Outage Clustering: From Leaves to Trees

John Heidemann

joint work with Yuri Pradkin, Aqib Nisar
USC/ISI

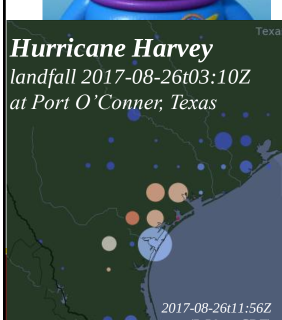
CAIDA Active Internet Measurments (AIMS) / 15 March 2018

This research is sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, HSARPA, Cyber Security Division, BAA 11-01-RIKA and Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0344, and contract number D08PC75599. The U.S. Gov't is authorized to reproduce and distribute reprints for Gov't purposes notwithstanding any copyright notation thereon. The views herein are those of the authors and do not necessarily represent those of DHS or the U.S. Gov't.

USC Viterbi School of Engineering · Information Sciences Institute

So Much Internet Outage Data…

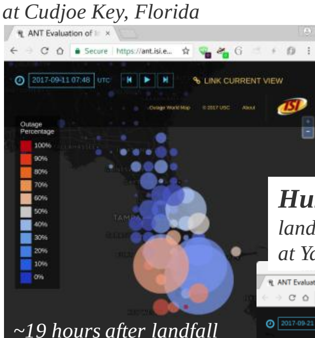
Trinocular
24x7 since Nov. 2013



Hurricane Harvey
landfall 2017-08-26t03:10Z
at Port O'Conner, Texas

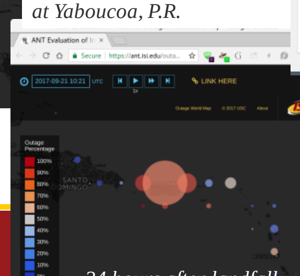
2017-08-26t11:56Z
(5:56am CDT)

Hurricane Irma
landfall 2017-09-10t13:10Z
at Cudjoe Key, Florida



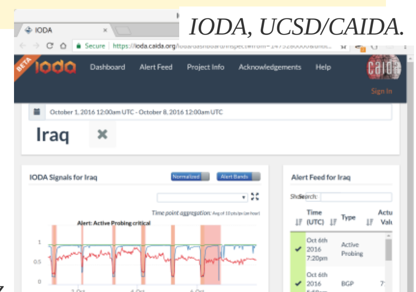
~19 hours after landfall

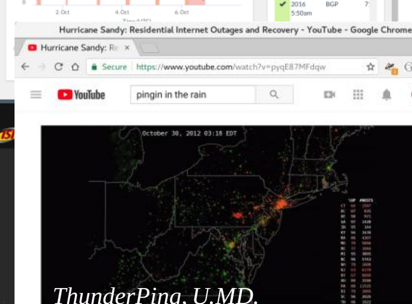
Hurricane Maria
landfall: 2017-09-20t10:15Z
at Yaboucoa, P.R.



~24 hours after landfall

IODA, UCSD/CAIDA.





ThunderPing, U.MD.

Too Much Long-Term Data?

- USC/ISI's Trinocular: outages, 24x7, since Nov. 2013
- about 40TB (!)
- about 20k observations x 4M blocks:
  80G datapoints (!!)

- how to make sense of it?
  - from leaves (edge networks)
  - to trees (events)
  - on the way to understanding the "forest" of Internet reliability

Making Sense of Too Much Data

- **geographic visualization**
  interactively explore the world

- **non-geographic visualization**
  begin to reveal patterns

with too much data
(40TB and
80G observations)

- **clustering by similarity**
  discover underlying dependencies

Making Sense of Too Much Data

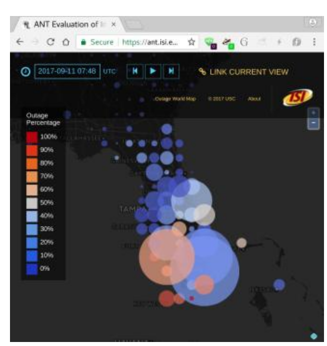
- **geographic visualization**
  interactively explore the world
- **non-geographic visualization**
  begin to reveal patterns
- **clustering by similarity**
  discover underlying dependencies

with too much data (40TB and 80G observations)

Geographic Visualization

- on the web: https://ant.isi.edu/outage/world/
- key features
  - circle size: *number* of blocks out
  - color: *percent* of blocks out
  - time selection
  - geographic zoom and pan
  - **geography: easy to relate to (what operators ask for!)**

Florida, ~19 hours after landfall of Hurricane Irma

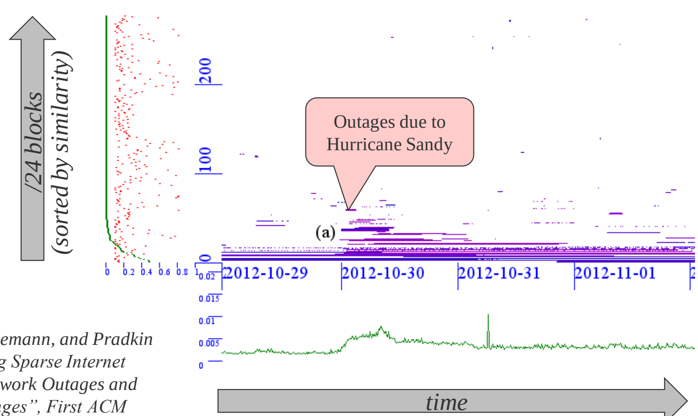


Making Sense of Too Much Data

- **geographic visualization**
  interactively explore the world
- **non-geographic visualization**
  begin to reveal patterns
- **clustering by similarity**
  discover underlying dependencies

with too much data (40TB and 80G observations)

Non-Geographic Visualizations: the *Network* in Outages



Quan, Heidemann, and Pradkin "Visualizing Sparse Internet Events: Network Outages and Route Changes", First ACM Workshop on Internet Visualization, Nov. 2012

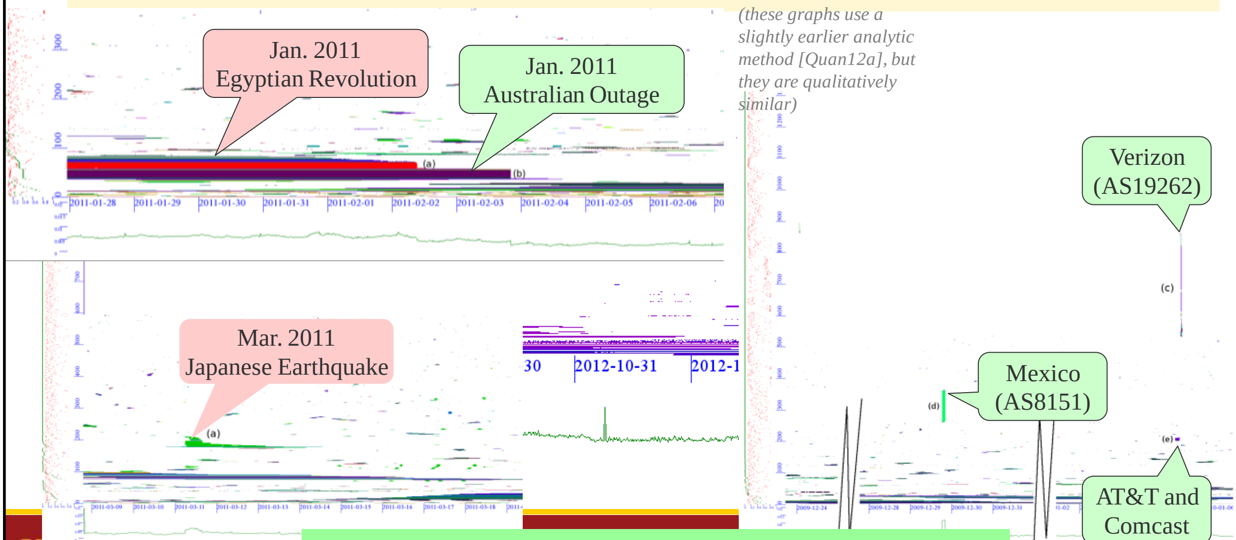
goal: reveal patterns

find dependencies among networks

(colored areas are outages, color shows location)

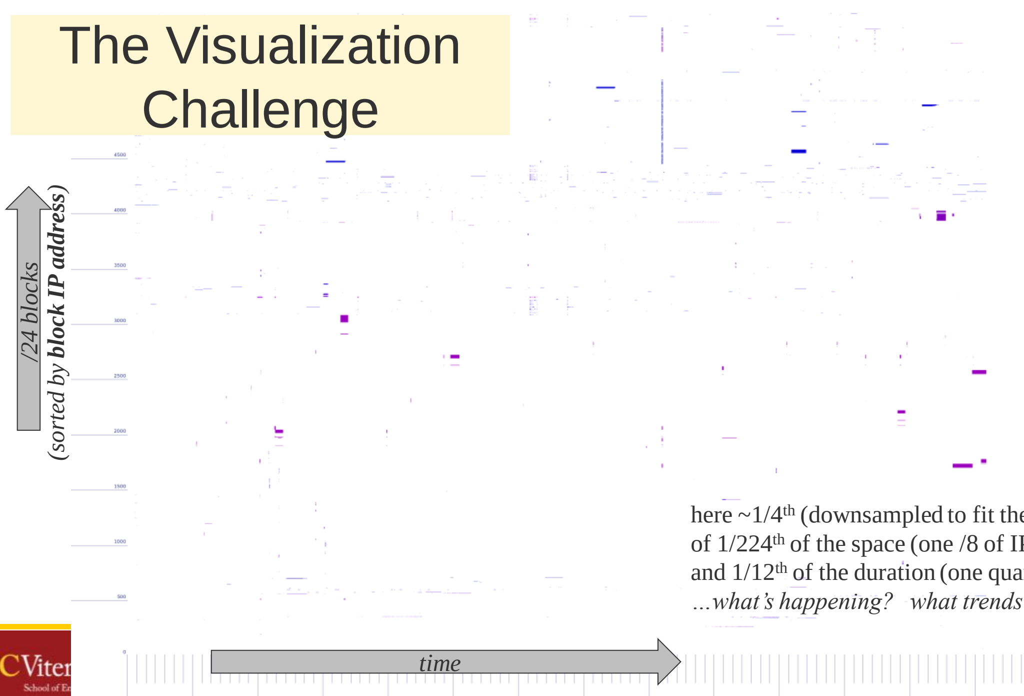
Global Network Outages: Prominent and *Unknown*

(these graphs use a slightly earlier analytic method [Quan12a], but they are qualitatively similar)



our goal: understand small *and* big

The Visualization Challenge



here ~1/4th (downsampled to fit the screen)
of 1/224th of the space (one /8 of IPv4)
and 1/12th of the duration (one quarter of ~3 years)
…what's happening? what trends? what's new?

Efficient Visualization

- **visualization with linear ordering algorithm**
  - runtime: O(n log n log m)
  - for n blocks and m duration timesteps
- approach:
  - map clustering to sorting: O(n log n) in time
  - sort on *multi-timescale bitmap:* O(log m) in space

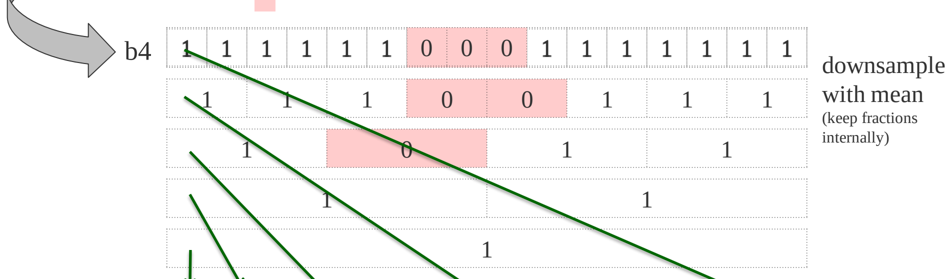
Presented at AIMS 2017 (last year!)

Details in "Back Out: End-to-end Inference of Common Points-of-Failure in the Internet (extended)". ISI-TR-724, Feb., 2018. *www.isi.edu/~johnh/PAPERS/Heidemann18b.pdf*

Multi-Timescale for Similarity

- input: outage timeseries from 5 /24 blocks
  - b1 1111 111**0** 1111 1111
  - b2 1111 1111 1111 111**0**
  - b3 1111 11**00** 1111 1111
  - b4 1111 11**00** **0**111 1111
  - b5 1111 111**0** 1111 1111

goal: cluster by "similarity"



concatenate: 1 - 11 - 1**0**11 - 111**0** **0**111 - 1111 11**00** **0**111 1111

Multi-Timescale Finds Similarity

- input: outage timeseries from 5 /24 blocks
  - b1 1111 111**0** 1111 1111
  - b2 1111 1111 1111 111**0**
  - b3 1111 11**00** 1111 1111
  - b4 1111 11**00** **0**111 1111
  - b5 1111 111**0** 1111 1111
- apply to all blocks…
  - b1 1 - 11 - 1111 - 111**0** 1111 - 1111 111**0** 1111 1111
  - b2 1 - 11 - 1111 - 1111 111**0** - 1111 1111 1111 111**0**
  - b3 1 - 11 - 1**0**11 - 111**0** 1111 - 1111 11**00** 1111 1111
  - b4 1 - 11 - 1**0**11 - 111**0** **0**111 - 1111 11**00** **0**111 1111
  - b5 1 - 11 - 1111 - 111**0** 1111 - 1111 111**0** 1111 1111

goal: cluster by "similarity"

Multi-Timescale Finds Similarity

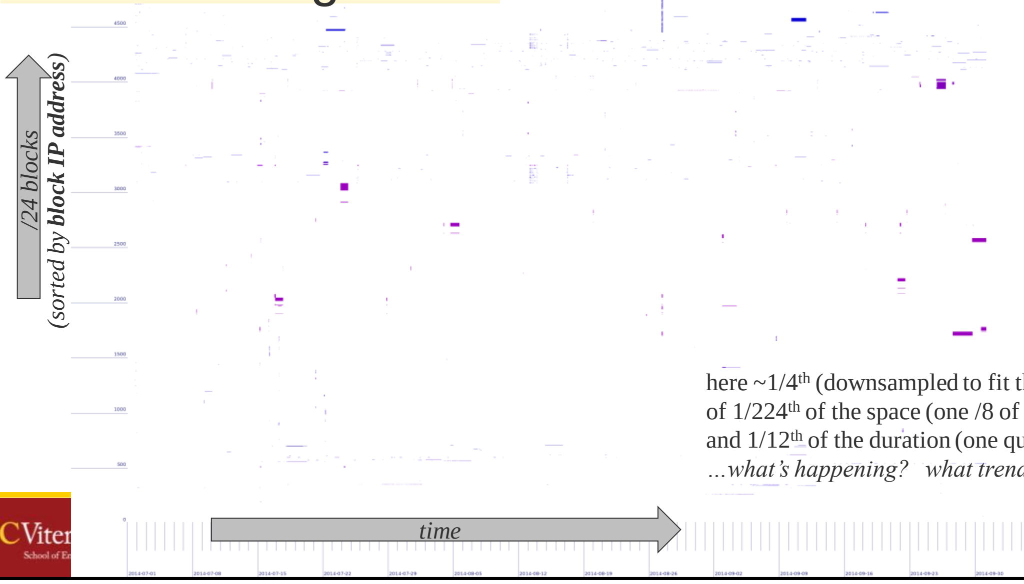
- input: outage timeseries from 5 /24 blocks
  - b1 1111 111**0** 1111 1111
  - b2 1111 1111 1111 111**0**
  - b3 1111 11**00** 1111 1111
  - b4 1111 11**00** **0**111 1111
  - b5 1111 111**0** 1111 1111
- apply to all blocks and **sort**
  - b2 1 - 11 - 1111 - 1111 111**0** - 1111 1111 1111 111**0**
  - b1 1 - 11 - 1111 - 111**0** 1111 - 1111 111**0** 1111 1111
  - b5 1 - 11 - 1111 - 111**0** 1111 - 1111 111**0** 1111 1111
  - b3 1 - 11 - 1**0**11 - 111**0** 1111 - 1111 11**00** 1111 1111
  - b4 1 - 11 - 1**0**11 - 111**0** **0**111 - 1111 11**00** **0**111 1111

goal: cluster by "similarity"

define similar as adjacent in multi-timescale vectors

result: better clusters
(Hamming distance from 8 to 4)

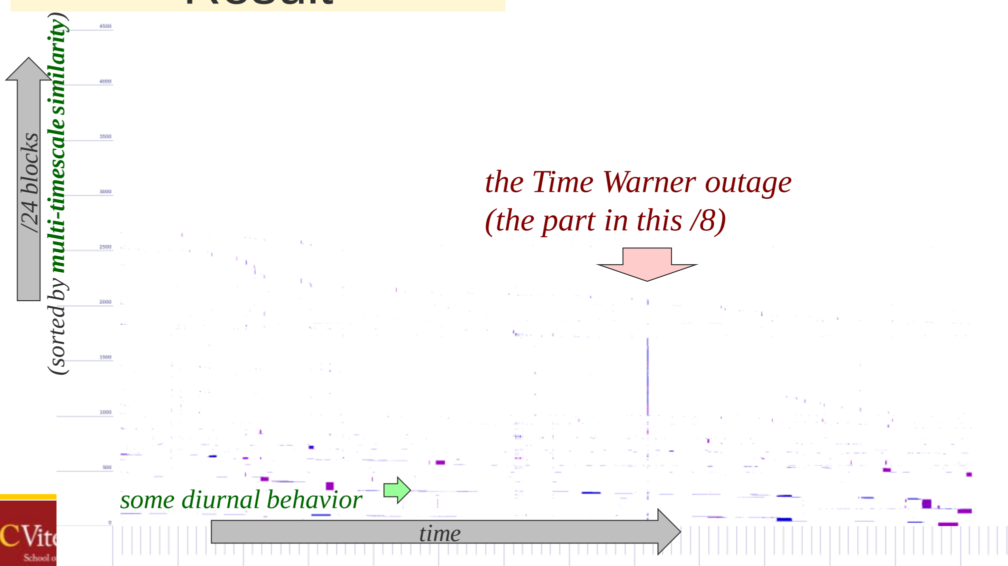
The Visualization Challenge



here ~1/4th (downsampled to fit the screen)
of 1/224th of the space (one /8 of IPv4)
and 1/12th of the duration (one quarter of ~3 years)
…what's happening? what trends? what's new?

One Visualization Result

here ~1/4th (downsampled to fit the screen)
of 1/224th of the space (one /8 of IPv4)
and 1/12th of the duration (one quarter of ~3 years)



Making Sense of Too Much Data

- **geographic visualization**
  interactively explore the world
- **non-geographic visualization**
  begin to reveal patterns

with too much data (40TB and 80G observations)

- **clustering by similarity**
  discover underlying dependencies

Clustering to Discovery Dependencies

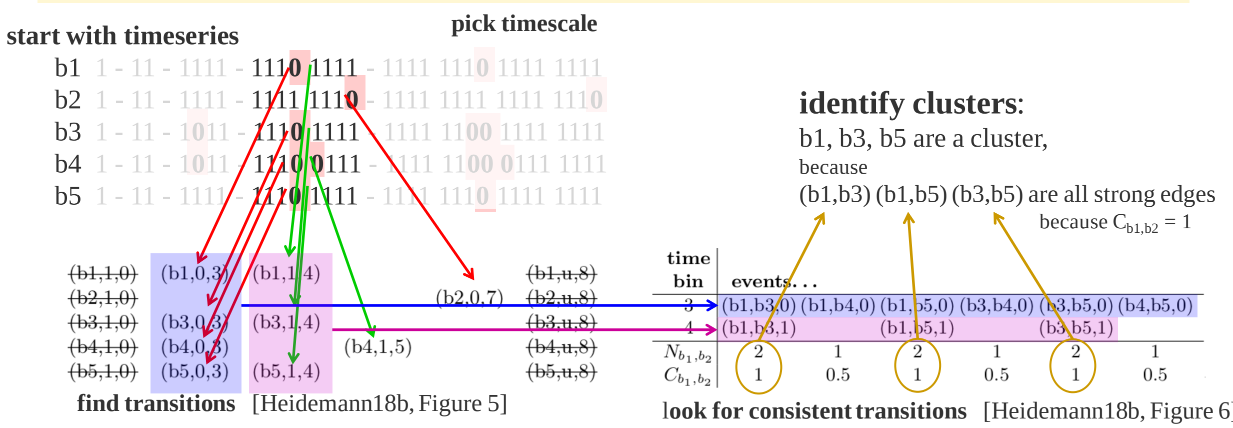
- visualization is nice, but humans can't look at everything
- new clustering algorithms can *discovery dependencies*
  – common failure patterns
  – implying common root causes
  – (unconstrained by 2-D visualization)

Clustering Insight

- things fail and recover together => possible dependency
- when *consistently, multiple times* => *probable* dependency

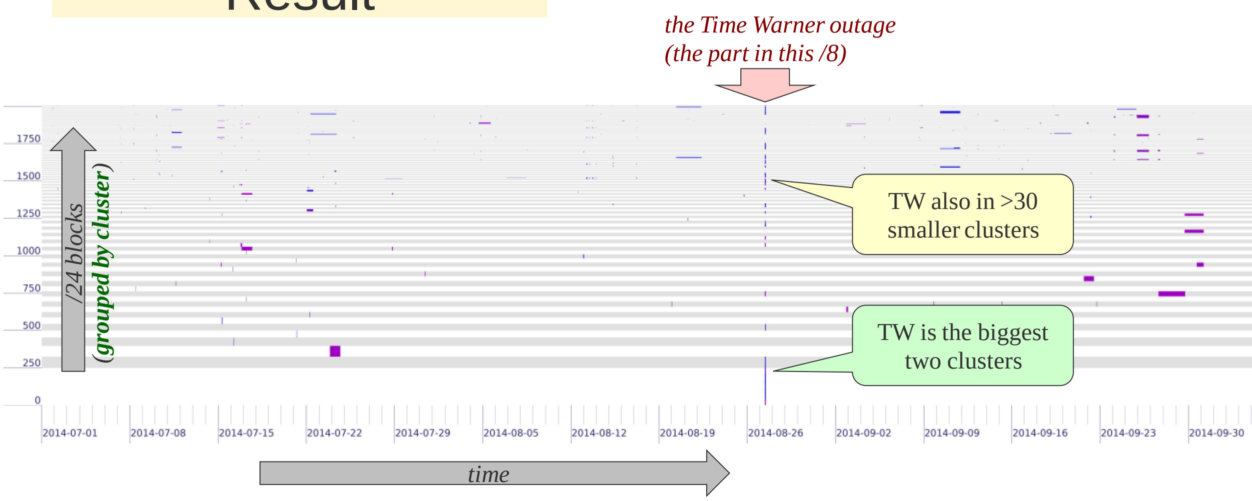
(Details: John Heidemann, Yuri Pradkin, and Aqib Nisar. Back Out: End-to-end Inference of Common Points-of-Failure in the Internet (extended). ISI-TR-724, February, 2018. https://www.isi.edu/%7ejohnh/PAPERS/Heidemann18b.html .)

Clustering Approach



One Clustering Result

1/224th of the space (one /8 of IPv4)
and 1/12th of the duration (one quarter of ~3 years)



Iterative Clustering

1/224th of the space (one /8 of IPv4)
and 1/12th of the duration (one quarter of ~3 years)
now just **3 days** of time

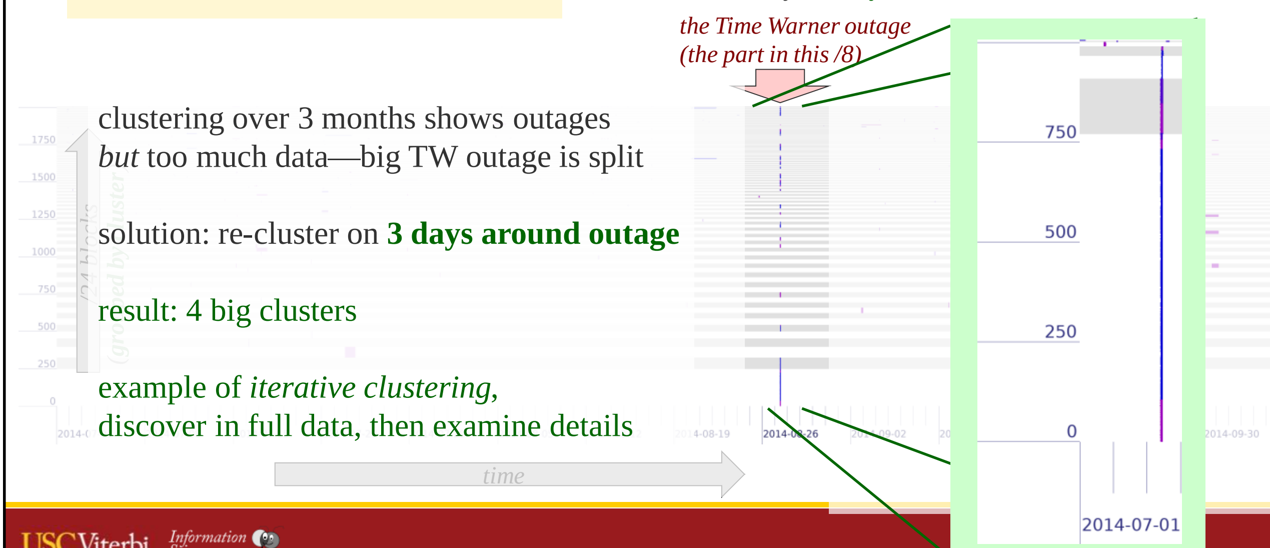
the Time Warner outage
(the part in this /8)

clustering over 3 months shows outages
but too much data—big TW outage is split

solution: re-cluster on **3 days around outage**

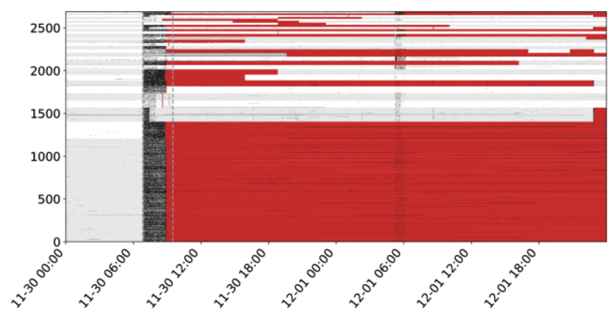
result: 4 big clusters

example of *iterative clustering*,
discover in full data, then examine details



Clustering Beyond Outages

- cluster generalizes:
  detects *temporal correlations*
  in *big timeseries*
- we've applied it to
  - outages
  - anycast catchments
  - routing updates
- for anycast:
  - map initial vs. new cluster to binary value
  - skip outages (from DDoS)

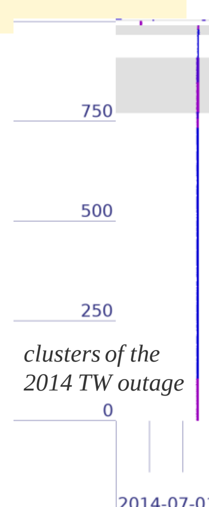


anycast catchments for J-Root around the 2015-11-30 DDoS attack

[Heidemann18b, Figure 9]

Outage Clustering from Here

- just released clustering technical report
- opens many new questions…
  - relating to other information? (like power outages)
  - what is "normal"?
  - can we evaluate policy <=> reliablity?
- datasets at https://ant.isi.edu/datasets/outage and https://imactcybertrust.org
- code available on request



clusters of the 2014 TW outage