BTP Presentation

Mapping the Maze: A Study of Internet shutdowns across the world

Ritik Malik
2018406

●●●

BTP Track : Research

BTP Advisors
Dr. Sambuddho Chakravarty
Dr. Aasim Khan

Internet Shutdown

- An absolute restriction placed on the use of internet services
- Limited to mobile internet or the wired broadband, or both
- Intentional vs unintentional
- Shutdown vs outages

Motivation

- Unknown procedure
- Huge economic loss
- Shutdown not a solution
- Even more problematic in pandemic

Problem Statement

- ★ How do various governments implement these shutdowns?
- ★ Are the same techniques implemented across all the ISPs?
- ★ Can we correlate historical shutdowns with some publicly available datasets?
- ★ Can we predict shutdowns in the future after analyzing the current trend?

Definitions :

- **Autonomous System :**
  - ➢ Collection of IP routing prefixes - /24, /18, /16, *etc.*
  - ➢ Under network operators
  - ➢ BHARTI AIRTEL AS9498,   VODAFONE AS38266

- **Border Gateway Protocol :**
  - ➢ Exchange routing & reachability information among AS
  - ➢ Interior Border Gateway Protocol (iBGP)
  - ➢ Exterior Border Gateway Protocol (eBGP)

Hypothesis

★ Stop advertising the BGP paths in showdown region

(pulling the plug)

Data Collection

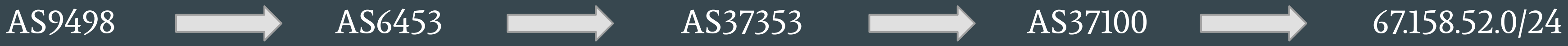
University of Oregon Route Views Archive Project

- Historical BGP information about the global routing system
- 31 collectors across the world
- Access to historical BGP dumps
- Dumps recorded every 2 hours

Data Collection

General output of a routeviews dump :

9498, 6453, 37353, 37100, 67.158.52.0/24



AS9498 → AS6453 → AS37353 → AS37100 → 67.158.52.0/24

- ➢ 100 - 140 unique paths
- ➢ Paths should decrease on shutdown

Previous Approach

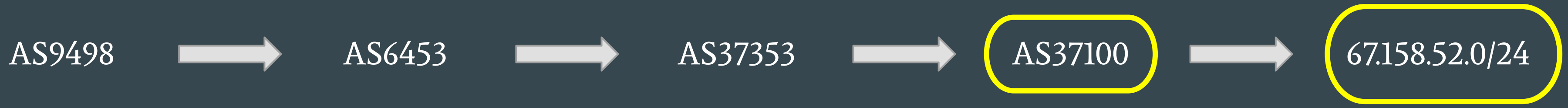
- ➢ Finding current prefixes from datasets like IPInfo, CIDR report
- ➢ Using these prefixes to correlate historical shutdown events

The Problem

- Current prefixes might not work for historical events
- Prefixes are changed overtime
- Generate false positives

The Solution

- Use the prefixes from historical data directly
- Sort the prefixes AS-wise
- Indeed we find noticeable number of prefixes that would not exist in current dataset

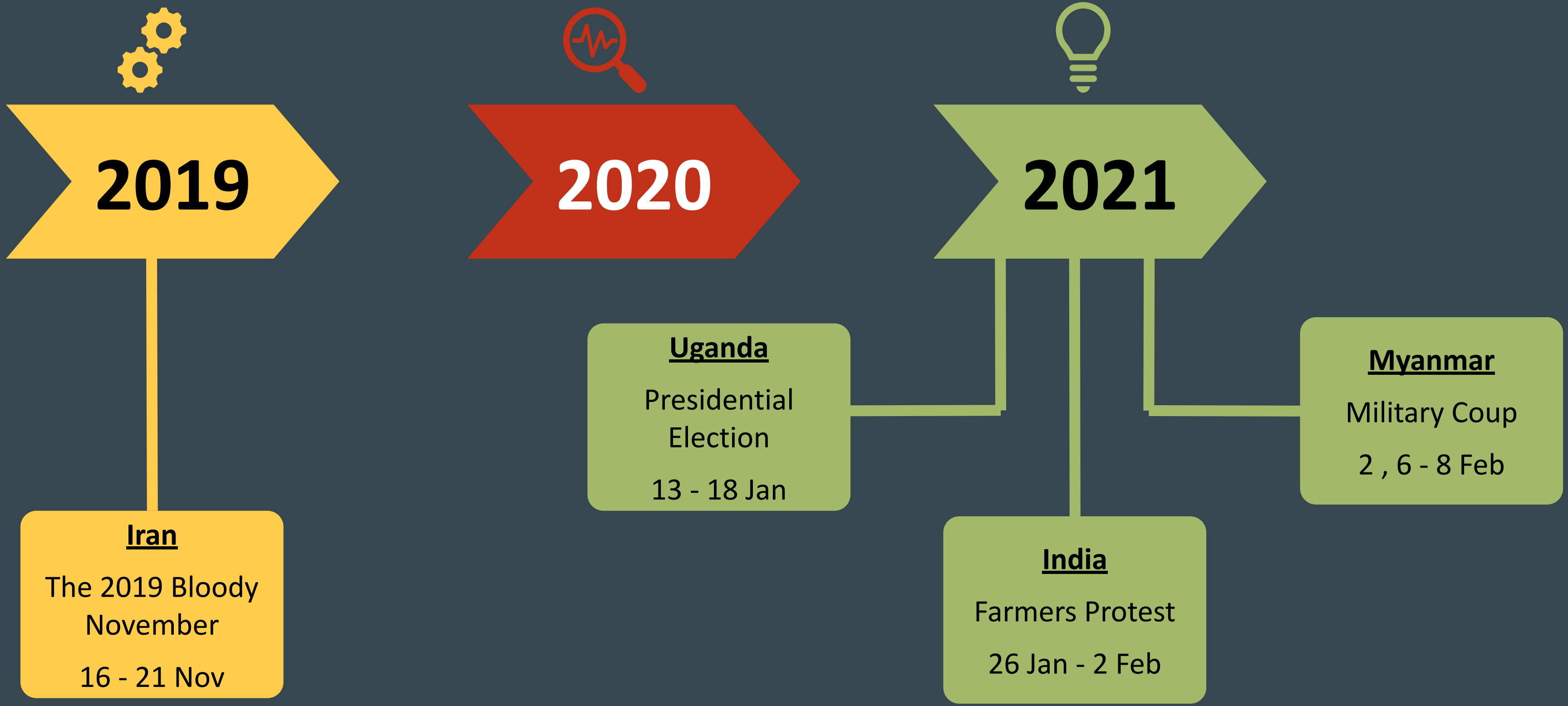


AS9498 → AS6453 → AS37353 → AS37100 → 67.158.52.0/24

New Pipeline

- Efficient Storage : mongoDB vs Py dicts
- Less memory usage : 6 GB now vs 24 GB earlier
- Incorporate the new technique for selecting prefixes
- Execution time reduced significantly : 7 hrs now vs 36 hrs earlier

Timeline



2019

Iran

The 2019 Bloody November

16 - 21 Nov

2020

2021

Uganda

Presidential Election

13 - 18 Jan

India

Farmers Protest

26 Jan - 2 Feb

Myanmar

Military Coup

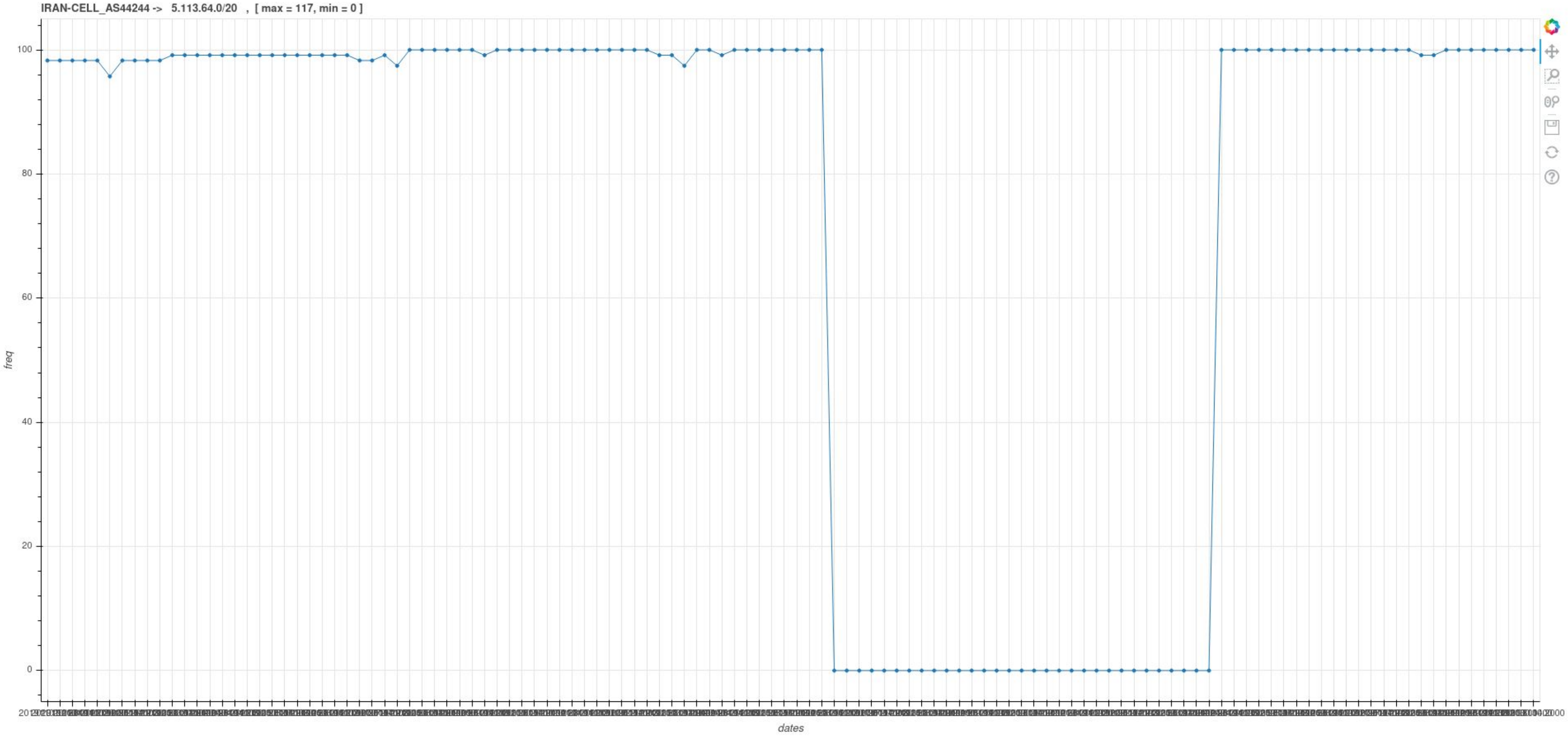
2 , 6 - 8 Feb

Case Study 1

- ➢ Country : Iran
- ➢ Shutdown duration : 16 Nov - 21 Nov 2019
- ➢ Reason for shutdown : The 2019 Bloody November
- ➢ Result : Success

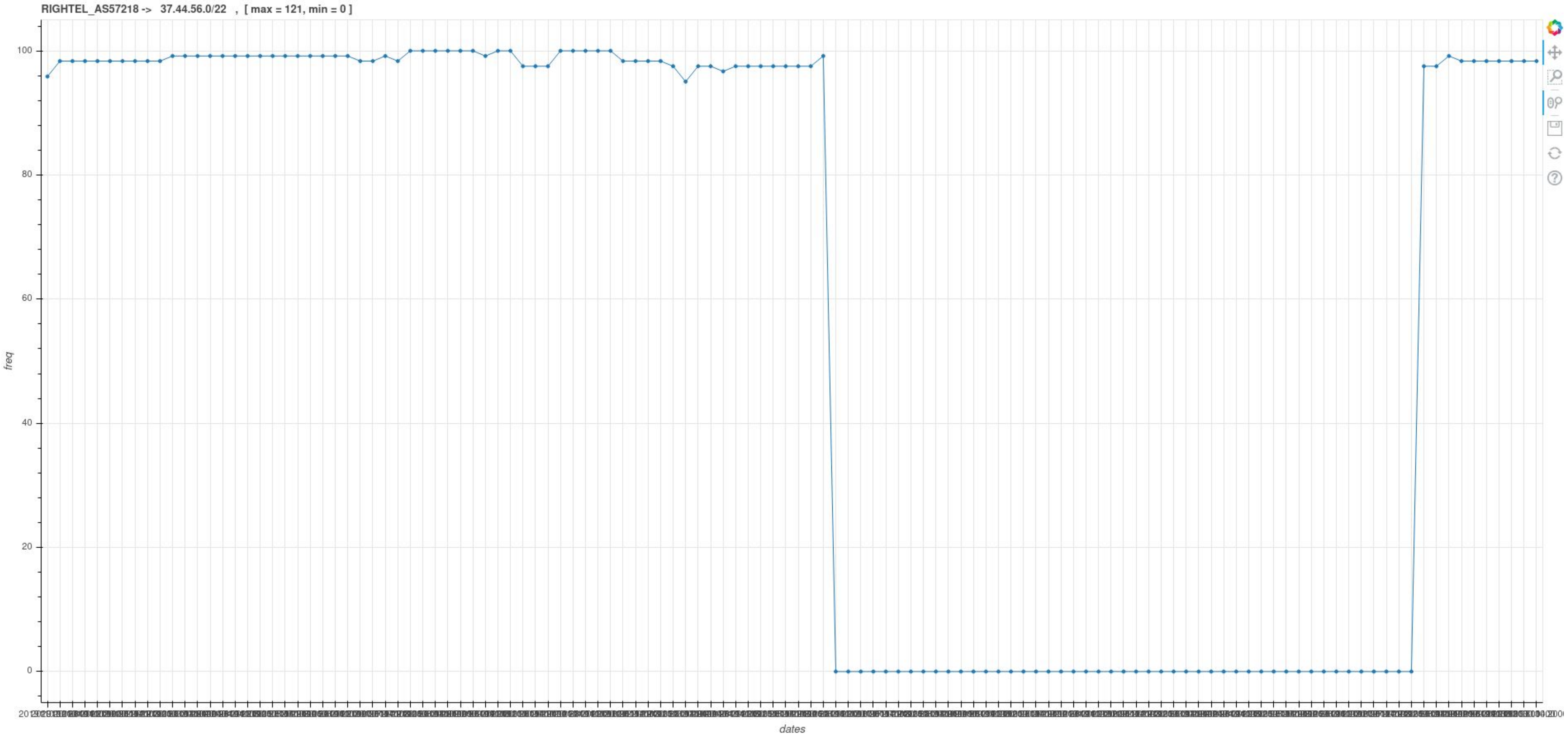
Iran #1

IRAN_CELL_AS4424 -> 5.113.64.0/20 , [max = 117 , min = 0]



Iran #2

RIGHTEL_AS5718 -> 37.44.56.0/22 , [max = 121 , min = 0]

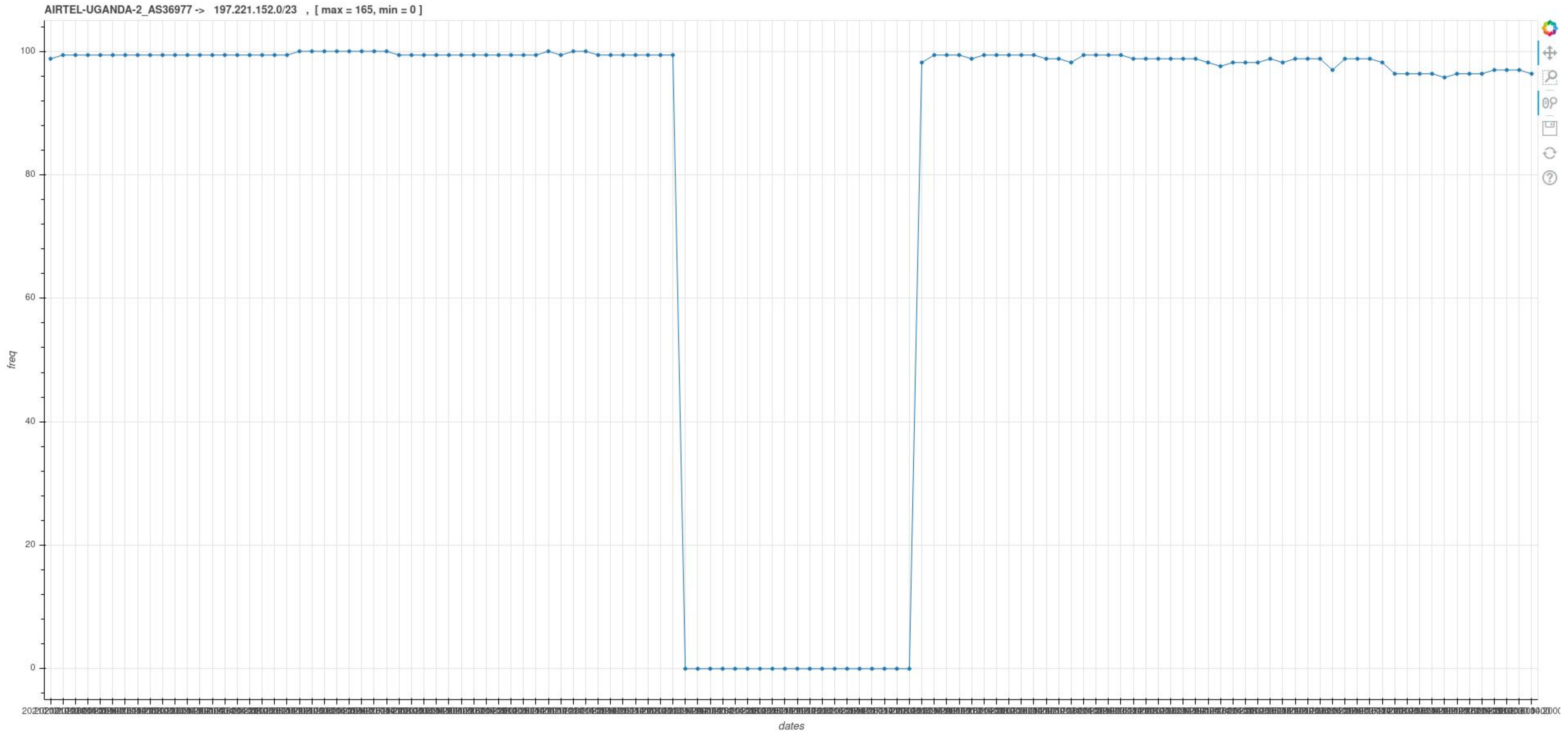


Case Study 2

- Country : Uganda
- Shutdown duration : 13 Jan - 18 Jan 2021
- Reason for shutdown : Presidential election
- Result : Success

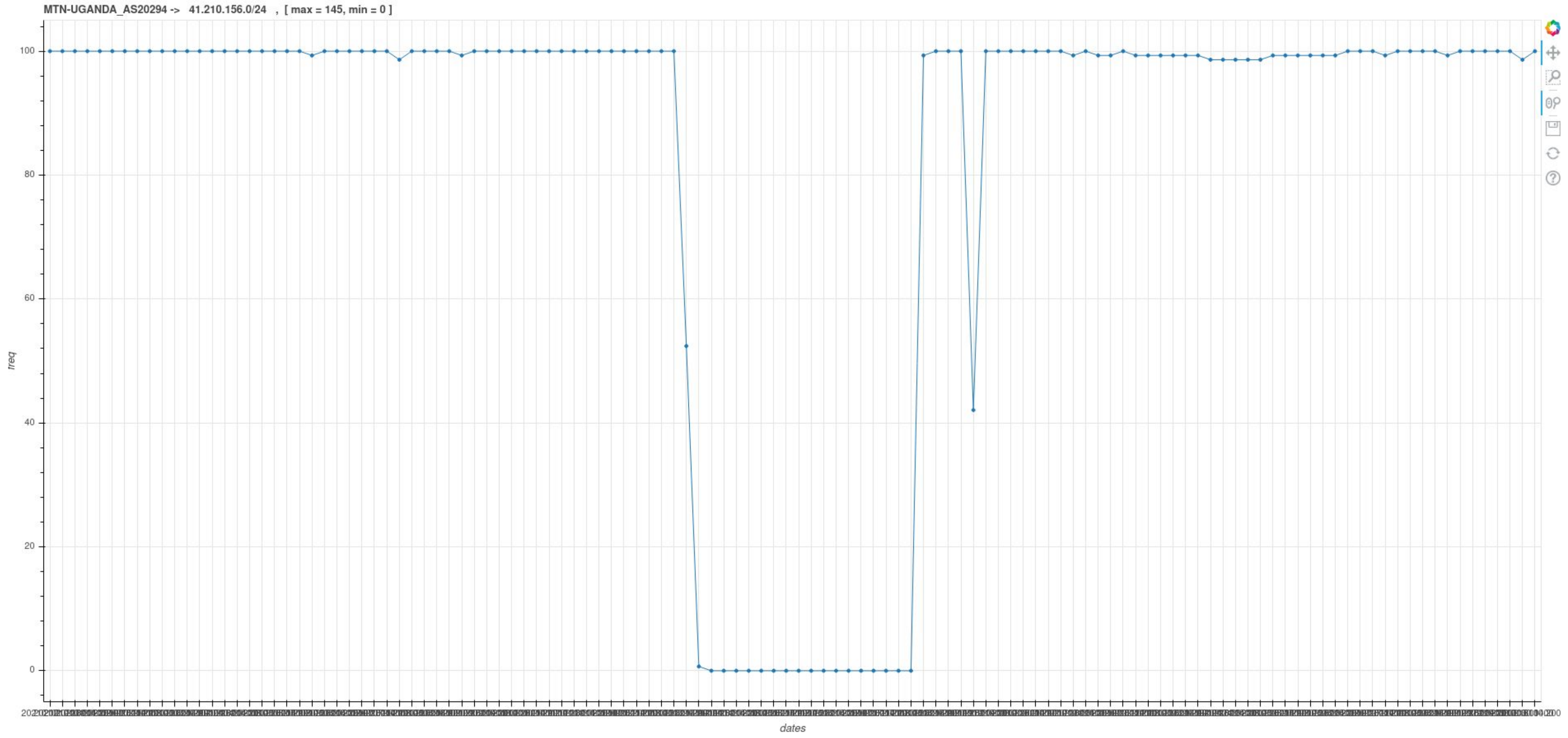
Uganda #1

AIRTEL-UGANDA-2_AS36977 -> 197.221.152.0/23 , [max = 165 , min = 0]



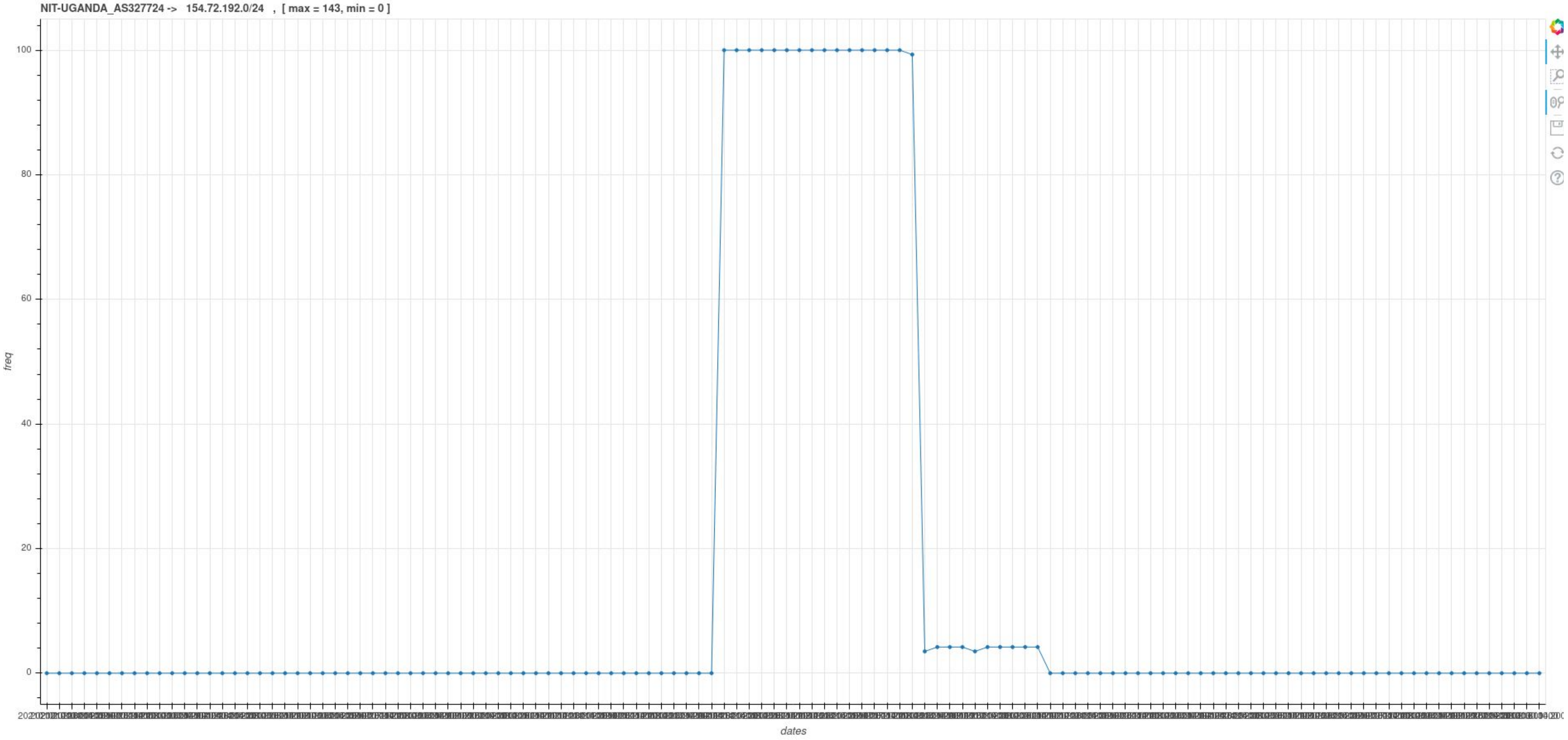
Uganda #2

MTN-UGANDA_AS20294 -> 41.210.156.0/24 , [max = 145 , min = 0]



Uganda #3

NIT-UGANDA_AS32774 -> 154.72.192.0/24 , [max = 143 , min = 0]

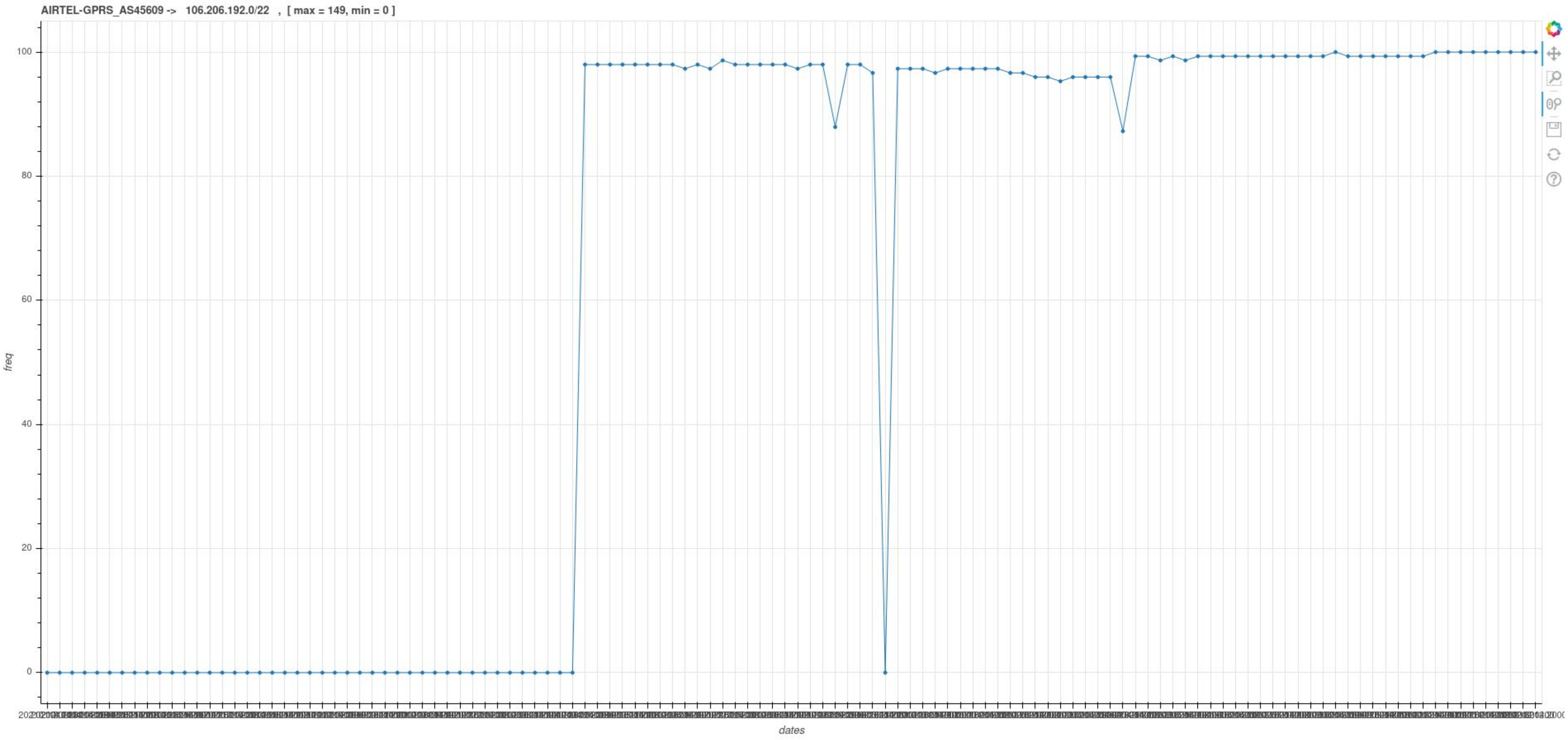


Case Study 3

- Country : India
- Shutdown duration : 26 Jan - 2 Feb 2021
- Reason for shutdown : Farmer protest
- Result : Failure

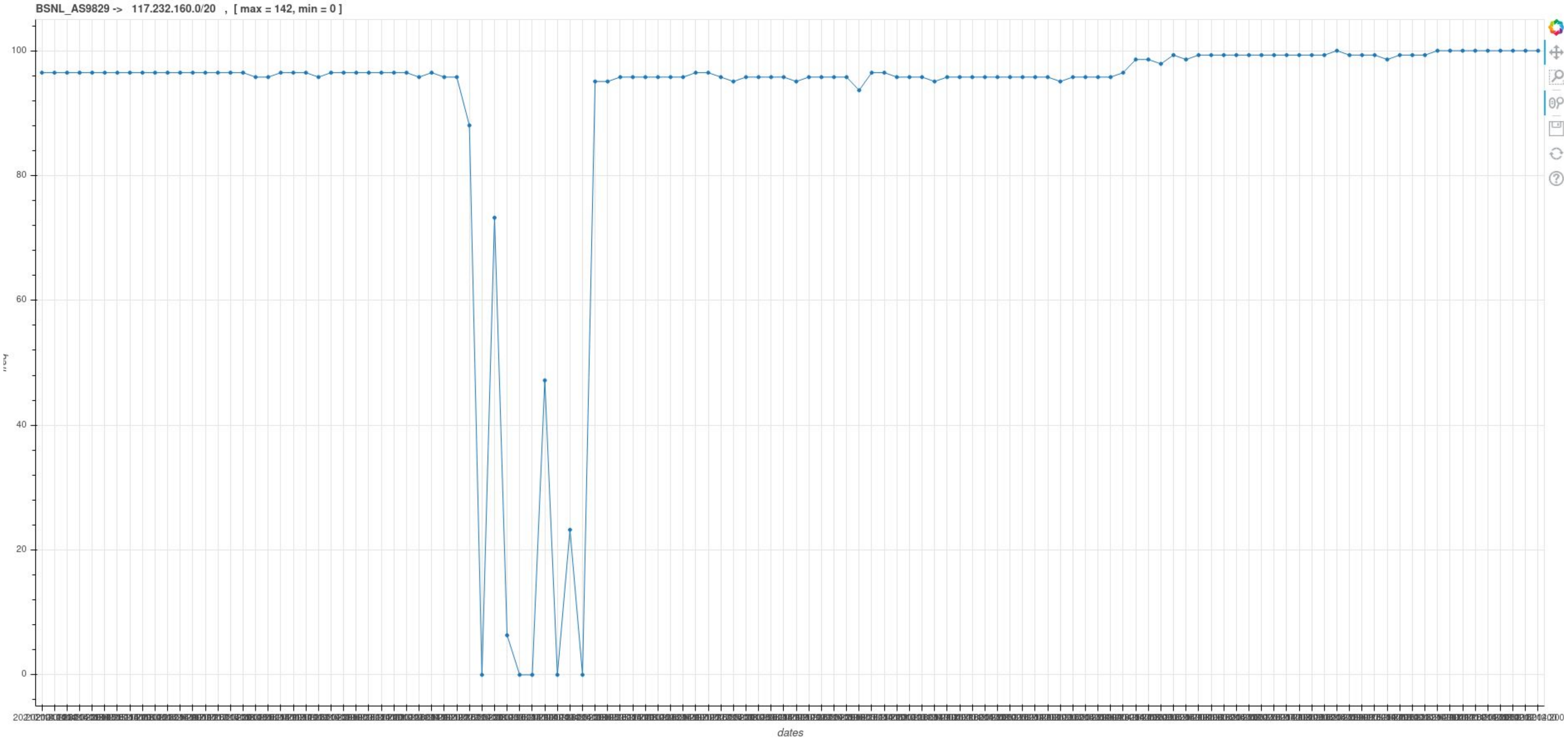
India #1

AIRTEL-GPRS_AS45609 -> 106.206.192.0/22 , [max = 149 , min = 0]



India #2

BSNL_AS9829 -> 117.232.160.0/20 , [max = 142 , min = 0]

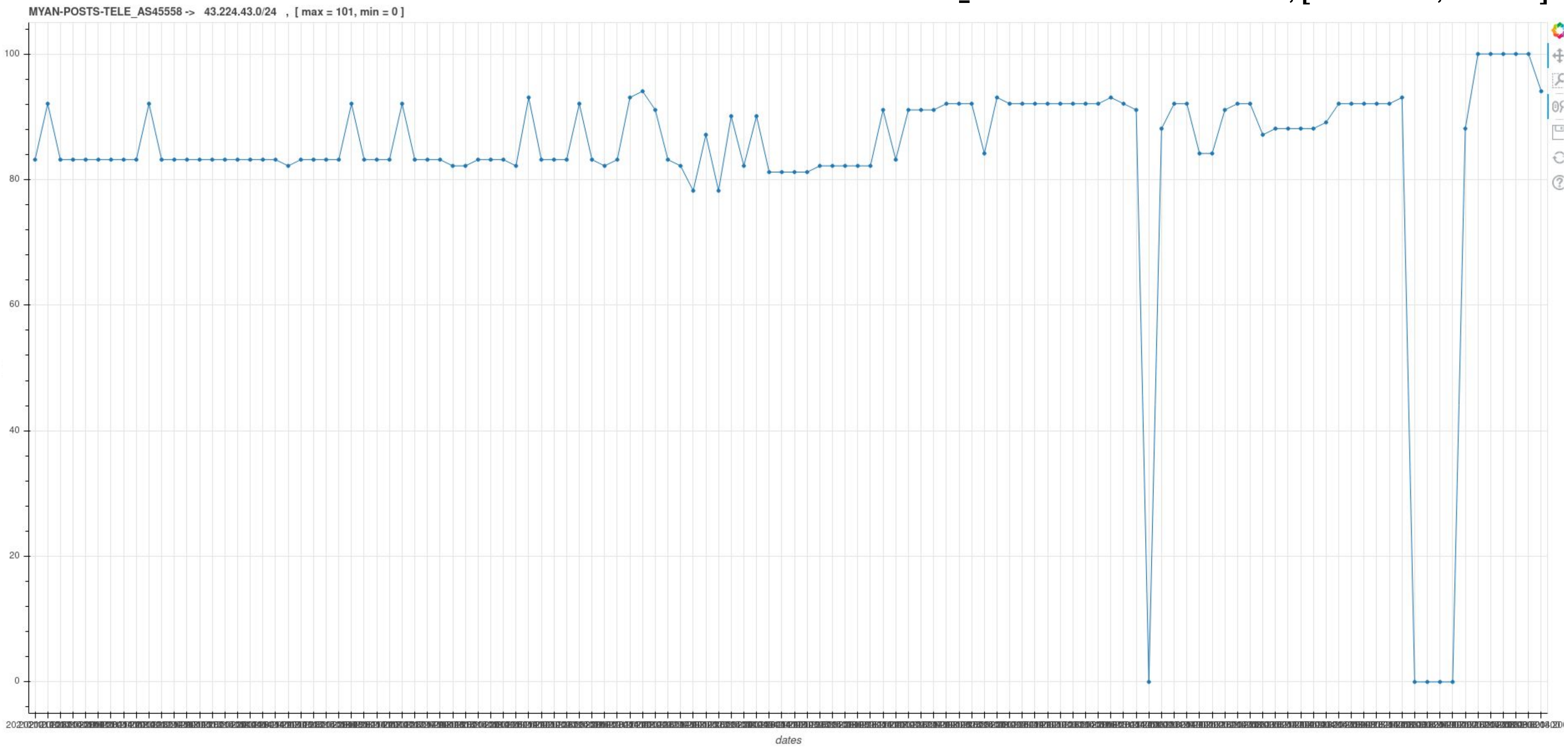


Case Study 4

- Country : Myanmar
- Shutdown duration : 2 Feb & 6 - 8 Feb 2021
- Reason for shutdown : Military coup
- Result : Success

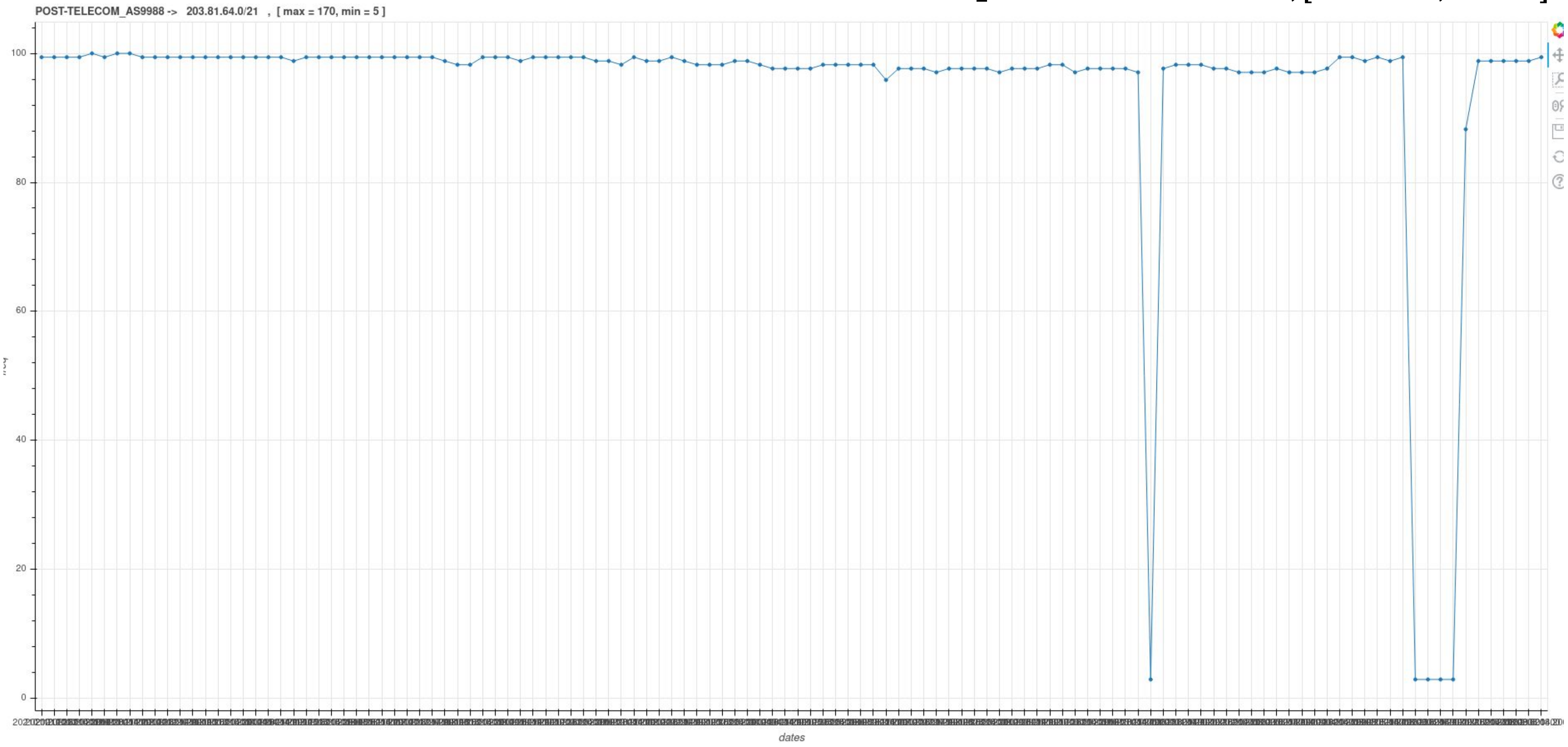
Myanmar #1

MYAN-POSTS-TELE_AS45558 -> 43.224.43.0/24 , [max = 101 , min = 0]



Myanmar #2

POST-TELECOM_AS9988 -> 203.81.64.0/21 , [max = 170 , min = 5]



Conclusion

- Good correlation for Iran, Uganda & Myanmar
- The number of BGP paths decreases for a prefix during an internet shutdown
- Bad or no correlation for India
  - Complicated network map
  - Large number of ASes
  - Microscopic shutdowns
  - Problem in geolocation

Conclusion

- BGP data can be used to correlate historical internet shutdown events

- BGP data is one of the many factors to detect internet shutdowns on a macroscopic scale

- More parameters need to be considered
  - CIADA ARK : Traceroute data
  - Round trip time

Limitations and future work

Limitations

- BGP is dominated by financial relationships than cost and efficiency
- Limited number of Routeviews probes
- Can take hours to register changes in the global routing tables
- Shutdowns/outages went unreported

Limitations and future work

Future Work

- Correlate with other months, when there was no reported incidents of internet shutdowns
- Geolocate the prefixes, & verify with the news
- More of such case studies, focussing on the regional ISPs
- Correlate for other countries, such as Belarus
- Correlate Routeviews with Censys, CAIDA ARK, IODA & RIPE Atlas

Thank You