

Background and Motivation

- Past research has shown at any given time 0.3% of internet is unavailable
- Outages can be detected using either data or control plane traffic
- Since all outages are not visible in both planes, we need ways to correlate outages from both planes and better understand relationships

Methodology

- We collect outages detected by the Trinocular^[1] project (3.5M /24s)
- We then fetch BGP updates from RouteViews for prefixes covering given /24s
- Finally, we map how each data plane outage was seen by peers in RouteViews

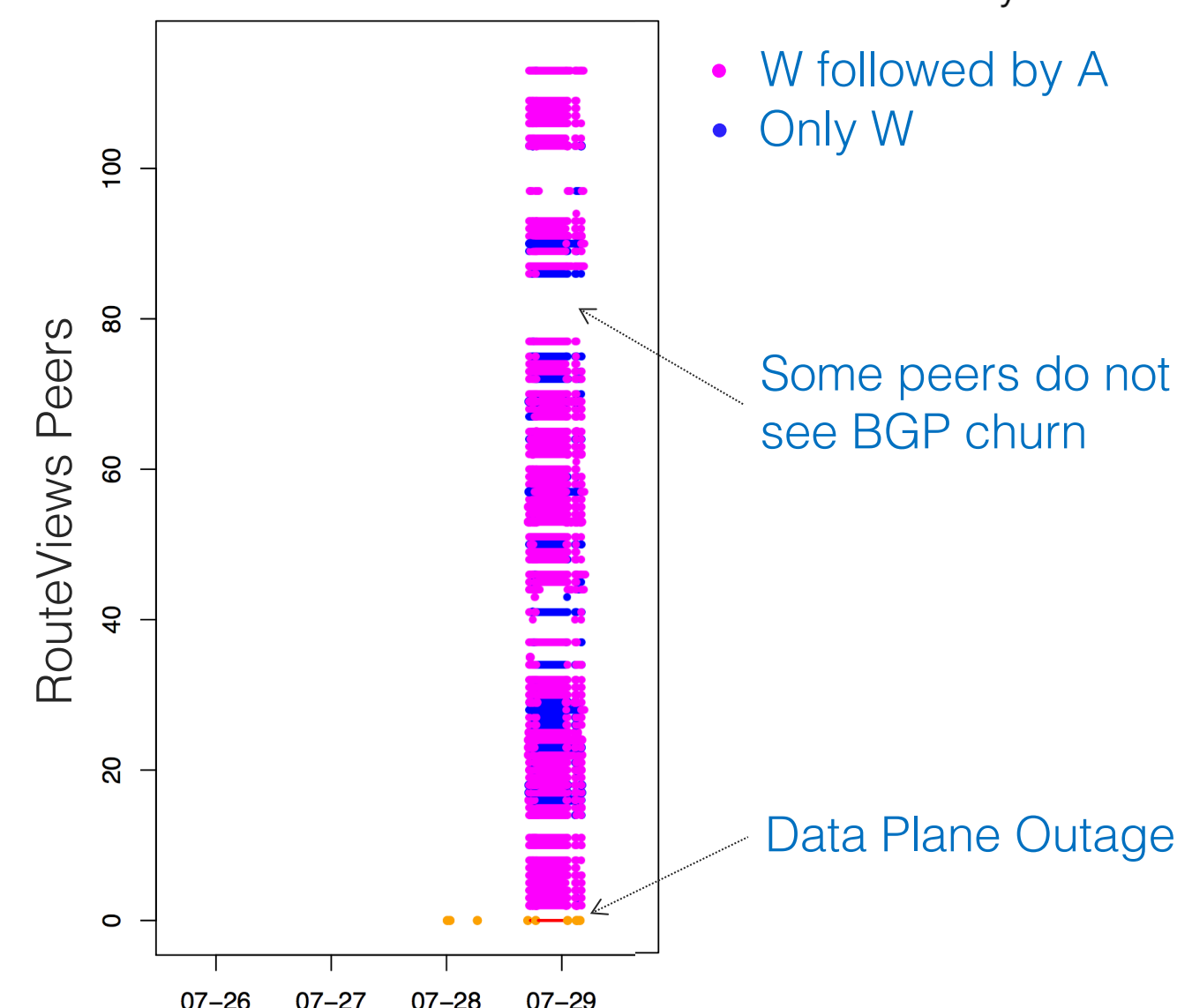
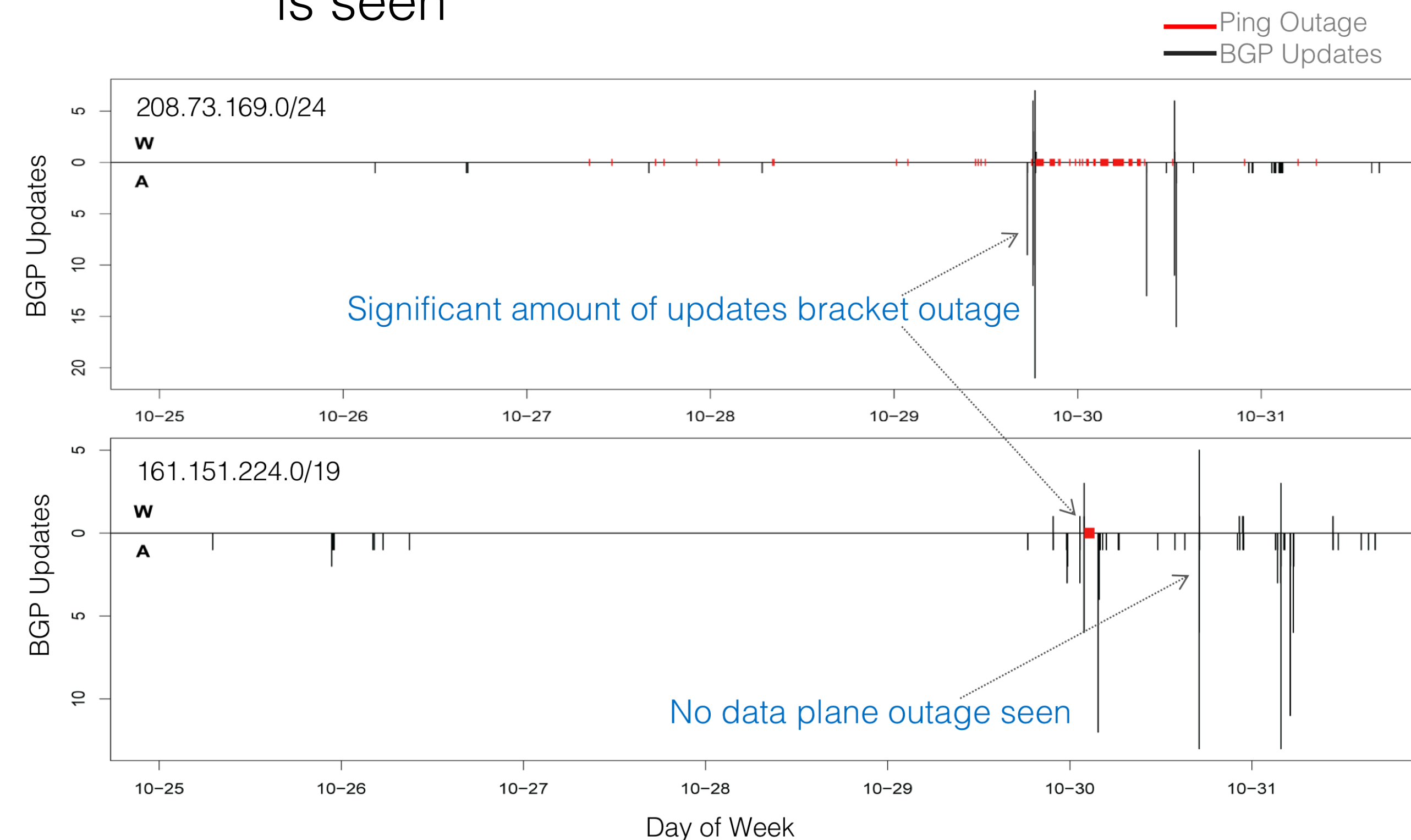
[1] L. Quan et al. "Trinocular: Understanding Internet Reliability through Adaptive Probing", SIGCOMM'13

[2] A. Shah et al. "Disco: Fast, Good, and Cheap Outage Detection", TMA'17

* Contributed by Yingnan Liu, Randy Paffenroth (Worcester Polytechnic Institute)

Preliminary Findings

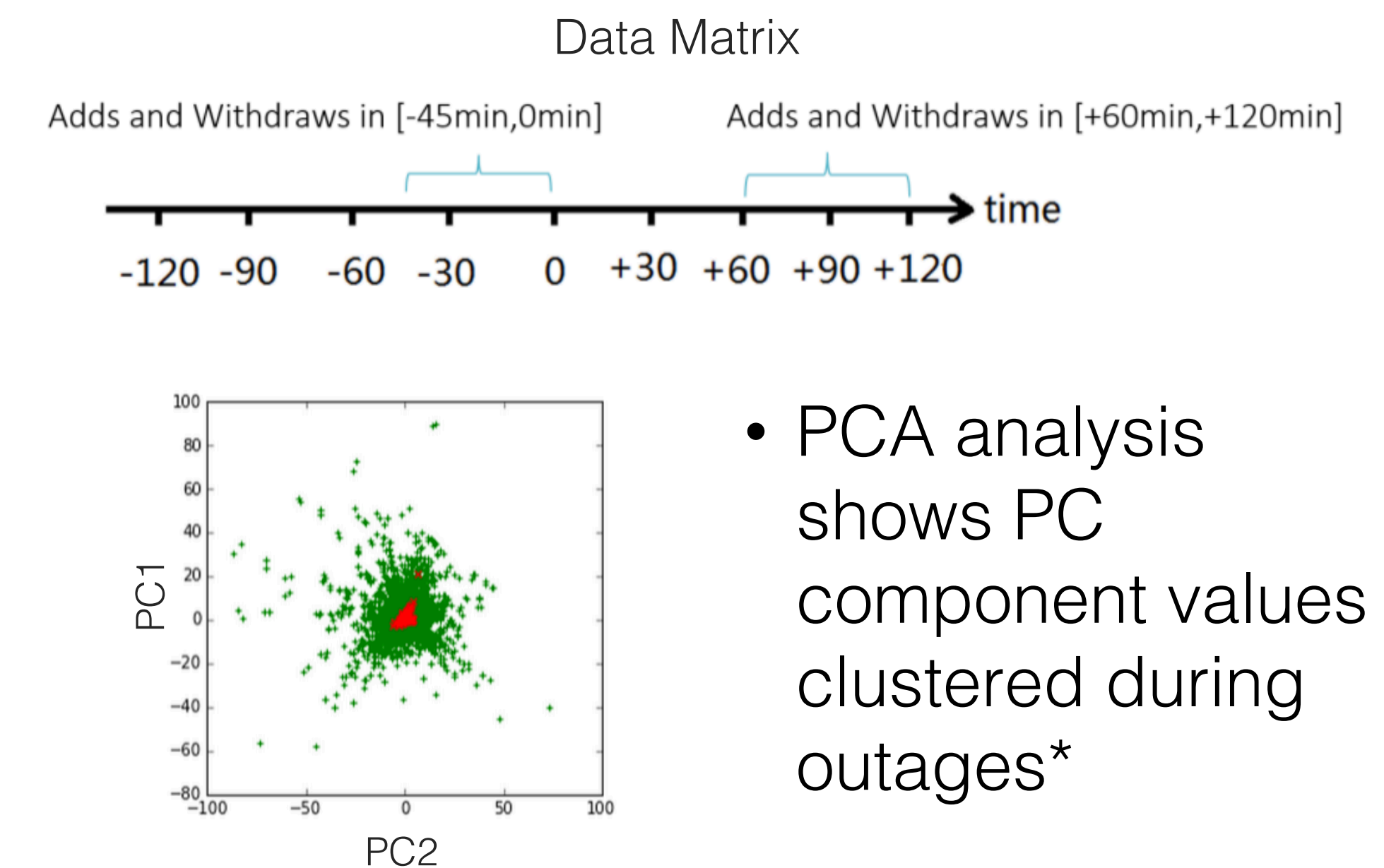
- In many cases, a large churn of BGP updates is observed before and after outage
- However, there are cases where either no BGP churn is seen or no data plane outage is seen



- Some BGP peers do not see any activity during the outage
- In most cases, peers see Withdraw followed by Announcement

Modeling BGP Activity

- Can we mathematically model BGP activity during outage?



- PCA analysis shows PC component values clustered during outages*

Visualization

- Prototype visualization of the outages on Google Maps at: iodb.netsec.colostate.edu
- Supports BGP prefix and country based queries

Further Directions

- Provide more statistics on how often overlap in outages occurs per peer
- Use data plane outage from RIPE Atlas^[2]
- API to query findings in near-real time