# Theory Training on BGPWatch:
# BGP Events Monitoring and Diagnosing Platform

**Tsinghua University**

**APAN 57**

**Jan. 29, 2024**

# Outline

- Project Overview
- BGP Hijacking Detection Algorithm
- Functionality of the BGPWatch Platform
- BGP Route Sharing and Looking Glass Platforms
- An Instructional Video of the Platform

# Collaborative Communities

- **Work of 19 Team members (listed alphabetically)**
  - AARNET (AU)
  - APAN-JP (JP)
  - BdREN (BD)
  - CERNET (CN)
  - DOST-ASTI (PREGINET, PH)
  - ERNET (IN)
  - Gottingen University (DE)
  - HARNET (JUCC,  HK)
  - ITB (ID)
  - KREONET (KR)
  - LEARN (LK)
  - MYREN (MY)
  - NREN (NP)
  - PERN (PK)
  - REANNZ (NZ)
  - SingAREN (SG)
  - Surrey University (UK)
  - ThaiREN (TH)
  - TransPAC (US, APAN/GNA-G Routing WG)

APNIC FOUNDATION

清華大學 Tsinghua University

# The 1st Phase of the Project

- **Project Name: Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform**
- **Time: Feb. 24, 2022 – Aug. 23, 2023 (18 months)**
- **Co-PI: Jilong Wang (CERNET, CN)**

  **Chalermpol Charnsripinyo (ThaiREN, TH)**

  **Simon Green (SingAREN, SG)**
- **Funding:**
  - **USD150,000 (APNIC Foundation)**
  - **USD69,660 (in-kind contribution from Tsinghua Univ., China)**

APNIC FOUNDATION

清華大學 Tsinghua University

# Extension Project (2nd phase)

- **Project Name: An Extension of the Ongoing Project "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform" Project**
- **Time: Dec.06, 2023 – June 06, 2025 (18 months)**
- **Co-PI: Jilong Wang (CERNET, CN)**

  **Chalermpol Charnsripinyo (ThaiREN, TH)**

  **Simon Green (SingAREN, SG)**
- **Funding:**
  - **USD85,000 (APNIC Foundation)**

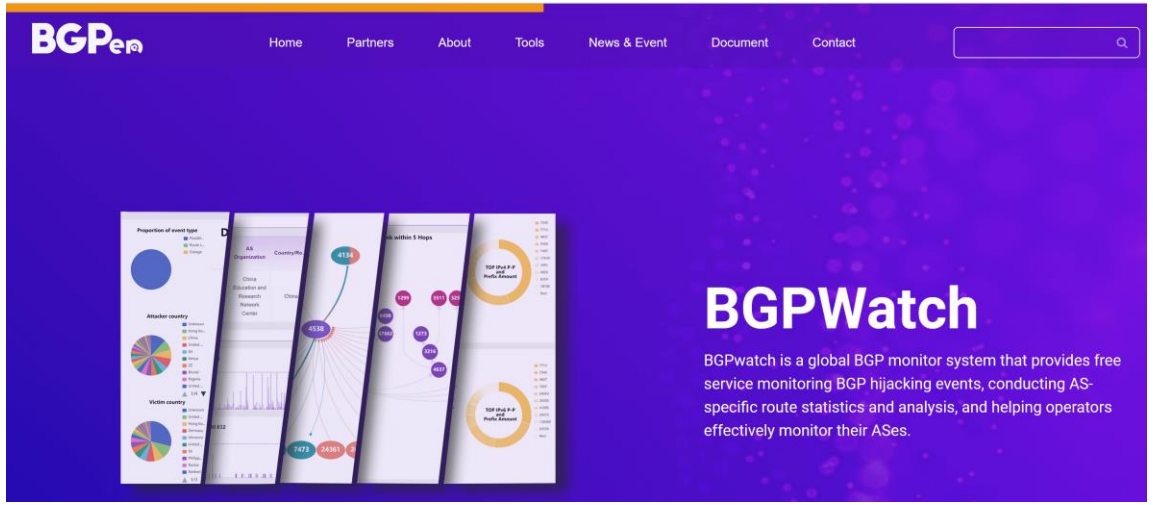
**Welcome new partners to join!**

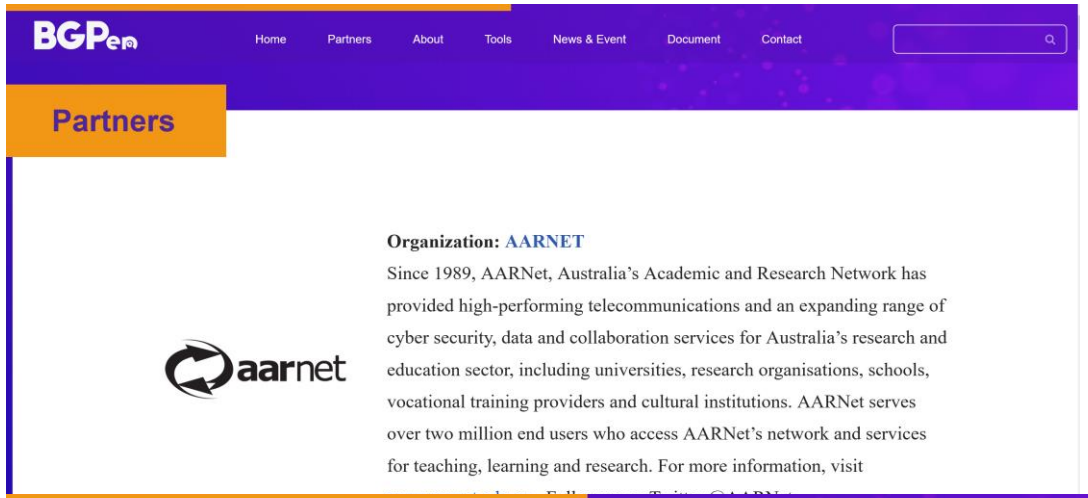
APNIC FOUNDATION

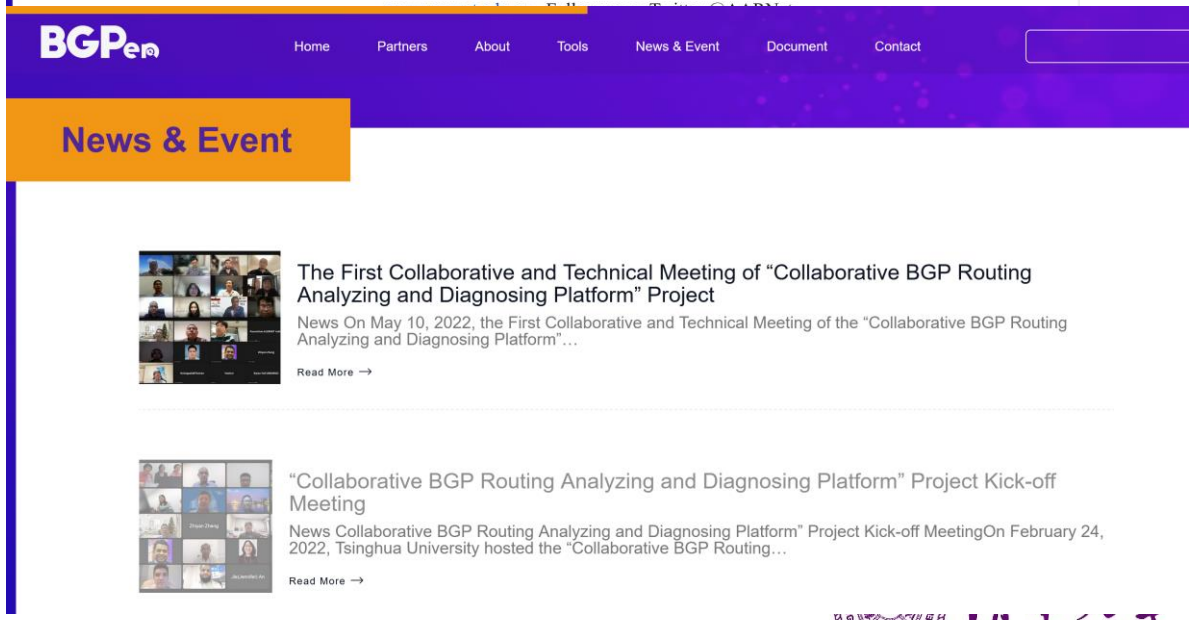
清華大學 Tsinghua University

# Project Website

https://bgper.net






APNIC FOUNDATION

Tsinghua University

# BGP Hijacking Detection Algorithm

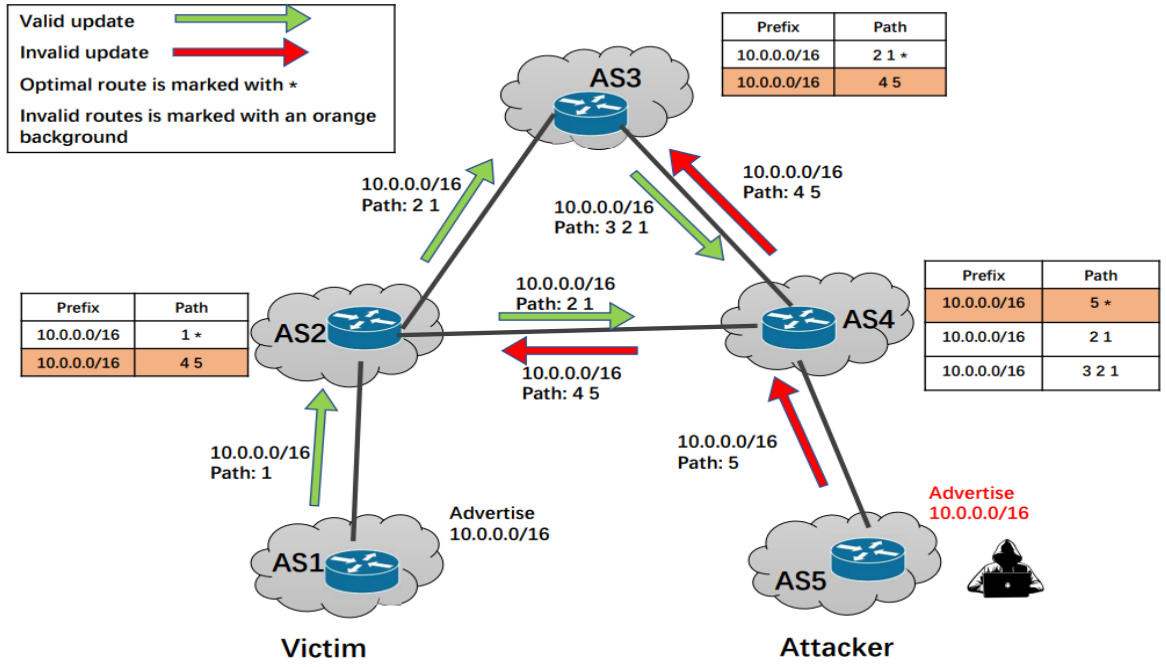
APNIC FOUNDATION

APAN57

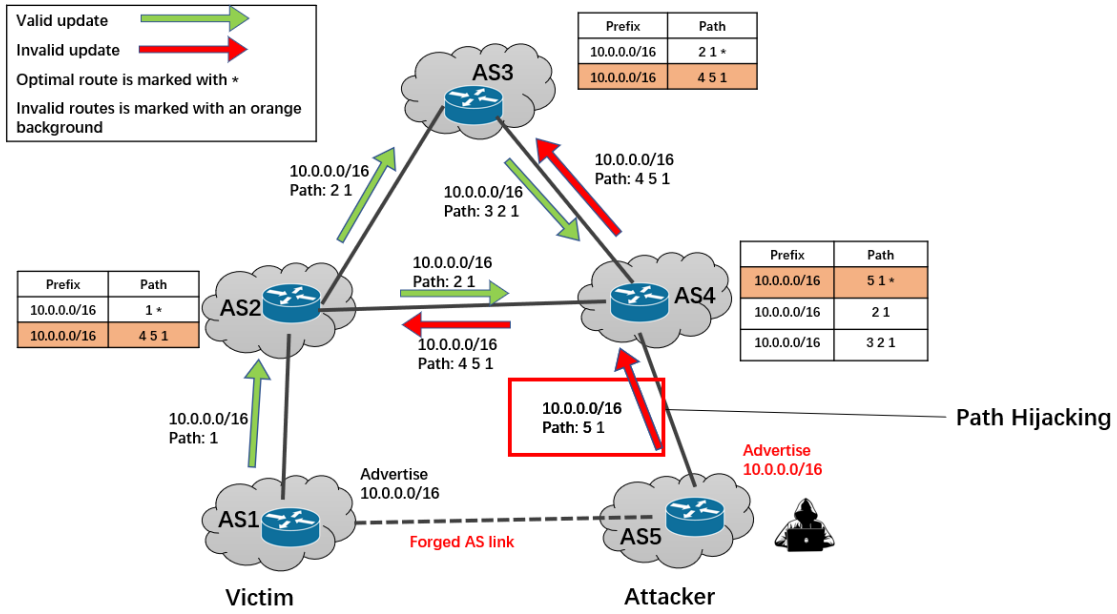
清華大學 Tsinghua University

# BGP Hijacking

BGP hijacking often leads to catastrophic consequences




Prefix Hijacking



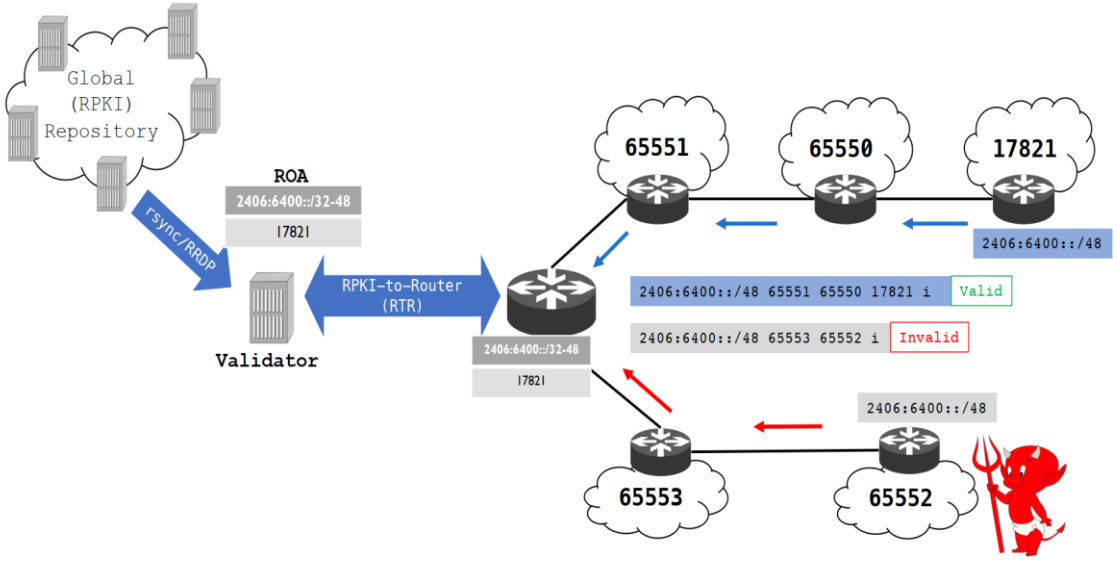

Path Hijacking

APNIC FOUNDATION

清華大學 Tsinghua University

# Solutions to BGP Hijacking

- Preventing the hijacking before it happens
  - RPKI (Resource Public Key Infrastructure)
  - ASPA(Autonomous System Provider Authorization)
- Monitoring to detect the hijacking
  - Route Views
  - RIPE RIS
  - BGPstream
  - GRIP
- Mitigating the hijacking
  - Announcing a more specific prefix
  - Contact other networks to filter routes



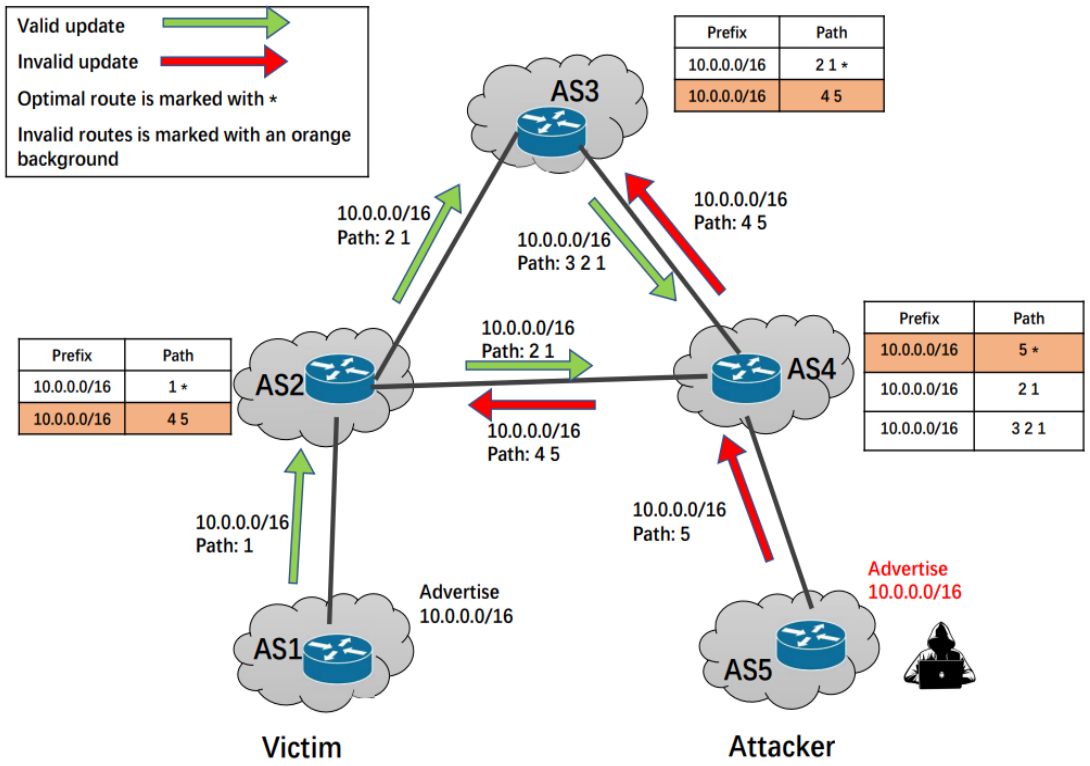

RPKI is very useful, but it's still in the process of deployment

APNIC FOUNDATION

清華大學 Tsinghua University

# MOAS and BGP Prefix Hijacking

- MOAS (Multiple Origin AS) : A single IP prefix has multiple AS numbers claiming to be the origin for that prefix
- MOAS is a critical characteristic of source hijacking
- MOAS is not solely caused by hijacking
  - Multihoming
  - Traffic Engineering
  - DDOS Mitigating
  - Anycast Address

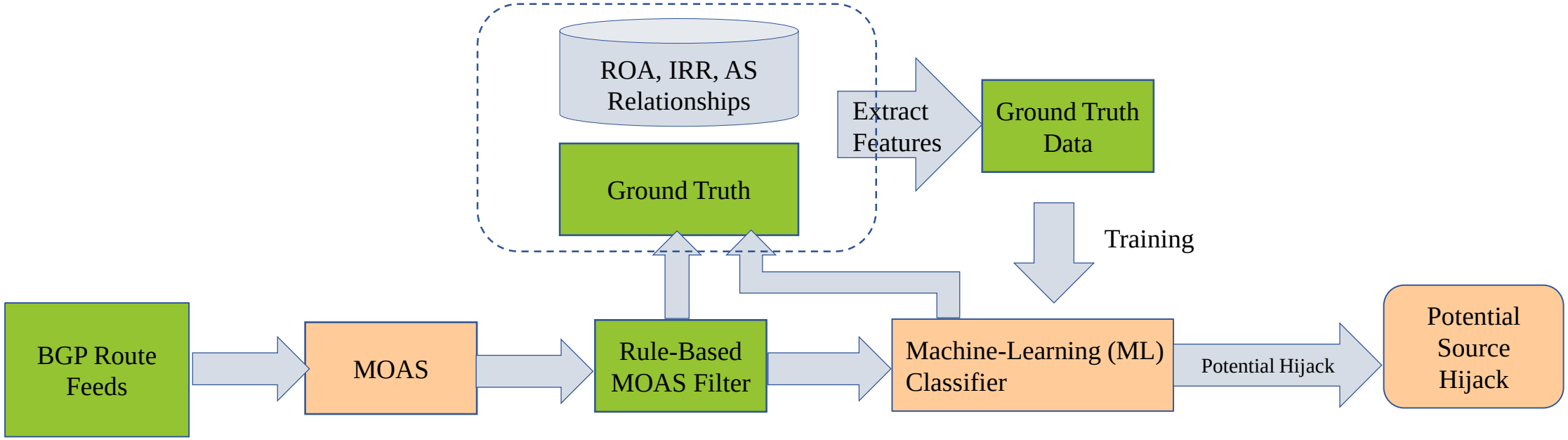



Determining the legitimacy of MOAS is a major challenge

APNIC FOUNDATION

清華大學 Tsinghua University

# Rules Combined with Machine Learning



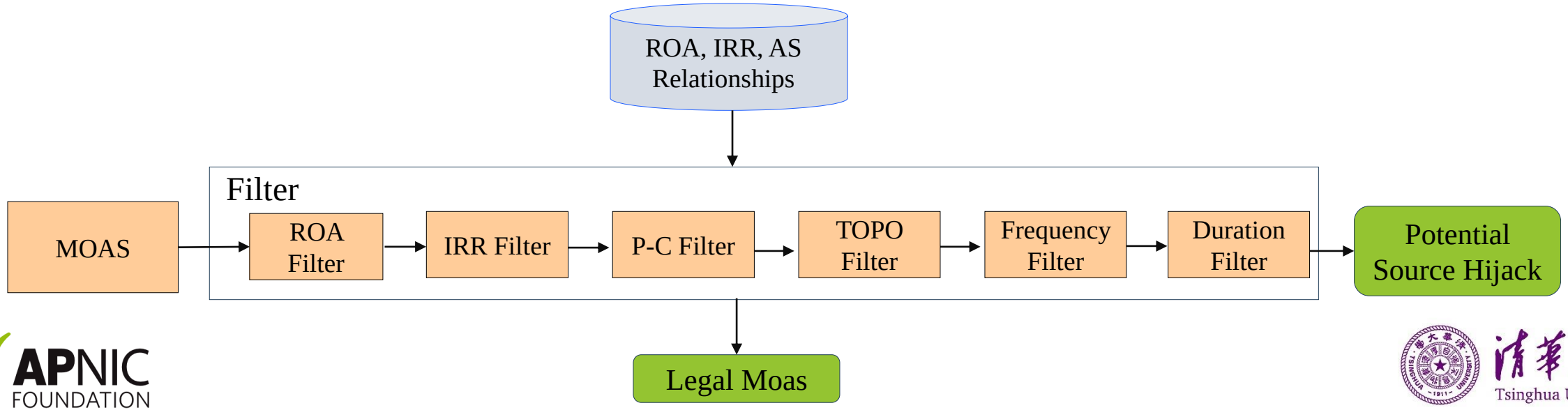

- Initially, employ rule-based filters to sift through a large volume of clearly legitimate MOAS.
- Subsequently, utilize a machine learning classifier to categorize the remaining MOAS.

APNIC FOUNDATION

清華大學 Tsinghua University

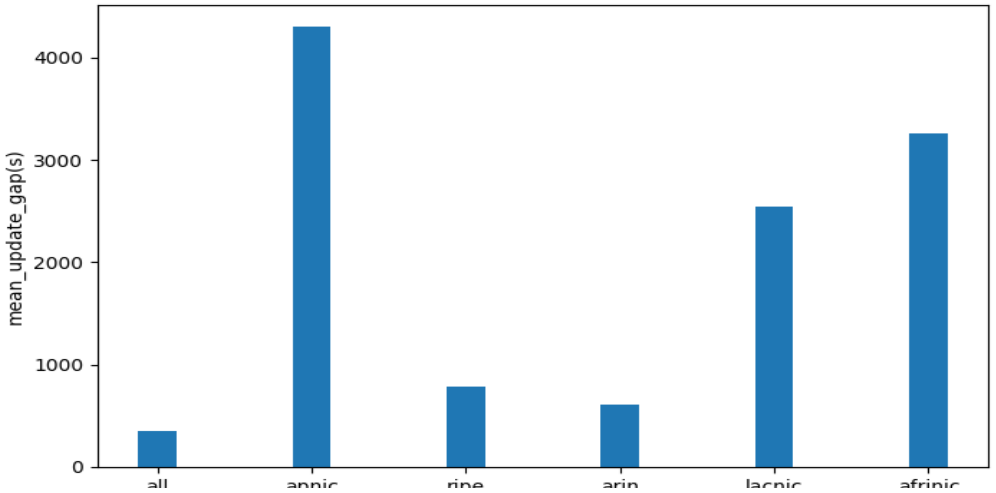
# Rule based Filtering

- ROA Filter: Sync ROA data with Routinator, every 5 minutes
- IRR Filter: Sync every day
- Provider-Customer Filter: CAIDA as relationship database
- TOPO Filter: Hijacker and Victim in the same AS-PATH
- Admin Filter: Same administrator etc., sync with WHOIS every day
- Frequency/Duration Filter: Frequency/Duration longer than a threshold

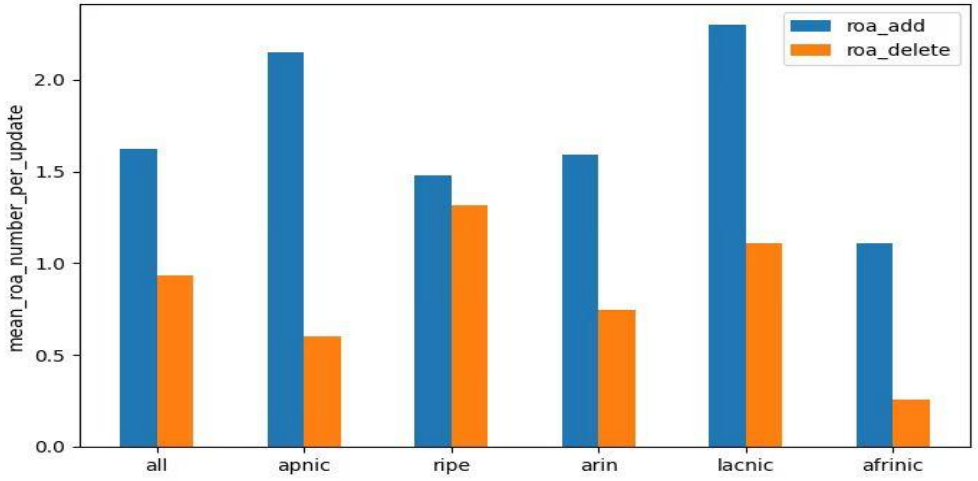


# Sync ROA Data

```
5.45.209.0/24   ['44534']
5.45.212.0/24   ['44534']
5.83.192.0/20   ['- 834', '+ 207645']
5.144.177.0/24  ['- 397373', '+ 142430']
5.144.182.0/24  ['- 30938', '+ 142430']
5.180.216.0/23  ['49544']
5.180.218.0/23  ['49544']
5.253.130.0/24  ['- 34643', '+ 212954']
5.255.236.0/22  ['44534']
14.102.237.0/24 ['- 834', '+ 142036']
14.102.238.0/24 ['- 834', '+ 142036']
14.102.239.0/24 ['- 834', '+ 142036']
23.26.0.0/24    ['- 400402', '+ 11798']
23.26.1.0/24    ['- 400402', '+ 11798']
23.26.2.0/24    ['- 400402', '+ 11798']
23.26.3.0/24    ['- 400402', '+ 11798']
23.26.4.0/24    ['- 400402', '+ 11798']
23.26.5.0/24    ['- 400402', '+ 11798']
23.26.6.0/24    ['- 400402', '+ 11798']
23.26.7.0/24    ['- 400402', '+ 11798']
23.26.8.0/24    ['- 400402', '+ 11798']
23.26.9.0/24    ['- 400402', '+ 11798']
23.26.10.0/24   ['- 400402', '+ 11798']
23.26.11.0/24   ['- 400402', '+ 11798']
23.26.12.0/24   ['- 400402', '+ 11798']
23.26.13.0/24   ['- 400402', '+ 11798']
23.26.14.0/24   ['- 400402', '+ 11798']
23.26.15.0/24   ['- 400402', '+ 11798']
23.26.253.0/24  ['+ 834', '- 14618', '- 16509']
```




**Change Every 400s**




**About 500 prefix ROA data change Per day**

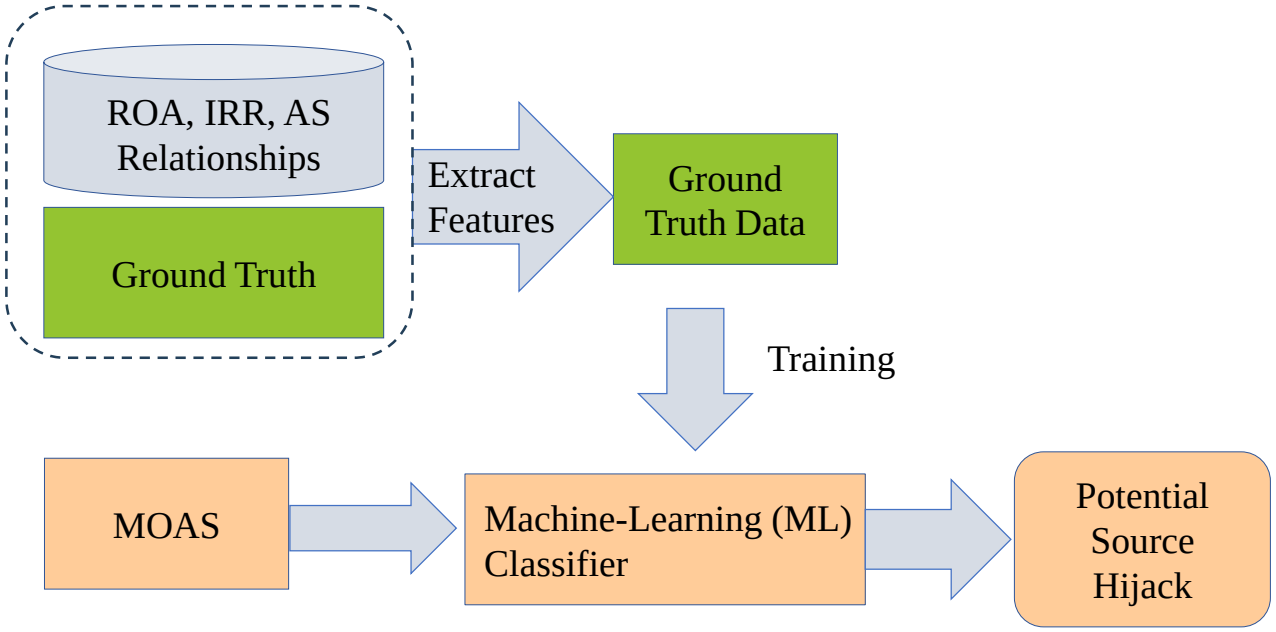
ROA data change frequently, the hijacking system must stay updated

APNIC FOUNDATION

清華大學 Tsinghua University

# Machine Learning based Filtering

- Features
  - MOAS TYPE, AS Rank Difference, Business Relationship, Geographical Relationship,
  - Announcement Activity, Hijacking Activity,
  - Edit Distance of AS name, org, desc,
  - AS type, Degree and Coreness of AS,
  - Prefix type
- Classifier
  - Extreme Randomized Trees




**Result:**

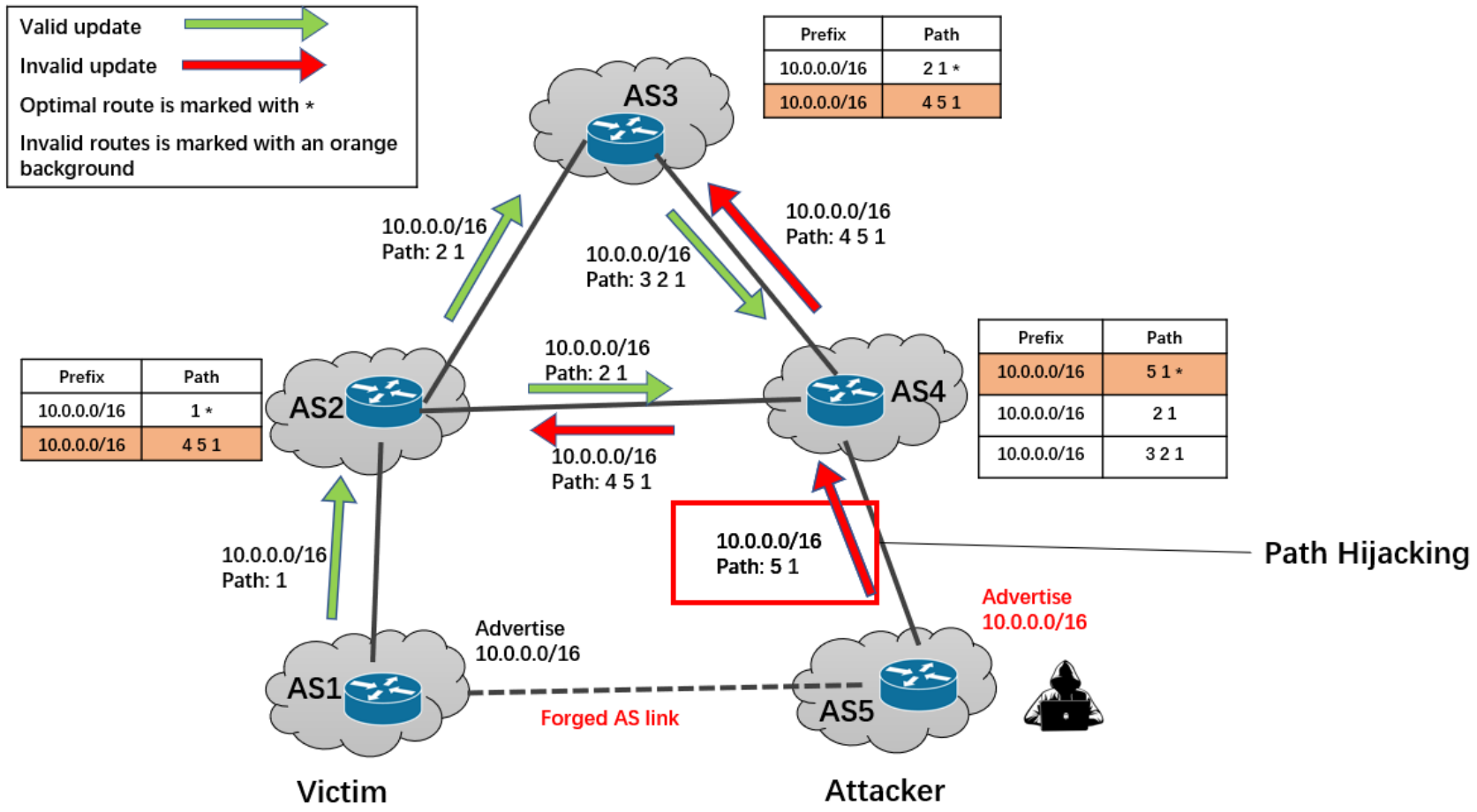
| Precision | Recall | Accuracy |
|---|---|---|
| 0.9410 | 0.9570 | 0.9622 |

APNIC FOUNDATION

清華大學 Tsinghua University

# Detecting Fake AS-PATHs based on Link Prediction

- Path hijacking can evade MOAS, but usually cause unseen AS link

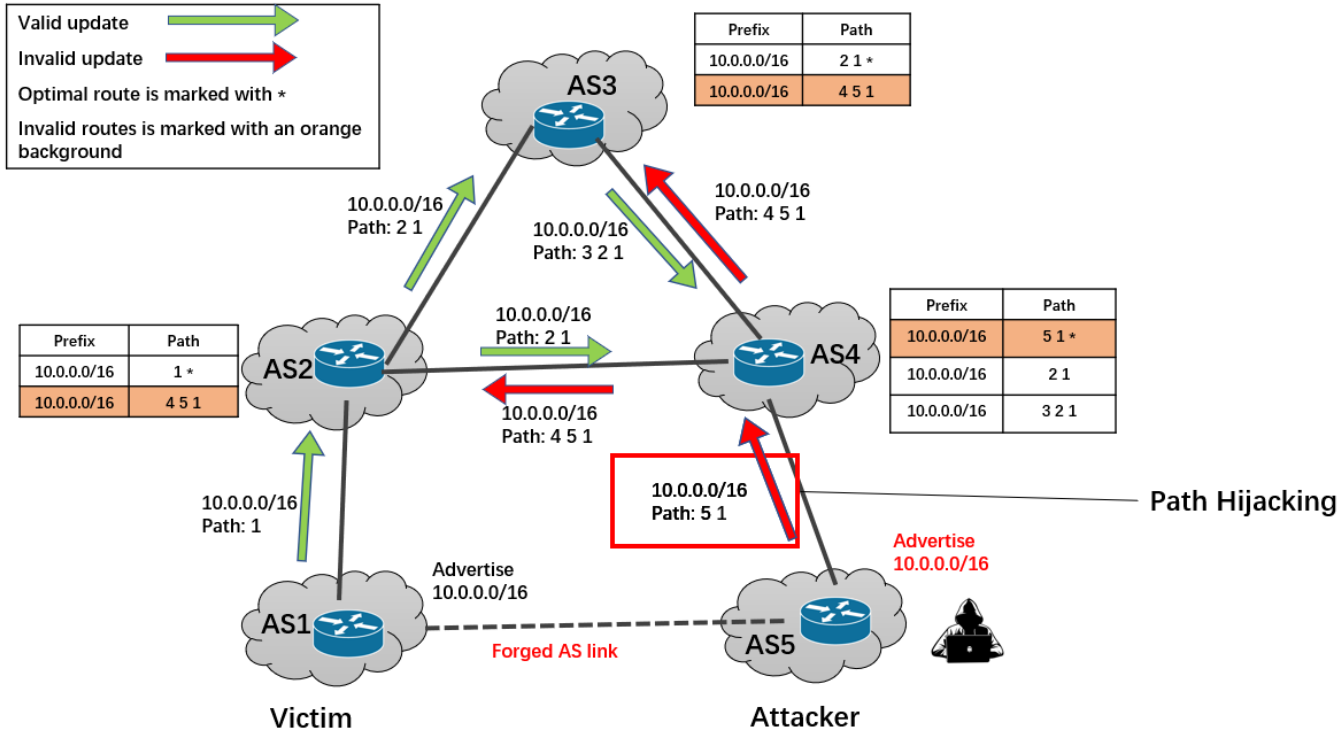



APNIC FOUNDATION

清華大學 Tsinghua University

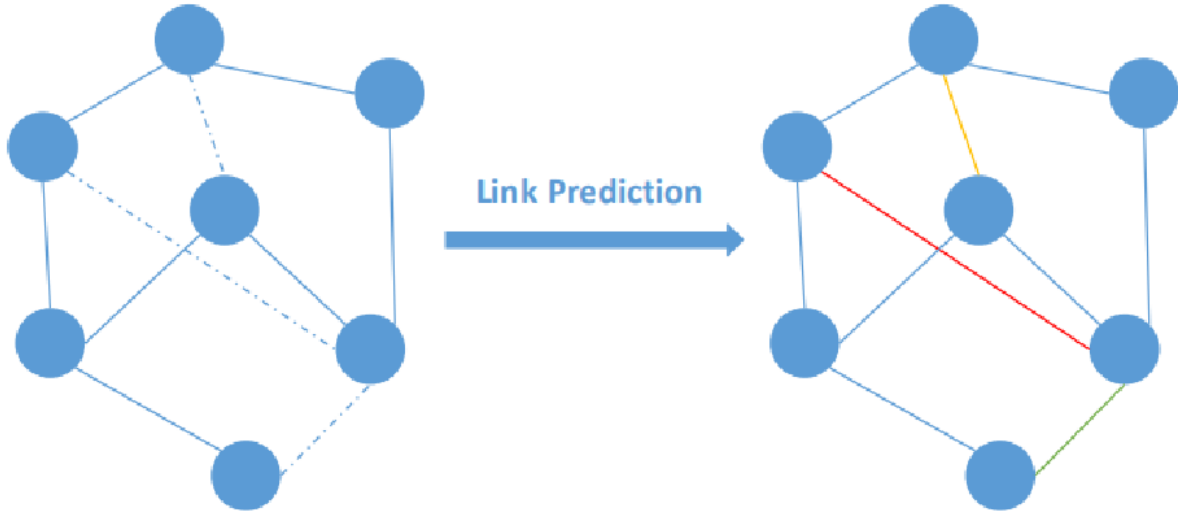
# Path Hijacking Detection

- Hybrid-plane detection technique
  - Treat all unseen links appearing in the control plane as suspicious event
  - Then validate the event through the data-plane probing
- Limitation
  - Unseen links are very common
  - Severe data-plane



# IDEA

- Evaluating the authenticity of unseen links with link prediction and filtering the benign unseen links
- Link prediction: a technique for inferring whether a link is likely to exist between two nodes from an existing observable portion of the network




APNIC FOUNDATION

清華大學 Tsinghua University

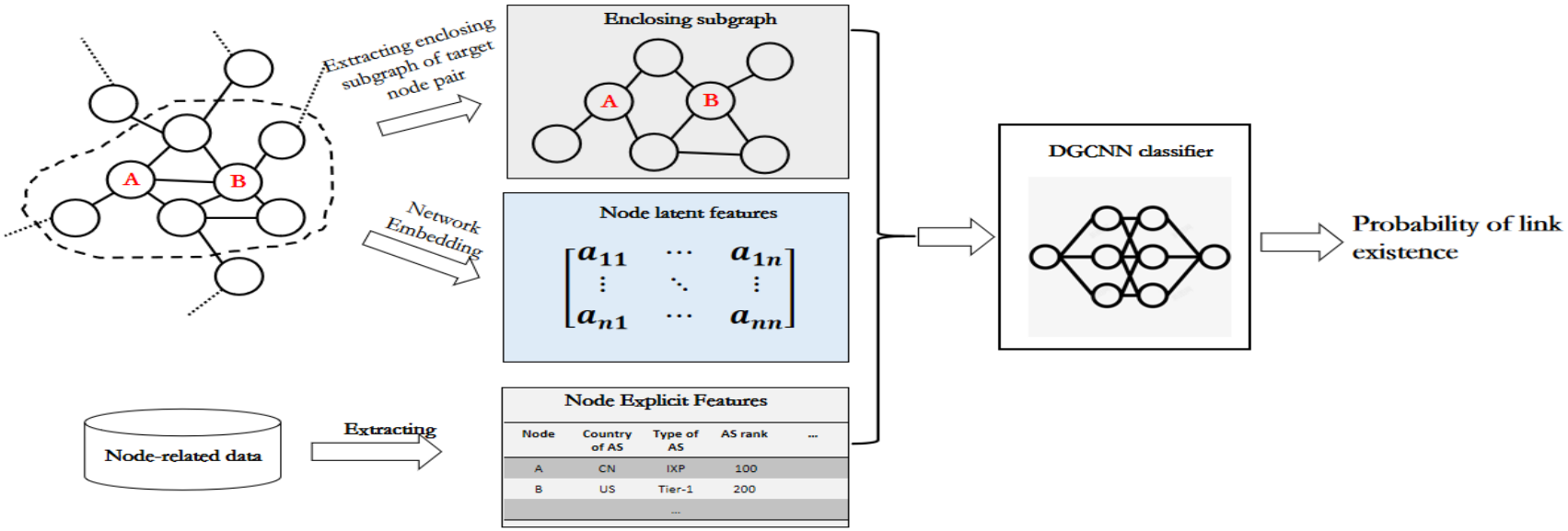
# Is AS Link Predictable?

- Zhuang et al., recently formulates the link prediction as a matrix completion task. Their work explained the predictability of AS link.

- Graph characteristics of AS-level topology
  - power-law distribution
  - negative degree-degree correlation
  - hierarchical
  - AS links usually connect two ASes with the same properties.

# Unseen Link Classification

- We select SEAL as the link prediction algorithm
- CAIDA AS relationship 2021 & AS location、 type and size
- Training with positive and negative samples
- The accuracy reached 0.95 and the AUC reached 0.98



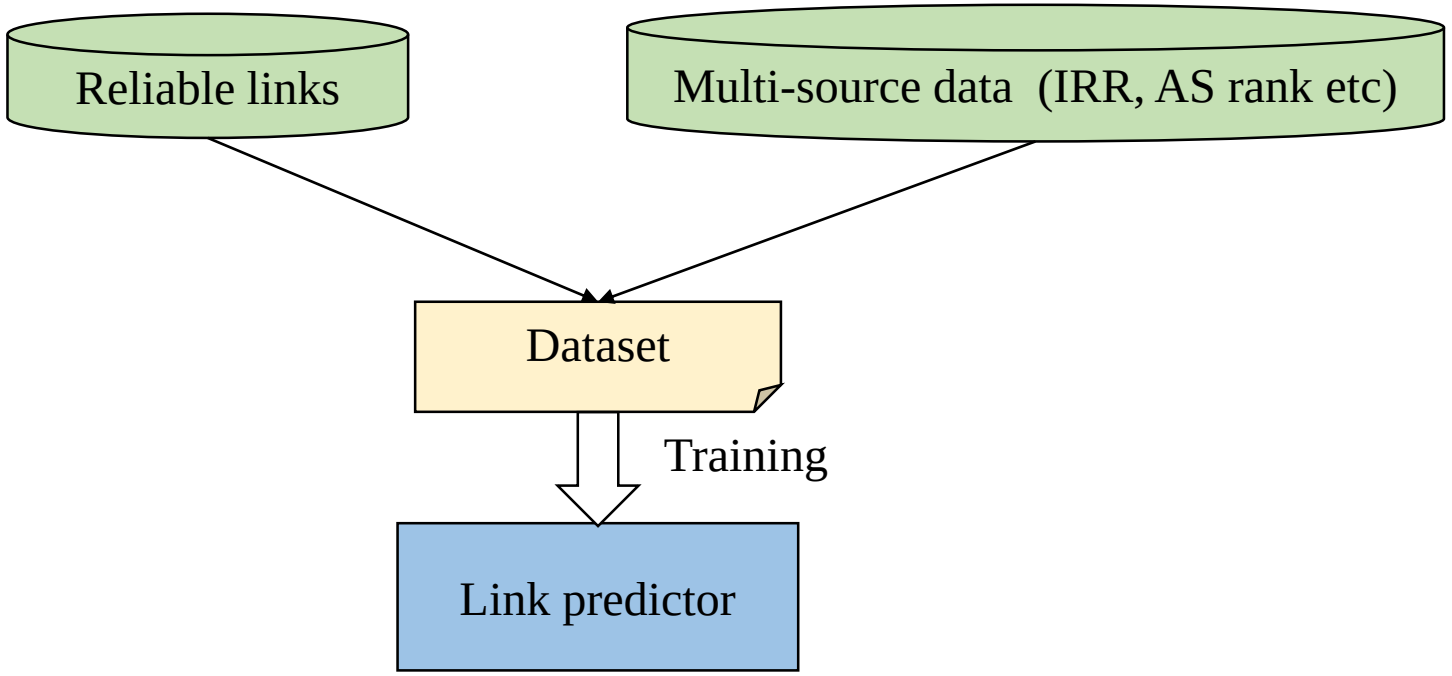

Workflow of SEAL

APNIC FOUNDATION

清華大學 Tsinghua University

# Link Predictor

- To evaluate the authenticity of unseen links
- Trained with reliable links and side information of ASes
- In the framework, it can use any link prediction algorithm

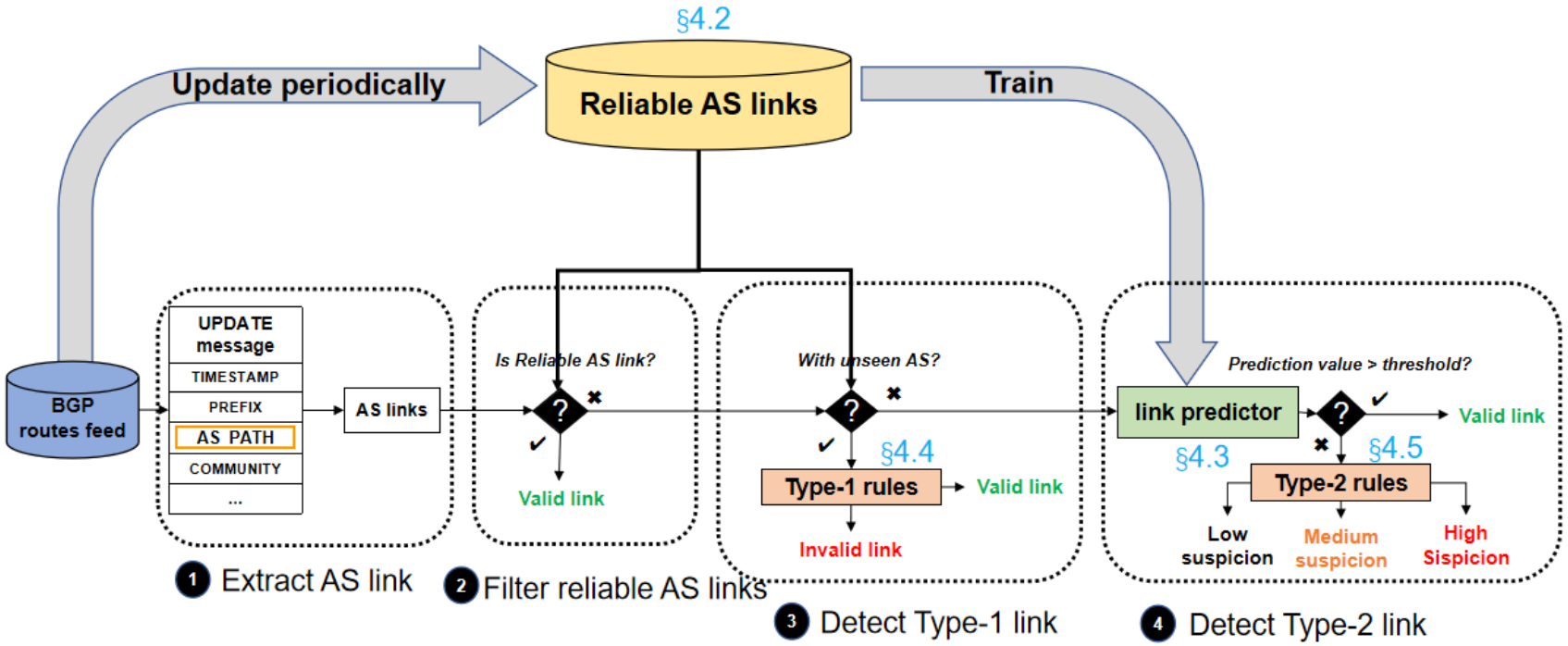



APNIC FOUNDATION

清華大學 Tsinghua University

# Metis: a Fake AS-PATHs Detection Framework

- Based on unseen links
- Combining link prediction and rules
- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level




APNIC FOUNDATION

清華大學 Tsinghua University

# Evaluation

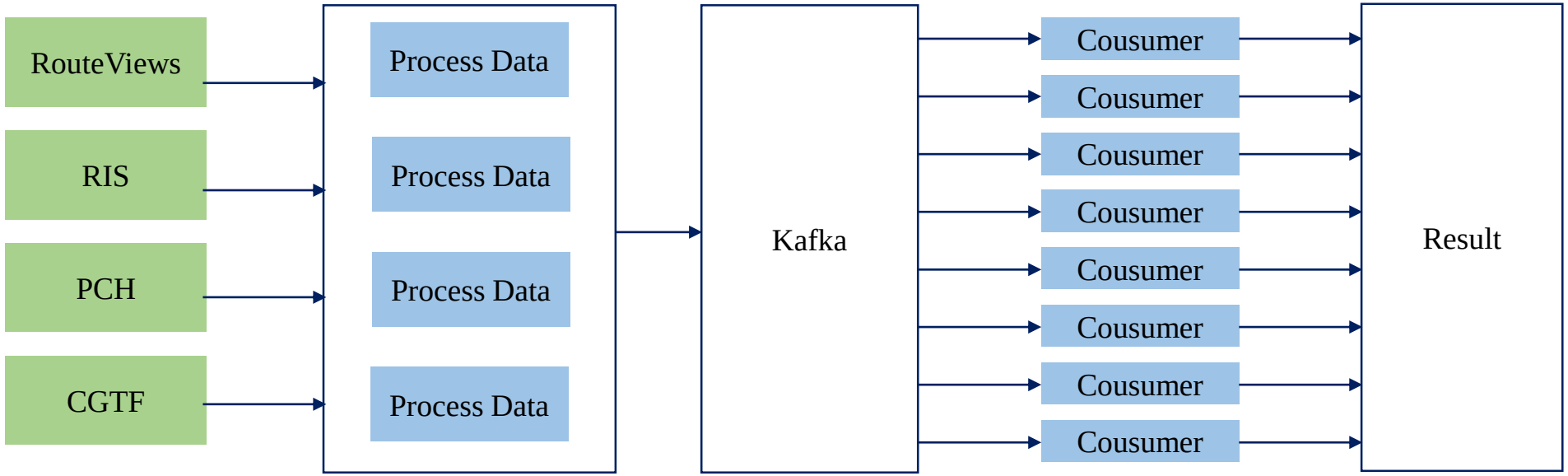
- The accuracy of positive AS-PATHs is about 99.5%
- The accuracy of Type-1 path hijacking is 87.5%

TABLE III: Result of crafted AS-PATHs

| Type of AS-PATH | Number | Reliable link | Type-1 link | Type-2 link | valid AS-PATH | Suspicious AS-PATH | | | | Accuracy |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Type-1 | high | medium | low | |
| GREEN AS-PATHs | 7000 | 11181 | 358 | 187 | 6966 | 5 | 3 | 6 | **20** | **99.5%** |
| Type-1 Misconfiguration | 1000 | 2231 | 108 | 985 | 167 | 0 | 924 | 0 | 0 | 92.4% |
| Type-2 Misconfiguration | 1000 | 2174 | 496 | 582 | 256 | 247 | 528 | 0 | 0 | 77.5% |
| Type-1 hijacking | 1000 | 2213 | 163 | 940 | 125 | 3 | 345 | 481 | 46 | **87.5%** |
| Type-2 hijacking | 1000 | 3018 | 153 | 984 | 493 | 2 | 322 | 176 | 7 | 50.7 % |
| Type-3 hijacking | 1000 | 3706 | 160 | 935 | 700 | 0 | 250 | 50 | 0 | 30.0% |
| Type-1 BGP poisoning | 1000 | 2237 | 236 | 940 | 107 | 14 | 879 | 0 | 0 | 89.3% |
| Type-2 BGP poisoning | 1000 | 2241 | 372 | 2731 | 11 | 15 | 974 | 0 | 0 | 98.9% |

# Parallel Computing and Clusters to Handle Big Routing Data

- There is a huge amount of routing data from RouteViews, RIS, PCH, CGTF.
- We improved the system by Parallel Computing and Clusters.




APNIC FOUNDATION

清華大學 Tsinghua University

# Evaluate Harm Level

- High level: The number of websites contained in the hijacked prefix is greater than 5.
- Middle level: The number of websites contained in the hijacked prefix is greater than 1 but less than 5; The victim AS is Hosting and Cloud Provider.
- Otherwise, the event level is low level.

**high level**

Possible SubHijack Events

**92.205.1.0/24-sub1700403156 Possible SubHijack Events**

Victim AS: 21499
Victim Country: DE ( Germany )
Victim Description: GODADDY-SXB
Start Time: 2023-11-19 14:12:36
During Time: 7:7:17

Hijacker AS: 20773
Hijacker Country: DE (Germany)
Hijacker Description: GODADDY
End Time: 2023-11-19 21:19:53
Time Zone: UTC

Prefix Info: [ [ "92.205.1.0/24", "92.205.0.0/20" ] ]

Website:

electricwhale.com, amplixx.com, altfithealth.com, nelsonfamilyjeweller.com, graduatemonkey.com, woolworthsmuseum.co.uk, alwaysdoubledown.com, argomas.co.uk, bartlettskennels.co.uk, tapasbar1572.nl, blogjam.com, rumstars.com, papiro-bookstore.com, aljameelfood.com, dcaction.org, glintcompany.com, juice.world, millionaire9ja.com, marsh-house.org, solutions-experts.net, themotherchip.co.uk, theglobalrelations.com, carbarandwheelspa.com, expressmedlabs.com, mobilecollective.co.uk, lngcapital.com, factualideas.com, ujcwebsites.co.uk, newsnuggets.co.uk, pitchdarkproductions.co.uk, nathanbeirnemusic.com, undine-scientific.com, themarketinghelpline.com, milamay.co.uk, fixedaccessladders.co.uk, northsurreymidwives.co.uk, cheapbeauty.co.uk, riverhorse.eu, kingoftoys.com.cy, pdfprof.com, globecardiffmusic.com

# Websites in Prefix

- TOP 1M domain:
  - Tranco: https://tranco-list.eu/
  - Cloudflare: https://radar.cloudflare.com/domains
- Convert domain name to IP through nslookup

**92.205.1.0/24-sub1700403156 Possible SubHijack Events**

high level

Possible SubHijack Events

Victim AS: 21499
Victim Country: DE ( Germany )
Victim Description: GODADDY-SXB
Start Time: 2023-11-19 14:12:36
During Time: 7:7:17

Hijacker AS: 20773
Hijacker Country: DE (Germany)
Hijacker Description: GODADDY
End Time: 2023-11-19 21:19:53
Time Zone: UTC

Prefix Info: [ [ "92.205.1.0/24", "92.205.0.0/20" ] ]

Website:

electricwhale.com, amplixx.com, altfithealth.com, nelsonfamilyjeweller.com, graduatemonkey.com, woolworthsmuseum.co.uk, alwaysdoubledown.com, argomas.co.uk, bartlettskennels.co.uk, tapasbar1572.nl, blogjam.com, rumstars.com, papiro-bookstore.com, aljameelfood.com, dcaction.org, glintcompany.com, juice.world, millionaire9ja.com, marsh-house.org, solutions-experts.net, themotherchip.co.uk, theglobalrelations.com, carbarandwheelspa.com, expressmedlabs.com, mobilecollective.co.uk, lngcapital.com, factualideas.com, ujcwebsites.co.uk, newsnuggets.co.uk, pitchdarkproductions.co.uk, nathanbeirnemusic.com, undine-scientific.com, themarketinghelpline.com, milamay.co.uk, fixedaccessladders.co.uk, northsurreymidwives.co.uk, cheapbeauty.co.uk, riverhorse.eu, kingoftoys.com.cy, pdfprof.com, globecardiffmusic.com

# AS TYPE

- Get AS type from ASdb:
  - https://asdb.stanford.edu/
  - ASdb is a research dataset that maps ASN to organizations and up to three industry types using data from business intelligence databases, website classifiers, and a machine learning algorithm.
  - Hosting and Cloud Provider

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | Ongoing Possible Hijack | middle 13886 is Cloud\|IDC or top content provider. | Victim:US/AS13886() Attacker:US/AS7922(COMCAST-IBONE) | 1 | 206.124.104.0/21 | 2024-01-19 04:51:24 | - | - | detail |
| 4 | Possible Hijack | middle 61945 is Cloud\|IDC or top content provider. | Victim:BR/AS52626(NOVANET) Attacker:BR/AS61945() | 1 | 2804:d70:50::/44 | 2024-01-19 03:54:48 | 2024-01-19 04:57:13 | 1:2:25 | detail |

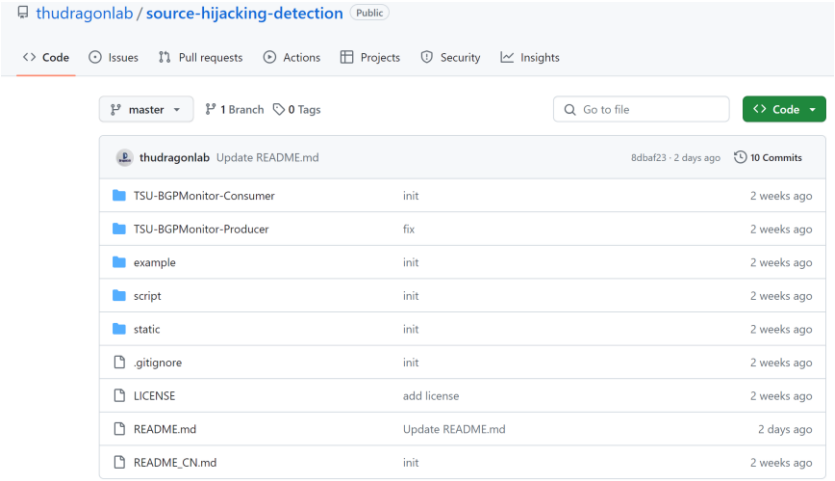
# Open Source

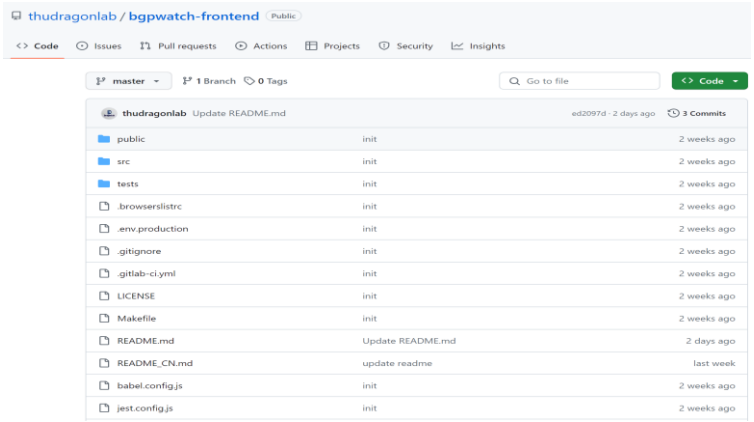
https://github.com/thudragonlab/source-hijacking-detection

https://github.com/thudragonlab/bgpwatch-frontend

https://github.com/thudragonlab/bgpwatch-backend

https://github.com/thudragonlab/bgp-analysis



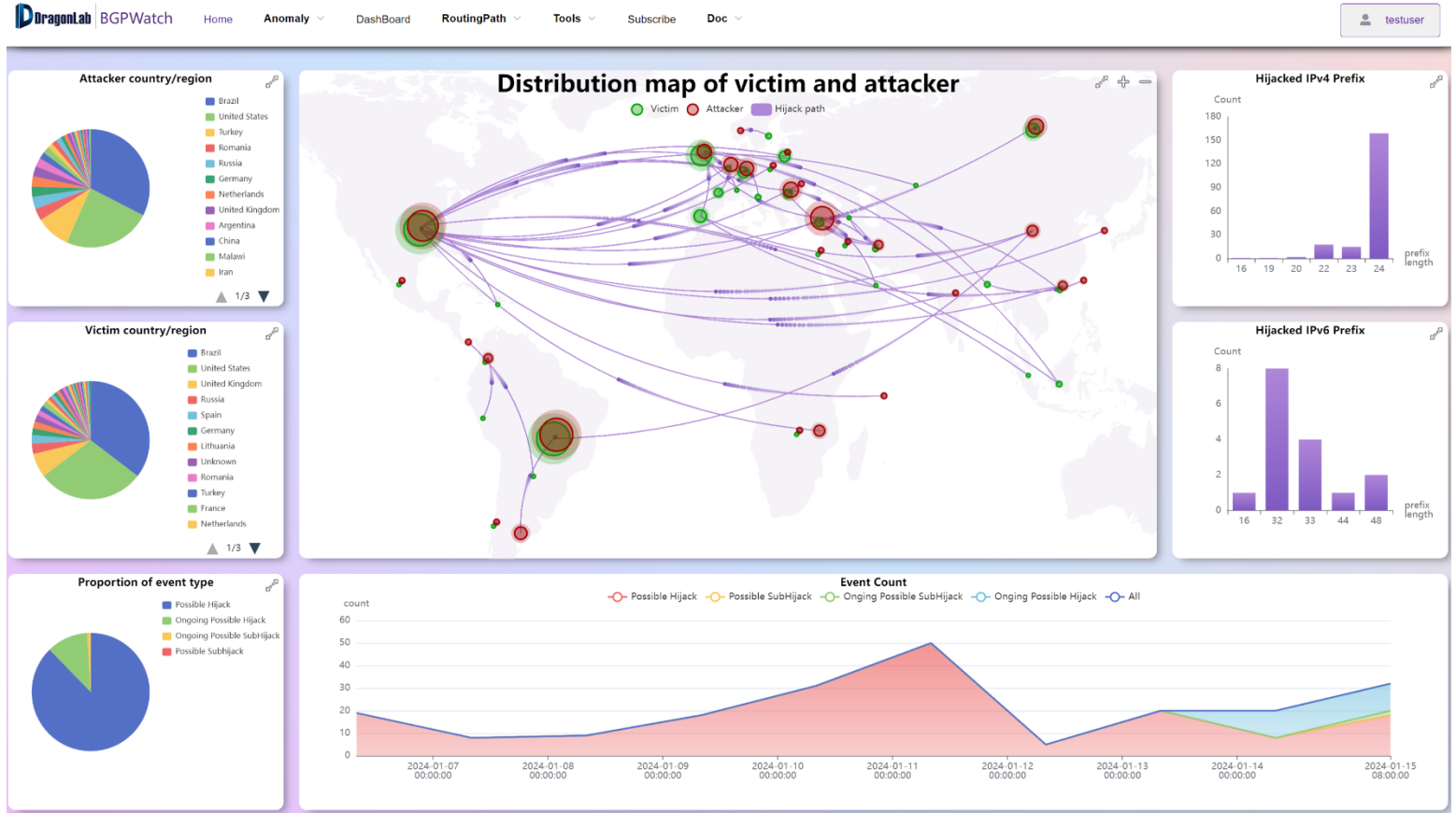

APNIC FOUNDATION

清華大學 Tsinghua University

# Functionality of the BGPWatch Platform

# BGPWatch: Prefix Hijacking Detection Platform

- Knowledge-based real-time BGP hijacking Detection System
- Public BGP event reporting service
- Based on MOAS/subMOAS
- Rely on Domain Knowledge (ROA, IRR, AS relationship, routing path, accumulated information, etc.)




APNIC FOUNDATION

清華大學 Tsinghua University

# BGP Hijacking Detection

DragonLab BGPWatch | Home | Overview | Anomaly | DashBoard | RoutingPath | Country/Region | Organization | Document | Login | Register

Select event type | Select harm level: All | Time zone: GMT+8 | Select time period (by Start Time): 2023-04-13 10:24:41 - 2023-04-23 10:24:41 | Duration: All | Select for event by keywords: Please enter search key

Download

Multi Prefix

| | Event Type | Level | Event Info | Prefix Nu | Prefix Example | Start Time | End Time | Duration | Detail |
|---|---|---|---|---|---|---|---|---|---|
| 221 | Possible Hijack | low | Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR) | 193.4.4.0/24<br>193.4.5.0/24 | 193.4.4.0/24 | 2023-04-13 13:56:24 | 2023-04-13 13:58:24 | 0:2:0 | detail |
| 222 | Possible Hijack | low | Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR) | 2 | 193.4.4.0/24 | 2023-04-13 13:43:36 | 2023-04-13 13:49:53 | 0:6:17 | detail |
| 223 | Possible Hijack | high 68 websites in the prefix. | Victim:US/AS398823 (PEGTECHINC-AP-02) Attacker:ZA/AS328608(Africa-on-Cloud-AS) | 1 | 154.93.32.0/19 | 2023-04-13 11:47:11 | 2023-04-14 06:47:14 | 19:0:3 | detail |
| 224 | Possible SubHijack | low | Victim:US/AS6253 (PRUASN) Attacker:US/AS8030(WORLDNET5-10) | 2 | prefix: 161.151.112.0/22 subprefix: 161.151.114.0/24 | 2023-04-13 10:52:15 | 2023-04-13 13:58:59 | 3:6:44 | detail |

Total 224 | 1 | ... | 18 | 19 | 20 | 21 | 22 | 23

Supports searching and downloading

APNIC FOUNDATION

清華大學 Tsinghua University

# Features – Event Level Evaluation

- Evaluating event impact based on importance of AS and prefix

high level

Possible SubHijack Events

**92.205.1.0/24-sub1700403156 Possible SubHijack Events**

Victim AS: 21499

Victim Country: DE ( Germany )

Victim Description: GODADDY-SXB

Start Time: 2023-11-19 14:12:36

During Time: 7:7:17

Hijacker AS: 20773

Hijacker Country: DE (Germany)

Hijacker Description: GODADDY

End Time: 2023-11-19 21:19:53

Time Zone: UTC

Prefix Info: [ [ "92.205.1.0/24", "92.205.0.0/20" ] ]

Website:

electricwhale.com, amplixx.com, altfithealth.com, nelsonfamilyjeweller.com, graduatemonkey.com, woolworthsmuseum.co.uk, alwaysdoubledown.com, argomas.co.uk, bartlettskennels.co.uk, tapasbar1572.nl, blogjam.com, rumstars.com, papiro-bookstore.com, aljameelfood.com, dcaction.org, glintcompany.com, juice.world, millionaire9ja.com, marsh-house.org, solutions-experts.net, themotherchip.co.uk, theglobalrelations.com, carbarandwheelspa.com, expressmedlabs.com, mobilecollective.co.uk, lngcapital.com, factualideas.com, ujcwebsites.co.uk, newsnuggets.co.uk, pitchdarkproductions.co.uk, nathanbeirnemusic.com, undine-scientific.com, themarketinghelpline.com, milamay.co.uk, fixedaccessladders.co.uk, northsurreymidwives.co.uk, cheapbeauty.co.uk, riverhorse.eu, kingoftoys.com.cy, pdfprof.com, globecardiffmusic.com

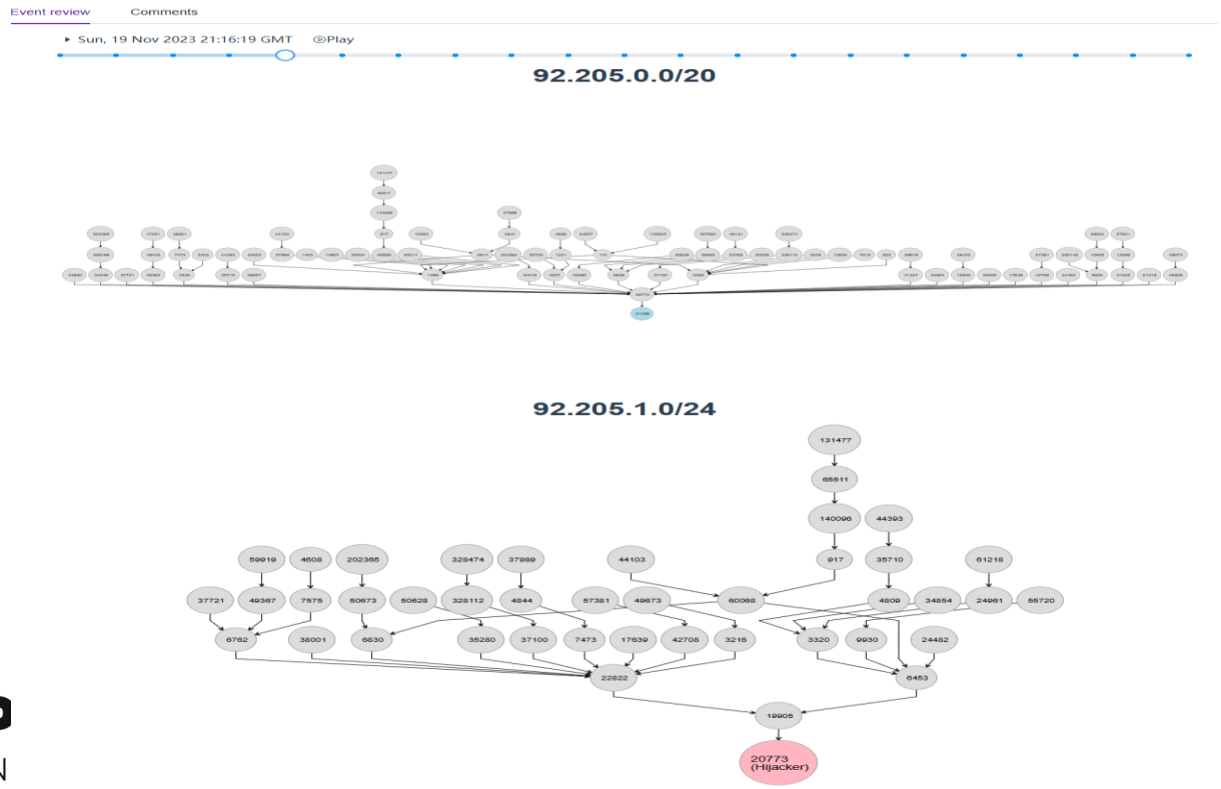
Provides website link of the prefix

APNIC FOUNDATION

清華大學 Tsinghua University

# Features – Quick Response, Event replay, Comments

- About 5 mins delay, much better than most systems
- Notify users immediately when an event is detected, minimizing damage from hijackings
- Understanding how the BGP routing changes
- Analyze the extent of the impact of the event



AP FOUN

清華大學 Tsinghua University

# Subscribe Hijacking Events for AS and Send Alarm

Prefix Change | Hijack | AS Peer Change | AS Path Change

Select event type: All
Select harm level: All
Time zone: GMT+8
Select time period (by Start Time): 2023-11-10 10:22:41 - 2023-11-20 10:22:41
Duration: All
Select for event by keywords: 945

| | Event Type | Level | Event Info | Prefix Num | Prefix Example | Start Time | End Time | Duration | Detail | Comment |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Possible Hijack | low | Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK) | 1 | 23.150.11.0/24 | 2023-11-19 11:01:13 | 2023-11-19 11:15:16 | 0:14:3 | detail | |
| 2 | Possible Hijack | low | Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK) | 1 | 23.150.11.0/24 | 2023-11-19 09:00:47 | 2023-11-19 09:15:20 | 0:14:33 | detail | |
| 3 | Possible Hijack | low | Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK) | 1 | 23.150.11.0/24 | 2023-11-18 19:00:46 | 2023-11-18 19:15:19 | 0:14:33 | detail | |

Hi,

Hope this message finds you well. Greetings from the Institute for Network Sciences and Cyberspace at Tsinghua University. We have developed a BGP hijacking detection system (BGPWatch, https://bgpwatch.cgtf.net).

Our system shows that prefix 23.150.11.0/24 is normally announced by your 945; however, at 2023-11-18 11:00:46 (UTC), prefix 23.150.11.0/24 is also announced by 200827 Detailed information is available here.

We would like to confirm with you whether this is a hijacking event or a false alarm of the system. Please click here to provide us with your feedback. Your time and response are greatly appreciated and will be very helpful for our research.

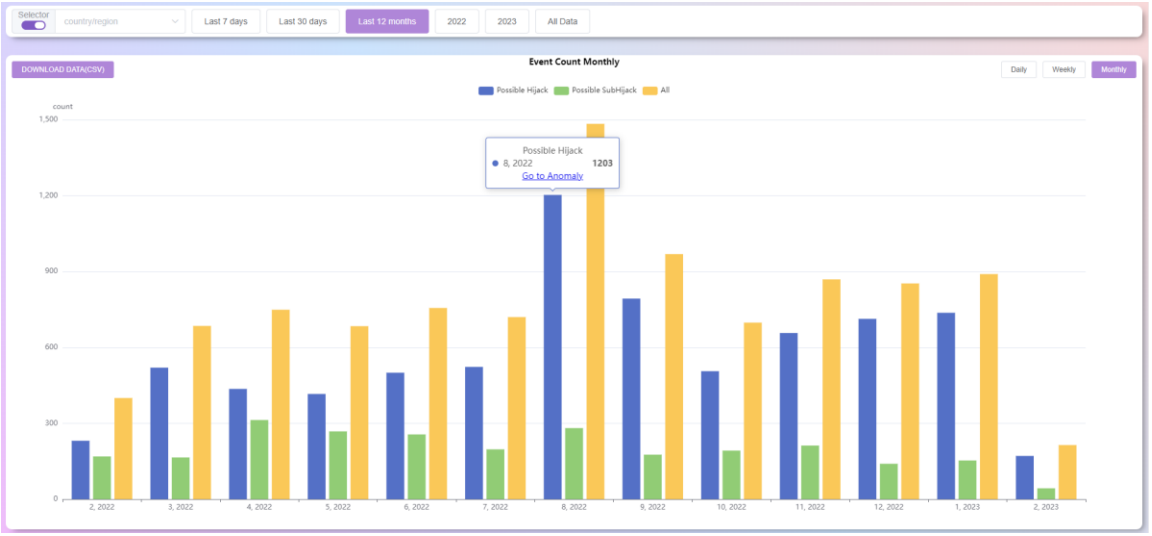
Have a good day!

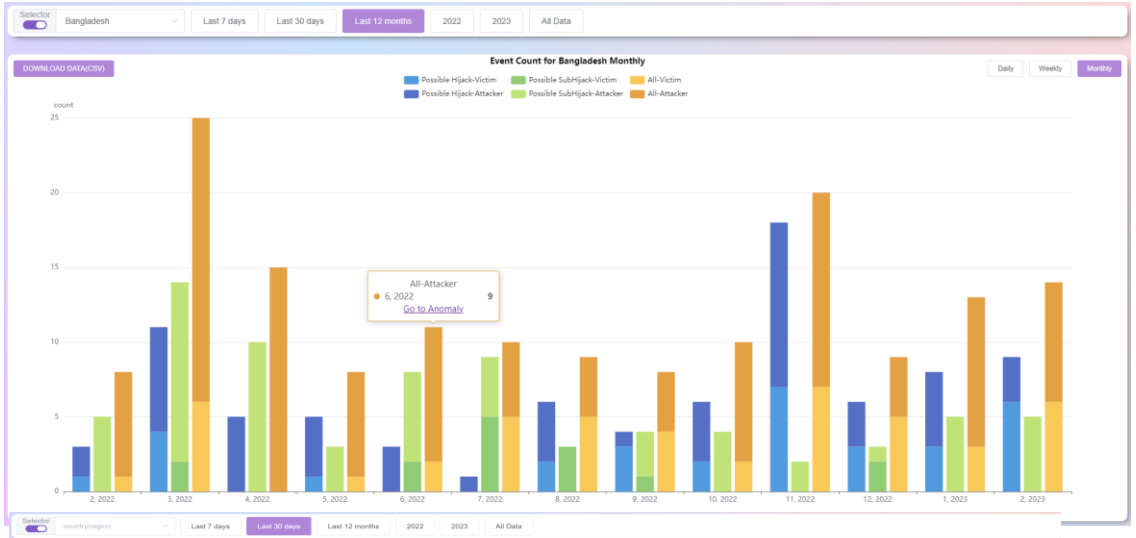
Best regards,
Institute for Network Sciences and Cyberspace
Tsinghua University

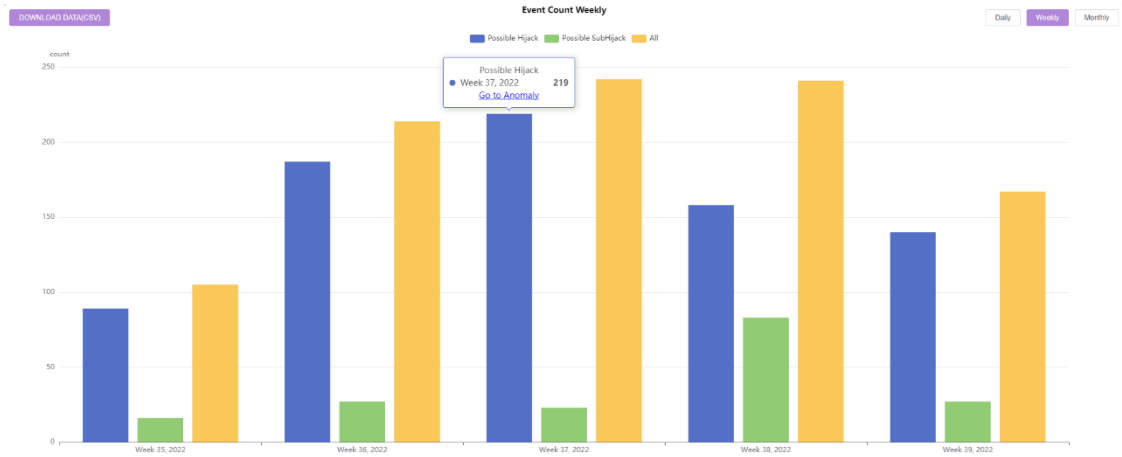
APNIC FOUNDATION

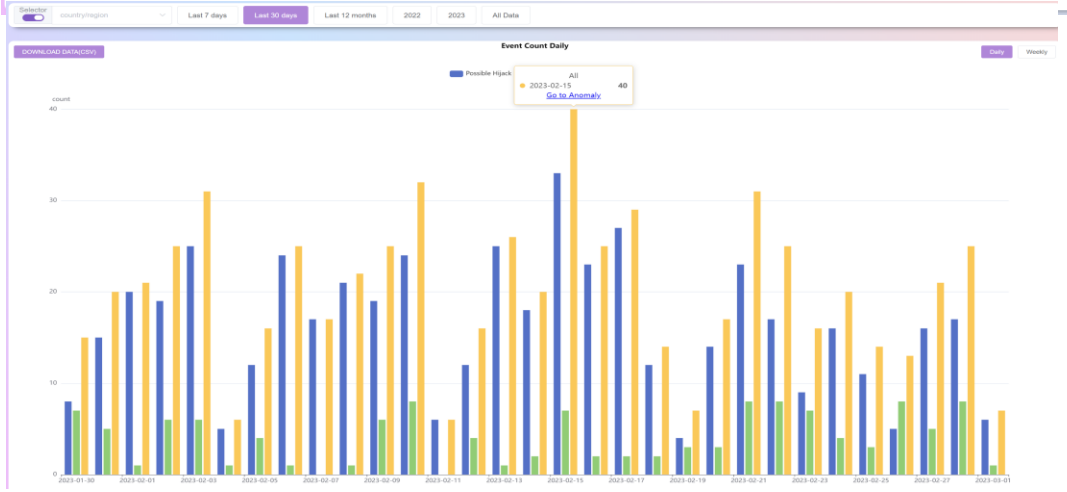
華大學 ua University

# Overview--Statistics for Anomaly Events




Do statistics by country/region, AS,

and by yearly, monthly, weekly, and daily

# Compare with other Platforms

## GRIP: Violate ROA

| Potential Victims | Potential Attackers | Largest (Sub)Prefix | # Prefix Events | Start Time | Duration | Suspicion | Category | Type |
|---|---|---|---|---|---|---|---|---|
| USAS834 NLAS49981 | PTAS24768 | 185.206.250.0/24 | 1 | 2023-11-15 15:15 | 5 hour | High | Default Tr Worthy | moas |

## BGPWatch: Compliant with ROA

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Possible Hijack | low | Victim:PT/AS24768(ALMOUROLTEC)<br>Attacker:US/AS834(IPXO) | 1 | 185.206.250.0/24 | 2023-11-15 23:18:07 | 2023-11-16 04:25:30 | 5:7:23 | deta |

## ROA

| ASN | Prefix | Max Length |
|---|---|---|
| AS24768 | 185.206.250.0/24 | 24 |

APNIC FOUNDATION

清華大學 Tsinghua University

# Compare with other Platforms

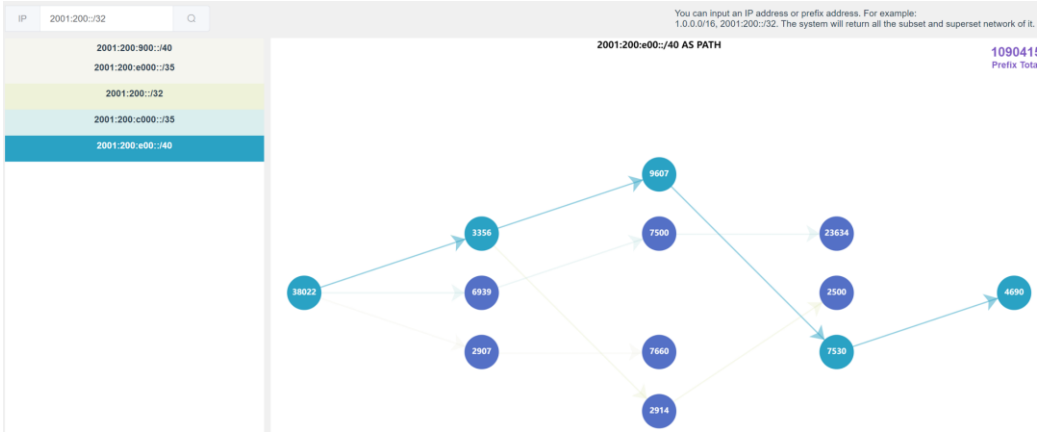
| | BGPWatch | GRIP | BGPStream |
|---|---|---|---|
| Real-time delay | 5mins delay | 5mins delay | More than 2 hours |
| Event replay | √ | × | √ |
| Event statistical analysis | √ | × | × |
| Event level evaluation | √ | × | × |
| Benign MOAS report | √ | √ | × |
| Email Alarm | √ | × | × |
| Accuracy | High | Medium to High | Low |

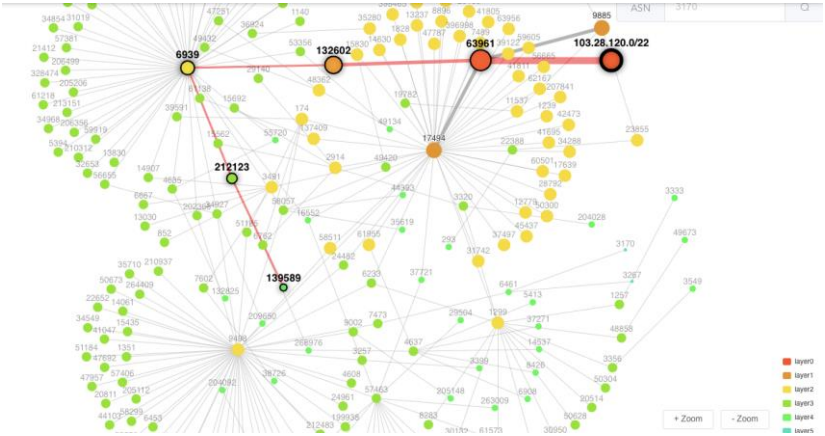
APNIC FOUNDATION

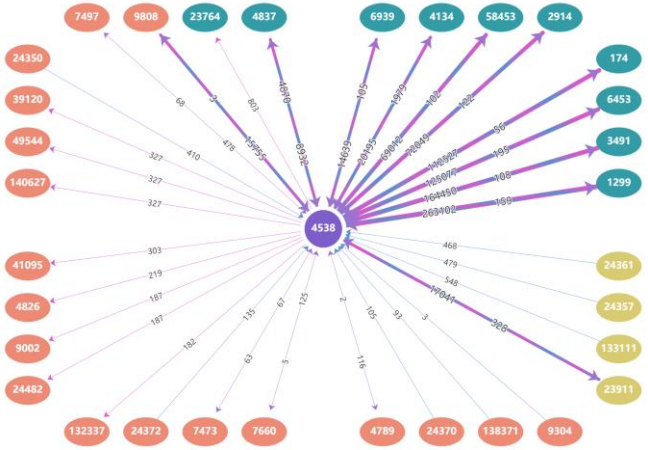
清華大學 Tsinghua University

# Tools for Network Operator

- Dashboard: AS info, prefix, peers
- Routing Search：
  - Aggregated forward routing path
  - Reverse routing path
  - Bi-direction routing path
- Subscribing, Alarming

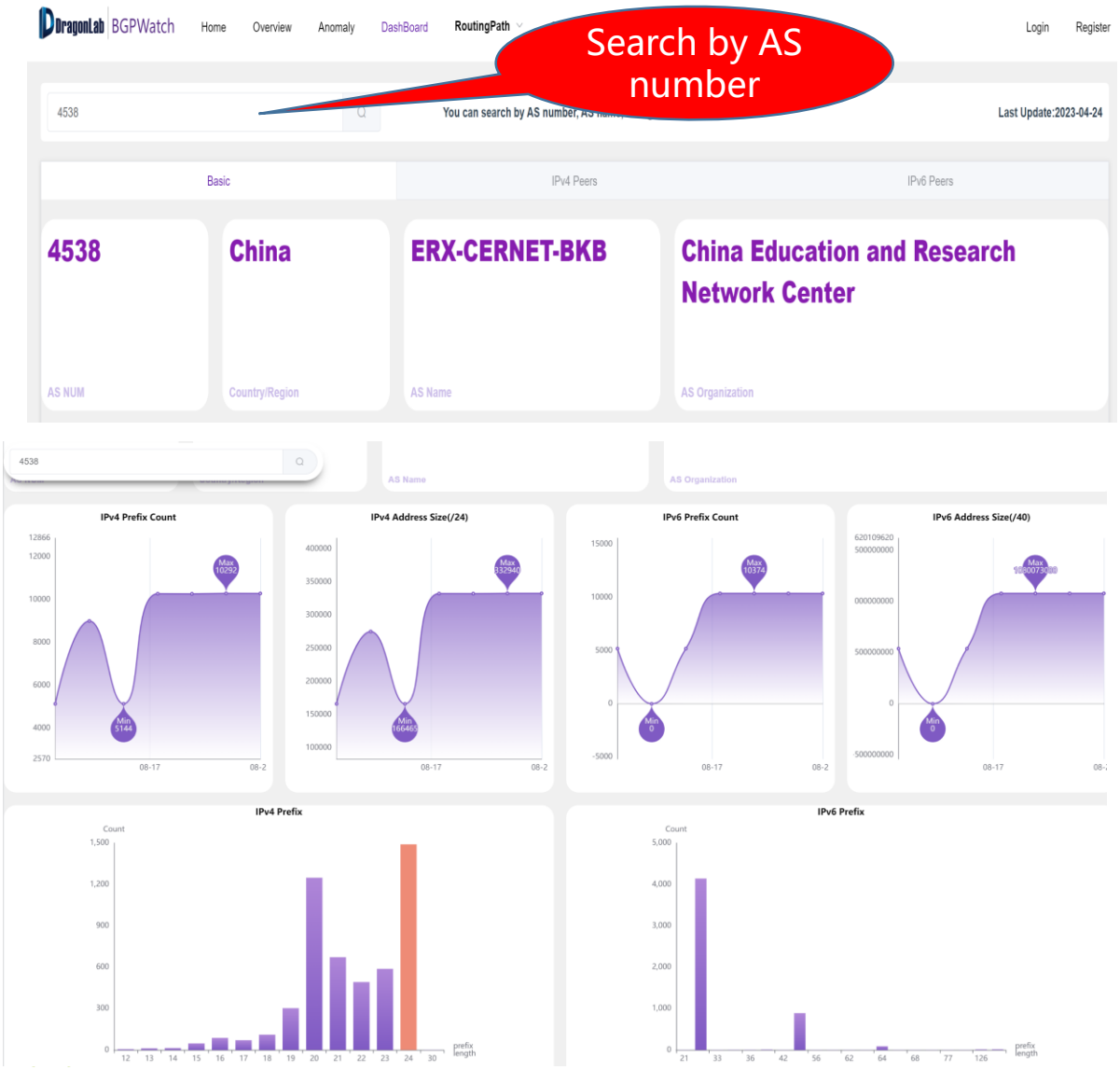


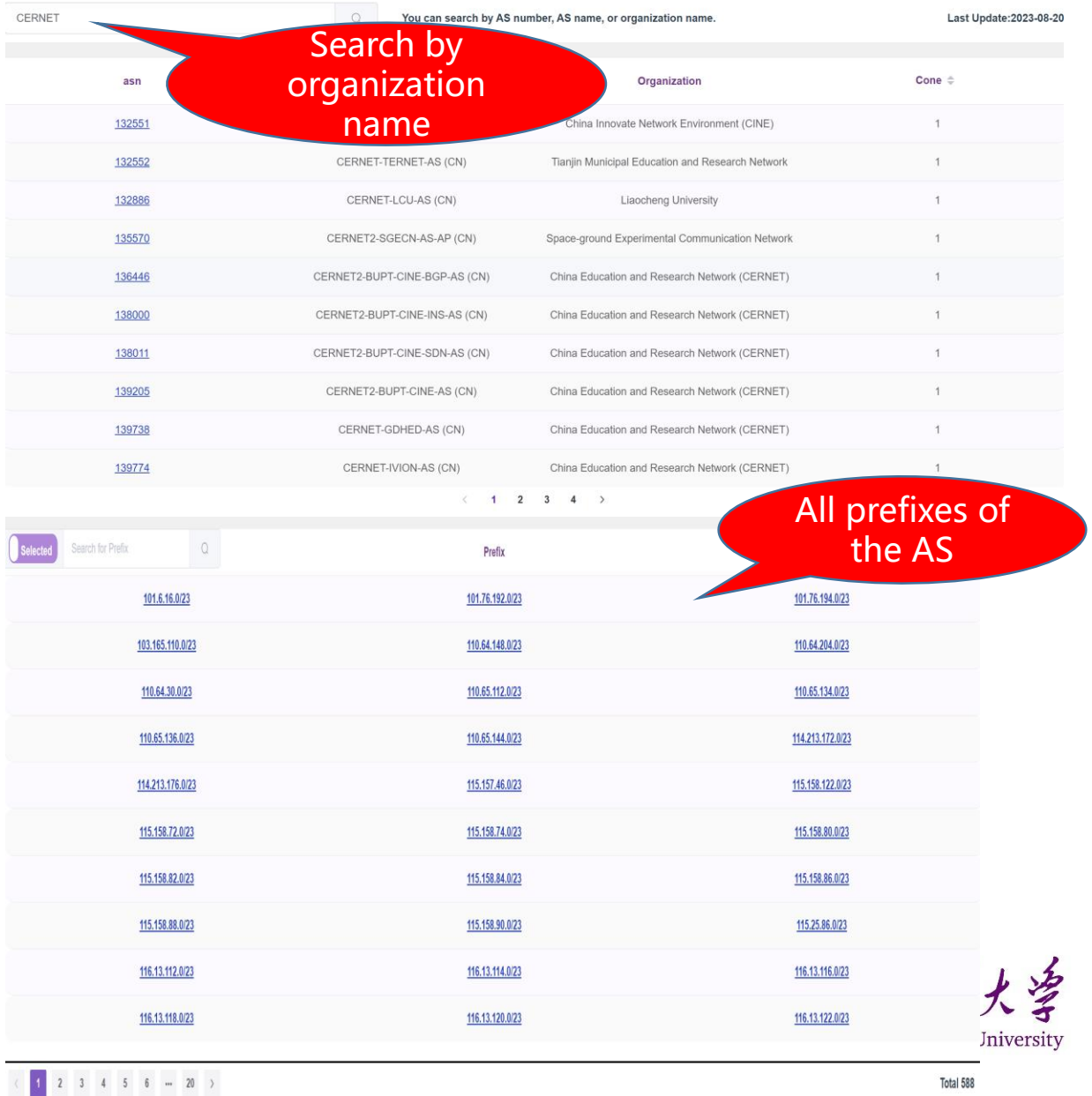



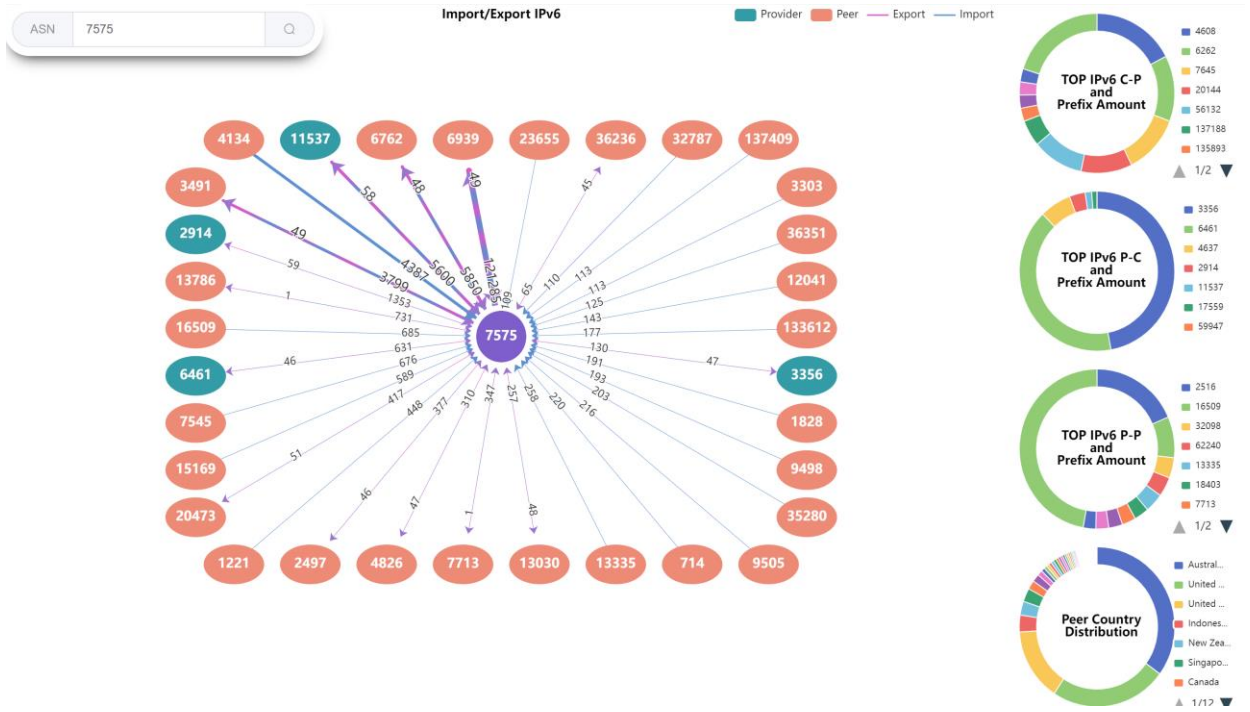

https://bgpwatch.cgtf.net

# Dashboard

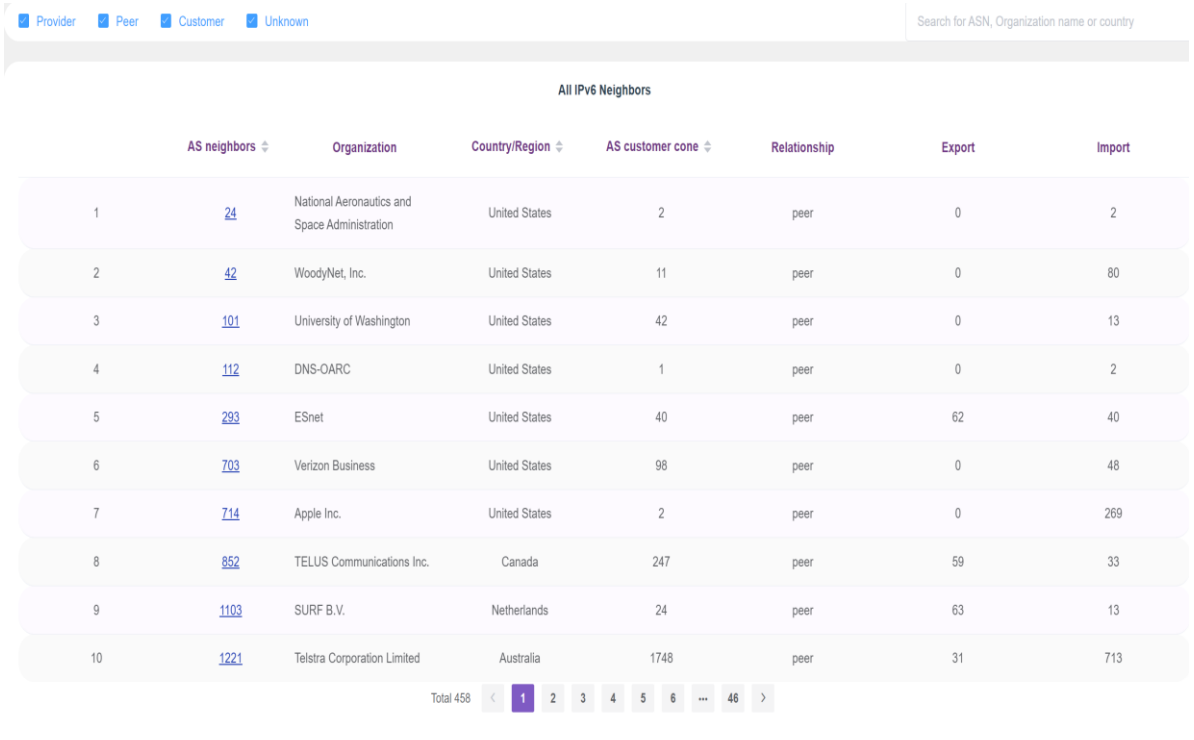

DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Login
Register
Search by AS number
4538
You can search by AS number, AS name, or organization name.
Last Update:2023-04-24
Basic
IPv4 Peers
IPv6 Peers
4538
AS NUM
China
Country/Region
ERX-CERNET-BKB
AS Name
China Education and Research Network Center
AS Organization
IPv4 Prefix Count
IPv4 Address Size(/24)
IPv6 Prefix Count
IPv6 Address Size(/40)
IPv4 Prefix
IPv6 Prefix


CERNET
You can search by AS number, AS name, or organization name.
Last Update:2023-08-20
Search by organization name
asn
Organization
Cone
132551
China Innovate Network Environment (CINE)
132552
CERNET-TERNET-AS (CN)
Tianjin Municipal Education and Research Network
132886
CERNET-LCU-AS (CN)
Liaocheng University
135570
CERNET2-SGECN-AS-AP (CN)
Space-ground Experimental Communication Network
136446
CERNET2-BUPT-CINE-BGP-AS (CN)
China Education and Research Network (CERNET)
138000
CERNET2-BUPT-CINE-INS-AS (CN)
138011
CERNET2-BUPT-CINE-SDN-AS (CN)
139205
CERNET2-BUPT-CINE-AS (CN)
139738
CERNET-GDHED-AS (CN)
139774
CERNET-IVION-AS (CN)
All prefixes of the AS
Selected
Search for Prefix
Prefix
101.6.16.0/23
101.76.192.0/23
101.76.194.0/23
103.165.110.0/23
110.64.148.0/23
110.64.204.0/23
110.64.30.0/23
110.65.112.0/23
110.65.134.0/23
110.65.136.0/23
110.65.144.0/23
114.213.172.0/23
114.213.176.0/23
115.157.46.0/23
115.158.122.0/23
115.158.72.0/23
115.158.74.0/23
115.158.80.0/23
115.158.82.0/23
115.158.84.0/23
115.158.86.0/23
115.158.88.0/23
115.158.90.0/23
115.25.86.0/23
116.13.112.0/23
116.13.114.0/23
116.13.116.0/23
116.13.118.0/23
116.13.120.0/23
116.13.122.0/23
Total 588

# Dashboard:
# IPv4/IPv6 Key Peers and All neighbors Information




Key Neighbors



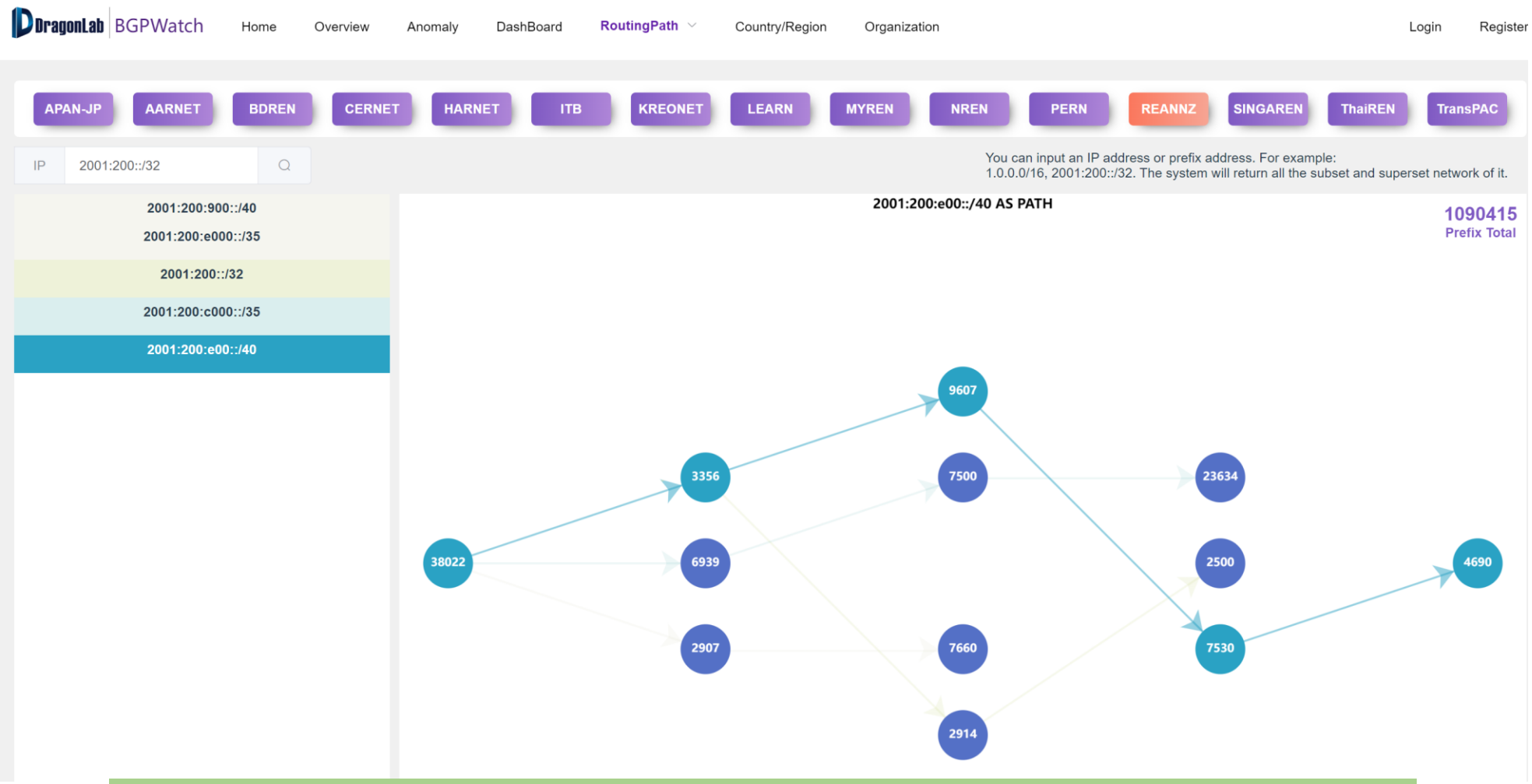

| | AS neighbors | Organization | Country/Region | AS customer cone | Relationship | Export | Import |
|---|---|---|---|---|---|---|---|
| 1 | 24 | National Aeronautics and Space Administration | United States | 2 | peer | 0 | 2 |
| 2 | 42 | WoodyNet, Inc. | United States | 11 | peer | 0 | 80 |
| 3 | 101 | University of Washington | United States | 42 | peer | 0 | 13 |
| 4 | 112 | DNS-OARC | United States | 1 | peer | 0 | 2 |
| 5 | 293 | ESnet | United States | 40 | peer | 62 | 40 |
| 6 | 703 | Verizon Business | United States | 98 | peer | 0 | 48 |
| 7 | 714 | Apple Inc. | United States | 2 | peer | 0 | 269 |
| 8 | 852 | TELUS Communications Inc. | Canada | 247 | peer | 59 | 33 |
| 9 | 1103 | SURF B.V. | Netherlands | 24 | peer | 63 | 13 |
| 10 | 1221 | Telstra Corporation Limited | Australia | 1748 | peer | 31 | 713 |

All Neighbors

APNIC FOUNDATION

清華大學 Tsinghua University

# Multiple Routing Path Search

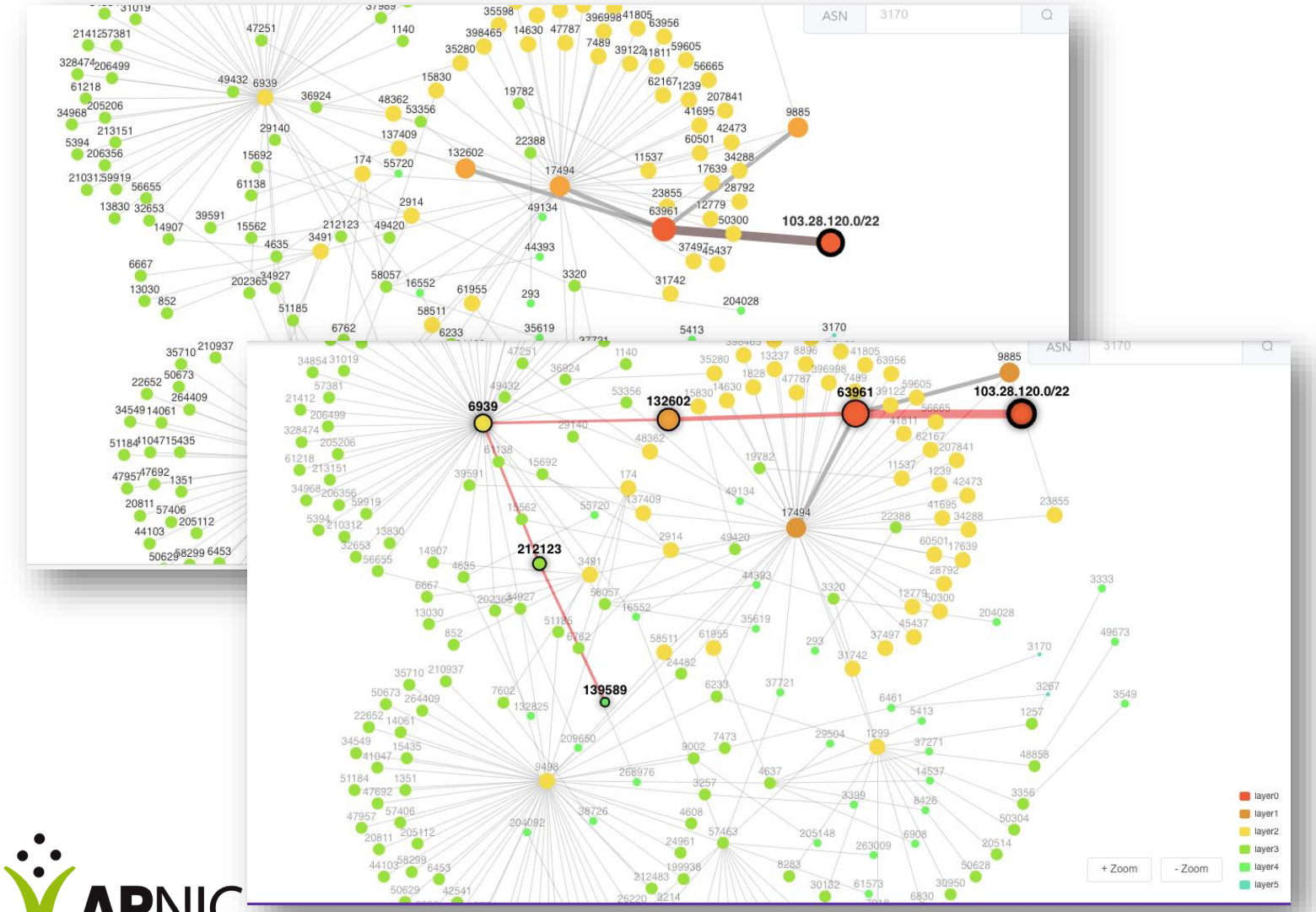



Support Prefix / IP, IPv4 / IPv6
Return paths of all sub networks and super networks of the input prefix
Group prefixes with the same routing path

APNIC FOUNDATION

清華大學 Tsinghua University

# Reverse Routing Path (TOPO)

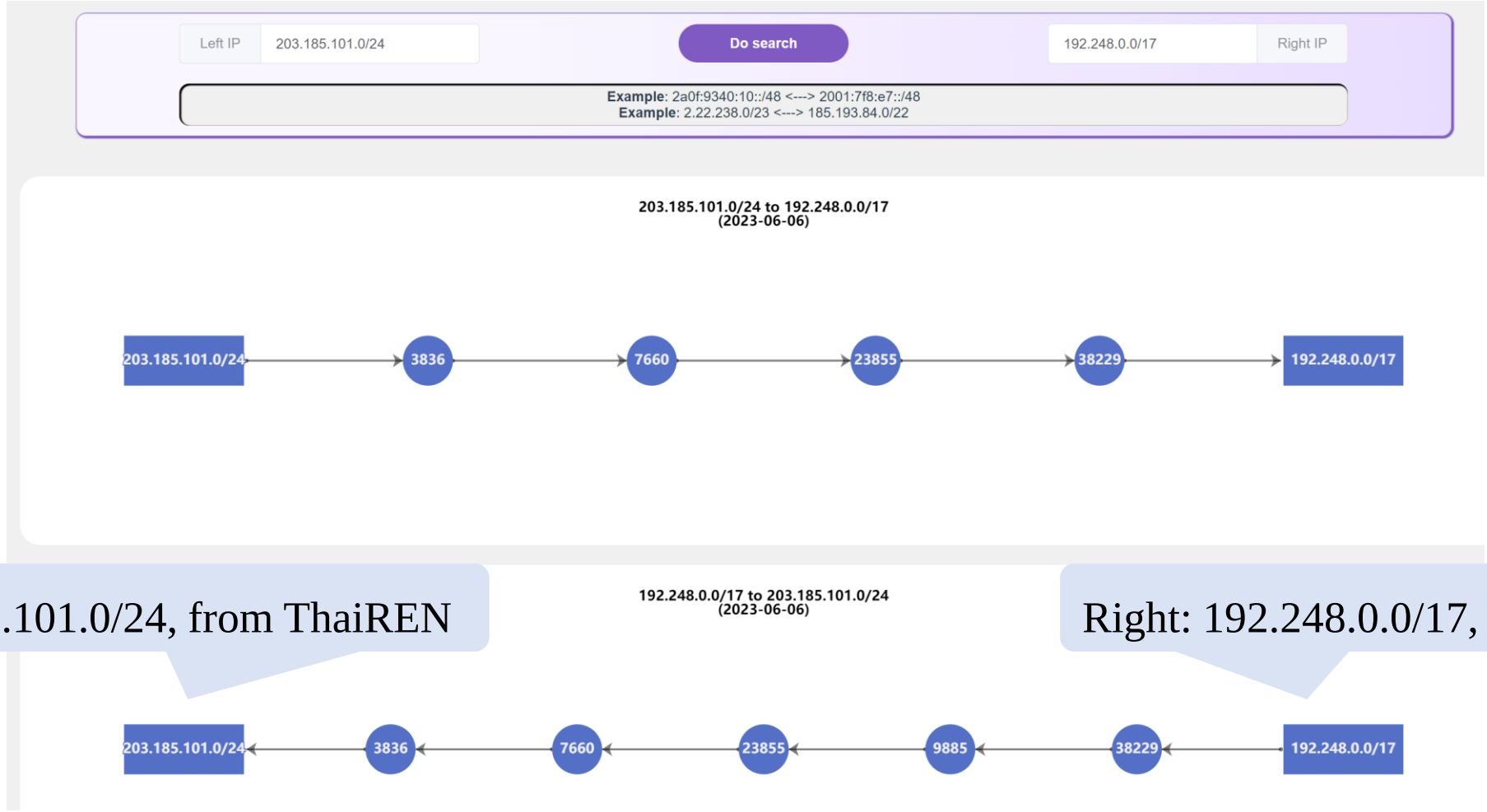



- Support Prefix / IP, IPv4 / IPv6
- The system will search the best matched prefix and return the reverse routing tree
- With better interactivity
- Select an AS or input AS number, the system will highlight the path to the AS
- The number of layers to display can be selected

APNIC FOUNDATION

Tsinghua University

# Bi-Routing Path




Left : 203.185.101.0/24, from ThaiREN

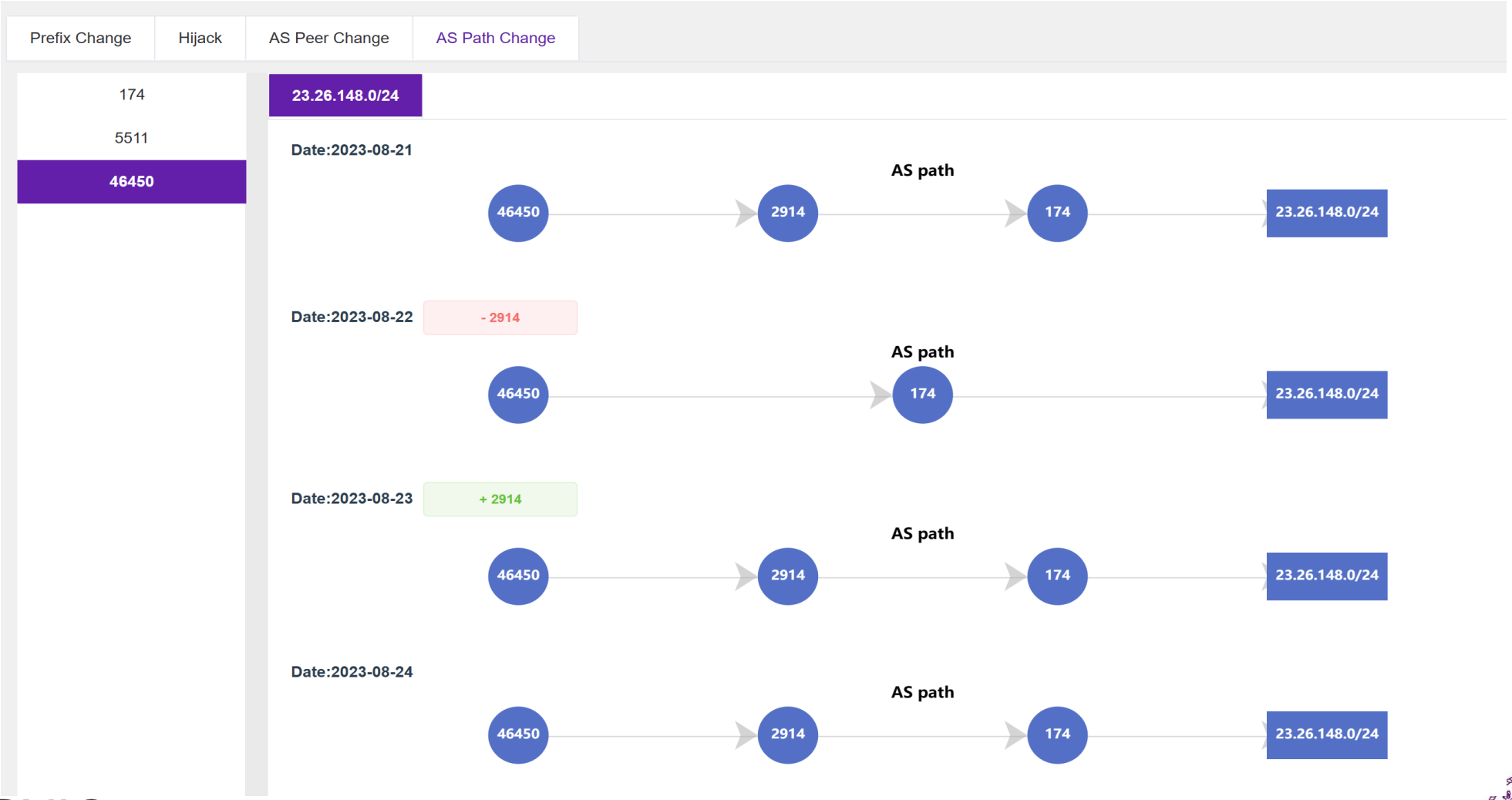
Right: 192.248.0.0/17, from LEARN

Support Prefix / IP, IPv4 / IPv6
The system will search the best matched prefix

APNIC FOUNDATION

清華大學 Tsinghua University

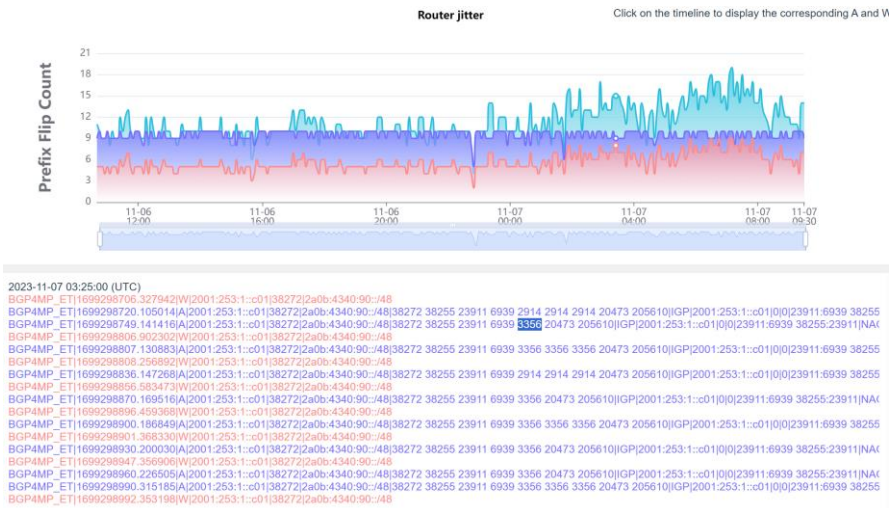
# Path Change

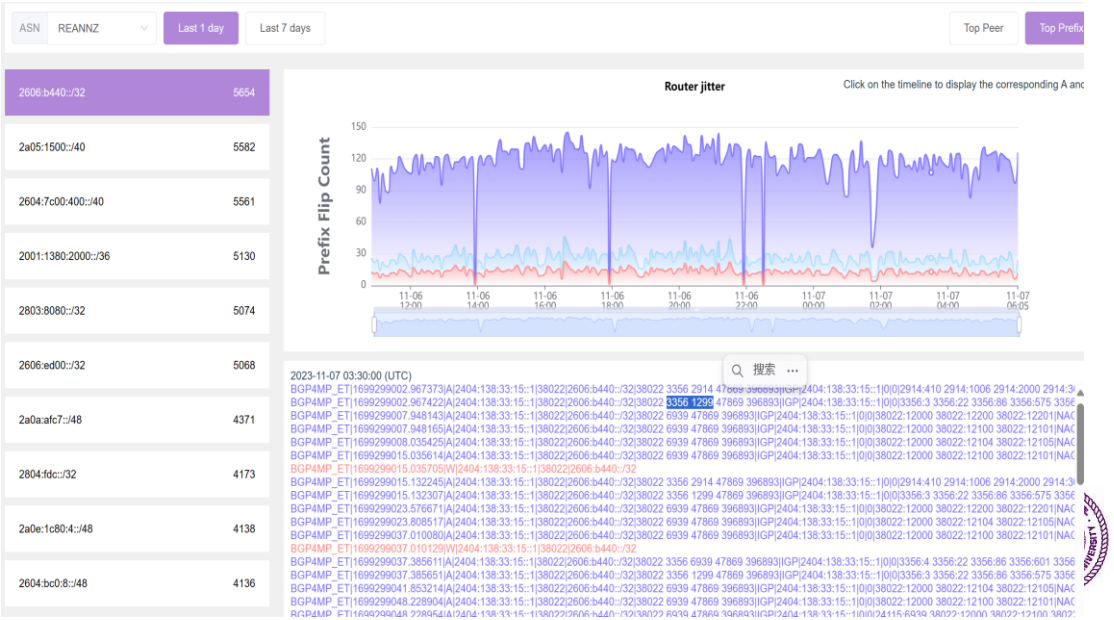



APNIC FOUNDATION

清華大學 Tsinghua University

# Router Jitter



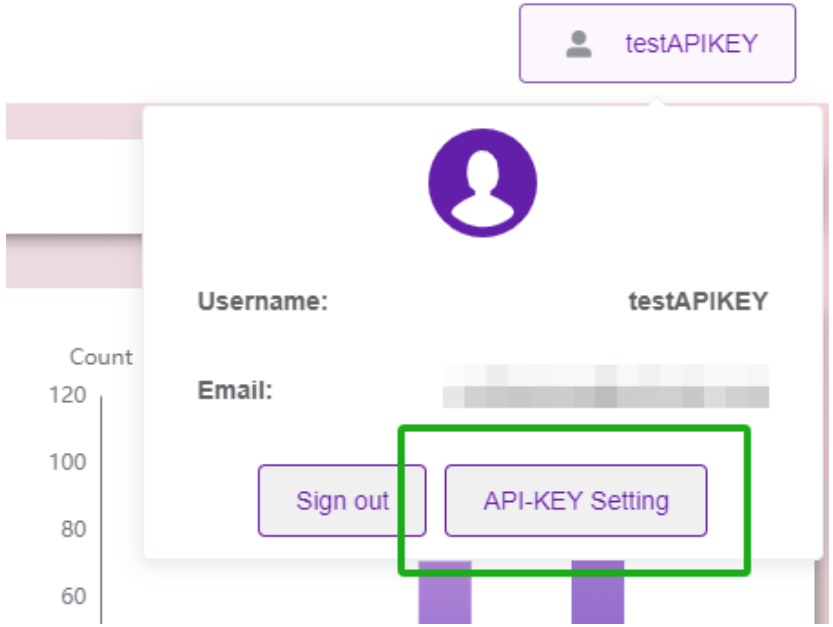



APNIC FOUNDATION

清華大學 Tsinghua University

# OPEN API

- /get_event_by_condition
- /get_event_detail




Body Params (application/json) | Code Generate | Example

type string required

Event Type

Allowed values: `Possible Hijack` `Possible SubHijack` `Ongoing Possible Hijack` `Ongoing Possible SubHijack`

Example: `Ongoing Possible SubHijack`

condition object {9} required

Find Condition (Support mongo scripts)

- start_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- level anyOf {2} anyOf, must be valid against any of the subschemas optional
- prefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- subprefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- end_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional

```
{
  "type": "Possible Hijack",
  "condition": {}
}
```

APNIC FOUNDATION

Tsinghua University

# BGP Route Sharing and Looking Glass Platforms

APNIC FOUNDATION

APAN57

清華大學 Tsinghua University

# Routing Collection VPs

- BGP route collection platforms collect and log BGP routing information observed from different ASes.
- This routing information can be used for network diagnosis, historical BGP event review, scientific research, etc.

RIPE RIS VPs (in the upper tier)

RouteViews VPs (in the upper tier)

Vantage points in the Asian region remain scarce

# CGTF RIS

https://bgp.cgtf.net

We have established BGP session with 15 partners.
Configuration manual can be accessed at
https://www.bgper.net/index.php/document/

| No. | Partner | No. | Partner |
|---|---|---|---|
| 1 | **APAN-JP** | 9 | **MYREN** |
| 2 | **AARNET** | 10 | **PERN** |
| 3 | **BDREN** | 11 | **REANNZ** |
| 4 | **CERNET** | 12 | **SINGAREN** |
| 5 | **HARNET** | 13 | **ThaiSARN** |
| 6 | **ITB** | 14 | **TransPAC** |
| 7 | **KREONET** | 15 | **NREN** |
| 8 | **LEARN** | | |

**Index of /ribs/2022/07**

| Name | Last modified | Size | Description |
|---|---|---|---|
| rib.20220730.0600.mrt.bz2 | 2022-07-30 06:00 | 13M | |
| rib.20220730.0800.mrt.bz2 | 2022-07-30 08:00 | 13M | |
| rib.20220730.1000.mrt.bz2 | 2022-07-30 10:00 | 13M | |
| rib.20220730.1200.mrt.bz2 | 2022-07-30 12:00 | 13M | |
| rib.20220730.1400.mrt.bz2 | 2022-07-30 14:00 | 13M | |
| rib.20220730.1600.mrt.bz2 | 2022-07-30 16:00 | 13M | |
| rib.20220730.1800.mrt.bz2 | 2022-07-30 18:00 | 13M | |
| rib.20220730.2000.mrt.bz2 | 2022-07-30 20:00 | 13M | |
| rib.20220730.2200.mrt.bz2 | 2022-07-30 22:00 | 13M | |
| rib.20220731.0000.mrt.bz2 | 2022-07-31 00:00 | 13M | |
| rib.20220731.0200.mrt.bz2 | 2022-07-31 02:00 | 13M | |
| rib.20220731.0400.mrt.bz2 | 2022-07-31 04:00 | 13M | |
| rib.20220731.0600.mrt.bz2 | 2022-07-31 06:00 | 13M | |
| rib.20220731.0800.mrt.bz2 | 2022-07-31 08:00 | 13M | |
| rib.20220731.1000.mrt.bz2 | 2022-07-31 10:00 | 13M | |

APNIC FOUNDATION

清華大學 Tsinghua University

# CGTF RIS Collector

- Just have your border router **establish an eBGP session** with our collector:
- Our Collector ASN: 65534

- Our Collector1 IPv4 address: 47.241.43.108
- Our Collector1 IPv6 address: 240b:4000:b:db00:8106:7413:738f:e9ed

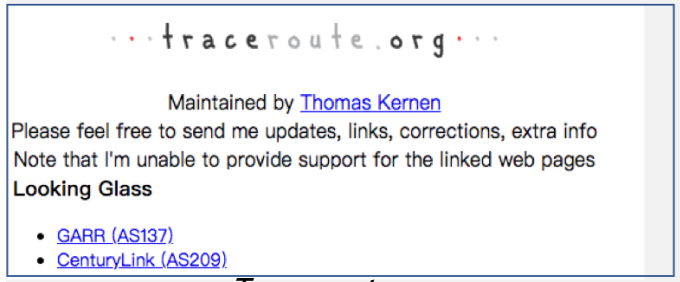
- Our Collector2 IPv4 address: 203.91.121.227
- Our Collector2 IPv6 address: 2001:da8:217:1213::227

APNIC FOUNDATION

清華大學 Tsinghua University

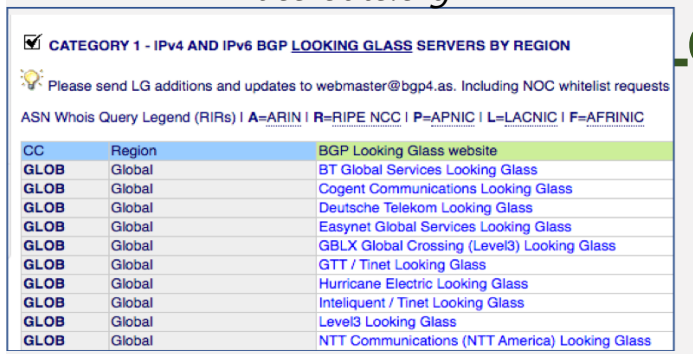
# Looking Glass VPs

- Looking Glass allows us to view the Internet from different locations
- Researchers usually find and use LG pages from several well-known portal pages

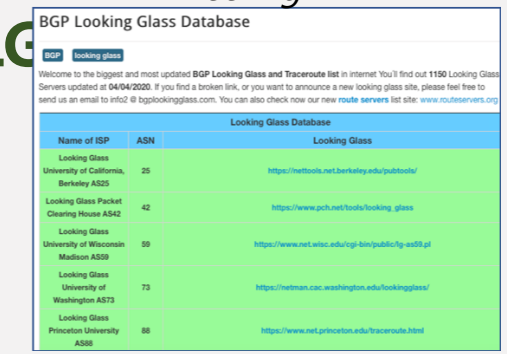



*Traceroute.org*

*PeeringDB*




*BGP4.as*




*BGPLookingglass.com*

- Explore other available LG pages
- Create more Looking Glass Vantage Points

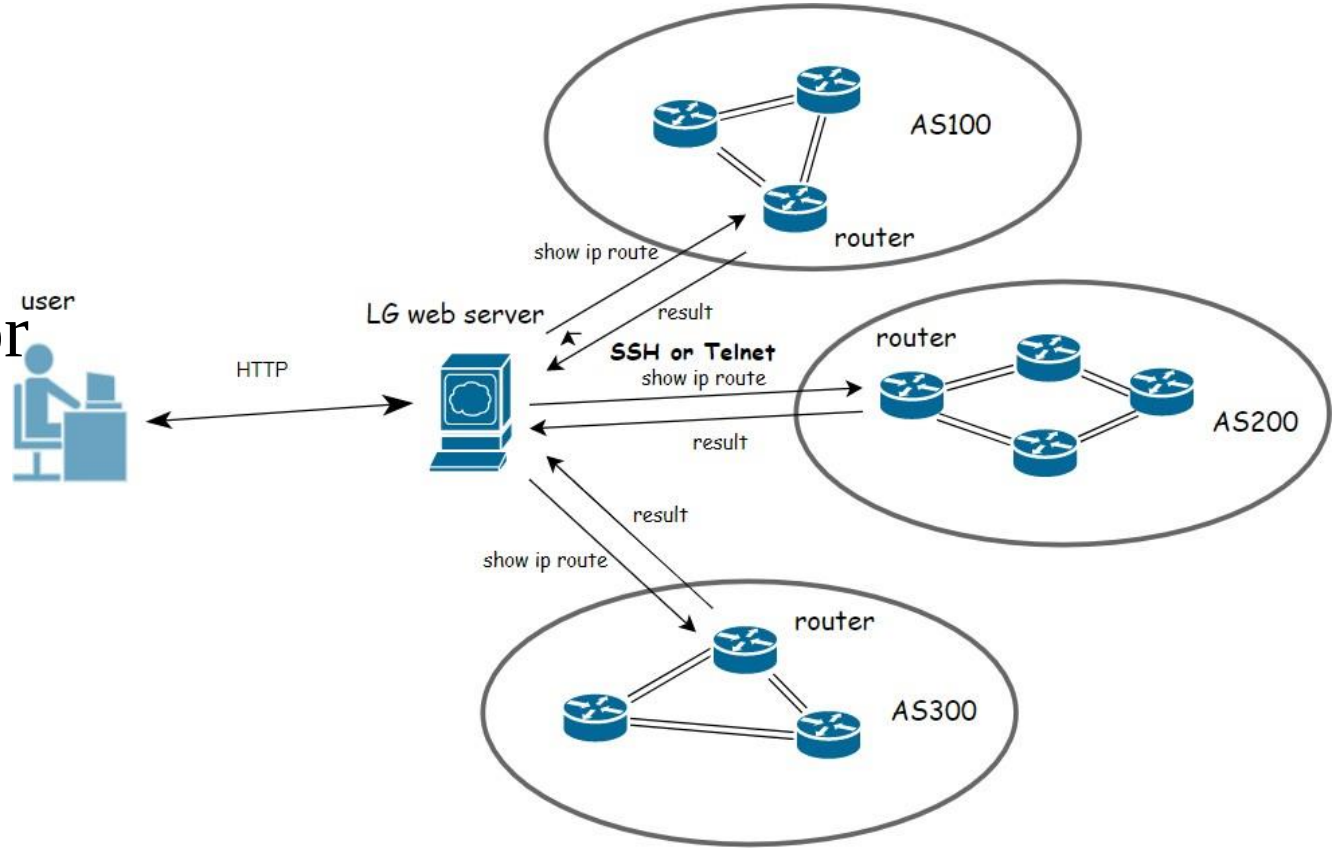
APNIC FOUNDATION

清華大學 Tsinghua University

# Web-based Looking Glass

A complete LG command execution process:

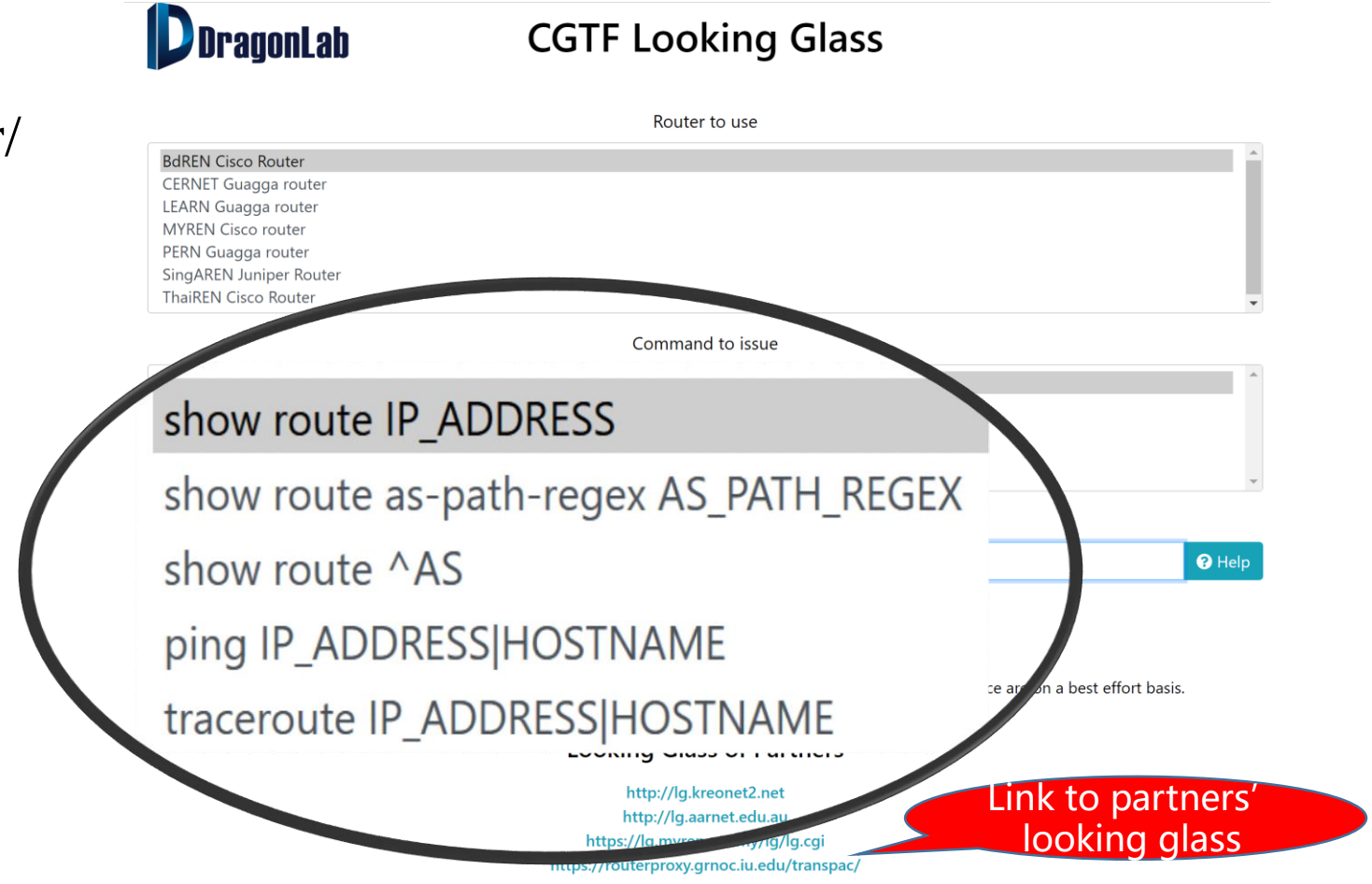
1. The user makes a command execution request to the LG web
2. The server connects to the corresponding router through SSH or Telnet based on the parameters selected by the user.
3. The router executes the command and returns the command execution result to the LG web server.



# CGTF Looking Glass

https://lg.cgtf.net

- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 5 commands
- Query speed limit for security
- More partners is welcomed




- 7 Education & Research network joined
- Add links to 4 partners' looking glass

APNIC FOUNDATION

清華大學 Tsinghua University

# Configuration on Router Side

- Create a router account **only for LG**, and this account **only has privileges of executing the above command**.
- Use **IP filtering mechanism**. Add the **web server IP** to the **whitelist**.

BIRD
Cisco
Cisco IOS XR
FRRouting
Juniper
Quagga
Vyatta, VyOS, EdgeOS

- Juniper JUNOS:

  Define the login class with permissions:

  set system login class lookinglass permissions network
  set system login class lookinglass permissions routing
  set system login class lookinglass permissions view

  Define the login user:

  set system login user lookinglass class lookinglass
  set system login user lookinglass authentication encrypted-password "encrypted-text"
  set system login user lookinglass authentication ssh-rsa "ssh-rsa rsa-pub-key-text"

https://www.bgper.net/index.php/document/
https://looking-glass.readthedocs.io/en/latest/

APNIC FOUNDATION

清華大學 Tsinghua University

# Security Concerns

- Where are the data stored?
  - BGP sharing platform:  Cloud server in Singapore
  - BGPWatch:  Cloud server in Hongkong
  - Looking Glass:  Cloud server in Hongkong
- Will peering harm my network?
  - We use routing FRR[2] to simulate a real BGP router and it won’t send routing anouncement.
- Will sharing routing information harm my network?
  - Routeviews and RIPE RIS are two most famous RIS sharing platform.
- Our security policy doesn’t permit ssh/telnet access from other network
  - Such as SingAREN, they use a VM to simulate a router, and peer with their real router. Then our looking glass access to the VM.

APNIC FOUNDATION

清華大學 Tsinghua University

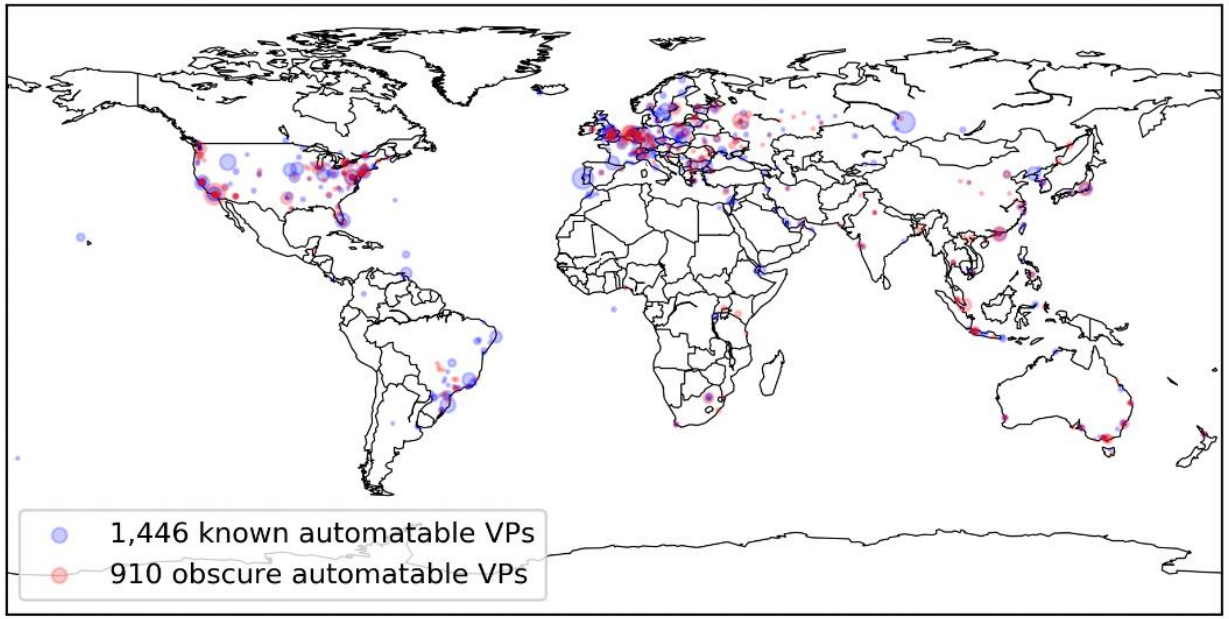
# Future Work

# Objectives and Work Plan for the Extension Project

| Objectives | Work Plan | Tentative Timeline |
|---|---|---|
| Develop an integrated Looking Glass platform | Find obscure Looking Glass VP regularly | Dec. 2023 |
| | Develop integrated Looking Glass platform | Feb. 2024 |
| | Develop Looking Glass API | Mar. 2024 |
| Use Looking Glass to further check routing hijacking at the data plan | Develop data plan detection method and decision algorithm | June 2024 |
| | Integrate the algorithm to the system | Aug. 2024 |
| Develop path hijacking detection and routing leak detection | Develop path hijacking detection method | Nov. 2024 |
| | Develop routing leak detection method | Jan. 2025 |
| Continue to maintain and fix bugs in the BGPWatch platform | Continually test and get suggestions from user | Throughout the entire project duration |
| Continue community development and engagement, and international collaboration | Plan to give presentations at APAN, APRICOT, and TNC conferences, and explore collaborations with communities in Europe and Africa | Throughout the entire project duration |
| | Plan to conduct project training at APAN57, with participants not limited to NRENs but also including commercial operators | Jan. 2024 |
| | Plan to Open source the Project | Jan. 2024 |
| Continue to secure the funds from other funding resources for future projects | Explore funds from China and other organizations | Throughout the entire project duration |

# Open Looking Glass Vantage Point

- **Paper: "Discovering obscure looking glass sites on the web to facilitate internet measurement research"——CoNEXT'21**

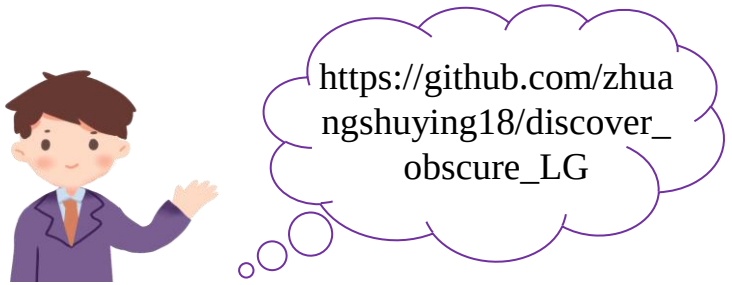



1,446 known LG VPs in 386 cities of 75 countries

910 obscure LG VPs in 282 cities in 55 countries

✓ The 910 obscure VPs cover **8 exclusive countries** and **160 exclusive cities,** where no known LG VPs have been found before

✓ The 8 countries are mainly distributed in **East Africa** and **South Asia**



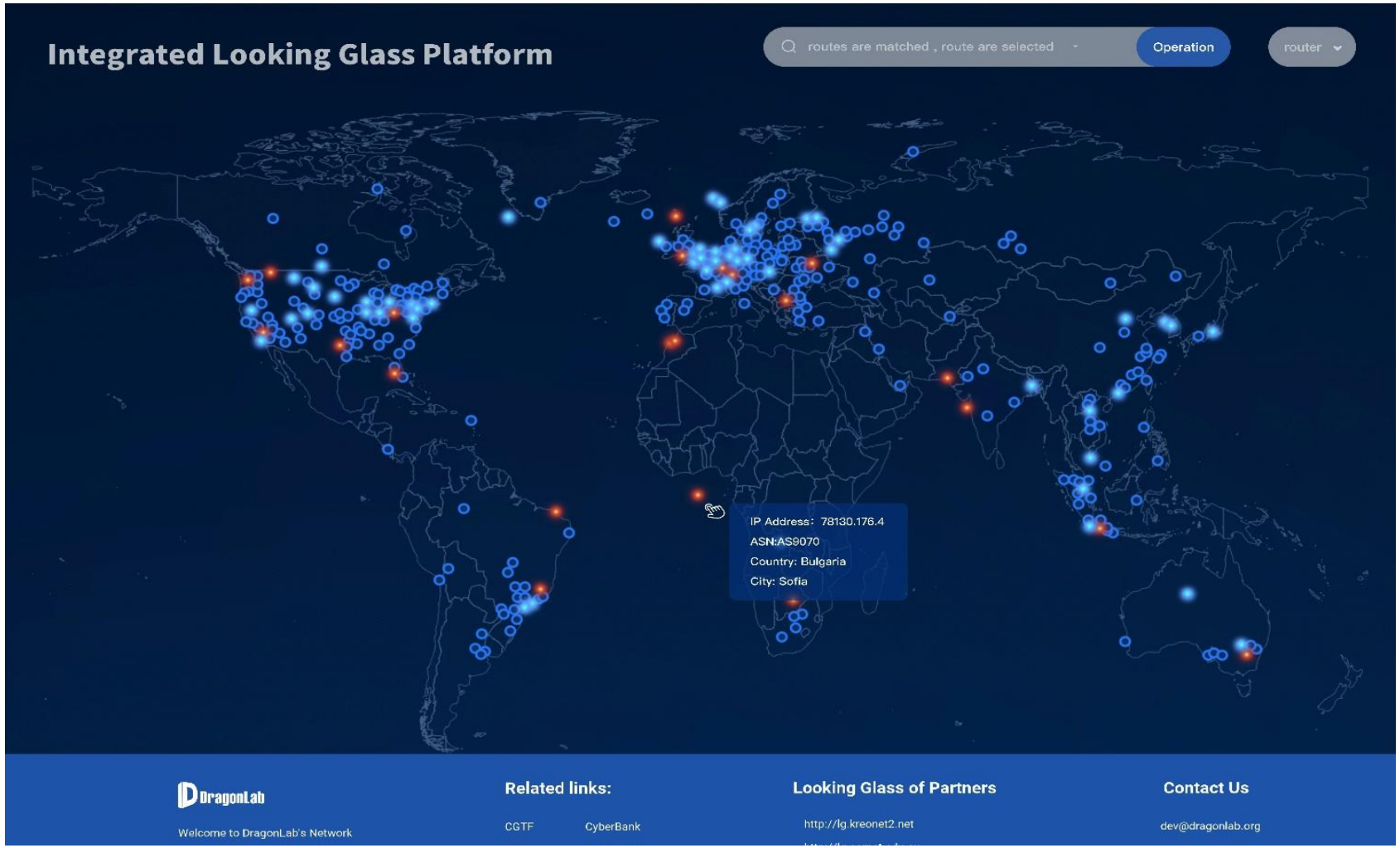

Periscope has found several hundred VPs (364)

APNIC FOUNDATION

清華大學 Tsinghua University

# An Integrated Looking Glass and Open API

DragonLab CGTF Looking Glass

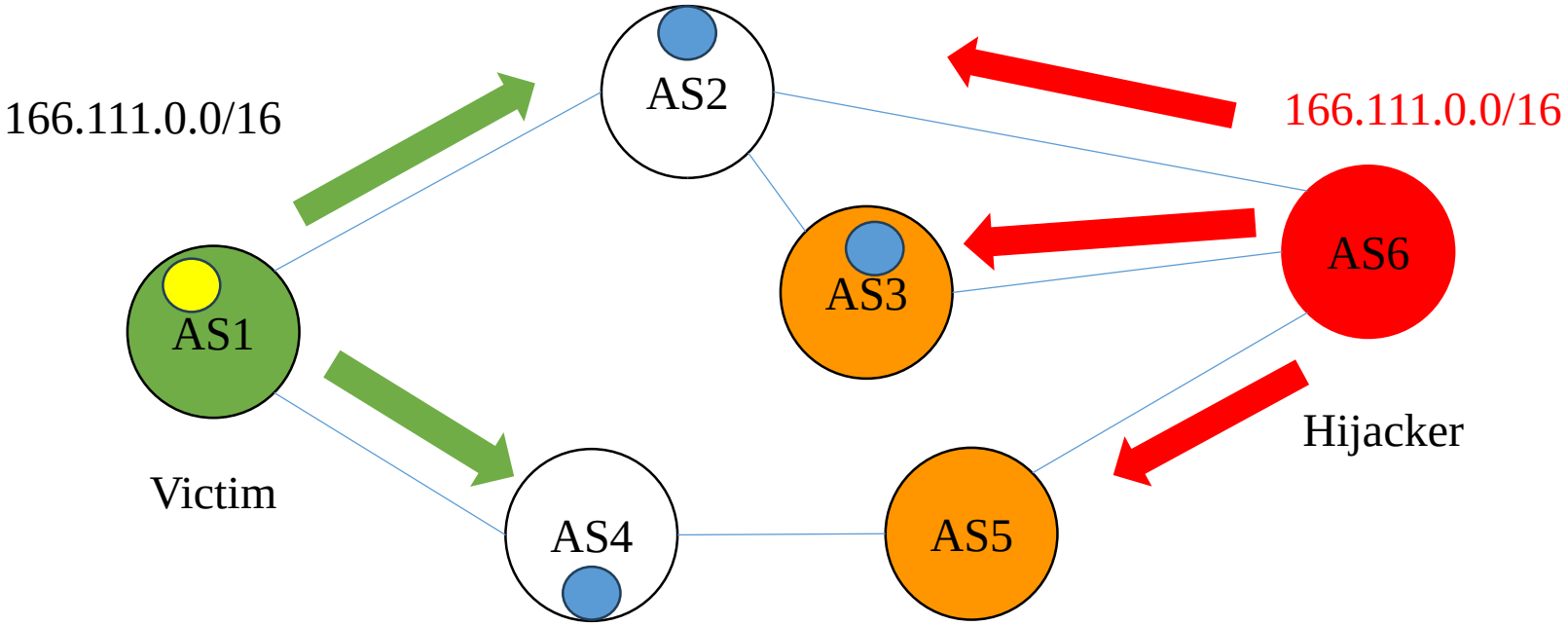



Based on the found VP, providing:
Open API, Open source, Open Platform

APNIC FOUNDATION

清華大學 Tsinghua University

# Data Plane Detection




Looking Glass vantage point

Representative services

- Possible Hijacking?

  1. Multi Home, Proxy
  2. Prefix Migration
  3. Hijacking

- When a hijacking occurs, it will affect the service
- Approach: Test representative service from VPs

APNIC FOUNDATION

清華大學 Tsinghua University

# Comments and Suggestions?

## Contact us at:

sec@cgtf.net

APNIC FOUNDATION

APAN57

清華大學 Tsinghua University