(APNIC Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Mar. 15, 2023
APAN 55

清華大學
Tsinghua University

APNIC
FOUNDATION

Outline

- Project Overview
- Project Progress
- Feedback from partners
- Future Plan
- Comments/Suggestions

Project Information

- Name: Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

- Co-PI: Jilong Wang, (Tsinghua University, CERNET, China)
  Co-PI: Chalermpol Charnsripinyo (ThaiREN, Thailand)
  Co-PI: Simon Peter Green (SingAREN, Singapore)

- Date: 2022.2.24 - 2023.8.24 (tbc with APNIC Foundation)
- APNIC ISIF Grants : US$150,000.00
- Tsinghua University In-Kind Contribution: US$69,660.00

清華大學 Tsinghua University

APNIC FOUNDATION

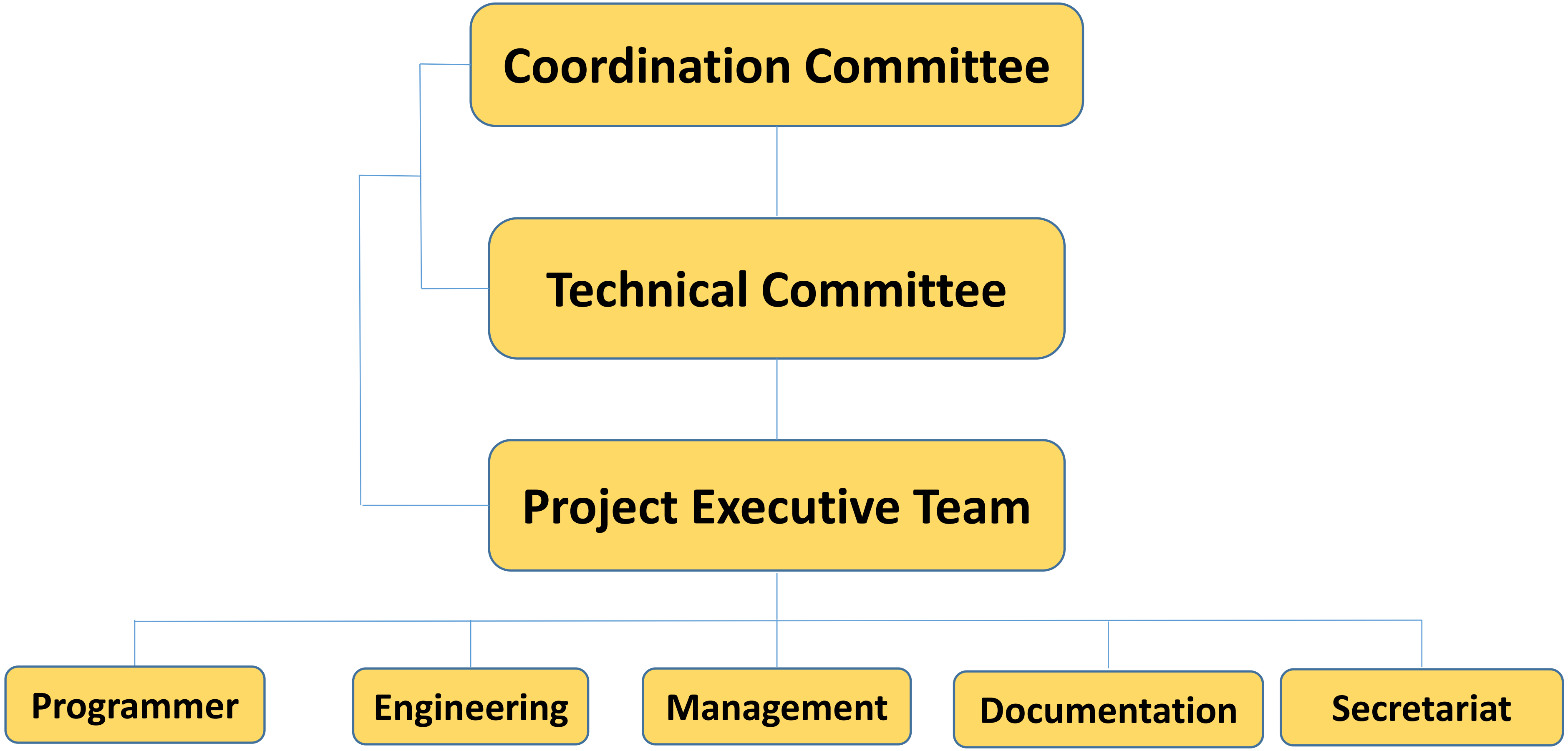
Objectives & Deliverables

- Build a collaborative BGP routing analyzing and diagnosing platform
  - Looking Glass platform
  - BGP routing sharing platform
  - BGP monitoring and diagnosing platform, focusing on routing hijacking detection and mitigation system
  - BGP analysis platform, focusing on invulnerability analysis of regional routing
- Set up a website for sharing knowledge
- Enhance the NREN capacity of network operation and measurement in Asia Pacific area and promote international collaborations

Partnership

- **19 Partner Organizations (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)
- **Keep open till June, 2023**

Project Governance



Coordination Committee

Technical Committee

Project Executive Team

Programmer

Engineering

Management

Documentation

Secretariat

The Responsibilities

	Who	Responsibility	Meetings
Coordination Committee	Representatives from all partner organizations	policy, strategy, project activity plan, monitoring project management and financial issues	quarterly meeting
Technical Committee	Representatives from all partner organizations	technical activity plan, technical discussion of project development and implementation, research paper/reports	monthly meeting
Project Executive Team	Programming, engineering, coordination and management, documentation, secretariat	service/platform program development, engineering collaboration, coordination of the committees and partners, and different teams, website and documentation, project management	bi-weekly meeting

The Coordination Committee

- Co-Chairs
  - Jilong Wang (CERNET)
    Shinji Shimojo (APAN-JP)
    Francis Lee (SingAREN)
- Members:
  - AARNET: David Wilde
  - CERNET team: Jie An, Changqing An, Xiaohong Huang
  - BdREN: Mohammad Tawrit
  - DOST-ASTI(PREGINET): Bayani Lara
  - ERNET: Paventhan Arumugam
  - Gottingen University: Xiaoming Fu

清華大學
Tsinghua University

APNIC
FOUNDATION

The Coordination Committee(Cont’d)

- **Members:**
  - **HARNET/JUCC: Wai Man Cheung**
  - **ITB: basuki Suhardiman**
  - **KREONET: Buseung Cho**
  - **LEARN: Roshan Ragel**
  - **MYREN: Mohd Noh Jasmani**
  - **PERN: Kamran Abid**
  - **REANNZ: Culley Angus**
  - **Surrey University: Ning Wang**
  - **ThaiREN: Chalermpol Charnsripinyo**
  - **TransPAC: Hans Addleman**

The Technical Committee

- Co-Chairs
  - Changqing An (CERNET)
    Chalermpol Charnsripinyo(ThaiREN)
    Simon Green (SingAREN)
- Members
  - AARNET: Warrick Mitchell
  - APAN-JP: Sato-san, Ikeda-san, MA Jian
  - CERNET: Zhonghui Li, Xiaohong Huang, Hui Hao, Jie An
  - BdREN: Md. Ariful Islam Arman, Abu Naser Md. Nafew, Md. Ariful Islam, Jamilur Rahman, Shamim Ahmed, Kamrul Hasan Shakil, Md. Sajidul Islam
  - DOST-ASTI(PREGINET): Bayani Lara, Jaros Lacerna, Mark Quilala
  - ERNET: Hari Krishna Atluri

The Technical Committee(Cont'd)

- **Members:**
  - **Gottingen University: Xiaoming Fu**
  - **HARNET/JUCC: David Choi, KW Pong, Wai Man Cheung**
  - **ITB: Gulam**
  - **KREONET: Chanjin Park, Seongjin Park, Buseung Cho**
  - **LEARN: Dhammika Lalantha**
  - **MYREN: Hafizi Jalil, Mohd Noh Jasmani**
  - **PERN:Yahya Khan**
  - **REANNZ: Yeshaswini Ramesh, Dylan Hall**
  - **Surrey University: Ning Wang**
  - **ThaiREN: Sittichai Sangdee, Kriangsak Lekdee**
  - **TransPAC: Brenna Meade**

Project Executive Team

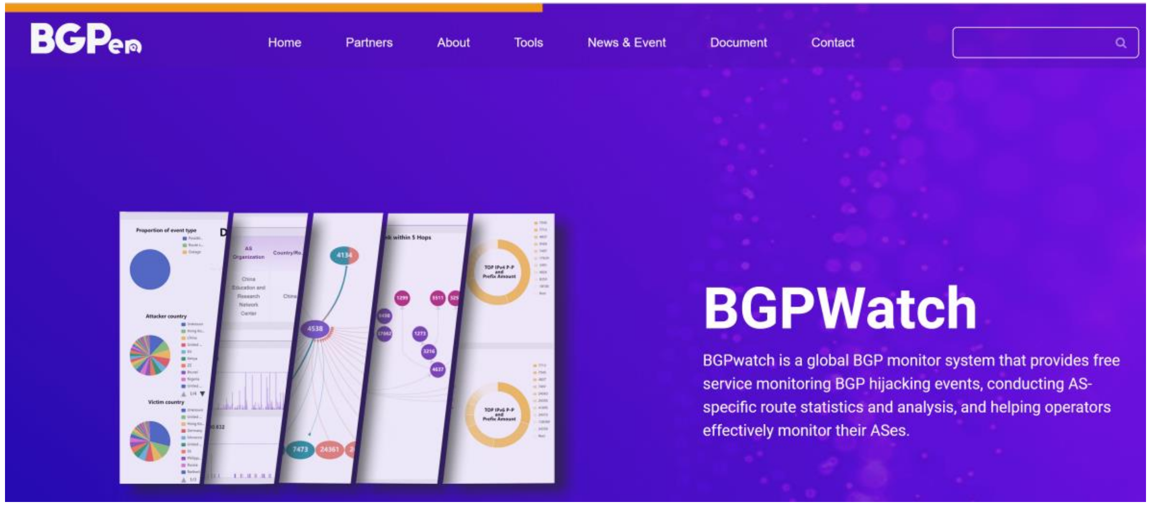
- **Team leaders**
  - **Jie An (CERNET), Changqing An(CERNET)**
- **Members(currently 10 members)**
  - **Chinese team will take the most responsibilities:**
    - **Zhonghui Li, Bei Zhang, Hui Hao, Zhiyan Zheng, Weiqi Zhao, Linmei Zu, Chengwan Zhang, Zhiquan Wang, Zidong Pei, Hang zhao**
  - **Welcome any contribution from other NREN partners**
- **Responsibility**
  - Coordination between the committees and partners
  - Programmer work of the platform development
  - Engineering collaboration
  - Coordination between technical and engineering teams
  - Project Management
  - Project Secretariat

Project Progress

- Project web site implementation
- Established BGP session with 15 partners
- Looking Glass connected with 7 Education & Research network
- BGPWatch: Analyzing and Diagnosing Platform
- Paper accepted by NOMS 2023
- Prefix Hijacking Annual Report
- Community Building and Knowledge Sharing

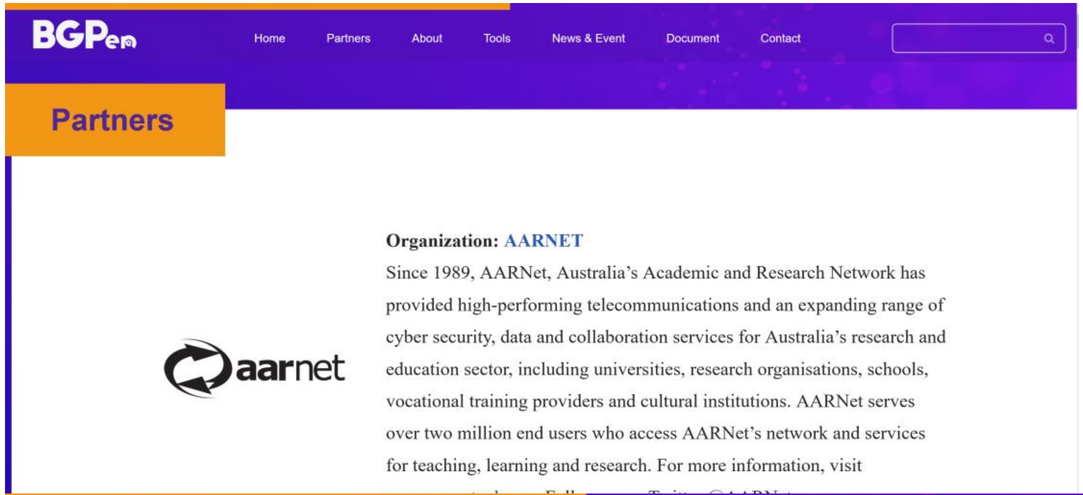
Project Web Site

https://bgper.net



BGPWatch

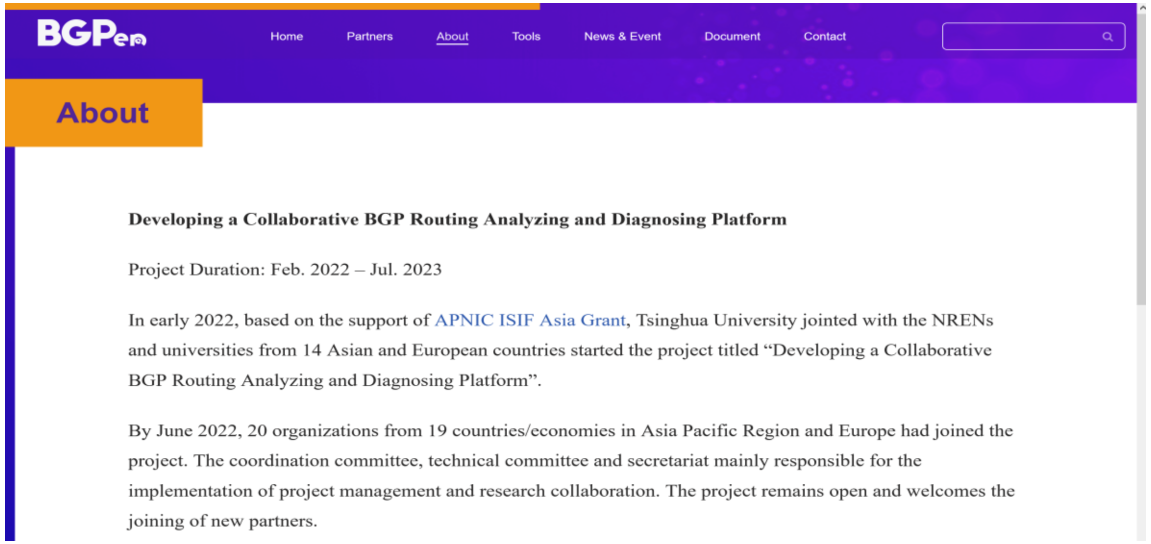
BGPwatch is a global BGP monitor system that provides free service monitoring BGP hijacking events, conducting AS-specific route statistics and analysis, and helping operators effectively monitor their ASes.



Partners

Organization: AARNET

Since 1989, AARNet, Australia's Academic and Research Network has provided high-performing telecommunications and an expanding range of cyber security, data and collaboration services for Australia's research and education sector, including universities, research organisations, schools, vocational training providers and cultural institutions. AARNet serves over two million end users who access AARNet's network and services for teaching, learning and research. For more information, visit



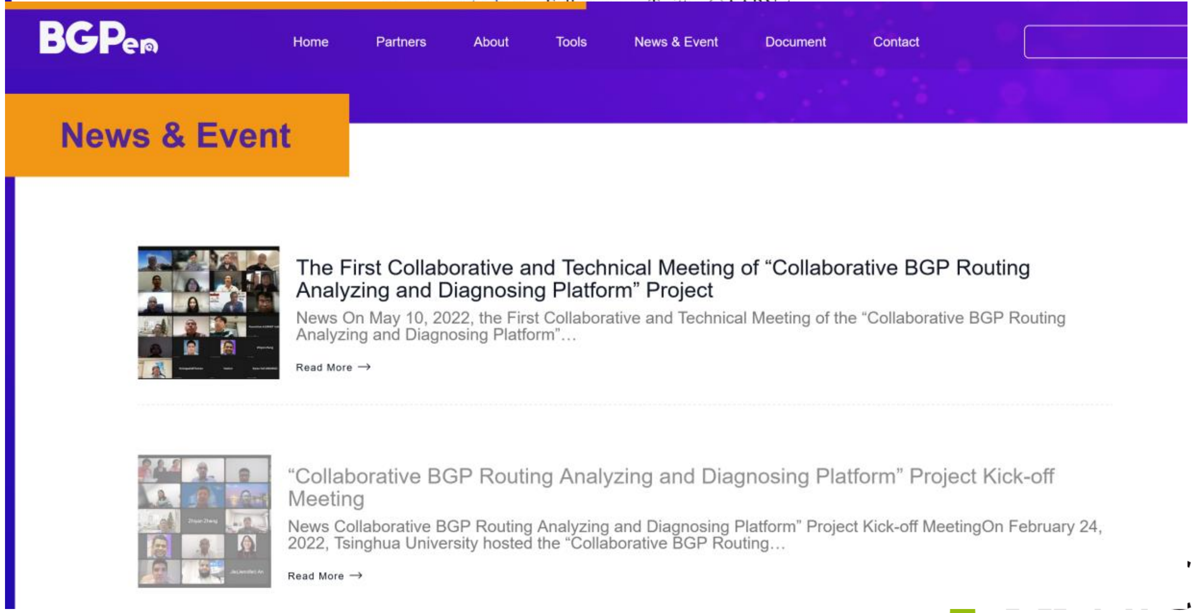
About

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Project Duration: Feb. 2022 – Jul. 2023

In early 2022, based on the support of APNIC ISIF Asia Grant, Tsinghua University jointed with the NRENs and universities from 14 Asian and European countries started the project titled "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform".

By June 2022, 20 organizations from 19 countries/economies in Asia Pacific Region and Europe had joined the project. The coordination committee, technical committee and secretariat mainly responsible for the implementation of project management and research collaboration. The project remains open and welcomes the joining of new partners.



News & Event

The First Collaborative and Technical Meeting of "Collaborative BGP Routing Analyzing and Diagnosing Platform" Project

News On May 10, 2022, the First Collaborative and Technical Meeting of the "Collaborative BGP Routing Analyzing and Diagnosing Platform"…

Read More →

"Collaborative BGP Routing Analyzing and Diagnosing Platform" Project Kick-off Meeting

News Collaborative BGP Routing Analyzing and Diagnosing Platform" Project Kick-off MeetingOn February 24, 2022, Tsinghua University hosted the "Collaborative BGP Routing…

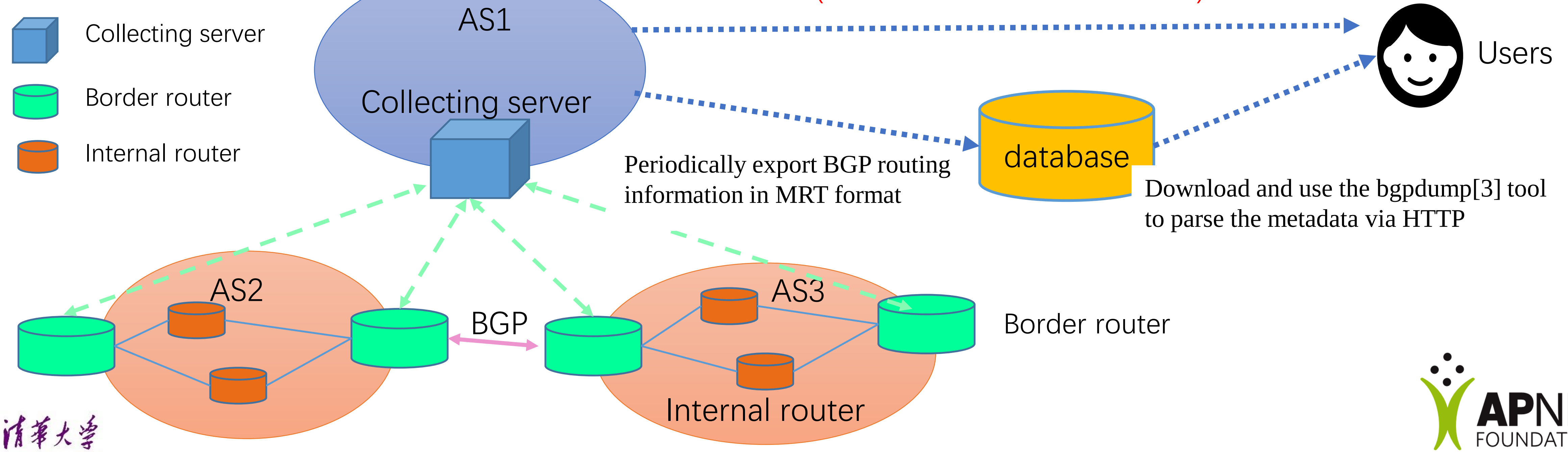
Read More →

BGP Routing Sharing: CGTF RIS

https://bgp.cgtf.net

- Collecting server： Use routing FRR[2] to simulate a real BGP router
- Border routers: Connect with the collecting server by BGP peering
- Feature: Lively Advertise Routing Announcements

Lively Advertise Routing Announcements through Web Socket (withdrawal/announcement)



Periodically export BGP routing information in MRT format

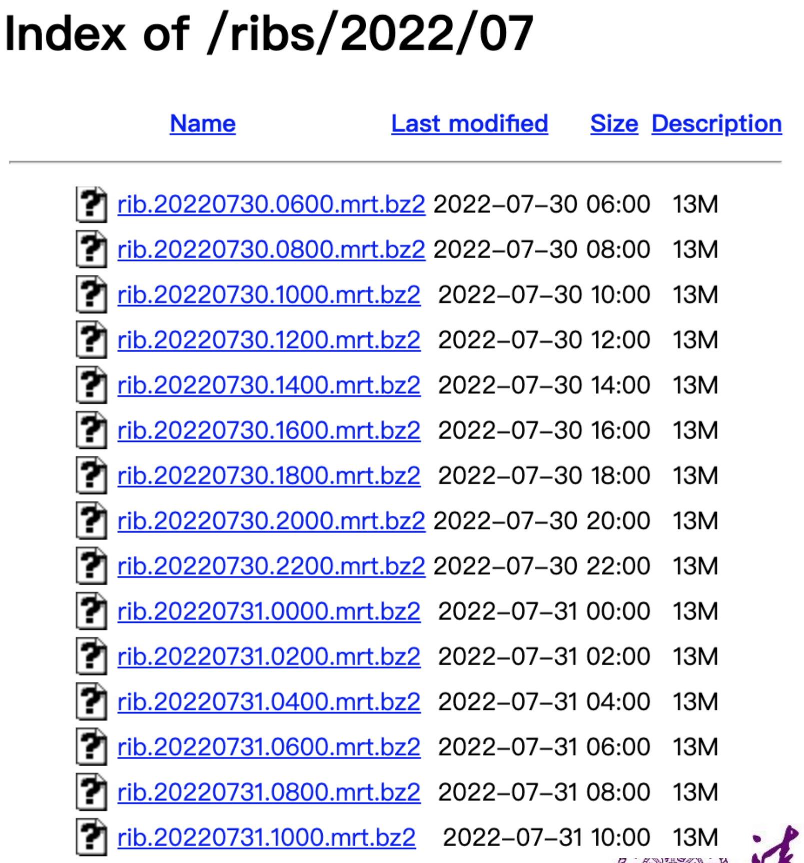
Download and use the bgpdump[3] tool to parse the metadata via HTTP

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

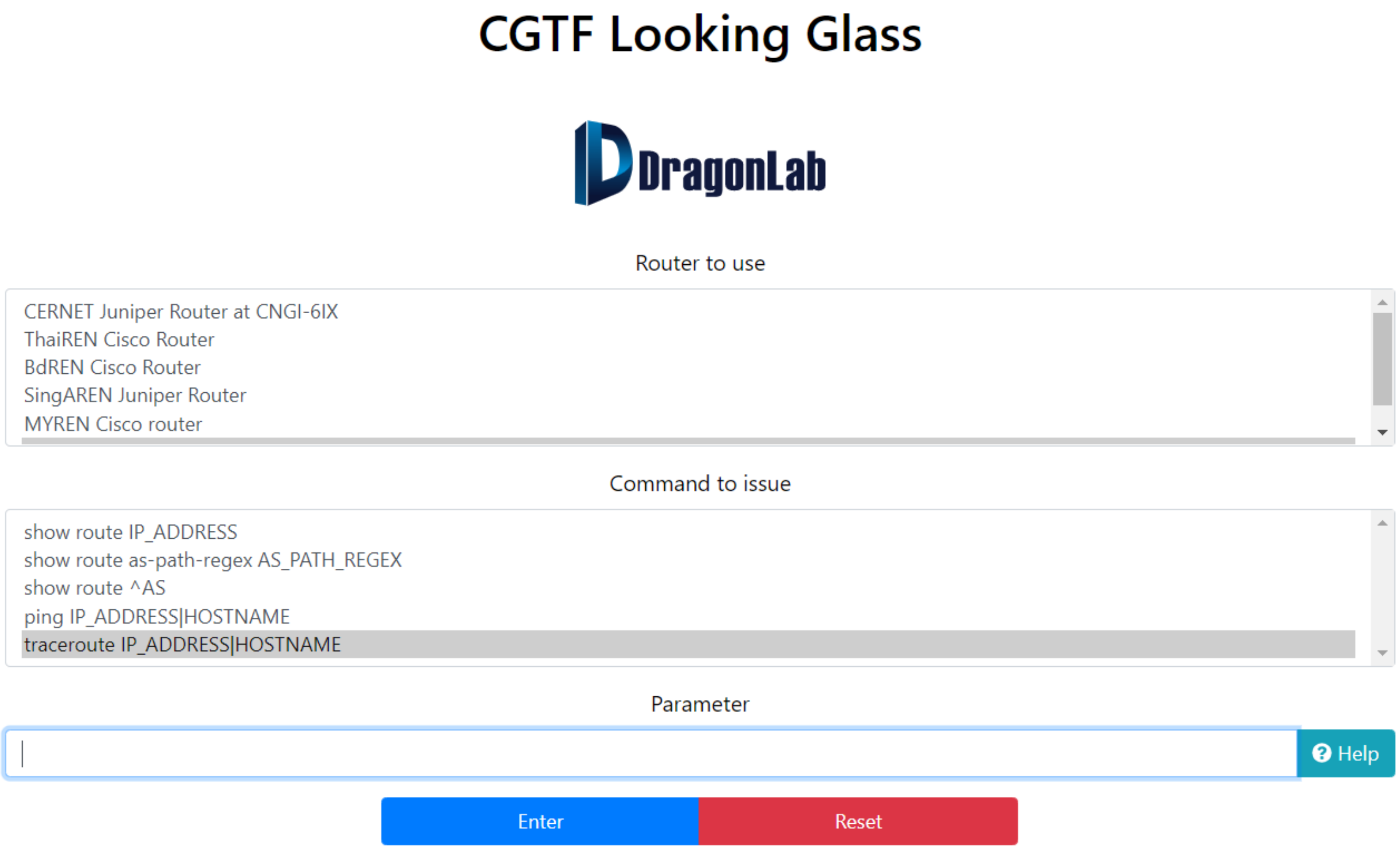
- Just have your border router **establish an eBGP session** with our collector:
- Our Collector ASN： 65534

- 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

CGTF Looking Glass

- https://lg.cgtf.net
- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 5 commands
- Query speed limit for security
- More partners are welcome



CGTF Looking Glass

DragonLab

Router to use

CERNET Juniper Router at CNGI-6IX
ThaiREN Cisco Router
BdREN Cisco Router
SingAREN Juniper Router
MYREN Cisco router

Command to issue

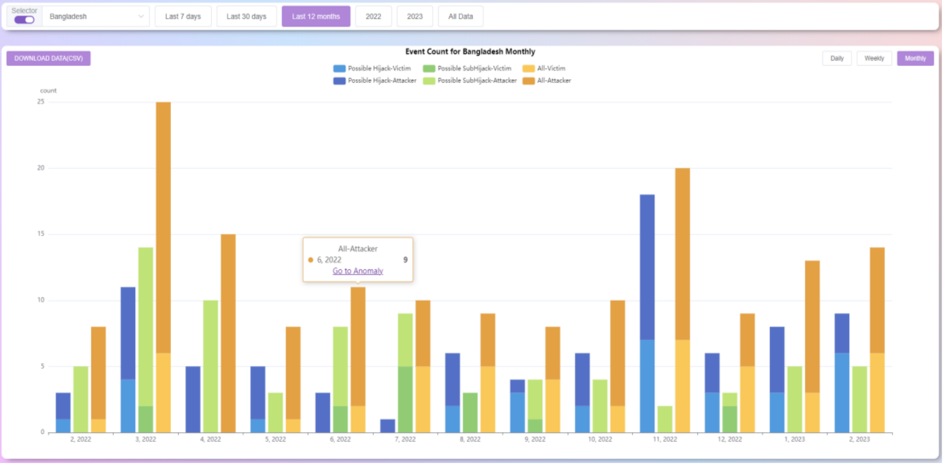
show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME

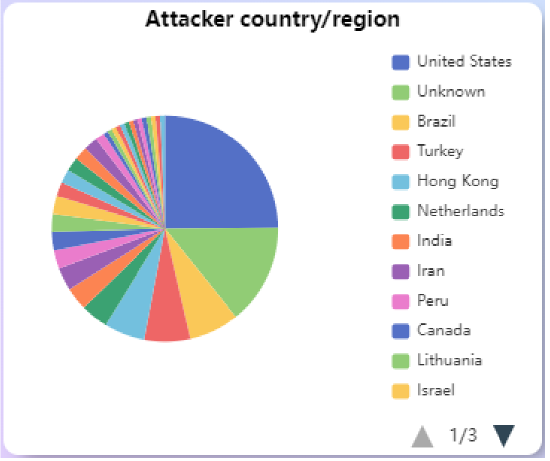
Parameter

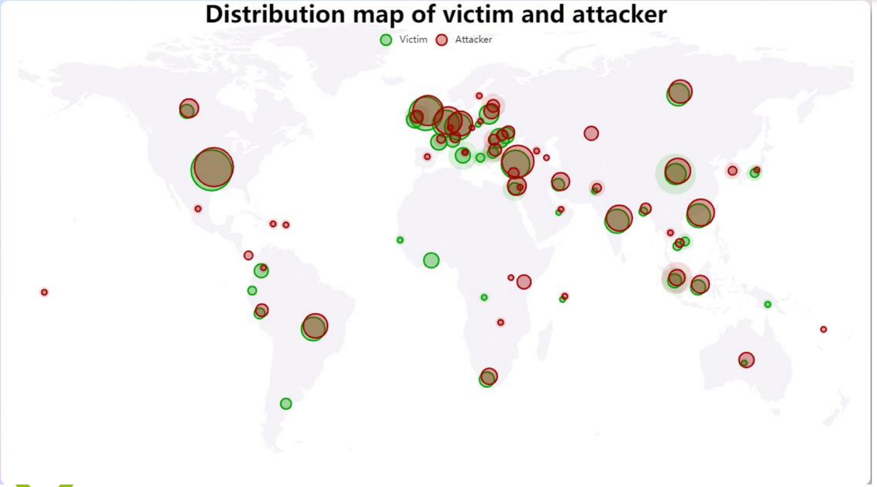
- 7 Education & Research network joined

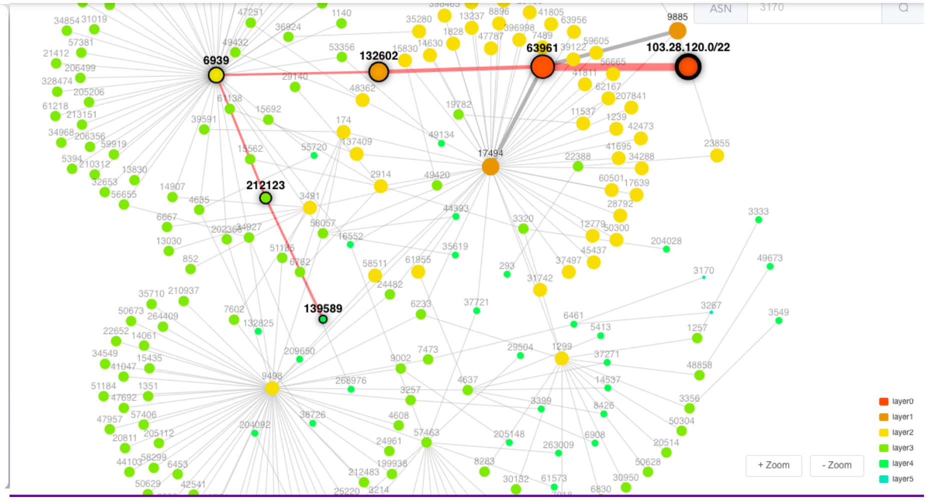
BGP Routing Monitoring and Analysis: BGPWatch

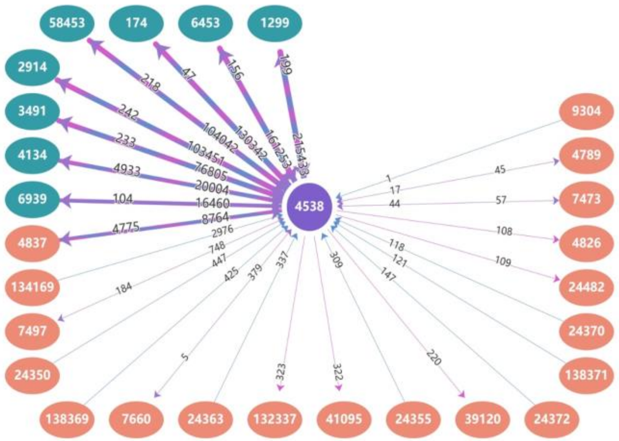
- Hijacking Detection
- Hijacking Statistics
- Dashboard:AS info
- Routing Search：
  - forward, reverse, bi-direction
- Subscribe, Alarming





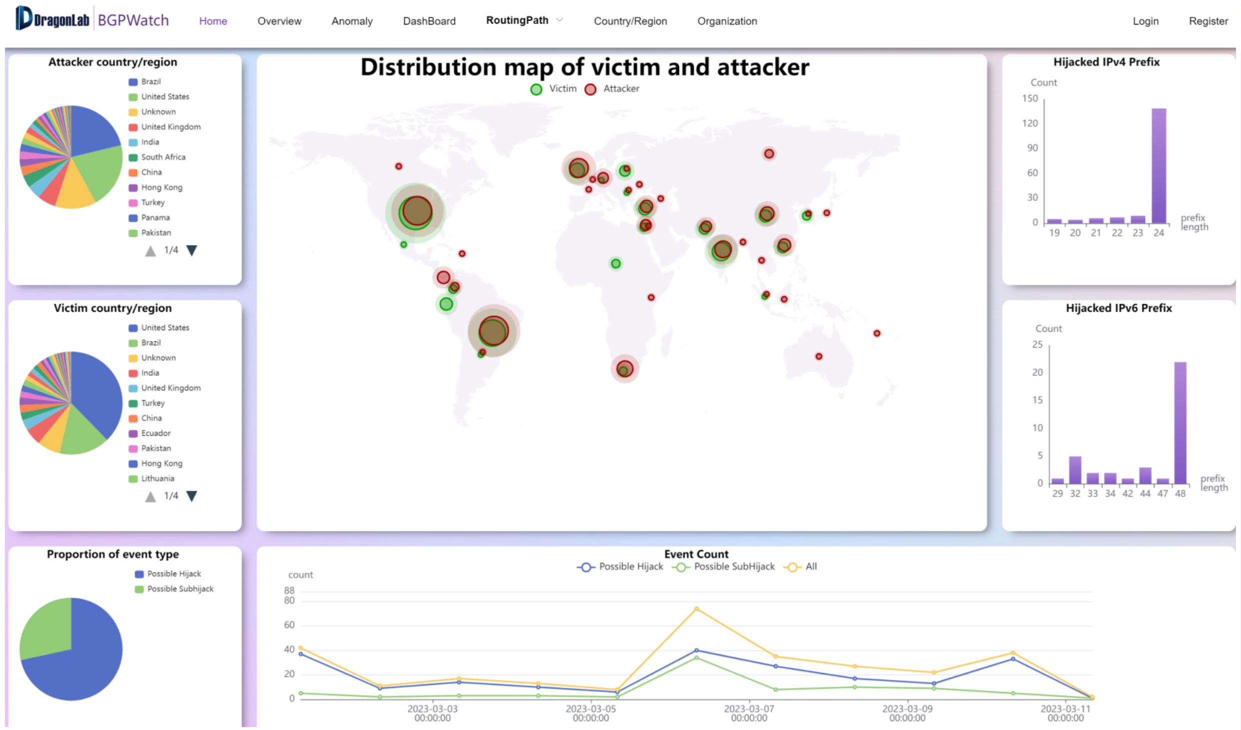


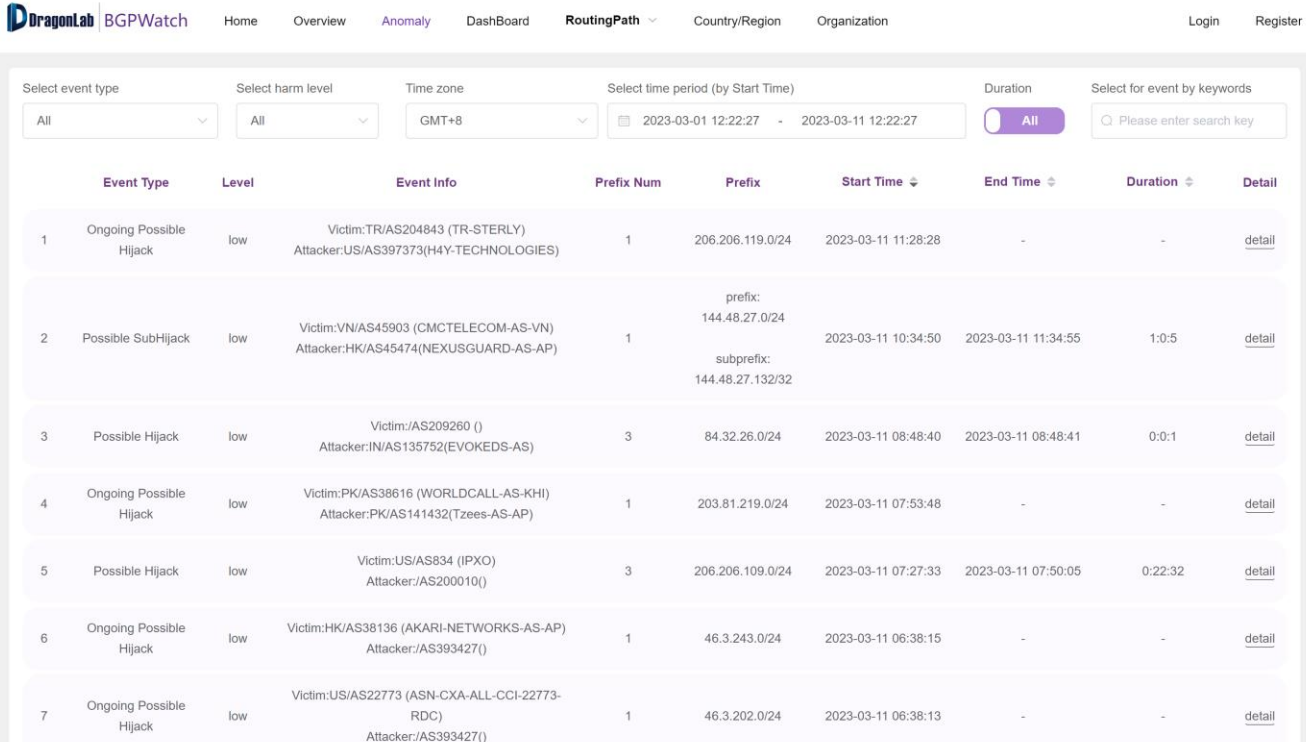




Hijacking Detection

- Knowledge-based real-tIme BGP hIjacking Detection System
- Public BGP event reporting servcie
- Based on MOAS(subMOAS)
- Rely on Domain Knowledge （ROA，IRR，AS relationship etc)
- URL: https://bgpwatch.cgtf.net





Select event type: All

Select harm level: All

Time zone: GMT+8

Select time period (by Start Time): 2023-03-01 12:22:27 - 2023-03-11 12:22:27

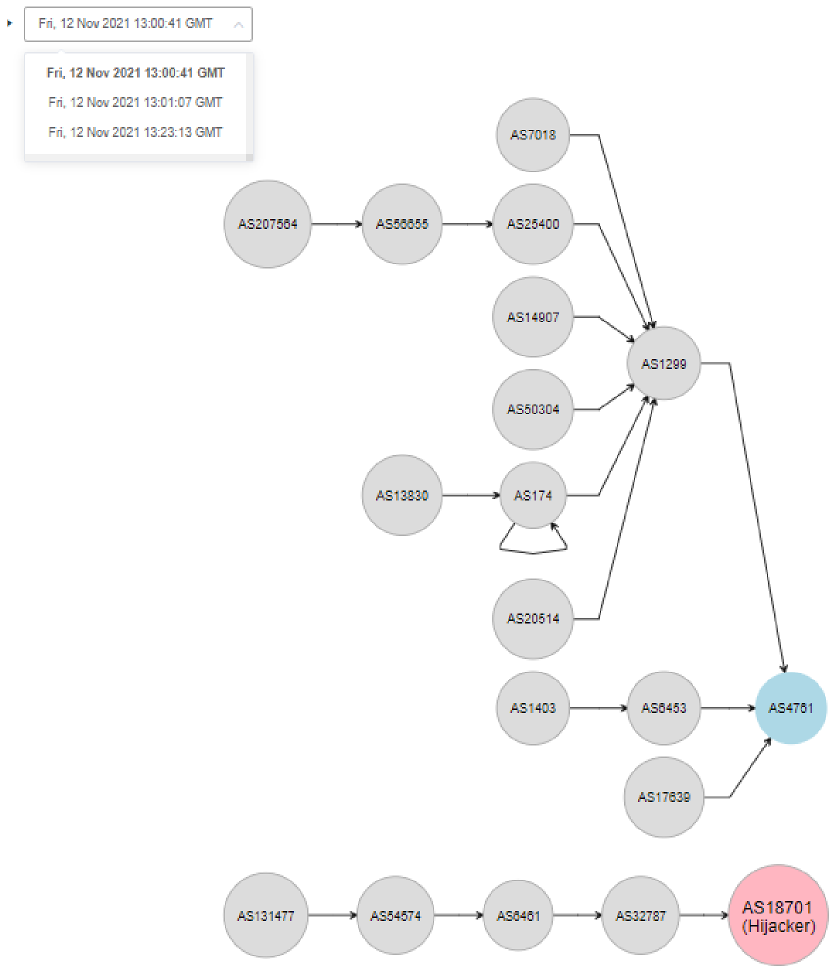
Duration: All

Select for event by keywords: Please enter search key

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2	Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail
3	Possible Hijack	low	Victim:/AS209260 () Attacker:IN/AS135752(EVOKEDS-AS)	3	84.32.26.0/24	2023-03-11 08:48:40	2023-03-11 08:48:41	0:0:1	detail
4	Ongoing Possible Hijack	low	Victim:PK/AS38616 (WORLDCALL-AS-KHI) Attacker:PK/AS141432(Tzees-AS-AP)	1	203.81.219.0/24	2023-03-11 07:53:48	-	-	detail
5	Possible Hijack	low	Victim:US/AS834 (IPXO) Attacker:/AS200010()	3	206.206.109.0/24	2023-03-11 07:27:33	2023-03-11 07:50:05	0:22:32	detail
6	Ongoing Possible Hijack	low	Victim:HK/AS38136 (AKARI-NETWORKS-AS-AP) Attacker:/AS393427()	1	46.3.243.0/24	2023-03-11 06:38:15	-	-	detail
7	Ongoing Possible Hijack	low	Victim:US/AS22773 (ASN-CXA-ALL-CCI-22773-RDC) Attacker:/AS393427()	1	46.3.202.0/24	2023-03-11 06:38:13	-	-	detail

Features --- Quick Response, Event replay

- About 5 mins delay, much better than other systems
- Notify 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



Fri, 12 Nov 2021 13:00:41 GMT

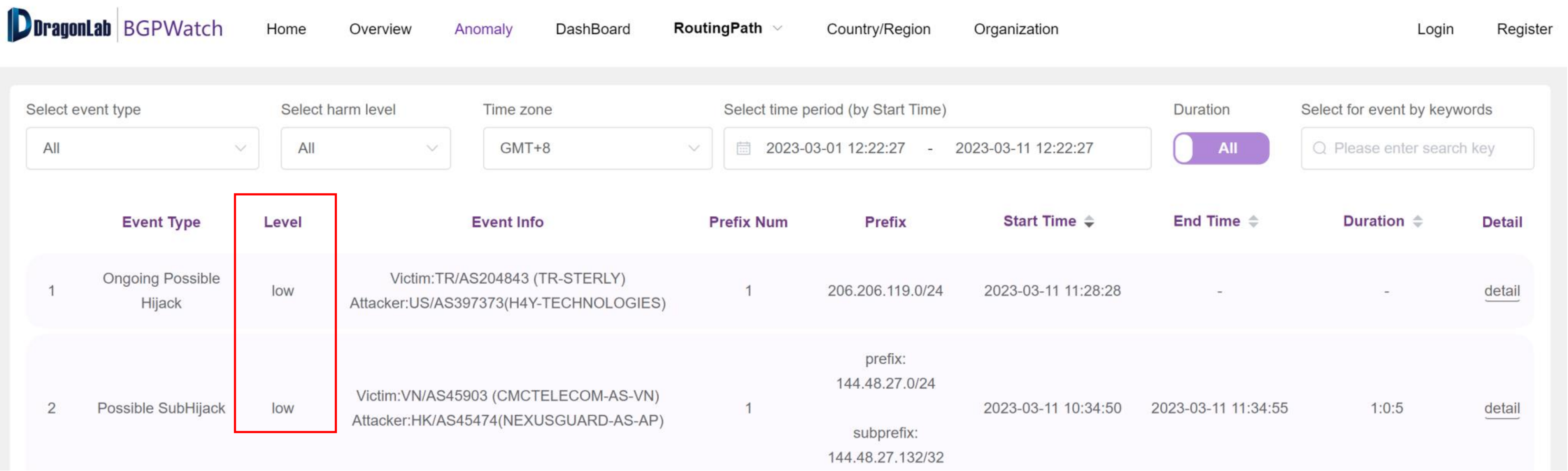
Fri, 12 Nov 2021 13:00:41 GMT

Fri, 12 Nov 2021 13:01:07 GMT

Fri, 12 Nov 2021 13:23:13 GMT

Features --- Event Level Evaluation

- **Evaluate event impact based on importance of AS and prefix.**



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

Select event type: All

Select harm level: All

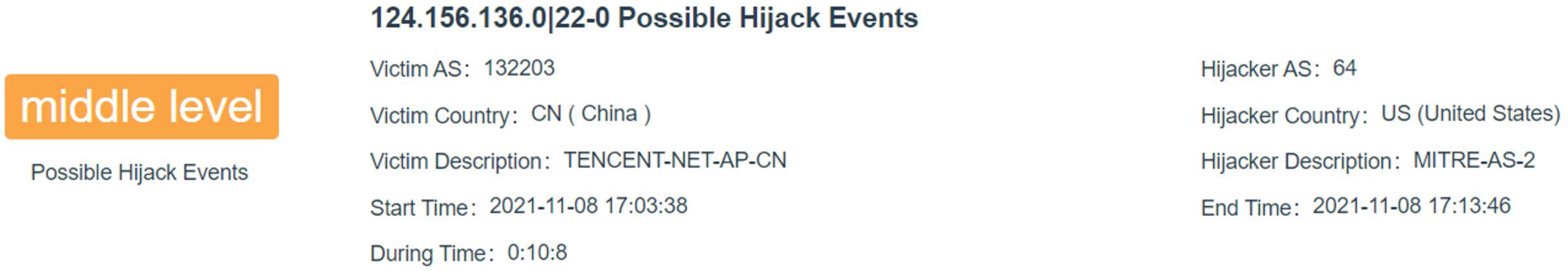
Time zone: GMT+8

Select time period (by Start Time): 2023-03-01 12:22:27 - 2023-03-11 12:22:27

Duration: All

Select for event by keywords: Please enter search key

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2	Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail



124.156.136.0|22-0 Possible Hijack Events

middle level

Possible Hijack Events

Victim AS： 132203

Victim Country： CN (China)

Victim Description： TENCENT-NET-AP-CN

Start Time： 2021-11-08 17:03:38

During Time： 0:10:8

Hijacker AS： 64

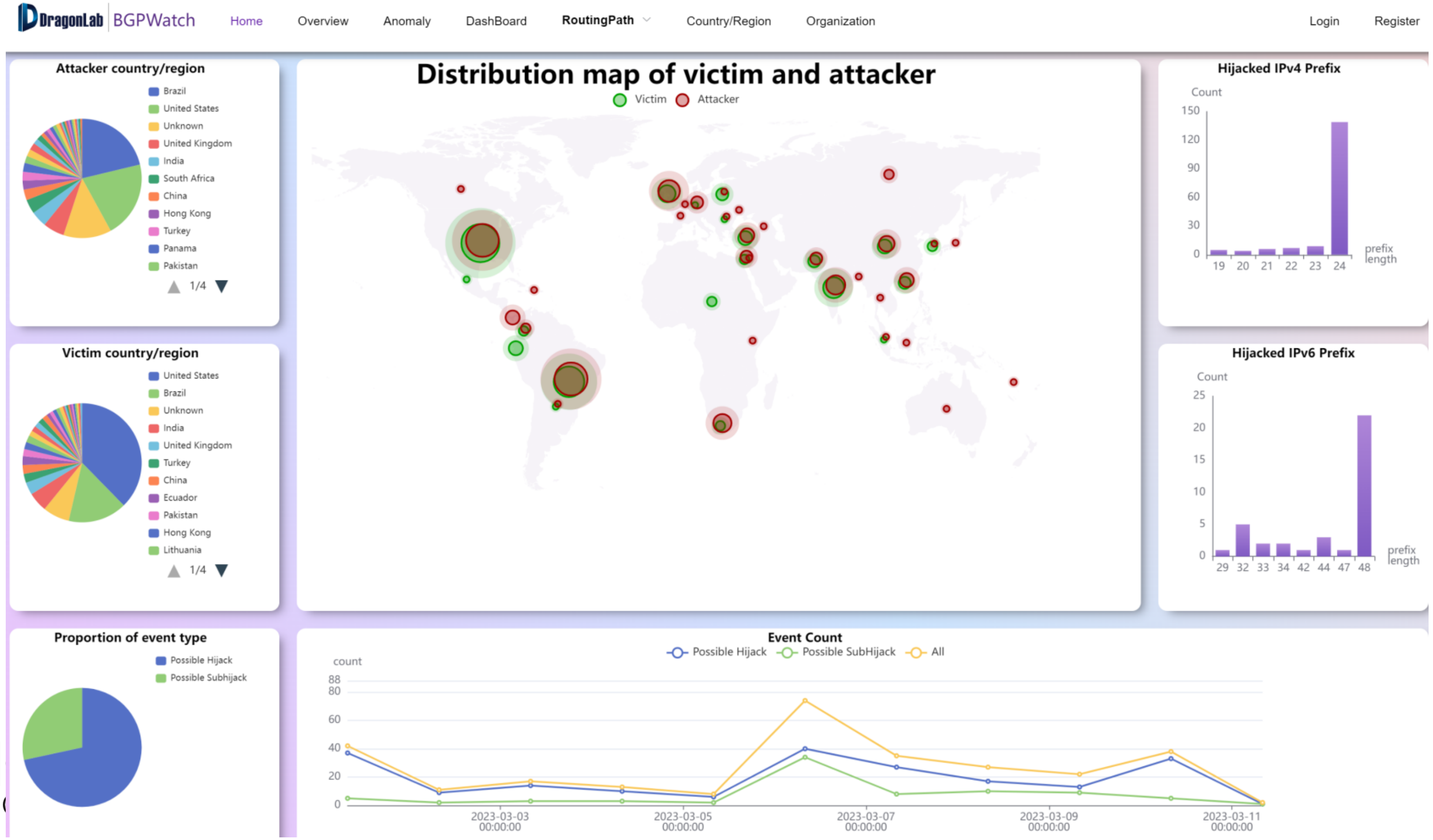
Hijacker Country： US (United States)

Hijacker Description： MITRE-AS-2

End Time： 2021-11-08 17:13:46

Features --- Event Statistics Analysis

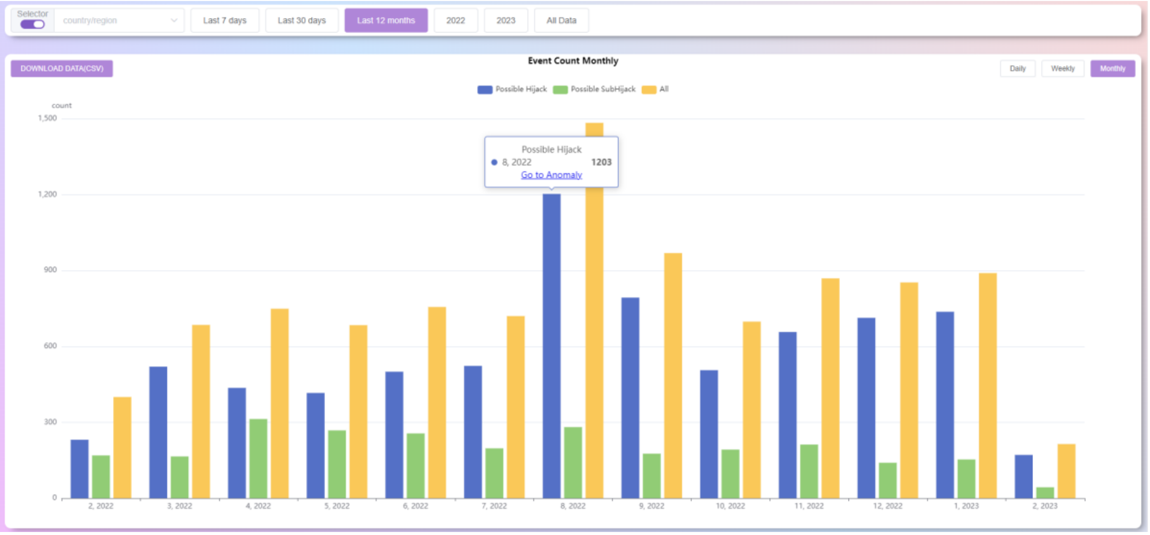
- Statistical analysis of event time,affected prefix, AS, country, etc.
- Global routing system security situational awareness

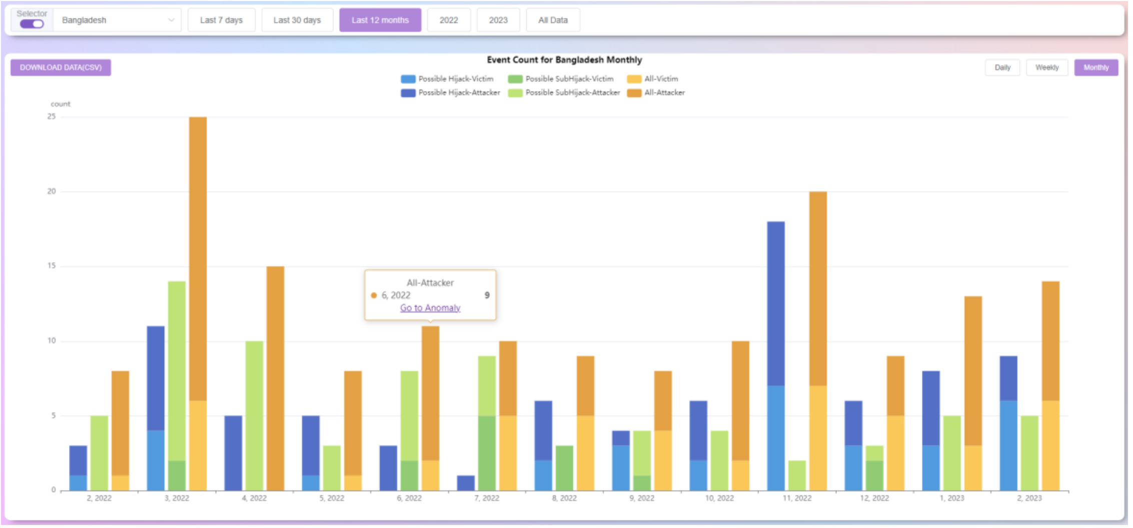


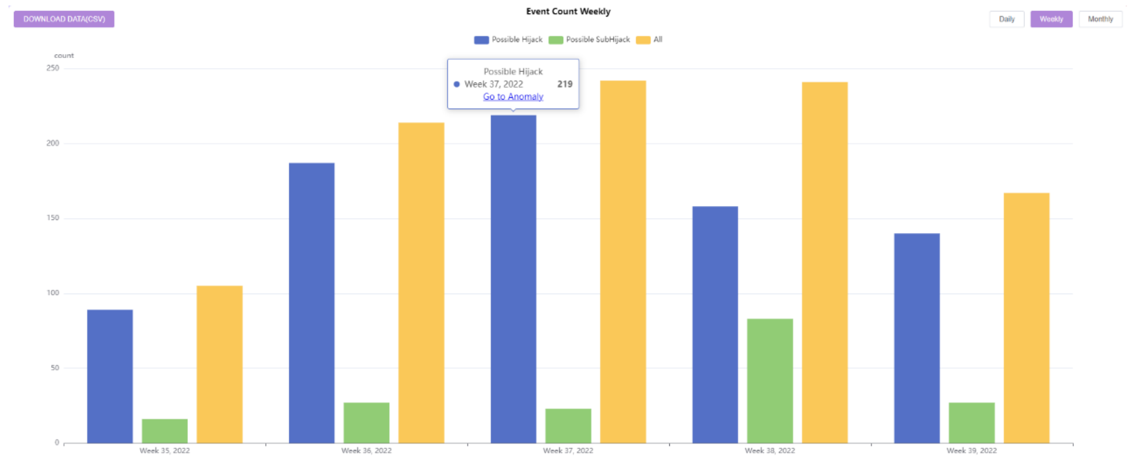
APNI FOUNDATI

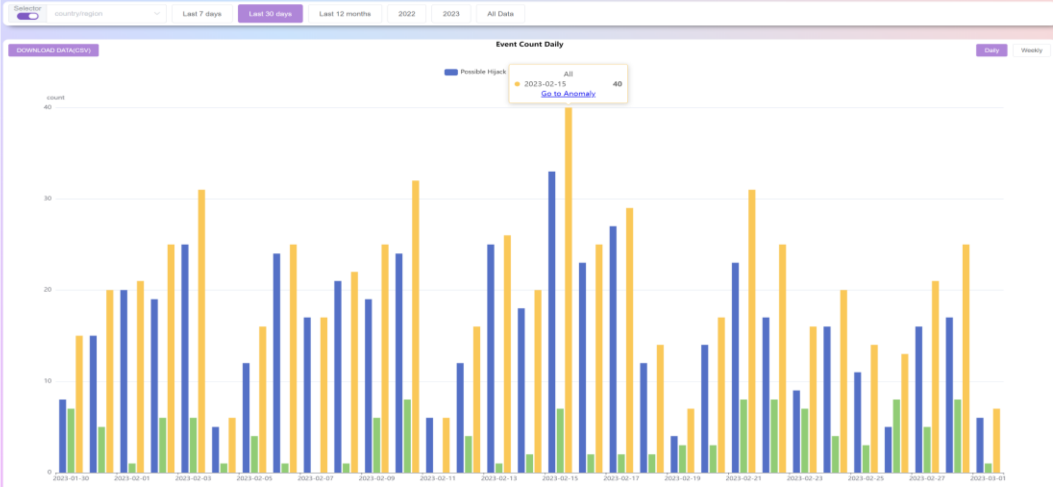
Tsinghua University

Overview--Statistics for Anomaly Events



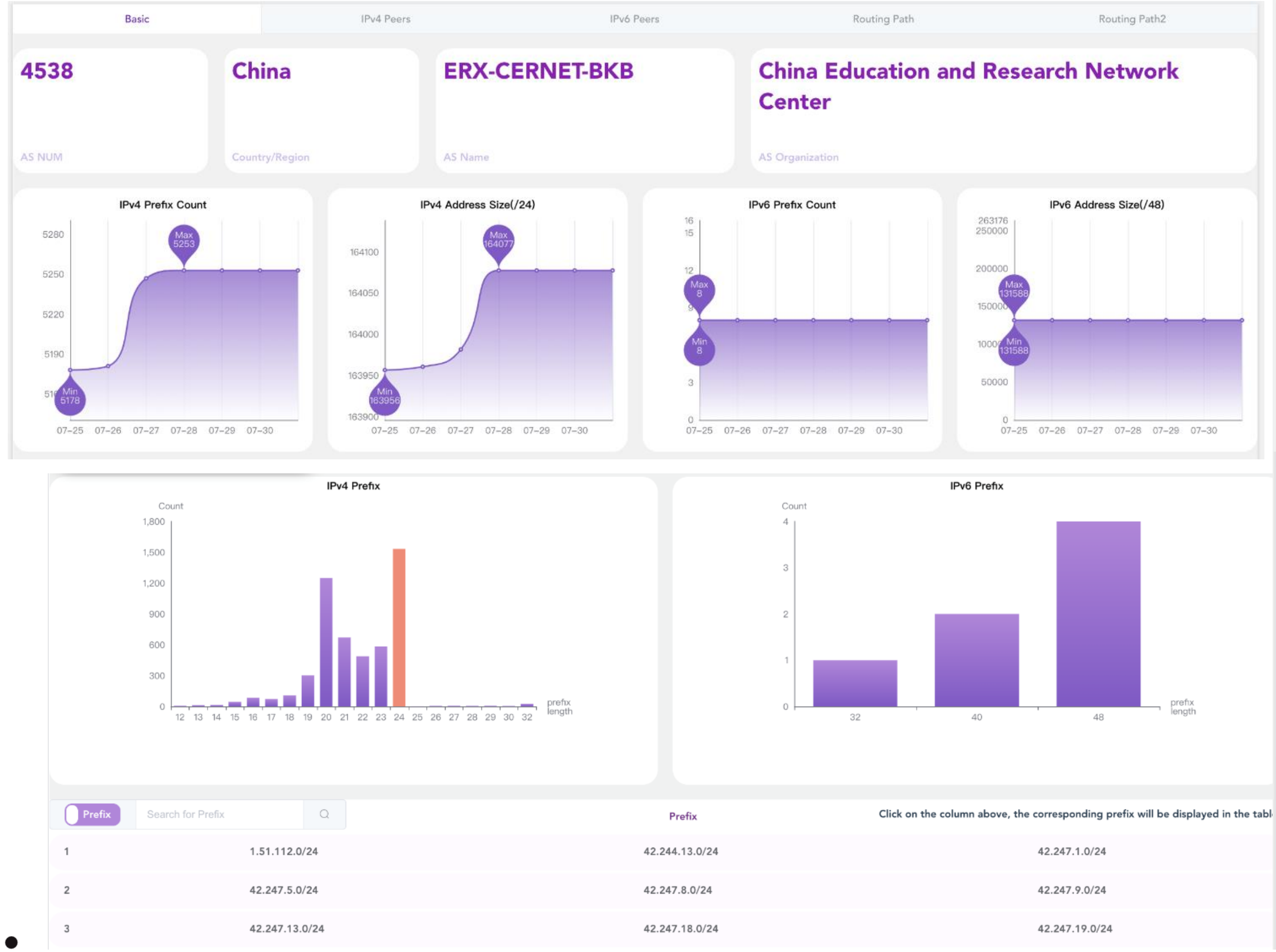






Do statistics by country/region, AS, and by yearly, monthly, weekly, and daily

DashBoard --Basic Info



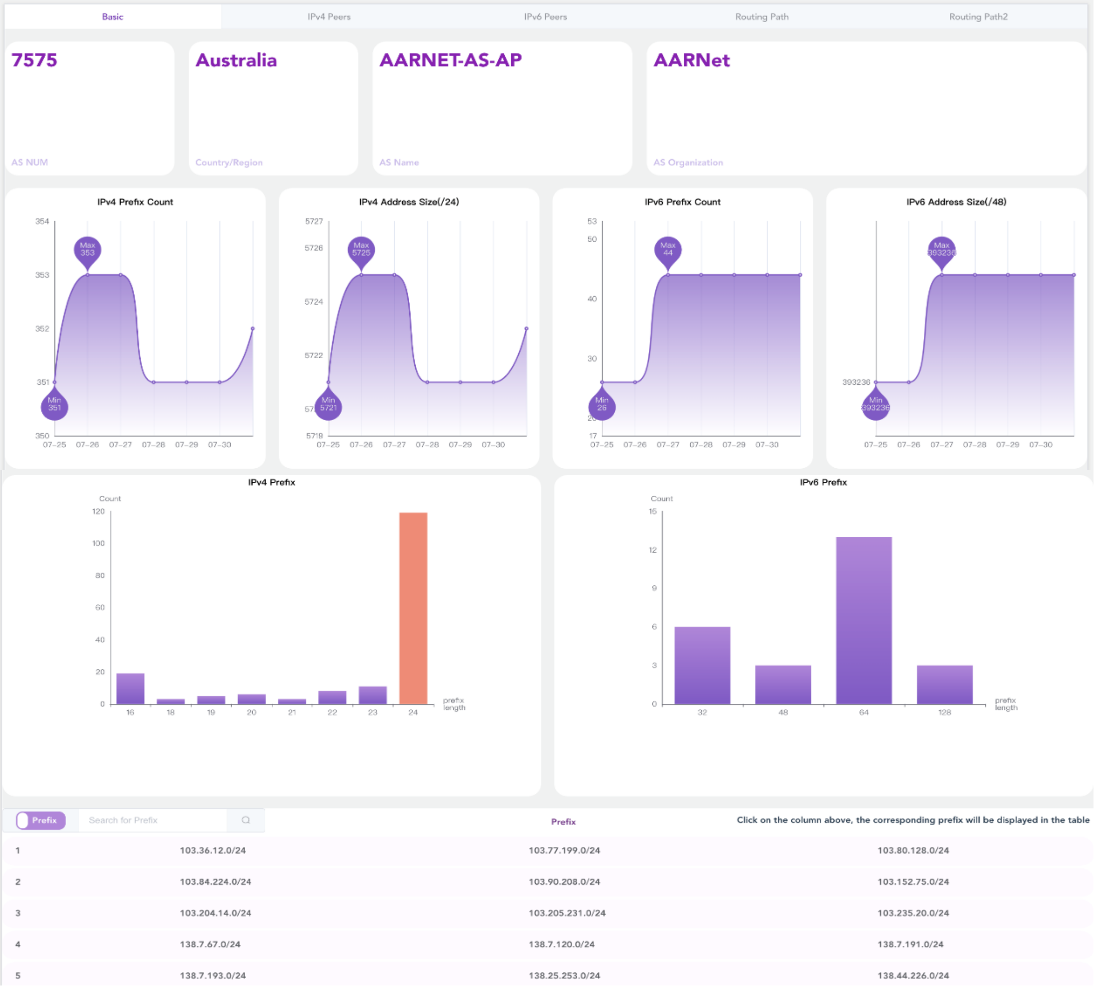
4538	China	ERX-CERNET-BKB	China Education and Research Network Center
AS NUM	Country/Region	AS Name	AS Organization

Prefix Search for Prefix

Prefix

Click on the column above, the corresponding prefix will be displayed in the tabl

1	1.51.112.0/24	42.244.13.0/24	42.247.1.0/24
2	42.247.5.0/24	42.247.8.0/24	42.247.9.0/24
3	42.247.13.0/24	42.247.18.0/24	42.247.19.0/24



7575	Australia	AARNET-AS-AP	AARNet
AS NUM	Country/Region	AS Name	AS Organization

Prefix Search for Prefix

Prefix

Click on the column above, the corresponding prefix will be displayed in the table

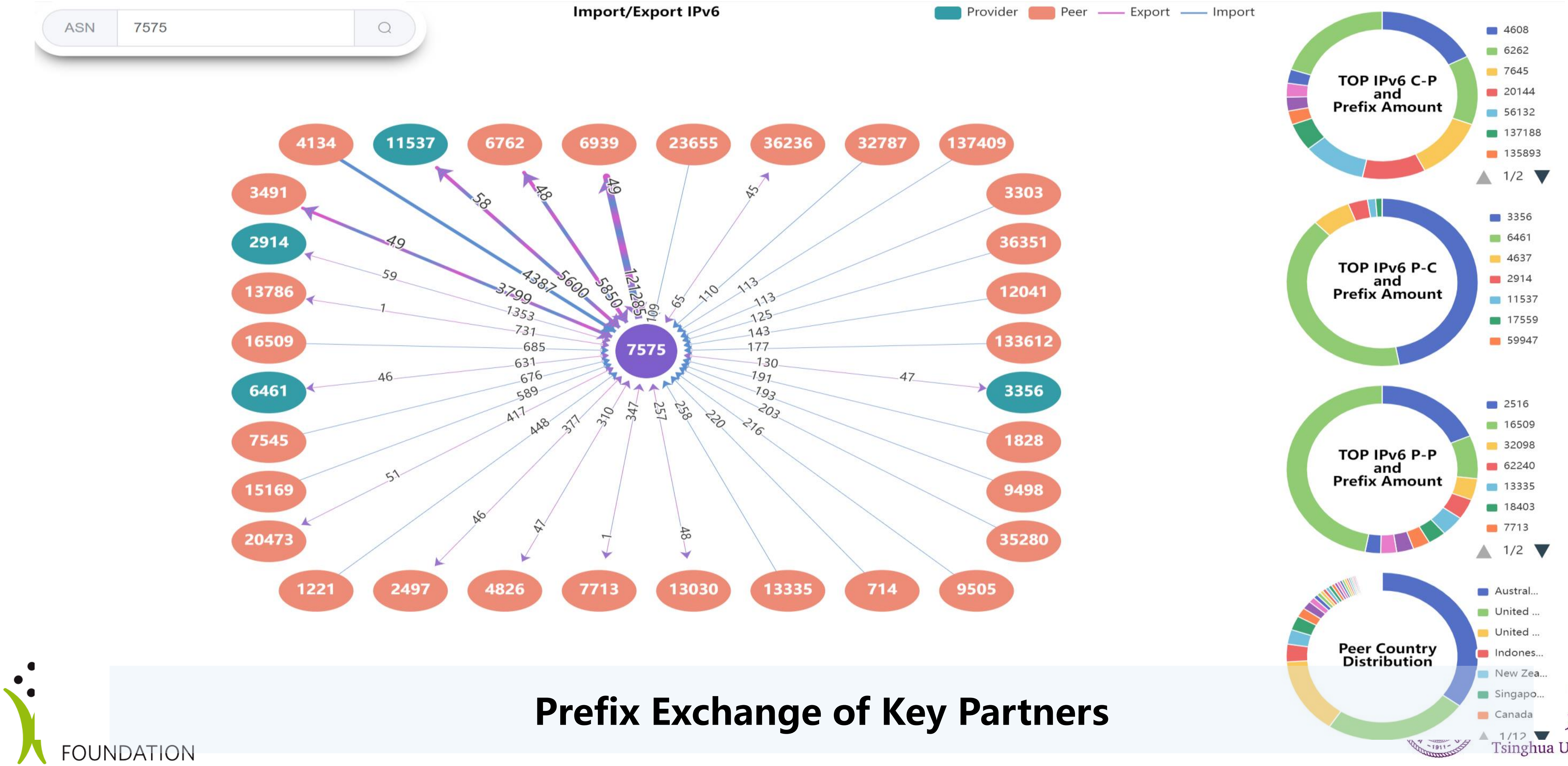
1	103.36.12.0/24	103.77.199.0/24	103.80.128.0/24
2	103.84.224.0/24	103.90.208.0/24	103.152.75.0/24
3	103.204.14.0/24	103.205.231.0/24	103.235.20.0/24
4	138.7.67.0/24	138.7.120.0/24	138.7.191.0/24
5	138.7.193.0/24	138.25.253.0/24	138.44.226.0/24

APNIC FOUNDATION

Support Prefix Search

清華大學 Tsinghua University

IPv6 Key Peers Information

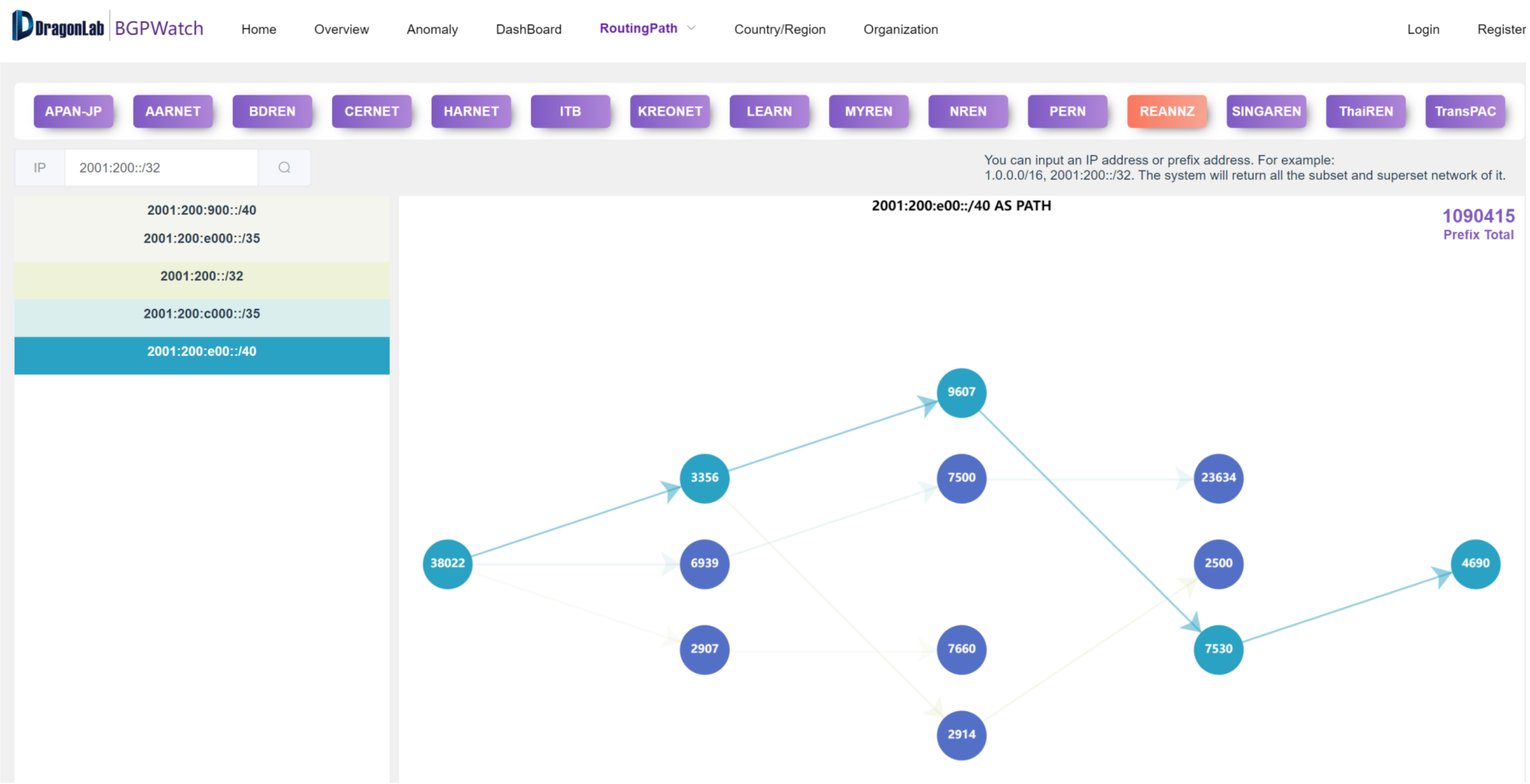


Prefix Exchange of Key Partners

FOUNDATION

Tsinghua University

Routing Path Search



You can input an IP address or prefix address. For example:
1.0.0.0/16, 2001:200::/32. The system will return all the subset and superset network of it.

2001:200:900::/40
2001:200:e000::/35

2001:200::/32

2001:200:c000::/35

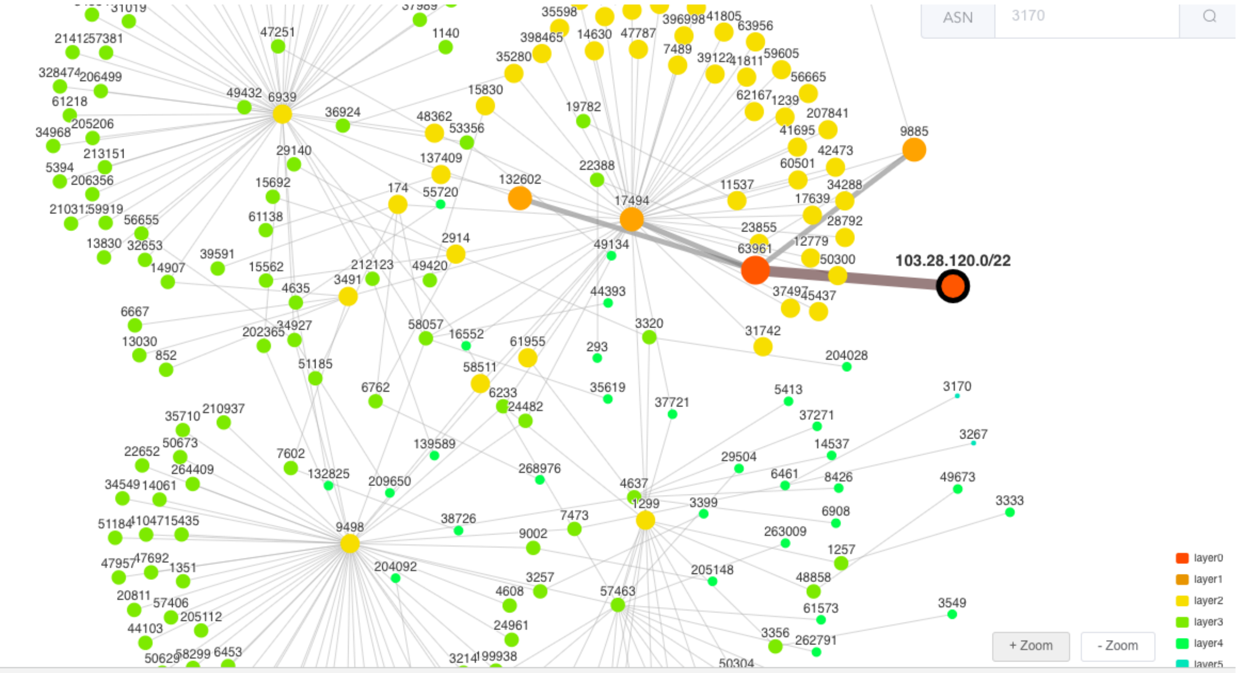
2001:200:e00::/40

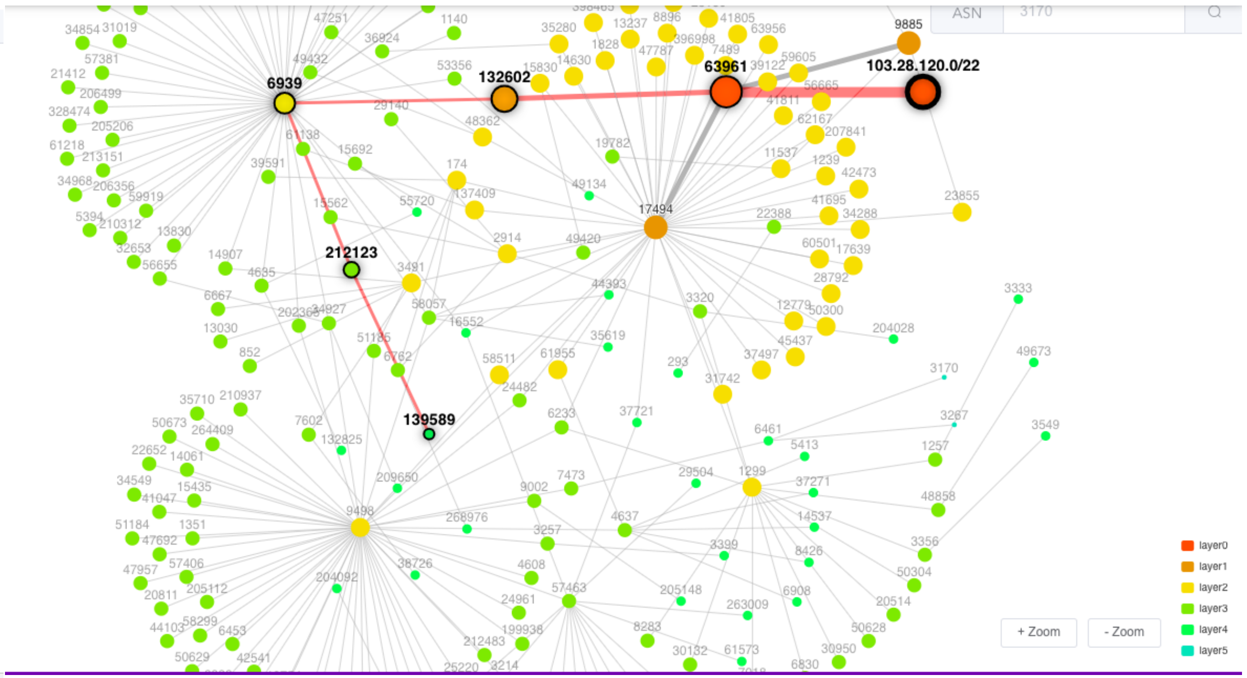
2001:200:e00::/40 AS PATH

1090415
Prefix Total

Put a prefix or an IP, they can be either IPv4 or IPv6. Return paths of all sub networks and super networks of the input prefix. **Group Prefixes with the same routing path.**

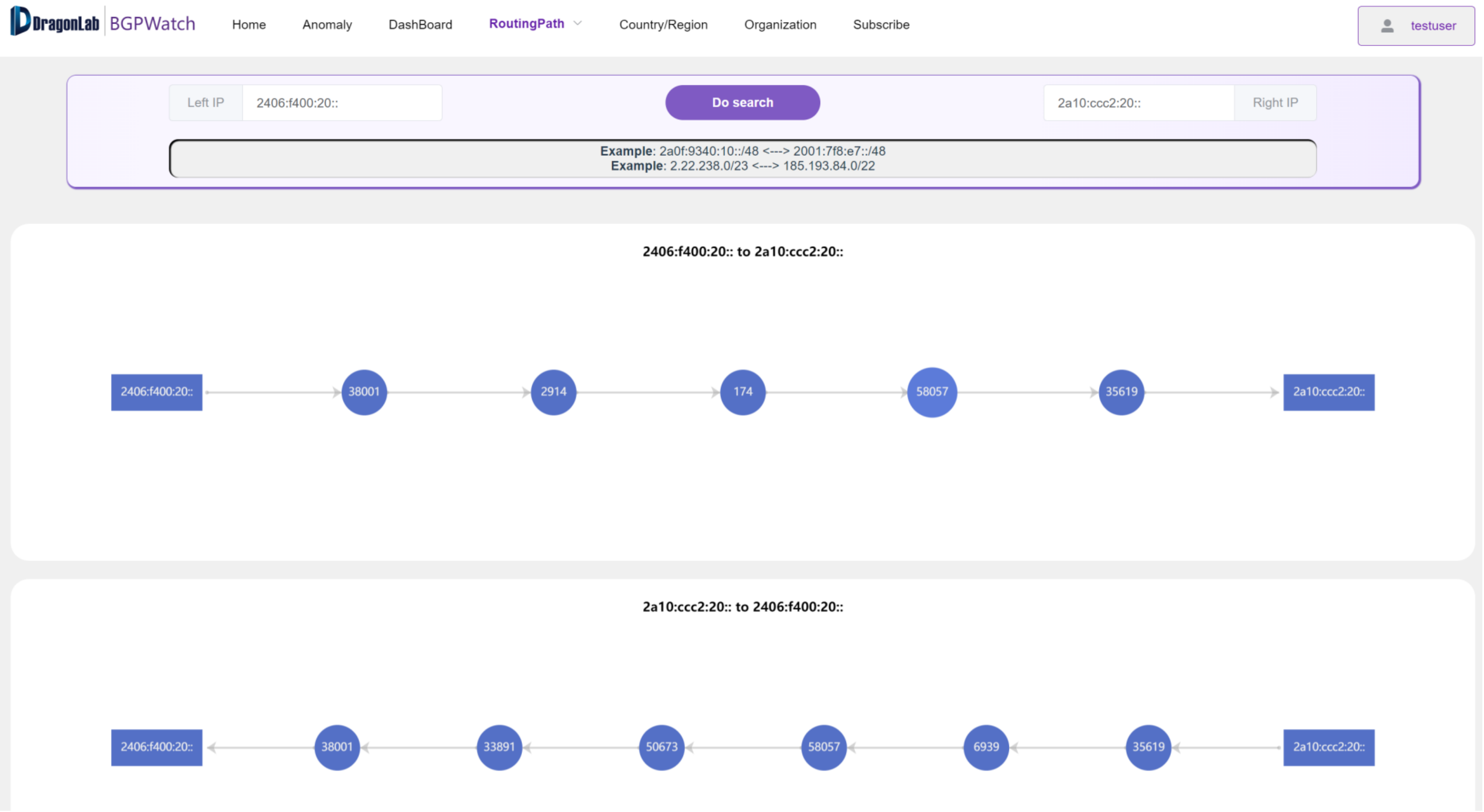
Reverse Routing Path (TOPO)





- With better interactivity
- Can display the path to an AS
- Support search
- The number of layers to display can be selected

Bi Direction Routing Path


DragonLab BGPWatch
Home
Anomaly
DashBoard
RoutingPath
Country/Region
Organization
Subscribe
testuser
Do search
2406:f400:20:: → 38001 → 2914 → 174 → 58057 → 35619 → 2a10:ccc2:20::
2406:f400:20:: ← 38001 ← 33891 ← 50673 ← 58057 ← 6939 ← 35619 ← 2a10:ccc2:20::

Left IP 2406:f400:20::

Right IP 2a10:ccc2:20::

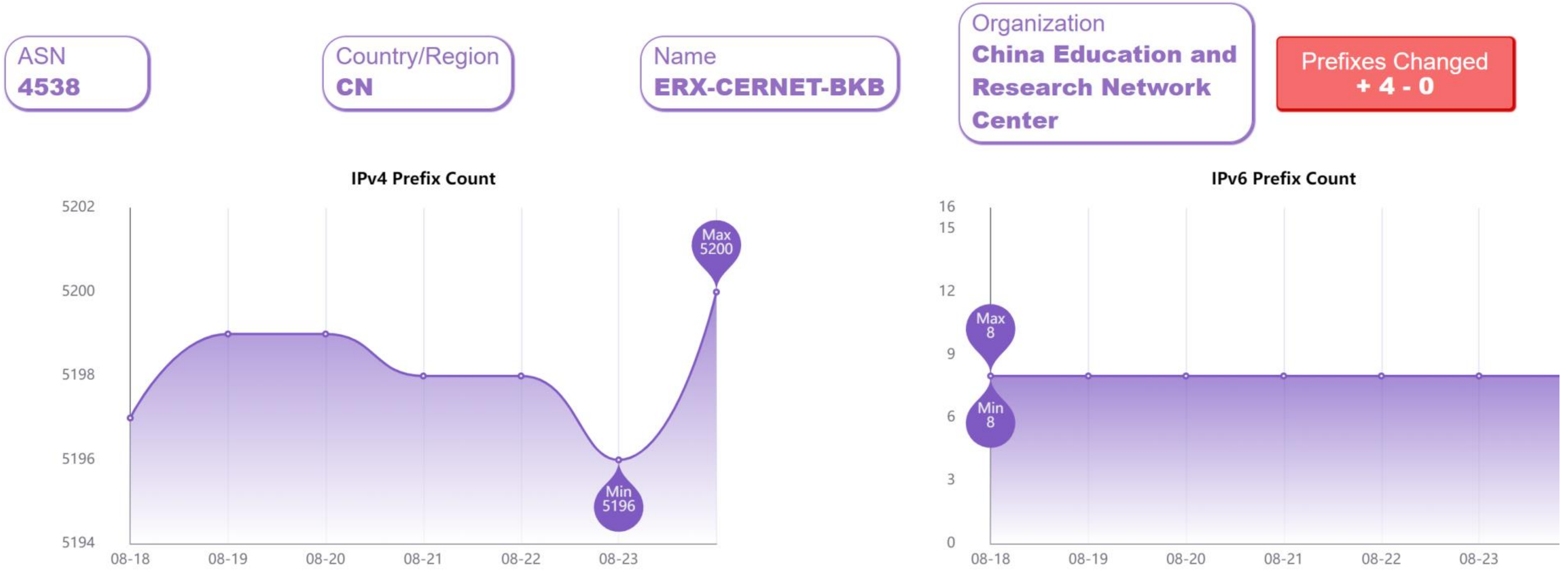
Example: 2a0f:9340:10::/48 <---> 2001:7f8:e7::/48
Example: 2.22.238.0/23 <---> 185.193.84.0/22

2406:f400:20:: to 2a10:ccc2:20::

2a10:ccc2:20:: to 2406:f400:20::

Put a prefix or an IP, they can be either IPv4 or IPv6.
The system will search the best matched prefix and return the reverse routing tree.

Subscribe and Send Alarm Email



ASN
4538

Country/Region
CN

Name
ERX-CERNET-BKB

Organization
China Education and Research Network Center

Prefixes Changed
+ 4 - 0

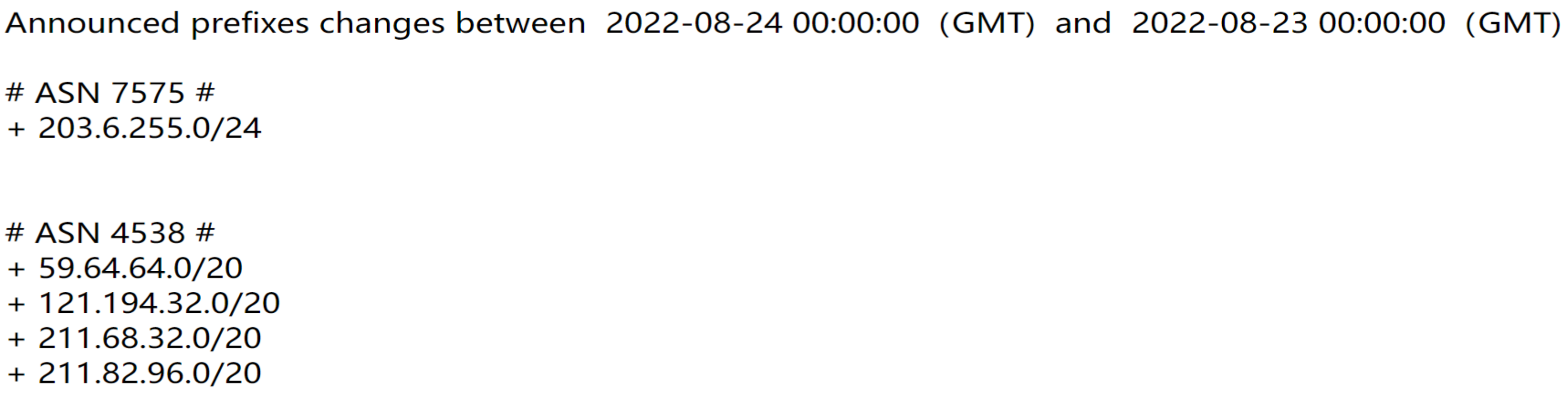
Prefix Change

+59.64.64.0/20

+121.194.32.0/20

+211.68.32.0/20

+211.82.96.0/20

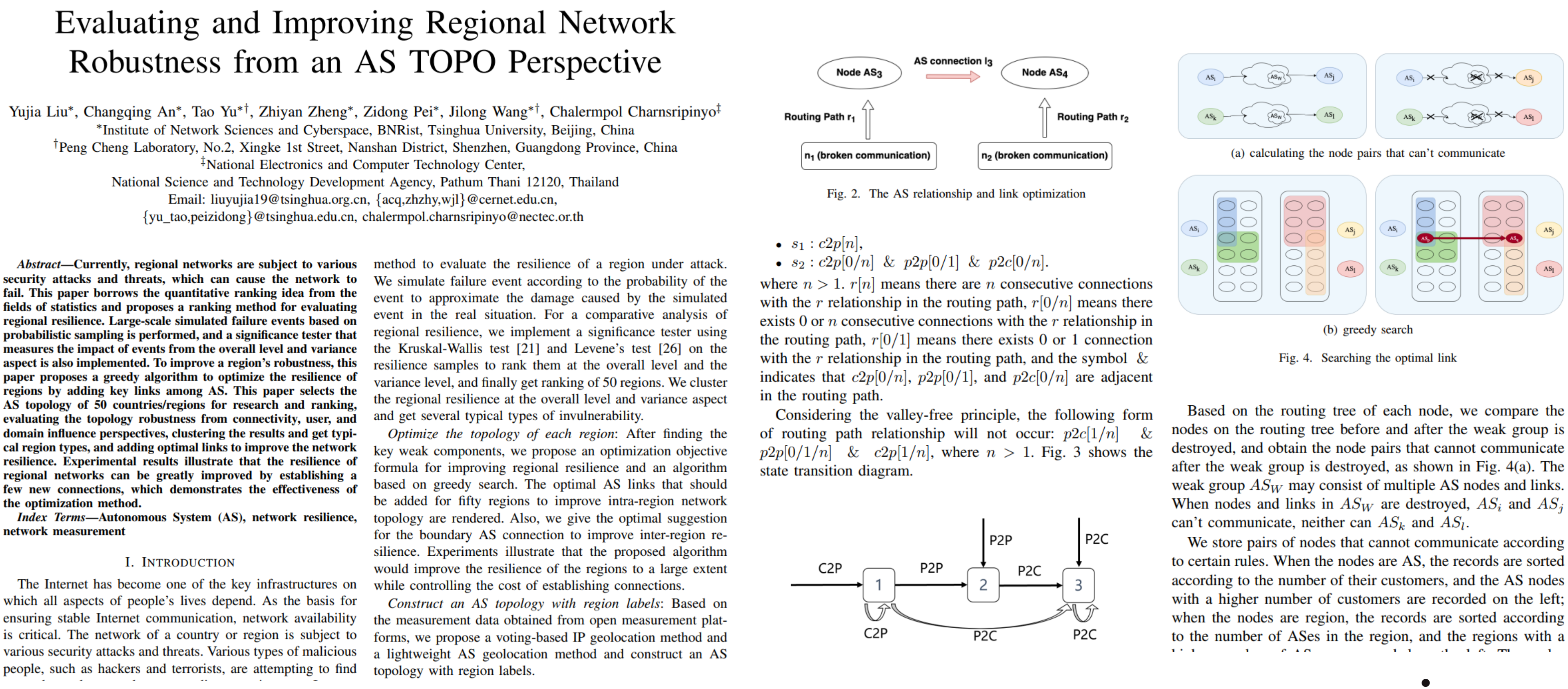


Announced prefixes changes between 2022-08-24 00:00:00 (GMT) and 2022-08-23 00:00:00 (GMT)

```
# ASN 7575 #
+ 203.6.255.0/24


# ASN 4538 #
+ 59.64.64.0/20
+ 121.194.32.0/20
+ 211.68.32.0/20
+ 211.82.96.0/20
```

Research Paper



Evaluating and Improving Regional Network Robustness from an AS TOPO Perspective

Yujia Liu*, Changqing An*, Tao Yu*†, Zhiyan Zheng*, Zidong Pei*, Jilong Wang*†, Chalermpol Charnsripinyo‡
*Institute of Network Sciences and Cyberspace, BNRist, Tsinghua University, Beijing, China
†Peng Cheng Laboratory, No.2, Xingke 1st Street, Nanshan District, Shenzhen, Guangdong Province, China
‡National Electronics and Computer Technology Center,
National Science and Technology Development Agency, Pathum Thani 12120, Thailand
Email: liuyujia19@tsinghua.org.cn, {acq,zhzhy,wjl}@cernet.edu.cn,
{yu_tao,peizidong}@tsinghua.edu.cn, chalermpol.charnsripinyo@nectec.or.th

***Abstract*—Currently, regional networks are subject to various security attacks and threats, which can cause the network to fail. This paper borrows the quantitative ranking idea from the fields of statistics and proposes a ranking method for evaluating regional resilience. Large-scale simulated failure events based on probabilistic sampling is performed, and a significance tester that measures the impact of events from the overall level and variance aspect is also implemented. To improve a region's robustness, this paper proposes a greedy algorithm to optimize the resilience of regions by adding key links among AS. This paper selects the AS topology of 50 countries/regions for research and ranking, evaluating the topology robustness from connectivity, user, and domain influence perspectives, clustering the results and get typical region types, and adding optimal links to improve the network resilience. Experimental results illustrate that the resilience of regional networks can be greatly improved by establishing a few new connections, which demonstrates the effectiveness of the optimization method.**

***Index Terms*—Autonomous System (AS), network resilience, network measurement**

I. Introduction

The Internet has become one of the key infrastructures on which all aspects of people's lives depend. As the basis for ensuring stable Internet communication, network availability is critical. The network of a country or region is subject to various security attacks and threats. Various types of malicious people, such as hackers and terrorists, are attempting to find

method to evaluate the resilience of a region under attack. We simulate failure event according to the probability of the event to approximate the damage caused by the simulated event in the real situation. For a comparative analysis of regional resilience, we implement a significance tester using the Kruskal-Wallis test [21] and Levene's test [26] on the resilience samples to rank them at the overall level and the variance level, and finally get ranking of 50 regions. We cluster the regional resilience at the overall level and variance aspect and get several typical types of invulnerability.

Optimize the topology of each region: After finding the key weak components, we propose an optimization objective formula for improving regional resilience and an algorithm based on greedy search. The optimal AS links that should be added for fifty regions to improve intra-region network topology are rendered. Also, we give the optimal suggestion for the boundary AS connection to improve inter-region resilience. Experiments illustrate that the proposed algorithm would improve the resilience of the regions to a large extent while controlling the cost of establishing connections.

Construct an AS topology with region labels: Based on the measurement data obtained from open measurement platforms, we propose a voting-based IP geolocation method and a lightweight AS geolocation method and construct an AS topology with region labels.

Fig. 2. The AS relationship and link optimization

- $s_1 : c2p[n]$,
- $s_2 : c2p[0/n]$ & $p2p[0/1]$ & $p2c[0/n]$.

where $n > 1$. $r[n]$ means there are n consecutive connections with the r relationship in the routing path, $r[0/n]$ means there exists 0 or n consecutive connections with the r relationship in the routing path, $r[0/1]$ means there exists 0 or 1 connection with the r relationship in the routing path, and the symbol & indicates that $c2p[0/n]$, $p2p[0/1]$, and $p2c[0/n]$ are adjacent in the routing path.

Considering the valley-free principle, the following form of routing path relationship will not occur: $p2c[1/n]$ & $p2p[0/1/n]$ & $c2p[1/n]$, where $n > 1$. Fig. 3 shows the state transition diagram.

(a) calculating the node pairs that can't communicate

(b) greedy search

Fig. 4. Searching the optimal link

Based on the routing tree of each node, we compare the nodes on the routing tree before and after the weak group is destroyed, and obtain the node pairs that cannot communicate after the weak group is destroyed, as shown in Fig. 4(a). The weak group AS_W may consist of multiple AS nodes and links. When nodes and links in AS_W are destroyed, AS_i and AS_j can't communicate, neither can AS_k and AS_l.

We store pairs of nodes that cannot communicate according to certain rules. When the nodes are AS, the records are sorted according to the number of their customers, and the AS nodes with a higher number of customers are recorded on the left; when the nodes are region, the records are sorted according to the number of ASes in the region, and the regions with a

- Accepted by NOMS 2023
- https://github.com/thudragonlab/Resilience

- The RPKI Online Basic Knowledge Training

Time：05:00-07:00(GMT) February 1, 2023

- The RPKI Online Hands-on Training

Time：05:00-07:30(GMT) February 3, 2023

RPKI Training

APNIC ISIF Project

www.bgper.net

The Online Training in February

RPKI Basic Knowledge		
Date/Time	Length	Trainer/APNIC
1st Feb. 2023 (Wednesday) 0500-0700 GMT	2 hours	Warren Finch(trainer), Awal Haolader(assistant)
RPKI Hands-on		
3rd Feb. 2023 (Friday) 0500-0730 GMT	2.5 hours	Warren Finch, Awal Haolader(assistant)
Remarks		

Open Links via APNIC Academy:

https://academy.apnic.net/en/events?id=a0B2e000000cg1jEAA

https://academy.apnic.net/en/events?id=a0B2e000000cg3BEAQ

80 Engineers and Technicians take part in

APNIC FOUNDATION · 清華大學 Tsinghua University · APNIC · APAN · NREN

APNIC ISIF Project – RPKI & MANRS Training at APAN55

13th, 15th and 16th March, 2023   Kathmandu, Nepal

13th March, 2023 (Monday)

Time (GMT+5:45)	Topic	Trainer
09:00 - 10:30	RPKI - Theory	Dibya Khatiwada APNIC Community Trainer
10:30 - 11:00	Tea/Coffee Break	
11:00 - 12:30	RPKI - Theory RPKI - Hands-on	Dibya Khatiwada APNIC Community Trainer
12:30 - 13:30	Lunch Break	
13:30 - 15:00	RPKI - Hands-on	Dibya Khatiwada APNIC Community Trainer
15:00 - 15:30	Tea/Coffee Break	
15:30 - 17:00	RPKI - Hands-on	Dibya Khatiwada\ APNIC Community Trainer

15th March, 2023 (Wednesday)

Time (GMT+5:45)	Topic	Trainer/Speaker
13:30 - 15:00	Panel: RPKI User Cases and Experience Sharing	**Jamie Gillespie**
15:00 - 15:30	Tea/Coffee Break	
15:30 - 17:00	APNIC ISIF Project Progress and BGPWatch Platform Demonstration	**BdREN&Tsinghua University**

16th March, 2023 (Thursday)

Time (GMT+5:45)	Topic	Trainer/Speaker
09:00 - 10:30	MANRS - What, Why and How	**Warrick Mitchell**
15:30 - 17:00	Panel: MANRS User Cases and Experience Sharing	**Warrick Mitchell**

清華大學 Tsinghua University

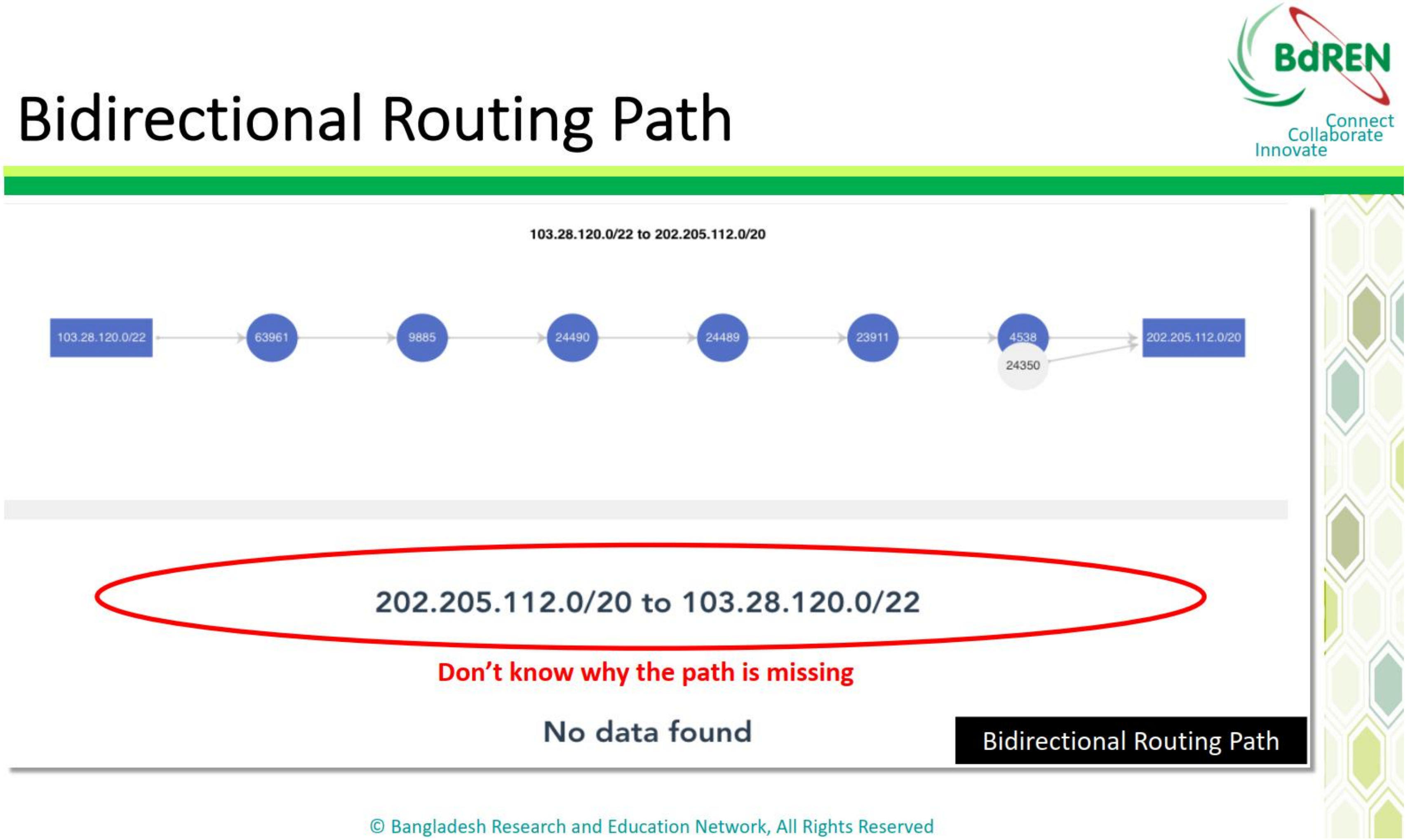
8 Sessions, 58 Registrants

Feedback from Partners

- Some bugs and imperfect
- Fault alarm
- Improve hijacking events information showing
- Configure interested prefix/AS, and send alert when anomaly/hijacking
- More bgp related alert, such as peer change/path change
- Send message by slack channel
- Show alternative routing path/track multi path
- Path performance
- Open API

Suggested Changes

- If you want to search an “Organization” using name, AS-name or AS-number you have to go to the “Organization” menu
  - Organization Name is “Case sensitive”, better if it is made “Case insensitive”
- The prefixes in “Dashboard=>IPv4 Peers” and that of “Routing Path” should match.
- Needs to put the “last date of update” for the records which will be periodically updated.



Bidirectional Routing Path

103.28.120.0/22 to 202.205.112.0/20

202.205.112.0/20 to 103.28.120.0/22

Don’t know why the path is missing

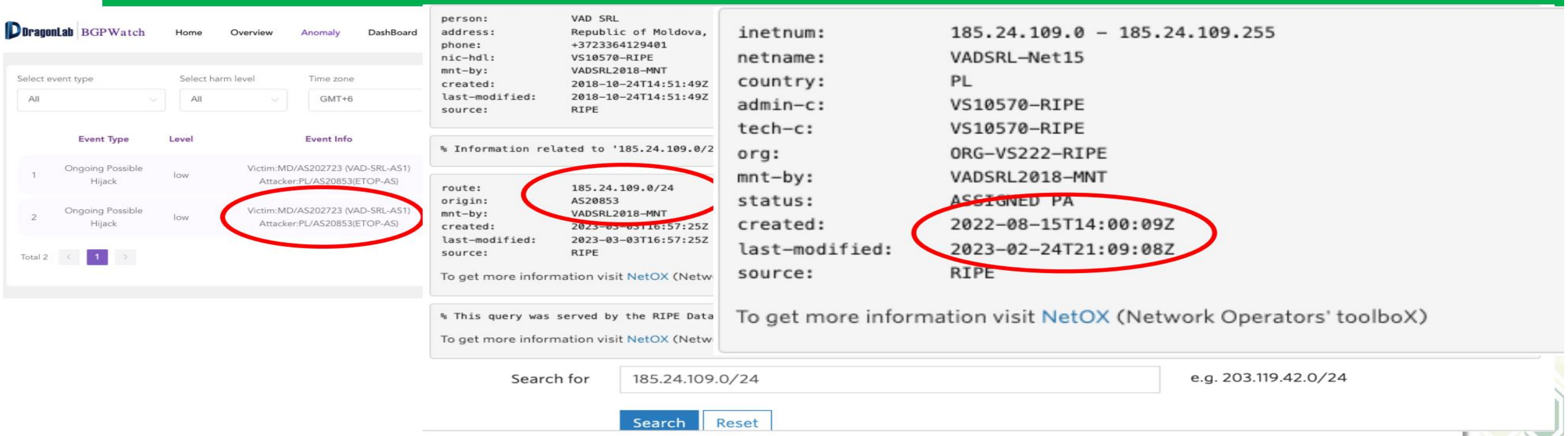
No data found

Bidirectional Routing Path

First, there are huge amount routing data from RouteViews, RIS, PCH, CGTF. Now we only use part of there data. We’ll try to process all the data by Parallel Computing and Clusters.

Even though, no one can get all the path information, so it’s a best effort system.

False Alarm



DragonLab | BGPWatch — Home · Overview · Anomaly · DashBoard

Select event type: All · Select harm level: All · Time zone: GMT+6

	Event Type	Level	Event Info
1	Ongoing Possible Hijack	low	Victim:MD/AS202723 (VAD-SRL-AS1) Attacker:PL/AS20853(ETOP-AS)
2	Ongoing Possible Hijack	low	Victim:MD/AS202723 (VAD-SRL-AS1) Attacker:PL/AS20853(ETOP-AS)

Total 2 ‹ 1 ›

```
person:          VAD SRL
address:         Republic of Moldova,
phone:           +3723364129401
nic-hdl:         VS10570-RIPE
mnt-by:          VADSRL2018-MNT
created:         2018-10-24T14:51:49Z
last-modified:   2018-10-24T14:51:49Z
source:          RIPE
```

```
% Information related to '185.24.109.0/2
```

```
route:           185.24.109.0/24
origin:          AS20853
mnt-by:          VADSRL2018-MNT
created:         2023-03-03T16:57:25Z
last-modified:   2023-03-03T16:57:25Z
source:          RIPE
```

To get more information visit NetOX (Netw

```
% This query was served by the RIPE Data
```

To get more information visit NetOX (Netw

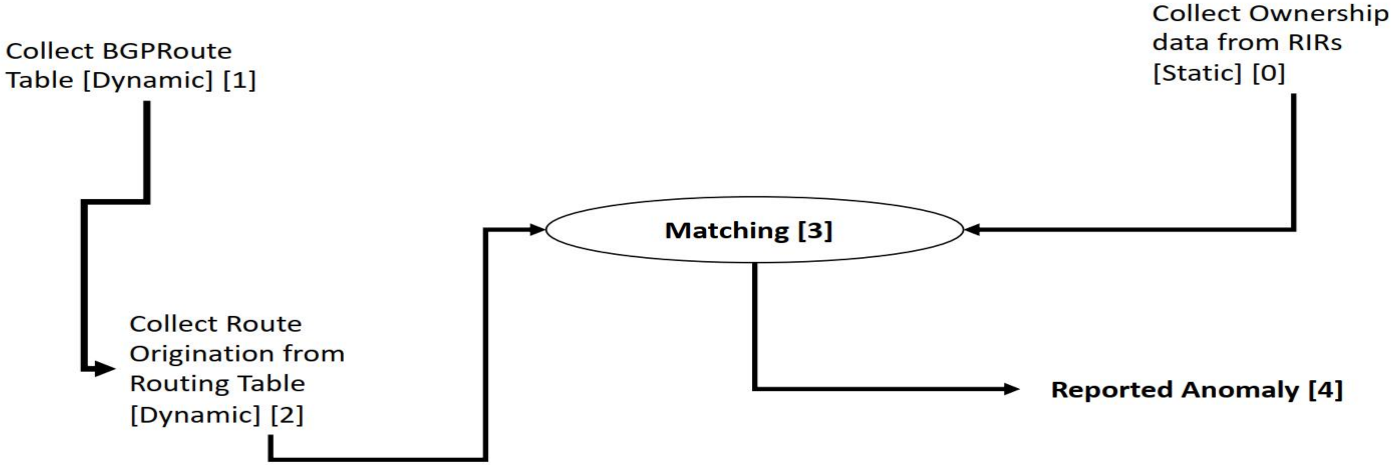
```
inetnum:         185.24.109.0 - 185.24.109.255
netname:         VADSRL-Net15
country:         PL
admin-c:         VS10570-RIPE
tech-c:          VS10570-RIPE
org:             ORG-VS222-RIPE
mnt-by:          VADSRL2018-MNT
status:          ASSIGNED PA
created:         2022-08-15T14:00:09Z
last-modified:   2023-02-24T21:09:08Z
source:          RIPE
```

To get more information visit NetOX (Network Operators' toolboX)

Search for: 185.24.109.0/24 e.g. 203.119.42.0/24

Search · Reset

Needs to verify the problems in the algorithm, if any.



Collect BGPRoute Table [Dynamic] [1]

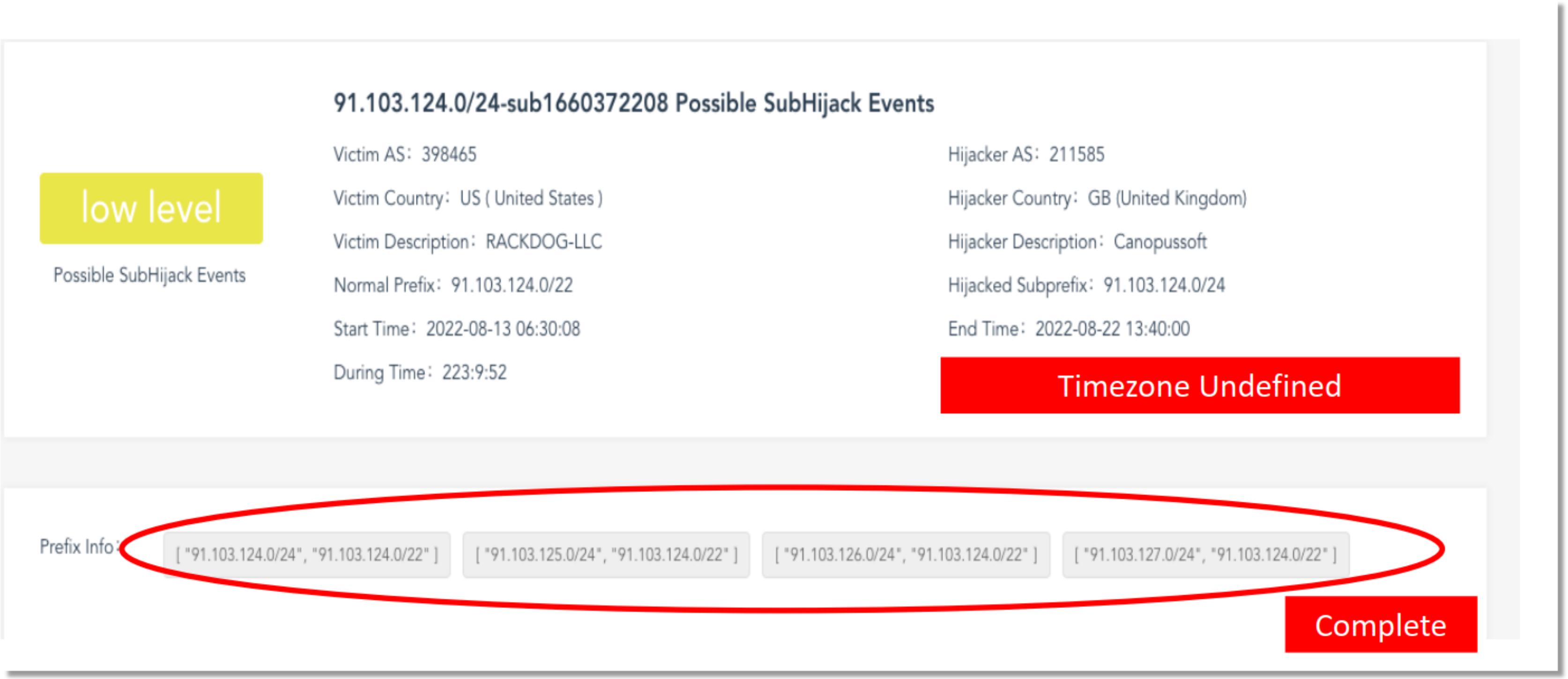
Collect Ownership data from RIRs [Static] [0]

Matching [3]

Collect Route Origination from Routing Table [Dynamic] [2]

Reported Anomaly [4]

Suggested Changes=>Anomaly and Prefixes



91.103.124.0/24-sub1660372208 Possible SubHijack Events

low level

Possible SubHijack Events

Victim AS：398465

Victim Country：US (United States)

Victim Description：RACKDOG-LLC

Normal Prefix：91.103.124.0/22

Start Time：2022-08-13 06:30:08

During Time：223:9:52

Hijacker AS：211585

Hijacker Country：GB (United Kingdom)

Hijacker Description：Canopussoft

Hijacked Subprefix：91.103.124.0/24

End Time：2022-08-22 13:40:00

Timezone Undefined

Prefix Info： ["91.103.124.0/24", "91.103.124.0/22"] ["91.103.125.0/24", "91.103.124.0/22"] ["91.103.126.0/24", "91.103.124.0/22"] ["91.103.127.0/24", "91.103.124.0/22"]

Complete

Some more suggestions

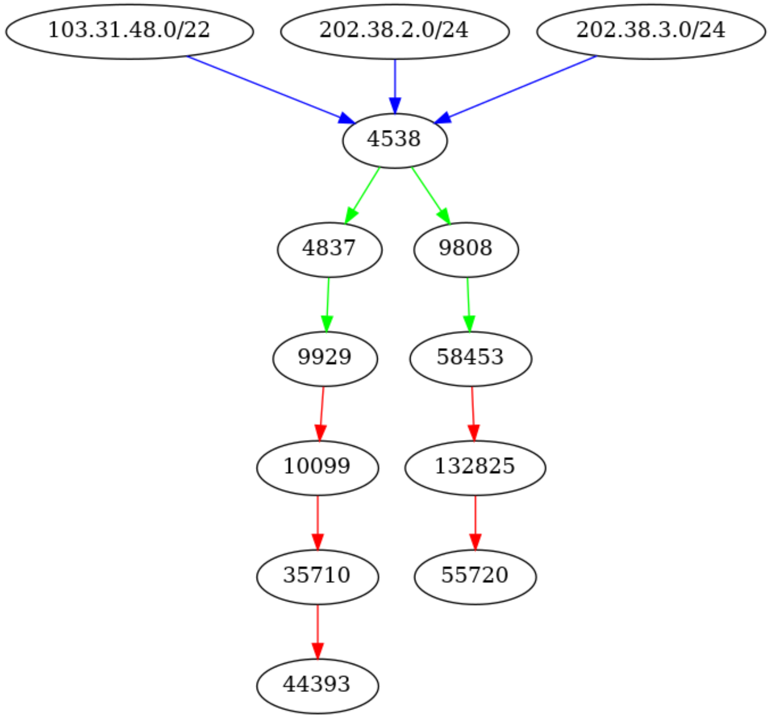
- Mitigation feature support is highly required
- Monitoring or alerting system for AS path change to a selected destination
- API for receiving data to display on partner customized applications and monitoring systems
- Some topologies does not show ASN details when hovering over the ASN nodes

Future Work

- Suggestion from partners
- Routing tree clustering
- Path hijacking detection

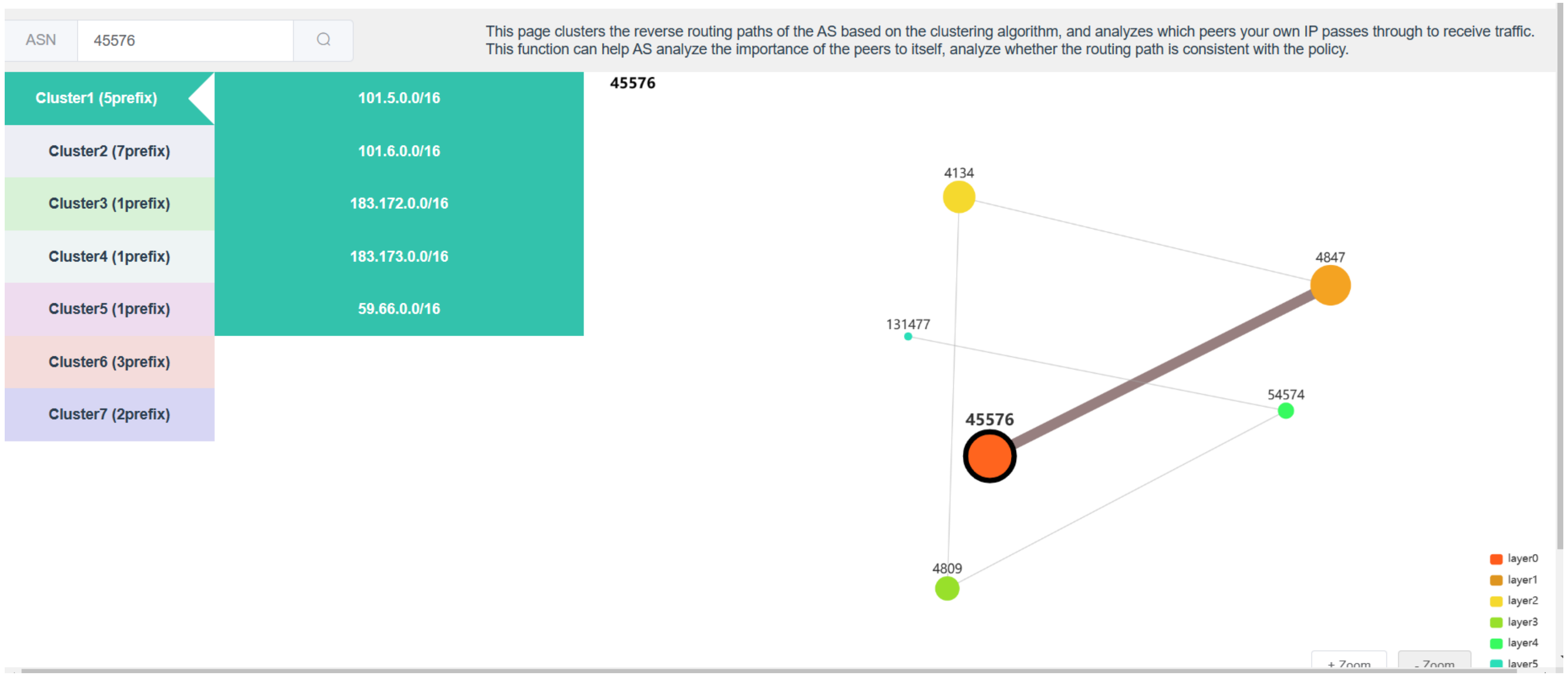
Routing tree Clustering

- Routing tree consists of all AS-PATHs from BGP monitors to target prefix.
- Observation: AS will set different routing policies for different groups of prefixes. Different policy lead to different routing trees.
- Routing tree clustering: grouping of identical or similar routing trees.



Application of Routing tree clustering

- Routing policy configuration consistency check
  - Administrators can check the consistency of external observations and internal routing policy configuration with the clustering result.



ASN 45576

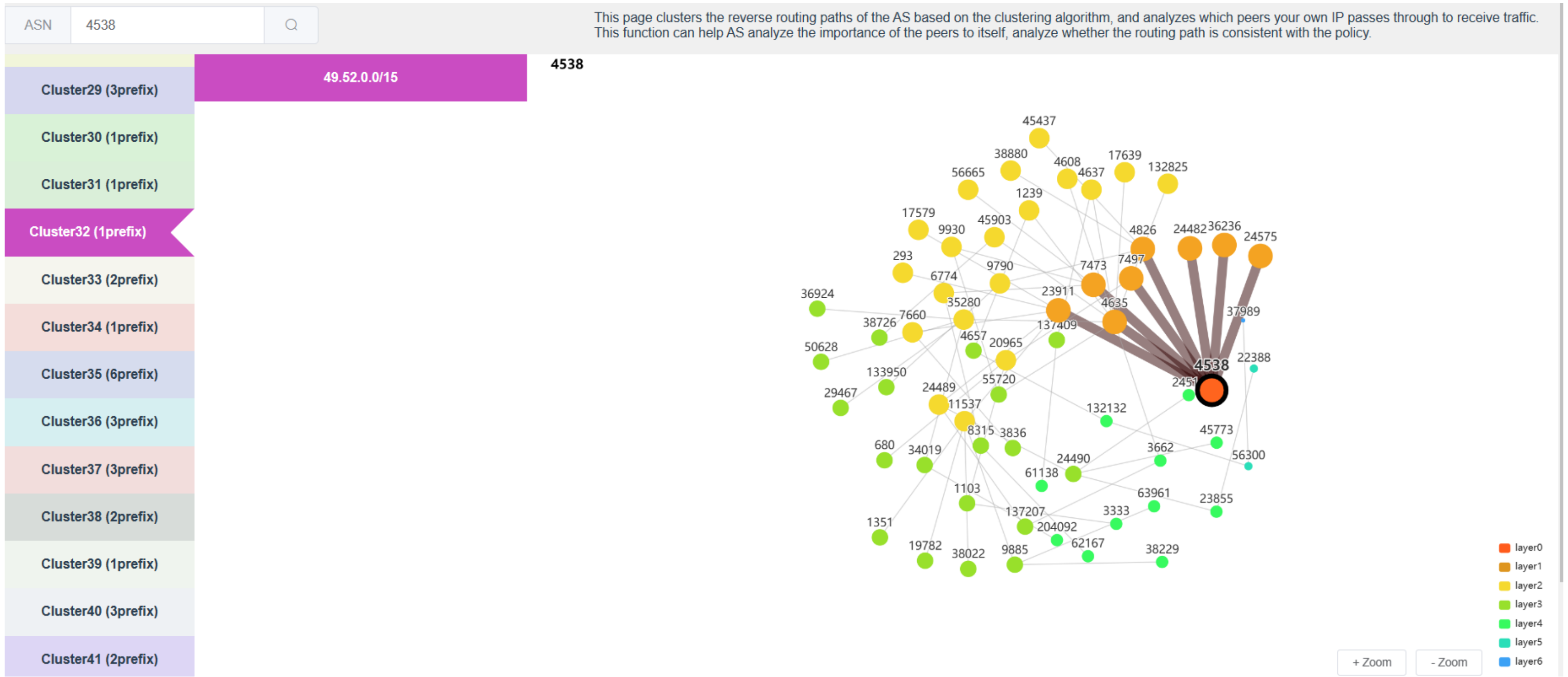
This page clusters the reverse routing paths of the AS based on the clustering algorithm, and analyzes which peers your own IP passes through to receive traffic.
This function can help AS analyze the importance of the peers to itself, analyze whether the routing path is consistent with the policy.

Cluster1 (5prefix)
Cluster2 (7prefix)
Cluster3 (1prefix)
Cluster4 (1prefix)
Cluster5 (1prefix)
Cluster6 (3prefix)
Cluster7 (2prefix)

101.5.0.0/16
101.6.0.0/16
183.172.0.0/16
183.173.0.0/16
59.66.0.0/16

Application of Routing tree clustering

- Important prefix/special prefix discovery
  - Some AS configure separate routing policies for a small number of prefixes, which may be some important prefixes or special prefixes.



This page clusters the reverse routing paths of the AS based on the clustering algorithm, and analyzes which peers your own IP passes through to receive traffic. This function can help AS analyze the importance of the peers to itself, analyze whether the routing path is consistent with the policy.

ASN: 4538

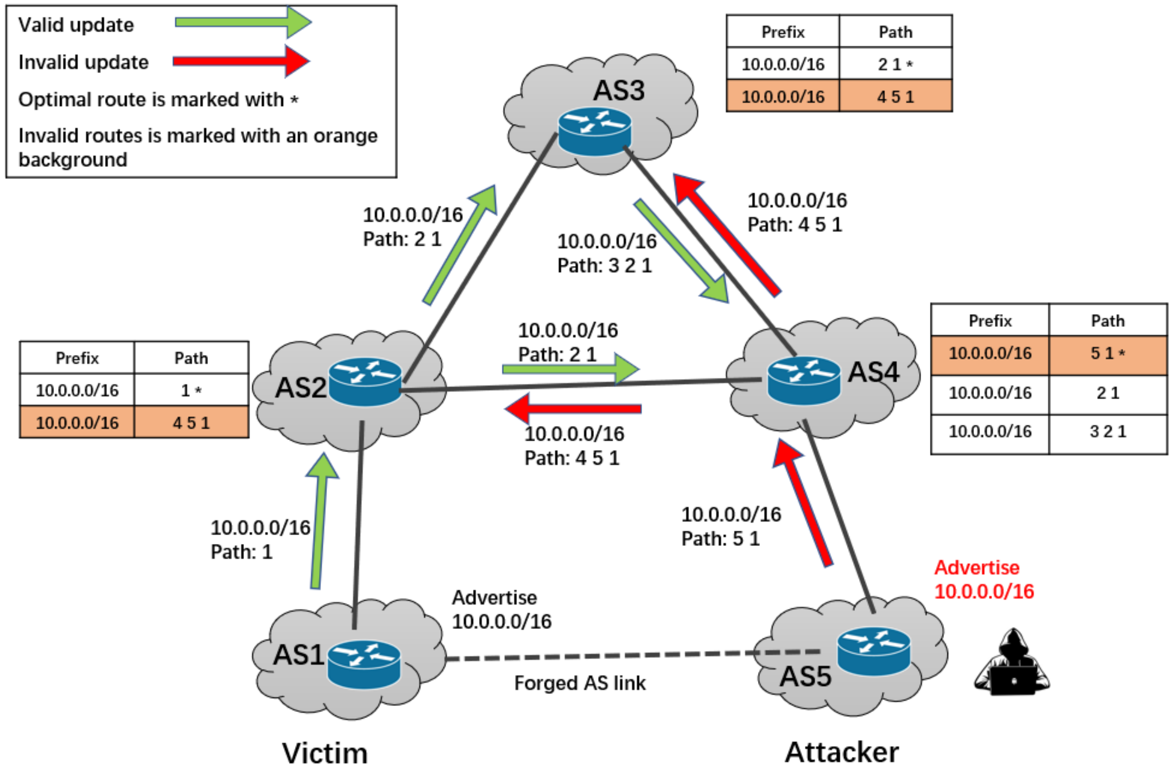
Cluster29 (3prefix)
Cluster30 (1prefix)
Cluster31 (1prefix)
Cluster32 (1prefix)
Cluster33 (2prefix)
Cluster34 (1prefix)
Cluster35 (6prefix)
Cluster36 (3prefix)
Cluster37 (3prefix)
Cluster38 (2prefix)
Cluster39 (1prefix)
Cluster40 (3prefix)
Cluster41 (2prefix)

49.52.0.0/15

4538

Path hijacking detection

- Path hijacking : the attacker announces the victim’s prefix while manipulating the AS-PATH.
- Observation: path hijacking usually causes unseen links, For example, the link AS5-AS1 in the figure is an actual non-existent link forged by the attacker.
- Existing path hijacking detection methods are based on unseen links, including Argus[IMC’12], Fingerprint-based[S&P’07], ARTEMIS[ToN’18], etc.



Valid update 🟩

Invalid update 🟥

Optimal route is marked with *

Invalid routes are marked with an orange background

Prefix	Path
10.0.0.0/16	2 1 *
10.0.0.0/16	4 5 1

Prefix	Path
10.0.0.0/16	1 *
10.0.0.0/16	4 5 1

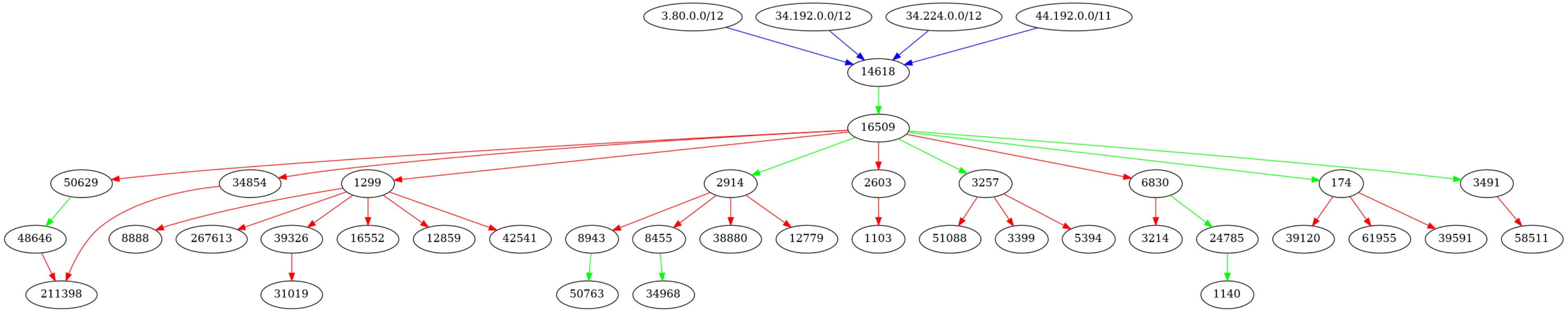
Prefix	Path
10.0.0.0/16	5 1 *
10.0.0.0/16	2 1
10.0.0.0/16	3 2 1

Application of Routing Tree Clustering

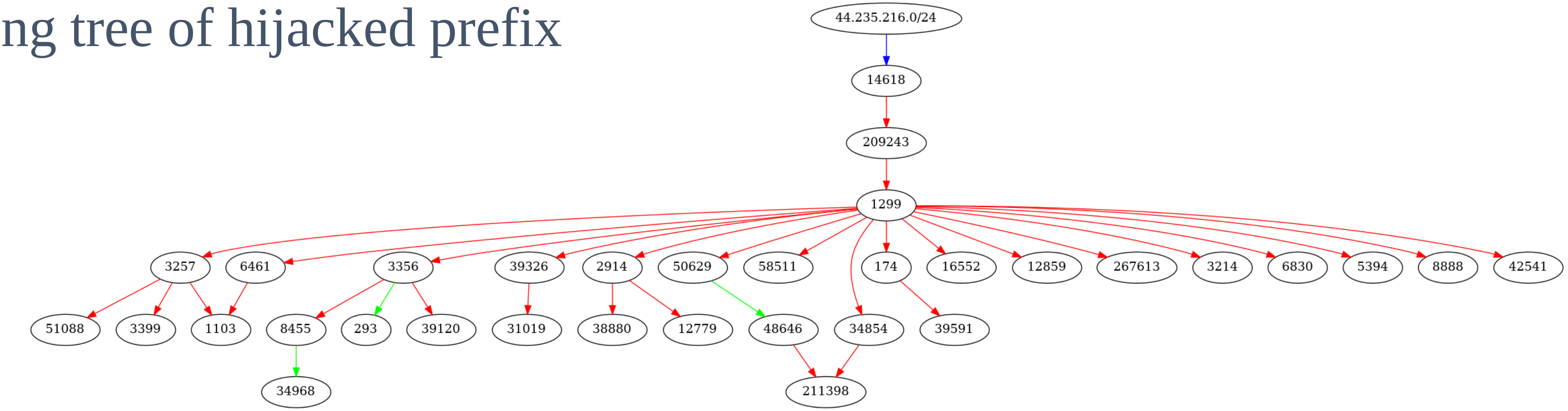
- Anomaly detection or Event review
  - Prefix hijacking or link failure, etc. can cause changes in clustering results, which can be used to detect anomalies.
  - For example, On August 17, 2022, 44.235.216.0/24 （belong to Amazon） was maliciously hijacked by attacker AS20943.
  - The results of clustering all prefixes of AS14618 by next-hop AS before and after hijacking.
  - 18:00 (before hijacking): 1 cluster, all paths go through AS16059 before arriving at AS14618.
  - 20:00 (during hijacking): 2 clusters， the hijacked prefixes form a separate cluster.
  - 24:00 (after hijacking recovery): 1 cluster.

Application of Routing Tree Clustering

- Routing tree of normal prefixes



- Routing tree of hijacked prefix



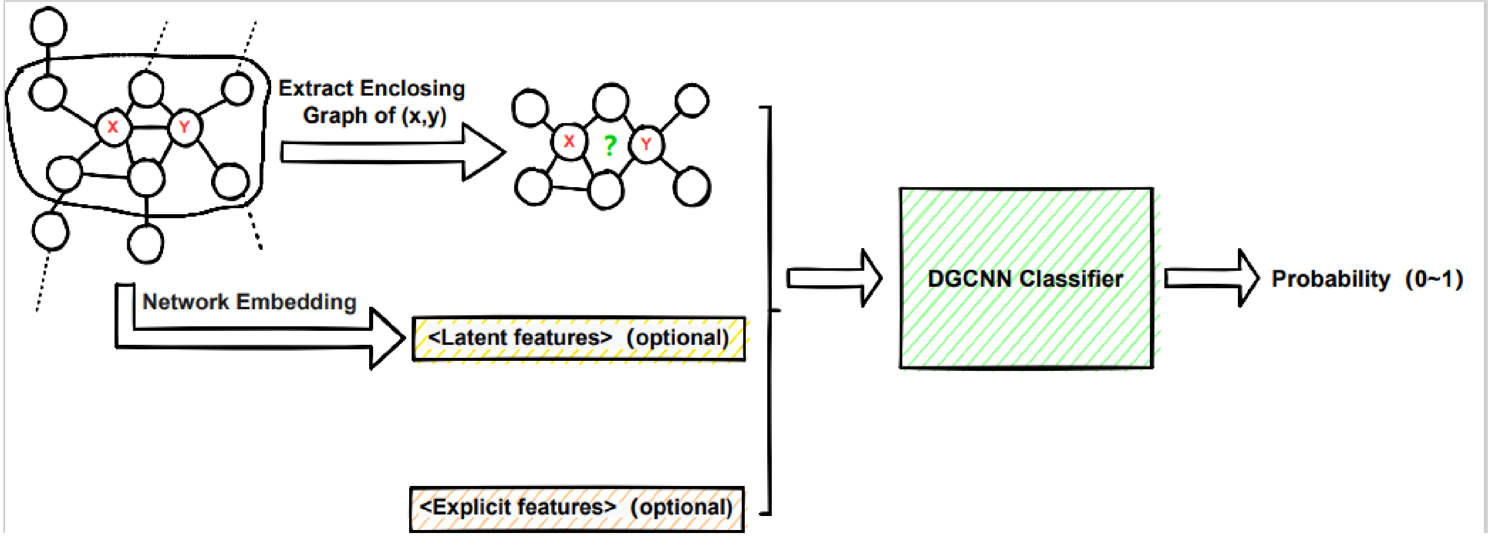
Path hijacking detection by link prediction

- Problem
  - Argus, fingerprints, and other methods directly treat unseen links as suspicious events, and then verify the events by data plane detection
  - Most unseen links are normal, and as the size of the Internet grows, the number of unseen links observed daily is increasing, and doing so would waste a lot of overhead and make it difficult to ensure real-time performance.

- Our idea
  - Evaluate the authenticity of unseen links and filter the links with high authenticity
- Our method
  - Use link prediction. Link prediction is used to evaluates the likelihood of the existence of an unseen link from the observed links.

Path hijacking detection

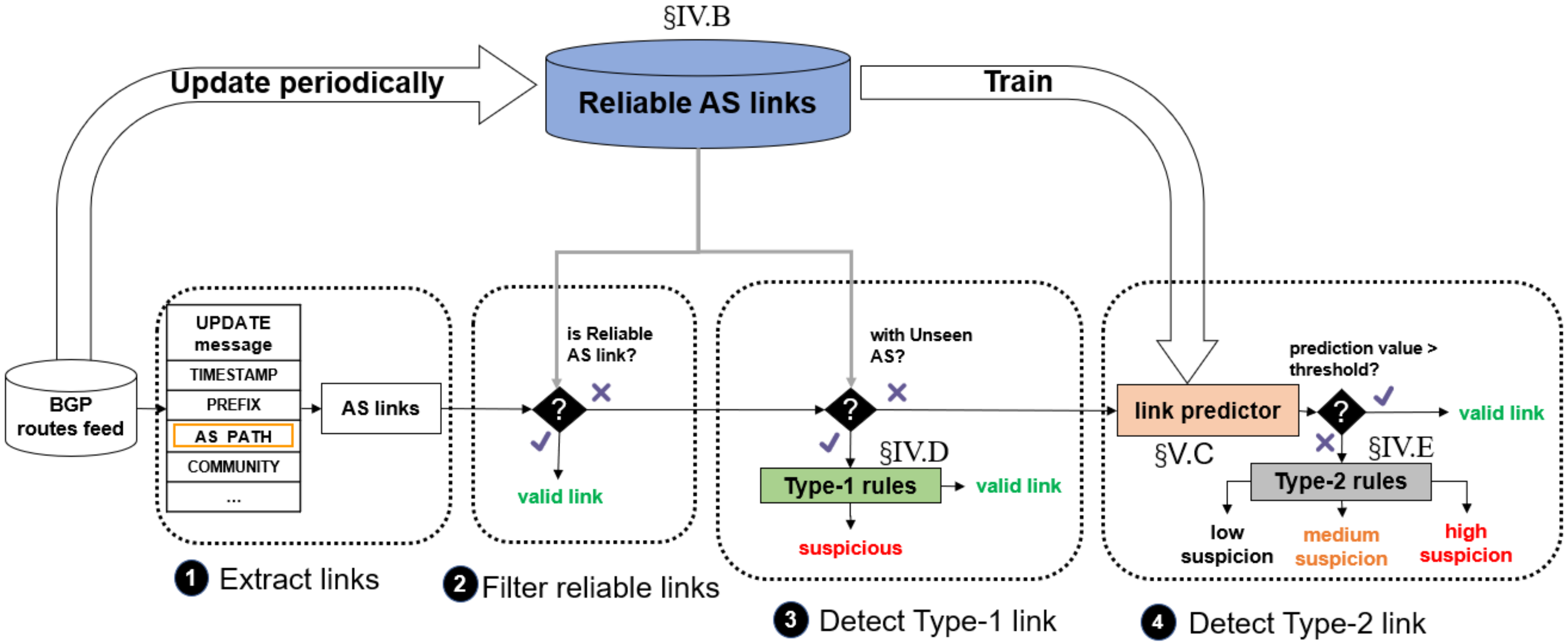
- We use SEAL, a link prediction framework based on graph neural networks, for our experiments.
- Get AS topology data from CAIDA, train the model using 80% of the links, and then go to predict the remaining 20% of the links (training requires negative samples, i.e., non-existent links, which can be randomly sampled from the invisible links).
- Experimental results: the accuracy and AUC of classifying unseen links was 0.95, 0.98,respectively.



Extract Enclosing Graph of (x,y)
X
Y
?
Network Embedding
<Latent features> (optional)
<Explicit features> (optional)
DGCNN Classifier
Probability (0~1)

Path hijacking detection

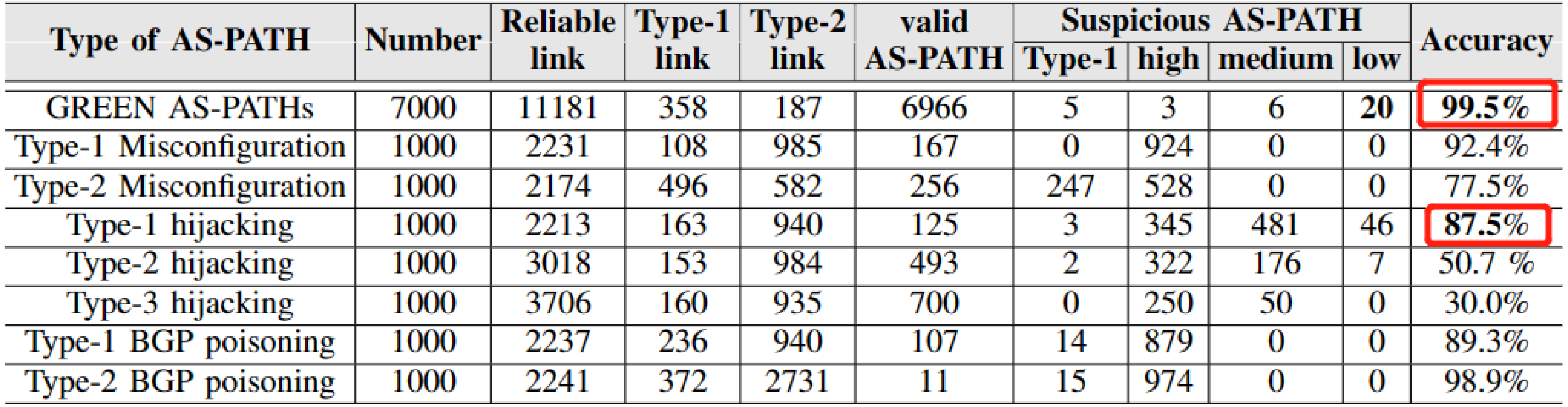
- Further, we combine the characteristics of false AS-PATH to design a series of rules and further propose a framework for detecting false AS-PATH under the control plane, METIS.



Experiment

- We extract the AS-PATHs in RIB as GREEN samples, and then simulate the actual scenario to craft some fake AS-PATHs as RED samples.
- The experimental results show that METIS can effectively detect the forged AS-PATH caused by path hijacking, misconfiguration, and BGP poisoning.

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%

Comments/Suggestions

Welcome more partners join the community

Contact us: sec@cgtf.net