verizon, 46037	701, Verizon, 225086
16509, Amazon, 73847	16509, Amazon, 92843	7018, AT&T, 18804	16509, Amazon, 167779
7018, AT&T, 50250	7018, AT&T, 78595	7029, Windstream, 8915	7018, AT&T, 147649

Summary

- Internet events are challenging to identify
- Tezzeract is an RPCA-based tool to identify events using NTP datasets
- NTP-based event detection provides a unique and complementary perspective
- 21-67% of events match with events identified by probe-based approaches
- Tezzeract identifies reported outages
- Future work:
    - Real-time NTP-based event detection
    - Gain additional perspective on OWD decrease events