(APNIC ISIF Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Tsinghua University

3 March 2025

Contents

- Project's Background
- Technical Work
- Knowledge Sharing
- Partners
- User Distribution
- Funding Expenses
- Future Work Plan

APNIC FOUNDATION

清華大學 Tsinghua University

Project's Background

01 Initiative

Previous Project:

- Joint Research on IPv6 Network Management: Research Development and Demonstration
- Funded by National Key Research and Development Program of China

02 Improvement

Previous Project:

- Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform
- Co-founded by APNIC Foundation and Tsinghua University

03 Enhancement

Current Project:

- **An Extension of the Ongoing Project "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform"**
- Co-founded by APNIC Foundation and Tsinghua University

APNIC FOUNDATION

Tsinghua University

Activities of the 2nd Phase

Objectives	Work Plan	Tentative Timeline
Develop an integrated Looking Glass platform	Find obscure Looking Glass VP regularly	Dec. 2023 Done
	Develop integrated Looking Glass platform	Feb. 2024 Done
	Develop Looking Glass API	Mar. 2024 Done
Use Looking Glass to further check routing hijacking at the data plan	Develop data plan detection method and decision algorithm	June 2024 Done
	Integrate the algorithm to the system	Aug. 2024 Done
Implement path hijacking detection and routing leak detection methods	Develop path hijacking detection method	Nov. 2024 Done
	Develop routing leak detection method	Jan. 2025 Ongoing
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	The second phase of the project (**Dec.06, 2023 – June 06, 2025 (18 months))** **Welcome new partners to join!**	Throughout the entire project duration

Project Overview

Data Collecting	Data Mining	Application
✓ Registration: WHOIS, RIR, PeeringDB, Radb， ROA ✓ Looking Glass ✓ Routing information ✓ Active Probing ✓ Passive measurement	✓ Statistics ✓ Machine learning ✓ Deep learning	✓ Hijacking, leaking, outage detection ✓ Inter-domain topology discovery ✓ Monitoring peering and path changing ✓ Performance monitoring ✓ Link-level congestion detection ✓ Cyber-attack detection

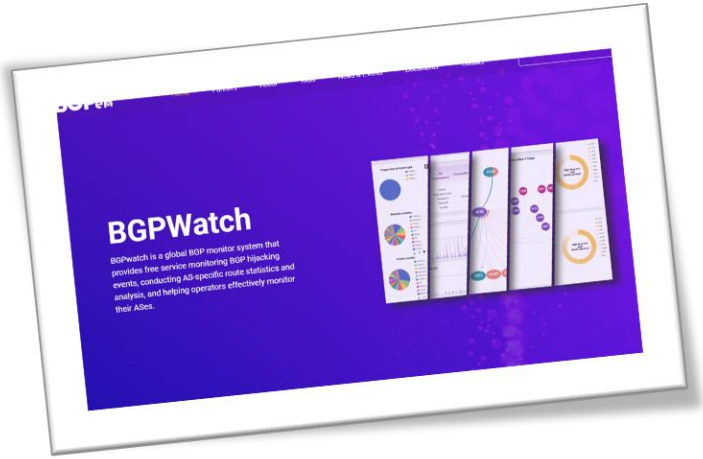
Objectives: Improve internet security, availability and provide tools for operators

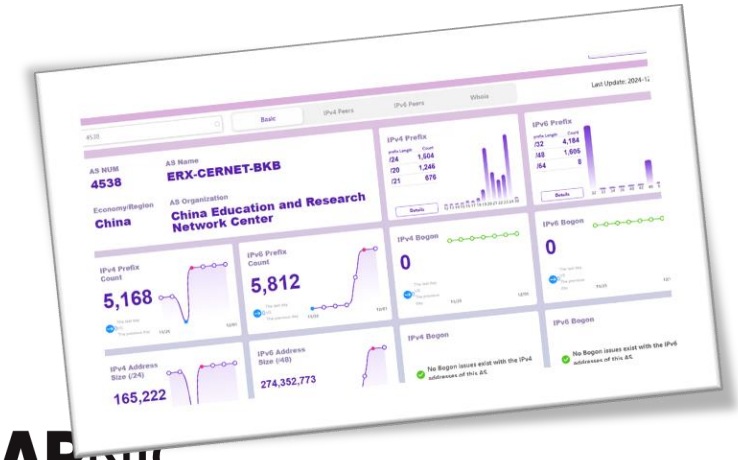
APNIC FOUNDATION

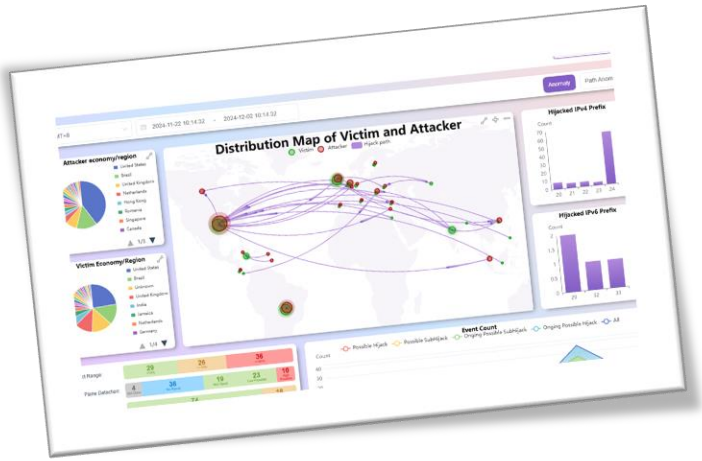
清華大學 Tsinghua University

Technical Work

- Looking Glass platform
- BGP routing sharing platform
- BGP anomaly detection
- BGP monitoring tools for operators



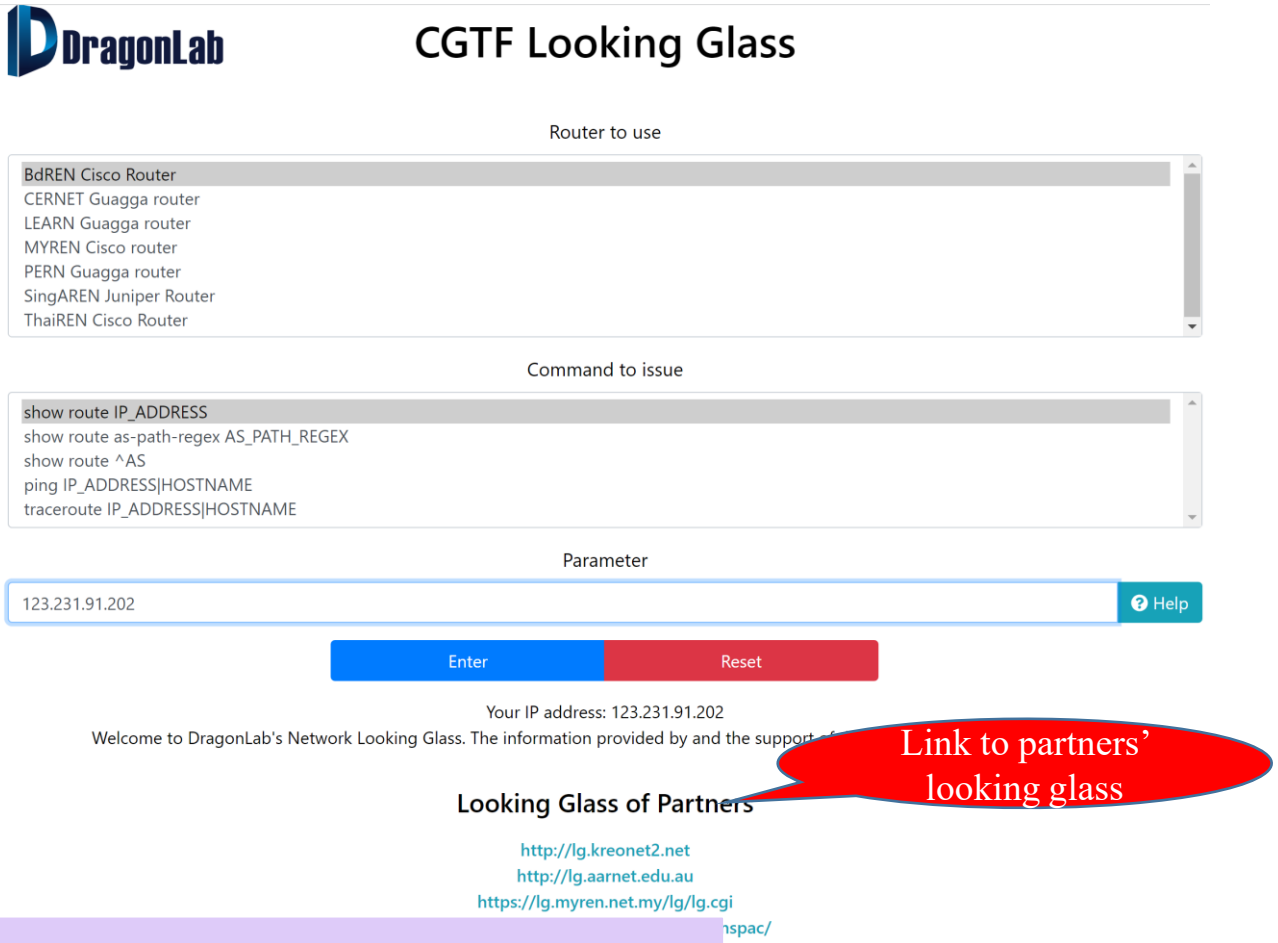




CGTF Looking Glass

https://lg.cgtf.net

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

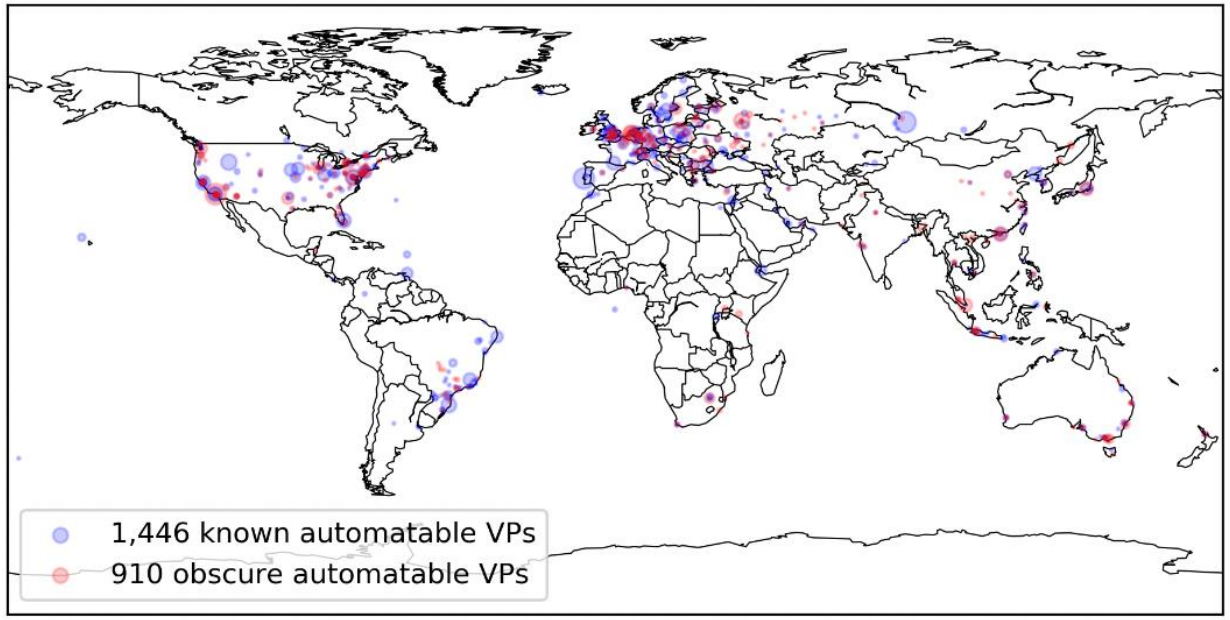


7 Education & Research network joined

Add links to 4 partners' looking glass

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 of 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**

https://github.com/zhuangshuying18/discover_obscure_LG

Periscope has found several hundred VPs (364)

APNIC FOUNDATION

Tsinghua University

Use obscure LG VPs to improve the completeness of AS-level topology

Collect AS paths from LG VPs

RUB Looking Glass - show bgp ipv4 unicast neighbors 10.12.1.163 advertised-routes

Router: RUB Border Router 2
Command: show bgp ipv4 unicast neighbors 10.12.1.163 advertised-routes

```
BGP table version is 36248632, local router ID is 10.12.0.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0/24       188.1.245.93             0    100      0 680 13335 i
 *>  1.0.4.0/24       188.1.245.93             0    100      0 680 6939 4826 38803 i
 *>  1.0.4.0/22       188.1.245.93             0    100      0 680 6939 4826 38803 i
 *>  1.0.5.0/24       188.1.245.93             0    100      0 680 6939 4826 38803 i
```

Automatically collect AS paths from 14 known LG VPs and **8 obscure VPs**

Improve AS-level topology completeness

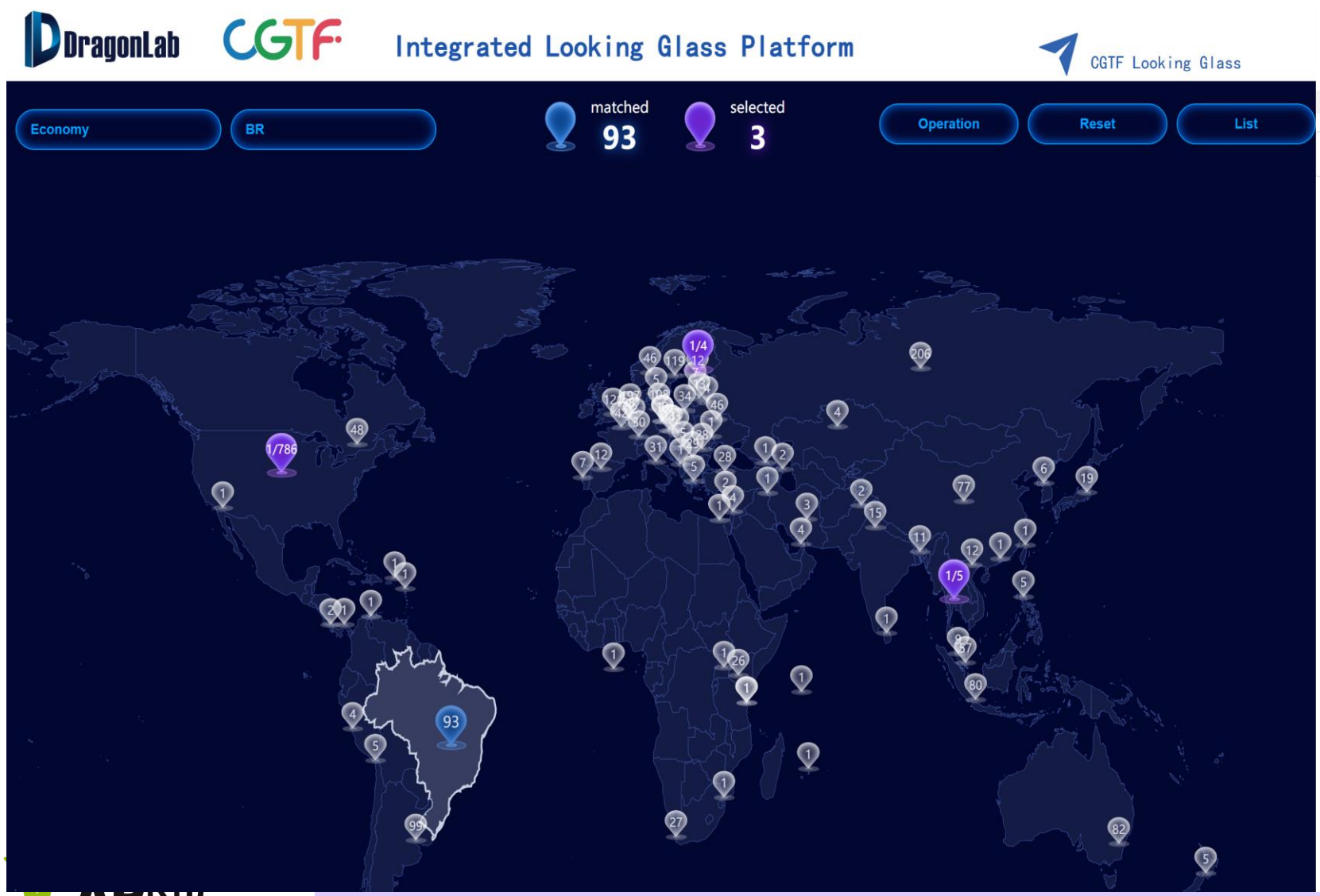
		Known LG VPs	Obscure LG VPs	RIPE RIS	RouteViews	ALL
ASes	Observed	44,955	44,355	44,952	45,339	45,635
	Exclusive	247	10	12	271	-
AS links	Observed	100,356	76,907	154,828	204,889	253,719
	Exclusive	8,318	1,428	37,383	85,450	-

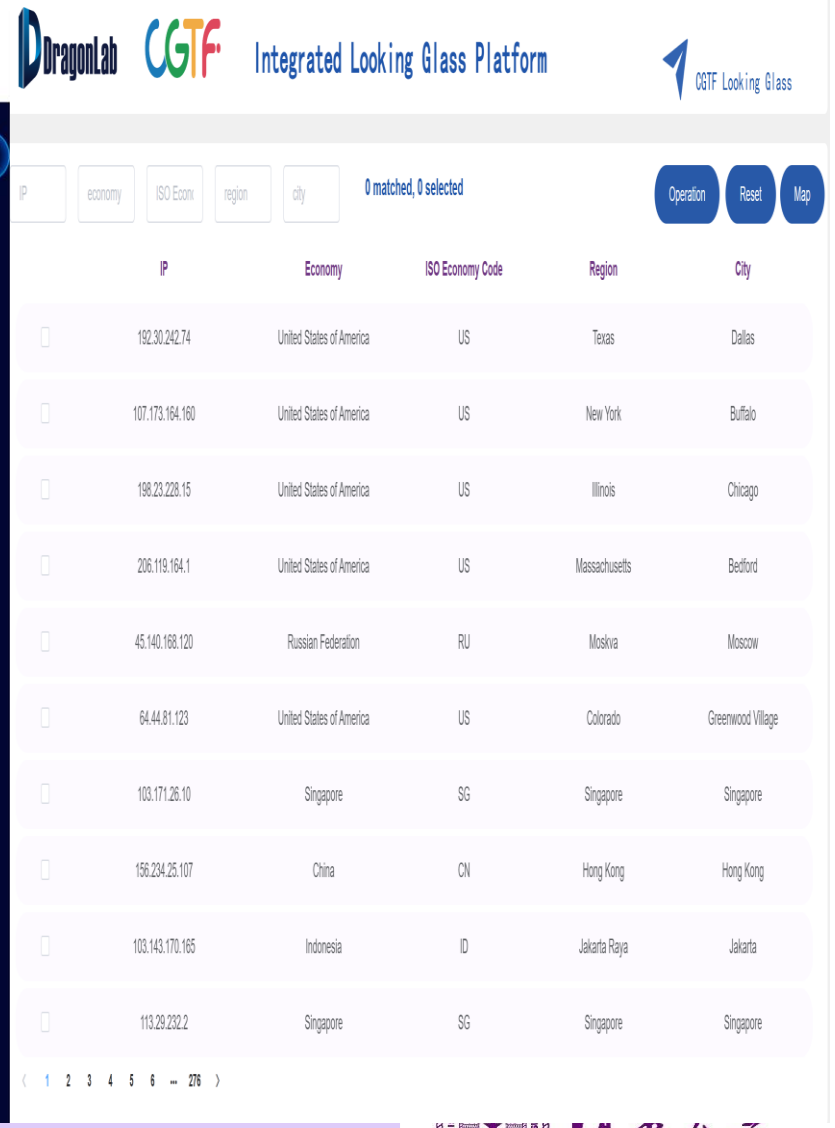
Table 6: The number of observed and exclusive ASes, AS links extracted from each dataset.

Compare with AS topologies collected from known LG VPs, RIPE RIS and RouteViews

10 new ASes, and 1428 new links

An Integrated Looking Glass Platform





https://gperf.cgtf.net/#/integrated

CGTF RIS

We have established BGP session with 17 partners.
Configuration manual can be accessed at
https://www.bgper.net/index.php/document/

https://bgp.cgtf.net

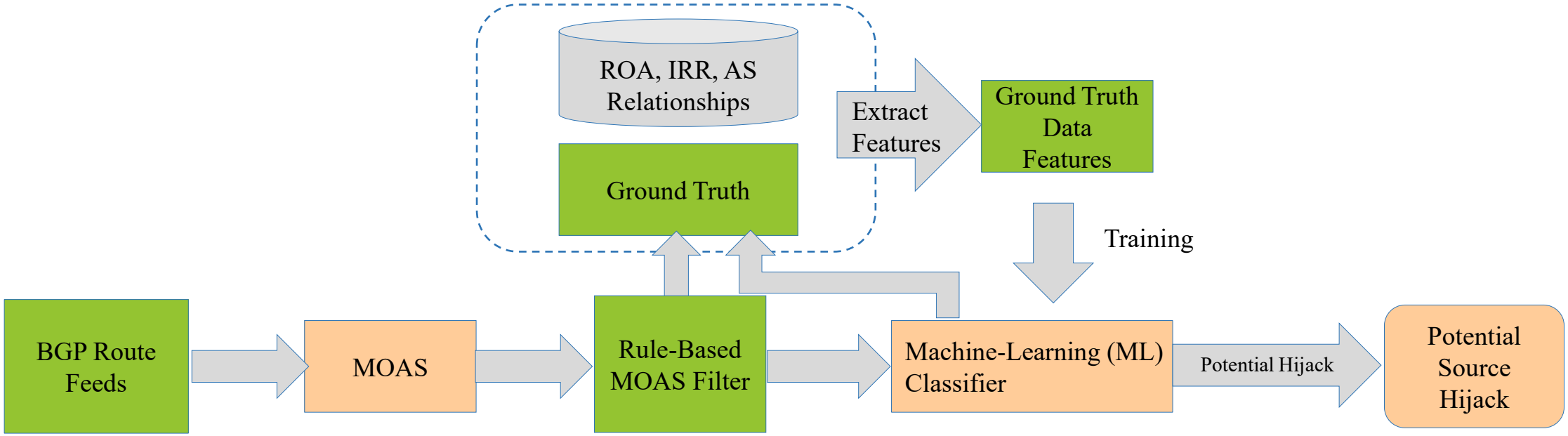
No.	Partner	No.	Partner
1	**APAN-JP**	9	**MYREN**
2	**AARNET**	10	**PERN**
3	**BDREN**	11	**REANNZ**
4	**CERNET**	12	**SINGAREN**
5	**HARNET**	13	**ThaiSARN**
6	**ITB**	14	**TransPAC**
7	**KREONET**	15	**NREN**
8	**LEARN**	16	**RedCLARA**
		17	**RNP**

Index of /collector1/ribs/2024/11/

../		
rib.20241101.0000.mrt.bz2	01-Nov-2024 00:16	34M
rib.20241101.0200.mrt.bz2	01-Nov-2024 02:16	35M
rib.20241101.0400.mrt.bz2	01-Nov-2024 04:16	35M
rib.20241101.0600.mrt.bz2	01-Nov-2024 06:16	35M
rib.20241101.0800.mrt.bz2	01-Nov-2024 08:16	35M
rib.20241101.1000.mrt.bz2	01-Nov-2024 10:16	35M
rib.20241101.1200.mrt.bz2	01-Nov-2024 12:16	35M
rib.20241101.1400.mrt.bz2	01-Nov-2024 14:16	35M
rib.20241101.1600.mrt.bz2	01-Nov-2024 16:16	35M
rib.20241101.1800.mrt.bz2	01-Nov-2024 18:16	35M
rib.20241101.2000.mrt.bz2	01-Nov-2024 20:16	35M
rib.20241101.2200.mrt.bz2	01-Nov-2024 22:16	35M
rib.20241102.0000.mrt.bz2	02-Nov-2024 00:16	35M
rib.20241102.0200.mrt.bz2	02-Nov-2024 02:16	35M
rib.20241102.0400.mrt.bz2	02-Nov-2024 04:16	35M
rib.20241102.0600.mrt.bz2	02-Nov-2024 06:16	35M
rib.20241102.0800.mrt.bz2	02-Nov-2024 08:16	35M
rib.20241102.1000.mrt.bz2	02-Nov-2024 10:16	35M

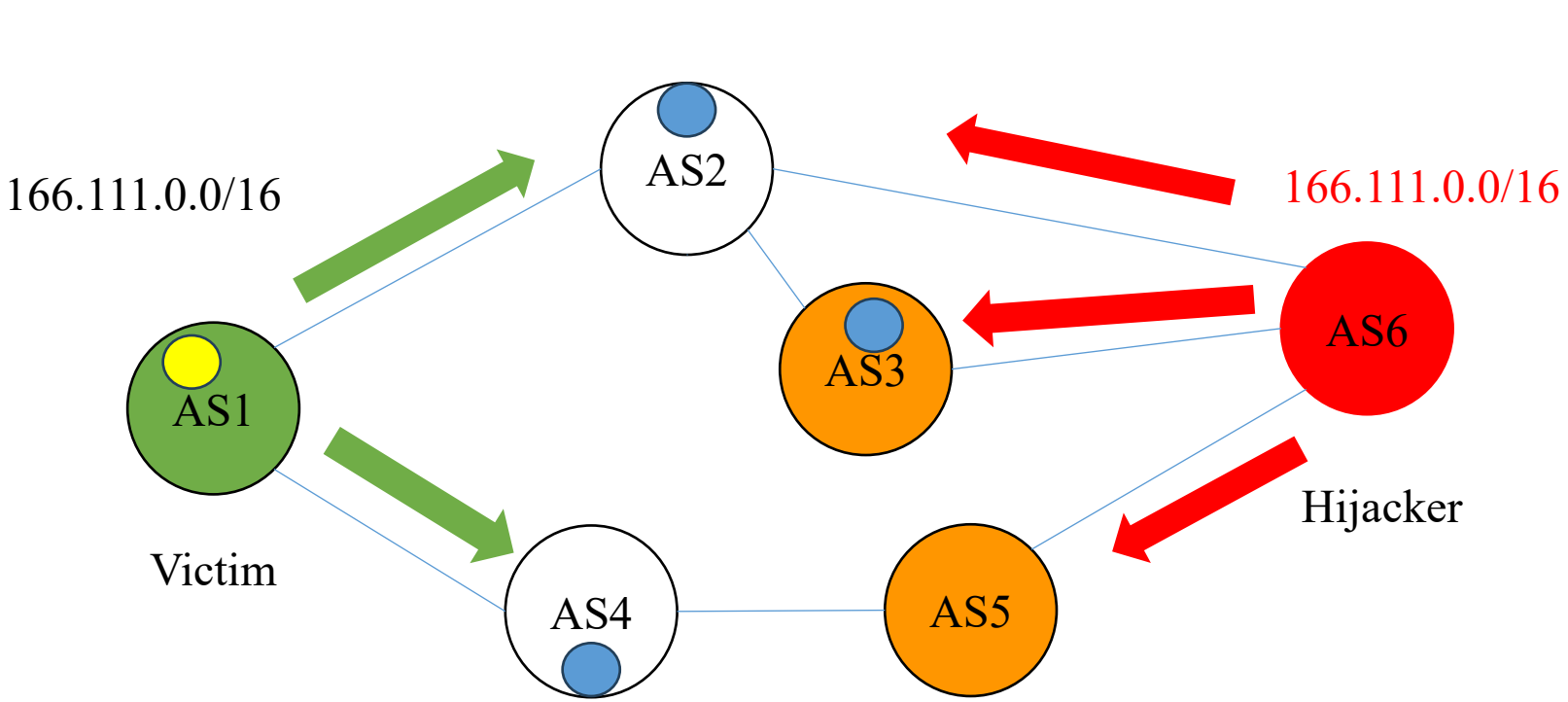
Tsinghua University

A Rules and Machine Learning Combined Method



- Initially, train the machine learning classifier.
- During operation, the platform fetches BGP ROUTE feeds, extracts MOAS.
- Rule-based filters are used to sift through a large volume of legitimate MOAS.
- Then, the machine learning classifier is utilized to categorize the remaining MOAS.

Data Plane Detection



Looking Glass vantage point

Representative services

- Possible Hijacking?

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

Approach: Test representative service from VPs

Data Plan Detection

- Choose probes in certain ASes
- Choose destinations from the hijacked prefixes
- Do Probing
- Calculate Correlation Coefficient

Correlation Coefficient:

$$r(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var[X]\,Var[Y]}}$$

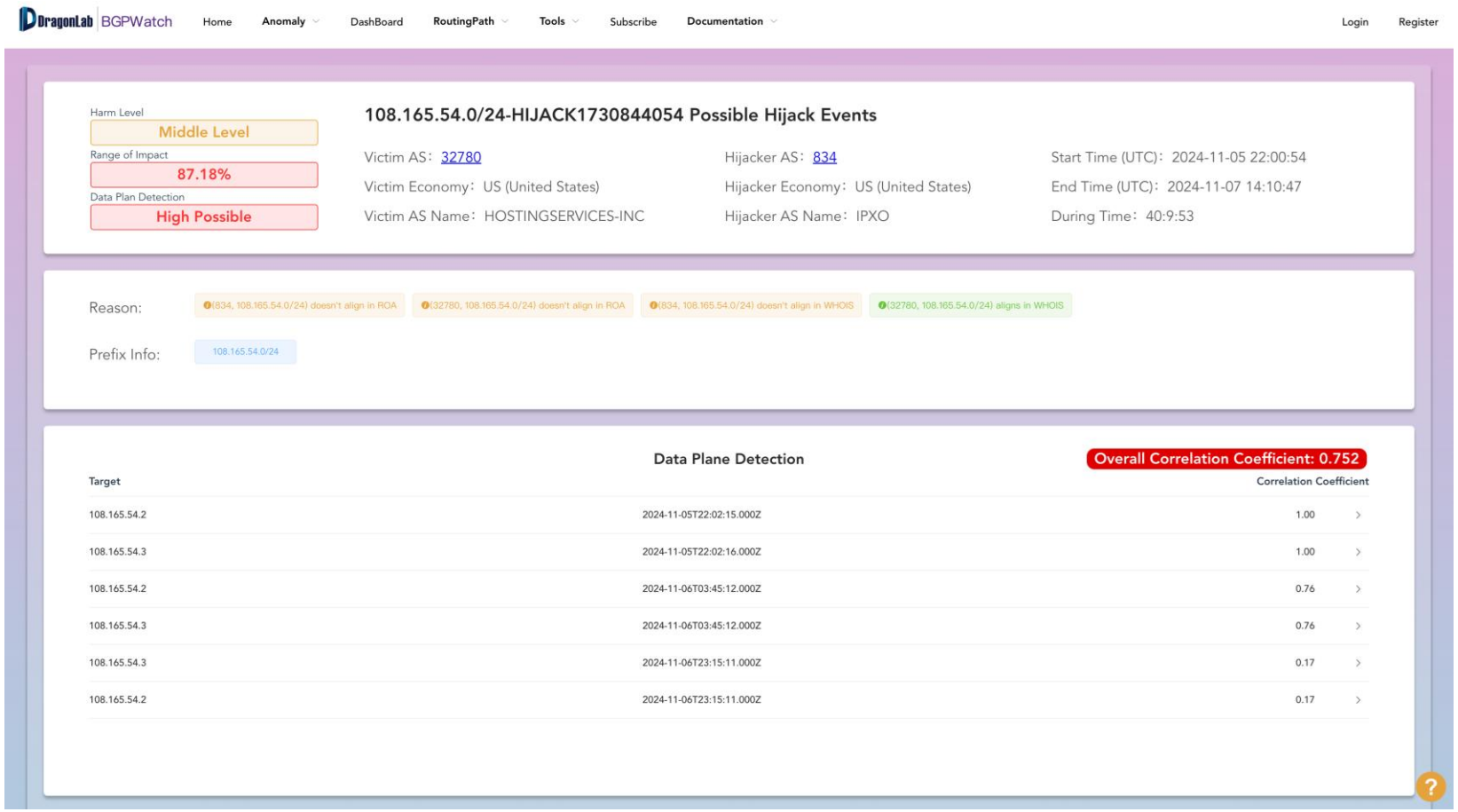
- Vector X:

For each prober, set to 0 if located in the affected AS; otherwise, set to 1.

- Vector Y:

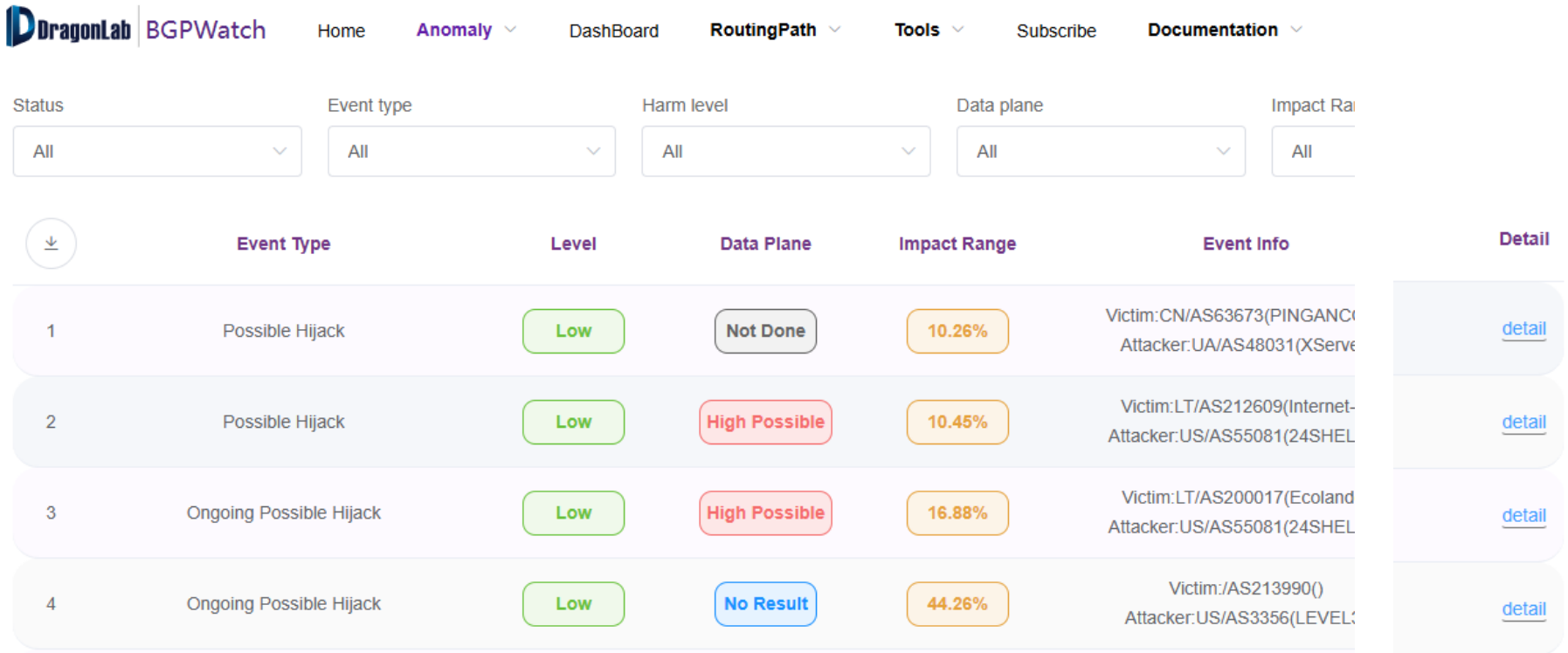
For probe result from each prober, set to 1 if reachable; otherwise, set to 0.

Anomaly – Detail



- **Data Plane Detection**
  - Not Done:
    No measurable target found
  - No Result:
    Probed, but received no results
  - Not Hijack:
    Correlation Coefficient = 0
  - Low Possible:
    Correlation Coefficient < 0.6
  - High Possible:
    Correlation Coefficient >= 0.6

Anomaly

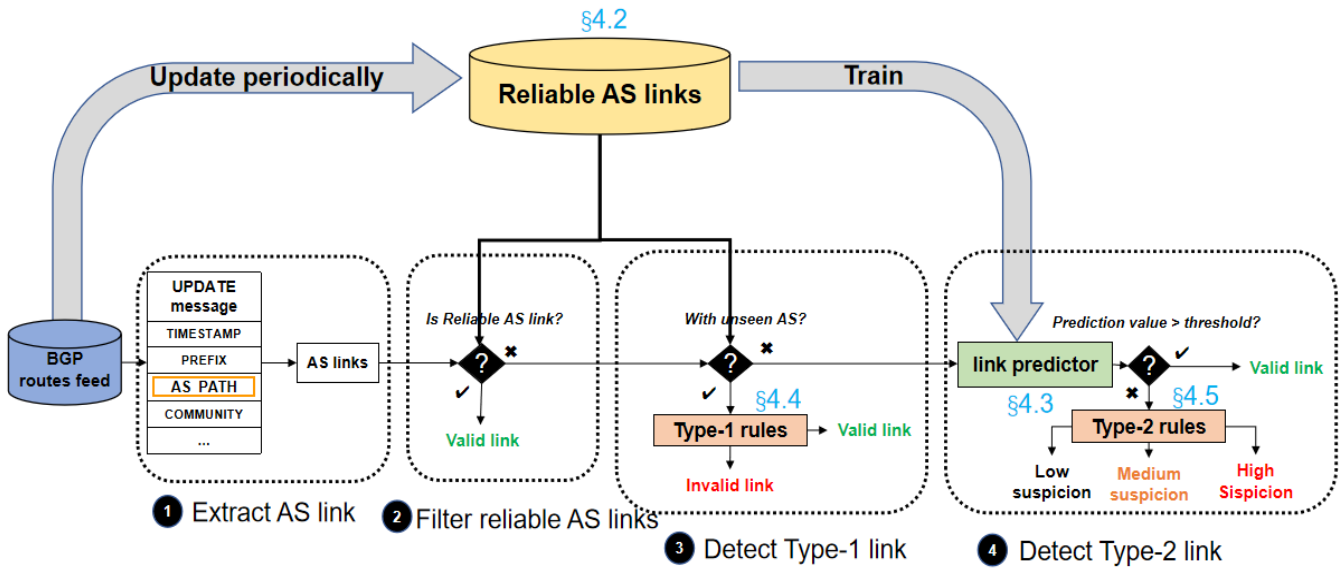


- **Impact Range**
  - <10%: Fewer than 10% of ASNs in the replay path are affected.
  - >=10%: More than 10% of ASNs in the replay path are affected.
  - >=50%: More than 10% of ASNs in the replay path are affected.

APNIC FOUNDATION

清華大學 Tsinghua University

Path Anomaly Detection: Combining Link Prediction and Rules



- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level.
- Two Type Events:
  - New Link: New and Suspicious Link
  - New AS: New and Suspicious AS

- Possible
  - Low Possible: Confidence level < 0
  - Middle Possible: Confidence level = 0
  - High Possible: Confidence level > 0

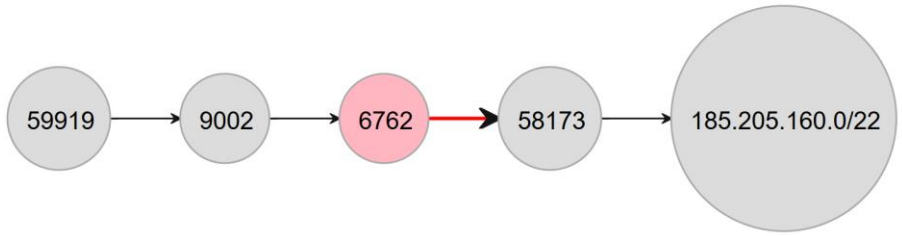
Reason	Confidence level
new link	
AS-PATH is too long	+1
The last hop is single-digital ASN	+1
The edit distance of ASNs in the link is 1	+1
There exists loop in the AS-PATH and the suspicious link is in the loop.	+1
The AS-PATH violates valley-free rule:'({a},{b},{c}).	+1
Domestic traffic ({country},{asn1},{asn2}) detour.	+1
Suspicious links is at the end of the AS-PATH and a demostic link ({irr_dict.get(self._u)}).	-4
Suspicious links is same country ({irr_dict.get(self._u)}).	-2
new as	
ASN{asn} is not registered.(new AS)	+1
ASN{asn} is reserved ASN.(new AS)	+1
ASN{asn} is not the last hop.(new AS)	+1

Path Anomaly

	Event Type	Level	Possible	Impact Range	Event Info	Prefix Num	Example Prefix	Start Time
61	Ongoing New Link	Low	Low Possible	<=1 path	New Link: 11014(AR) -> 269818(AR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (AR)	1	45.184.152.0/24	2024-11-13 15:05:30
62	Ongoing New AS	Low	High Possible	>5 path	New AS: 31196 Reason:ASN31196 is not the last hop	1	202.36.221.0/24	2024-11-13 14:40:48
63	Ongoing New Link	Low	Low Possible	<=1 path	New Link: 32307(US) -> 400707(US) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (US)	1	38.109.250.0/24	2024-11-13 14:29:20
64	Ongoing New Link	Low	High Possible	<=1 path	New Link: 58212(DE) -> 214309(GB) Reason:Detour of domestic traffic (34854,GB) (1299,SE) (199524,LU) (58212,DE) (214309,GB)	1	45.151.91.0/24	2024-11-13 14:14:44
65	Finish New Link	Low	Low Possible	<=1 path	New Link: 52863(BR) -> 264485(BR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (BR)	1	189.91.147.0/24	2024-11-13 14:10:47

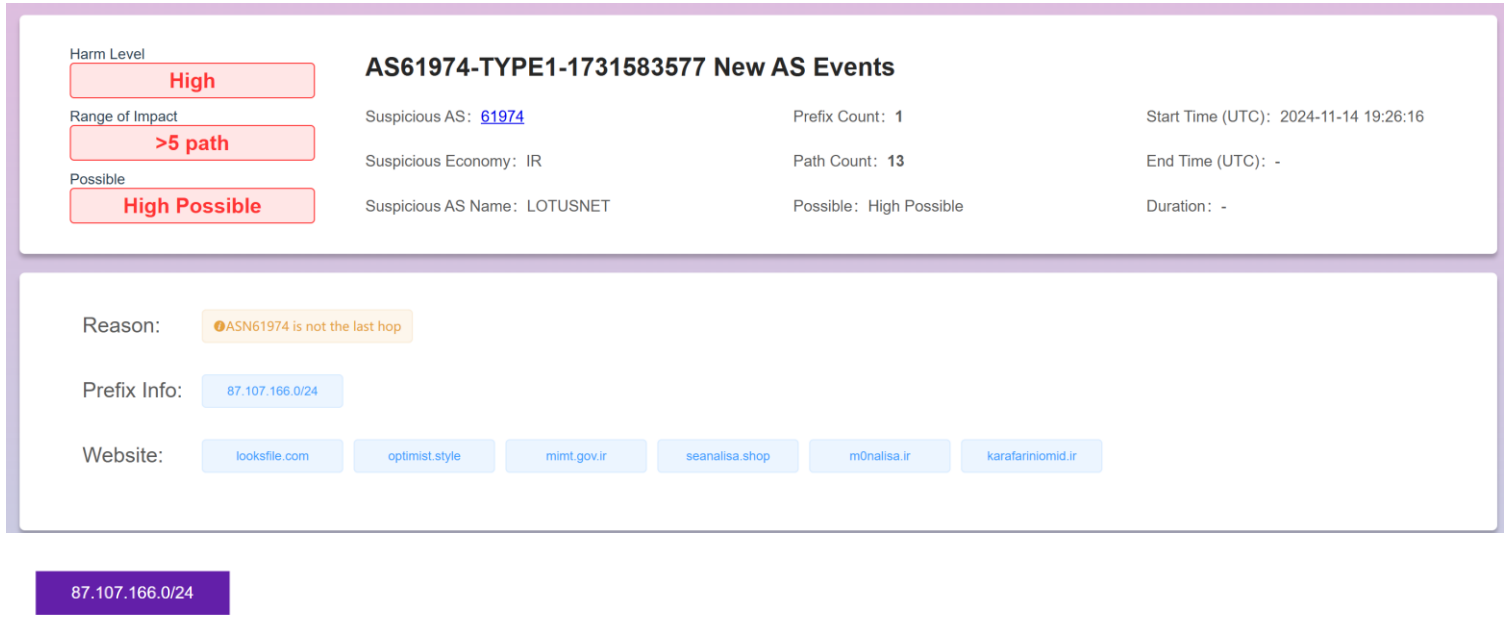
Path Anomaly Detail – Suspicious New Link

Reason:
Detour of domestic traffic (58173,GB) (6762,IT) (9002,GB)



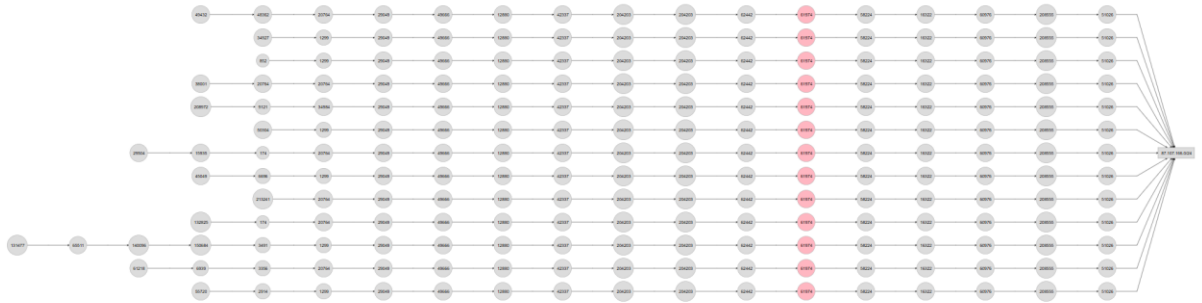
The suspicious AS and link are marked red.

Path Anomaly Detail – Suspicious New AS



87.107.166.0/24

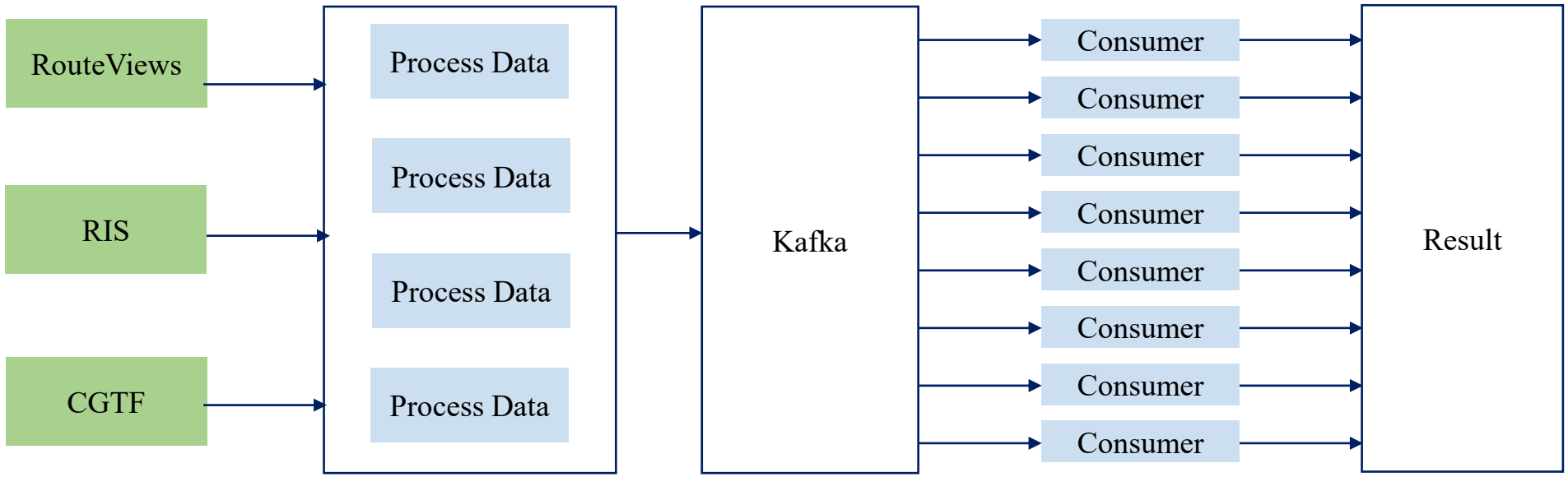
Reason:
ASN61974 is not the last hop.



All the paths affected.

Parallel Computing and Clusters to Handle Big Routing Data

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



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!

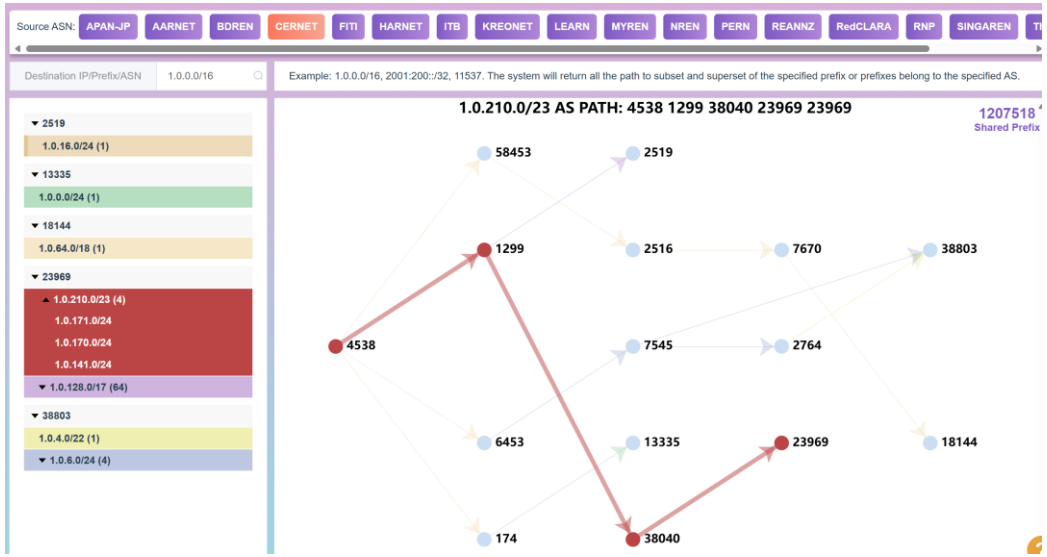
Best regards,
Institute for Network Sciences and Cyberspace
Tsinghua University

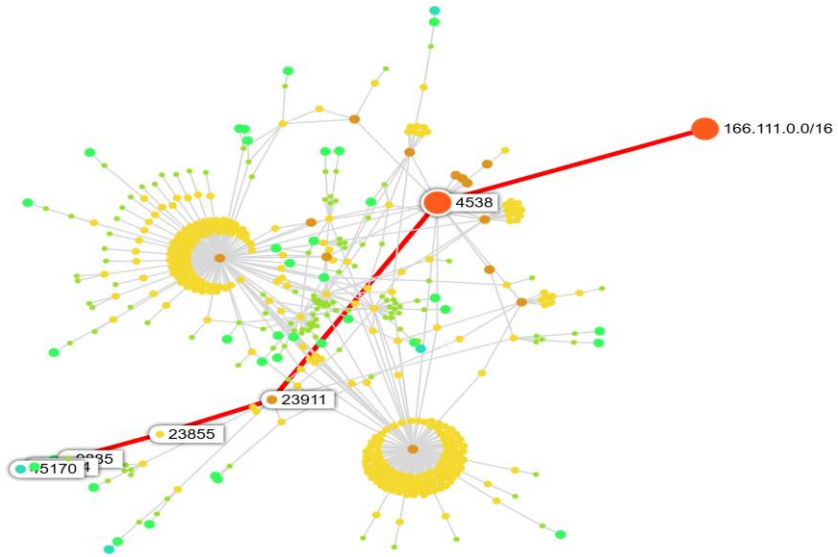
APNIC FOUNDATION

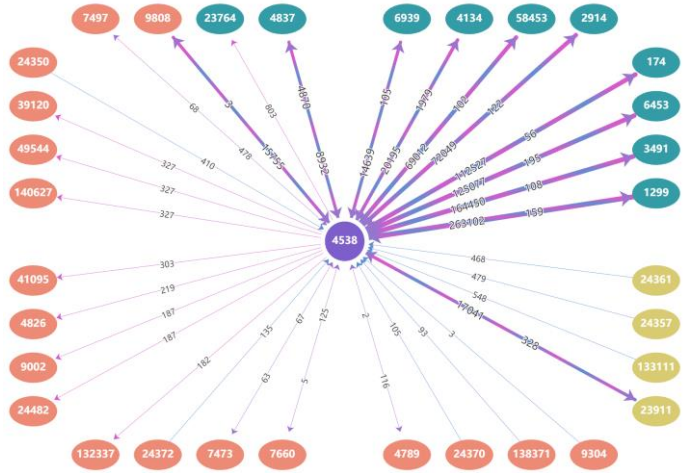
Tsinghua University

Tools for Network Operator

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



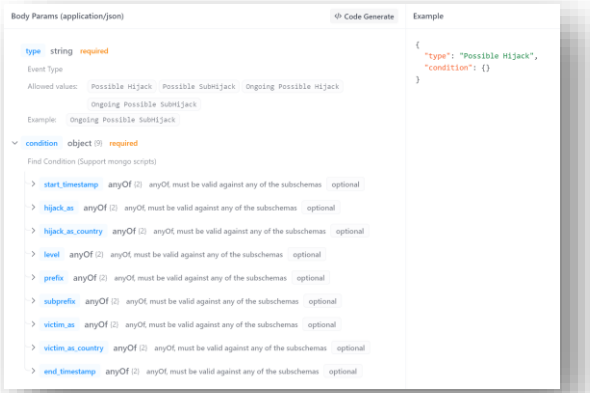


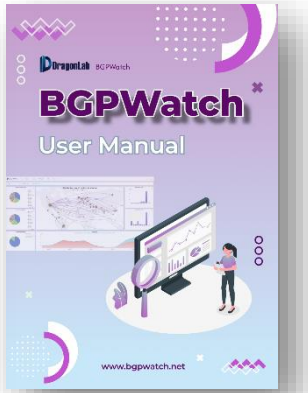


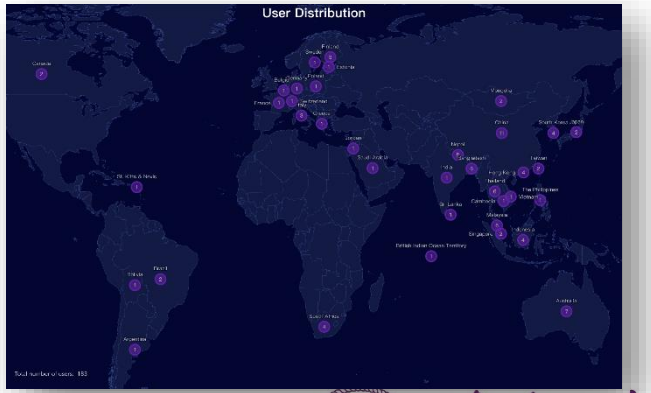
https://bgpwatch.cgtf.net

Knowledge Sharing – Deliverables and Dissemination

Websites	Free access to the public	bgpwatch.cgtf.net	lg.cgtf.net
Open source & Open API	Open to the public		
Manual Document & Video	Updated and provided Platform Demonstration		
Platform User & Work Cited by	Total: 198, from NOC of large ISP Other: 93, Asia: 64, Africa: 8, Europe: 19, North America: 3, Oceania: 7, South America: 4	RIS data was cited by CAIDA	





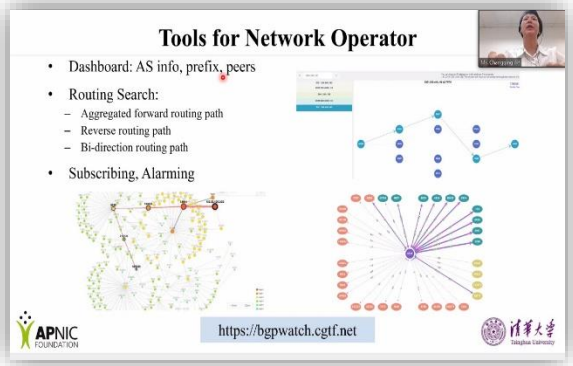


APNIC FOUNDATION

Tsinghua University

Knowledge Sharing – Conference Presentations

- **APAN57**
  - 1/29-2/3/2024, Thailand
  - Hosted 3 sessions
  - Over 100 attendees joined
  - Sponsored 7 project members
- **APRICOT2024**
  - 2/21-3/1/2024, Thailand
  - Presentation on BGPWatch
  - Over 80 attendees joined
- **APNIC Webinar**
  - 5/22/2024, Online
  - Webinar
  - 124 attendees joined
- **TNC24**
  - 6/10-6/14/2024, France
  - Presentation on BGPWatch
  - Over 100 attendees joined



Outreaching

- **ErdemNet**
  - Mongolian national research and education network
- **Rede Nacional de Ensino e Pesquisa (RNP)**
  - Brazilian network for education and research
- **Cooperación Latino Americana de Redes Avanzadas (RedCLARA)**
  - Contribute to the development of science, education, technology and innovation in Latin America and the Caribbean through the articulation, connection and strengthening of their national research and education networks
- **South African National Research Network (SANReN)**
  - The South African National Research Network (SANReN) is a high-speed network dedicated to science, research, education and innovation traffic and has been rolled-out in a phased manner.

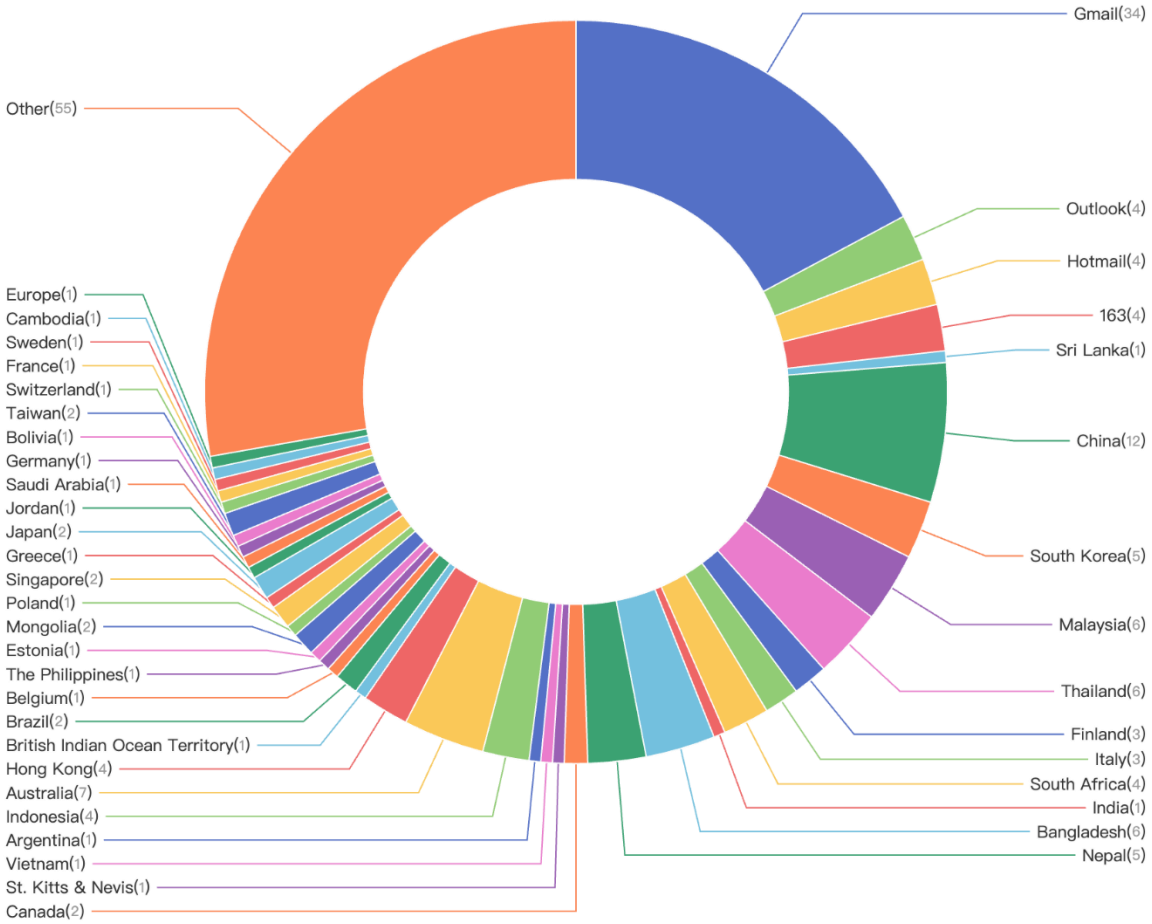
Partners

- Asia:
  - APAN-JP
  - BDREN
  - HARNET
  - ITB
  - KREONET
  - LEARN
  - DOST-ASTI
  - MYREN
  - NREN
  - PERN
  - SINGAREN
  - ThaiREN
  - ERNET
- Oceania:
  - AARNET
  - REANNZ
- America:
  - TransPAC
- Europe:
  - University of Surrey
  - University of Göttingen

- **2024 new partners:**
- America:
  - RedCLARA
  - RNP
- Africa:
  - SANReN

Current BGPWatch User Distribution

- According to the registered email, grouped by economy and email provider
- Totally 198 users, from 37 economies



APNIC FOUNDATION

Tsinghua University

Funding Status

		ISIF Asia Grant Grant	Tsinghua in-kind Contribution	ISIF Asia Grant Expenses	Outstanding fees	Balance
International Engagement/ Community Engagement	The costs associated with training and professional development for the staff project team.	$33,000		$15,754.44	$14,100.00	$3,145.56
Capacity and Professional Development	This covers the training fees of project team staffs and engineers.	$15,000		$13,913.92		$1,086.08
Support Services Fee	This cost is related to hosting, translation, office supplies, tax, administration fee, website, etc.	$37,000		$37,762.36		-$762.36
Human Resources of Project Coordination Committee/ Technical Support/ Secretariat	The cost of human resources from Tsinghua University for the work of Project Coordination Committee/Technical Committee/Secretariat.		$65,000			$0
Total		$85,000	$65,000	$67,430.72	$14,100.00	$3,469.28

APNIC FOUNDATION

Outstanding fees: Pay for the 2 project meetings held in May and November of last year, registration fee for speakers at APAN59, and a future project meeting.

清華大學 Tsinghua University

Future Work

- Conduct development and project review
  - Finish development
  - Collect feedback and insights from partners and users
  - Review the project
- Explore more international collaborations
- Continue to secure new funds
  - Conduct fine-grained routing policy learning through AI methods
  - Infer the unobservable routing paths
  - Predict accident consequence. If some network incidents occur and cause network outages, what impacts will their routing paths be subject to and which backup links will be used

Thank you!

Contact us at: sec@cgtf.net

APNIC FOUNDATION

清華大學 Tsinghua University