(APNIC Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

--The 5th Technical Committee Meeting

Jan 19, 2023

清華大學
Tsinghua University

APNIC
FOUNDATION

Outline

- Feedback from Partners
- Detailed Project Progress in Last Three Month
- Future Plan
- Comments/Suggestions

Feedback from Partners

- Screen Resolution Auto Adaption (done)
- Error when search IPv6 address routing(done)
- Statistics error on Home page(done)
- 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
- Bi direction routing path(done)
- Reverse routing path(done)
- Monthly /weekly summary
- Show alternative routing path/track multi path
- Path performance

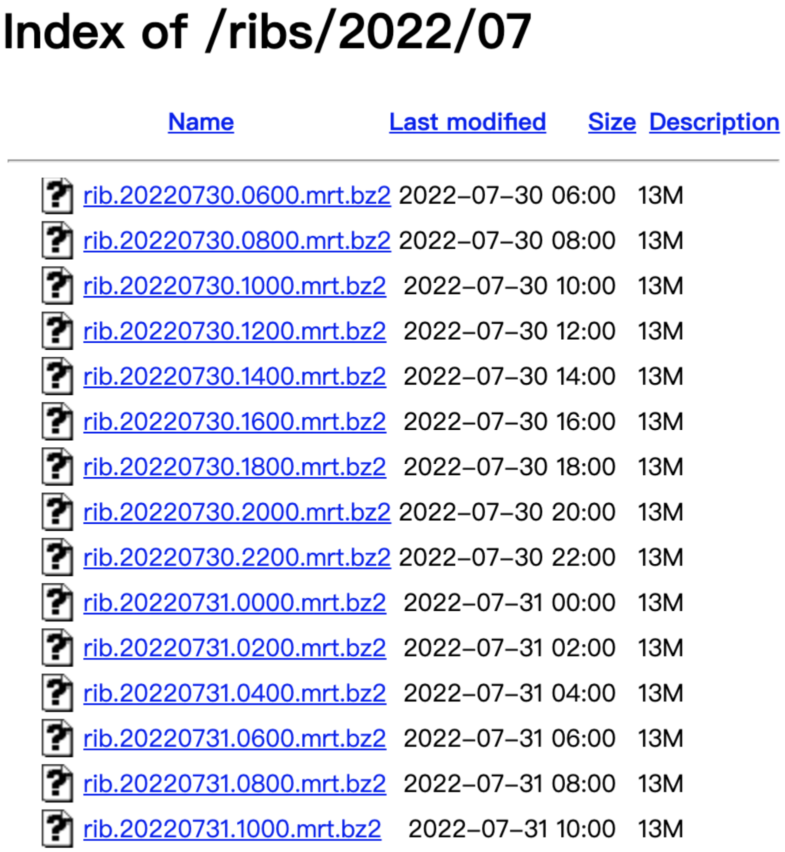
Project Progress

- Established BGP session with 14 partners
- Looking Glass connected with 7 Education & Research network
- Fixed Bugs
- New function:
  - ✓ Bi direction routing path(done)
  - ✓ Reverse routing path(done)
- Paper accepted by NOMS 2023
- Prefix Hijacking Annual Report
- Training Preparation

BGP Route Information Sharing

We have established BGP session with 14 partners.
Data can be accessed at https://bgp.cgtf.net
Configuration manual can be accessed at
https://www.bgper.net/index.php/document/

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



Index of /ribs/2022/07

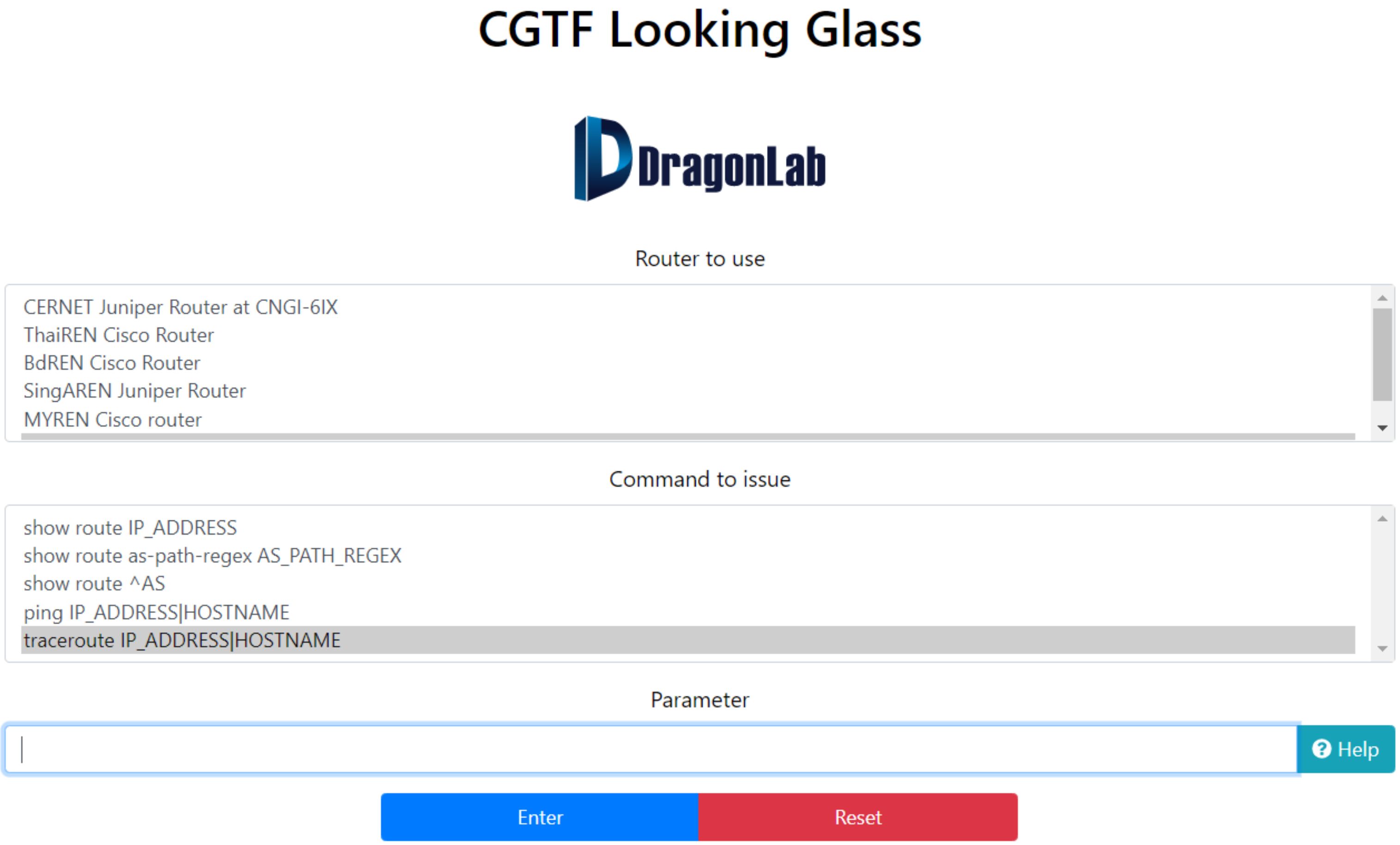
Name	Last modified	Size	Description
rib.20220730.0600.mrt.bz2	2022-07-30 06:00	13M	
rib.20220730.0800.mrt.bz2	2022-07-30 08:00	13M	
rib.20220730.1000.mrt.bz2	2022-07-30 10:00	13M	
rib.20220730.1200.mrt.bz2	2022-07-30 12:00	13M	
rib.20220730.1400.mrt.bz2	2022-07-30 14:00	13M	
rib.20220730.1600.mrt.bz2	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	

清華大學 Tsinghua University

APNIC FOUNDATION

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



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
```

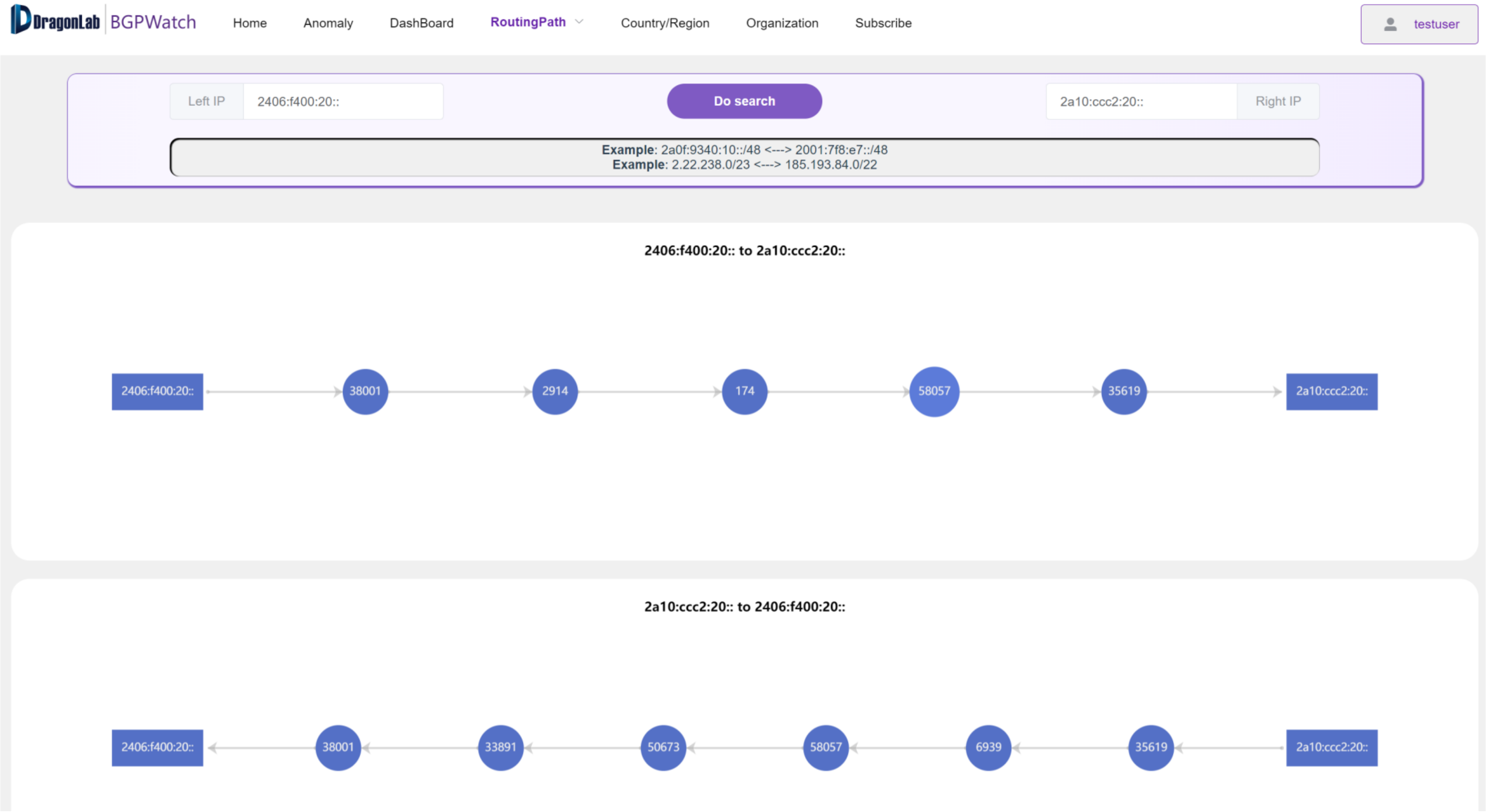
Parameter

- 7 Education & Research network joined

Tsinghua University

APNIC FOUNDATION

Bi direction routing path



Left IP: 2406:f400:20::

Right IP: 2a10:ccc2:20::

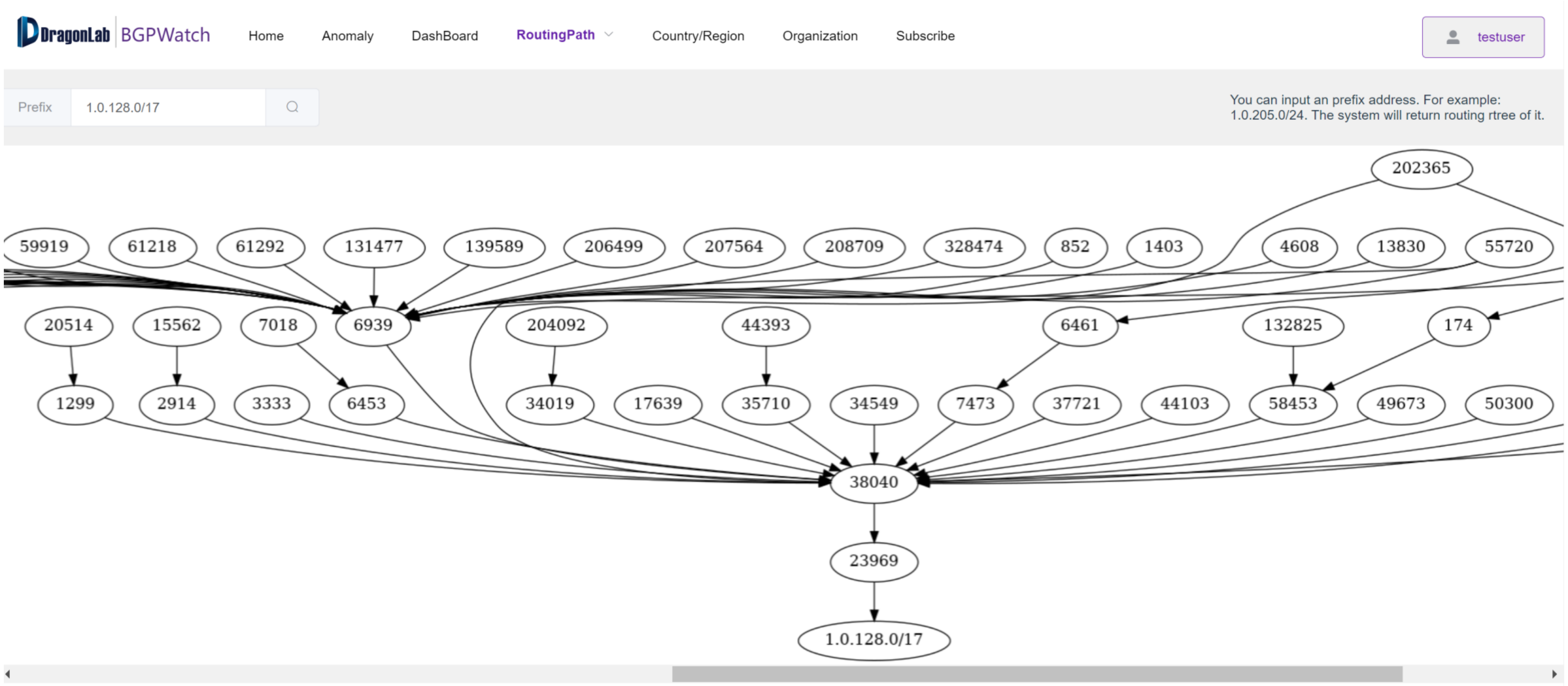
Example: 2a0f:9340:10::/48 <---> 2001:7f8:e7::/48
Example: 2.22.238.0/23 <---> 185.193.84.0/22

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

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

- Best matched prefix in routing table
- https://bgpwatch.cgtf.net

Reverse Path



1.0.128.0/17

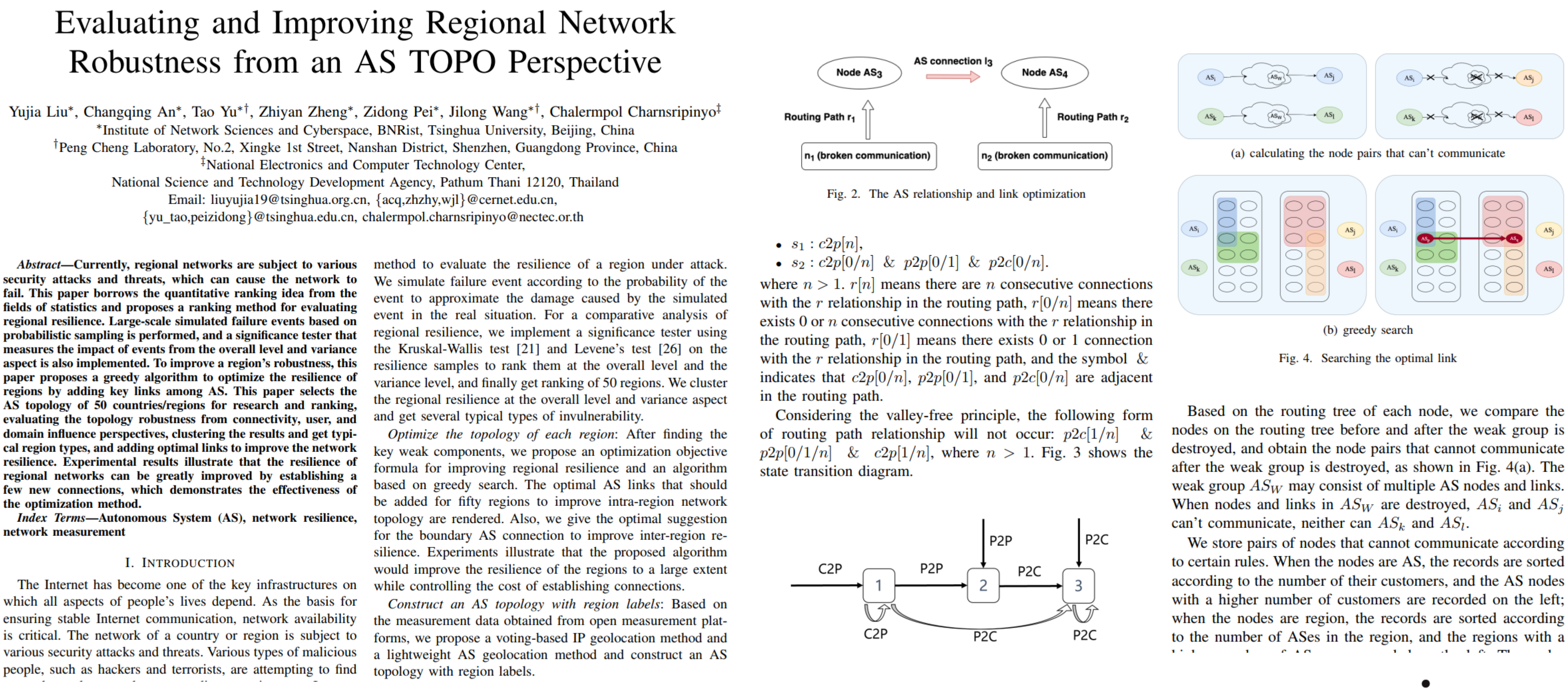
You can input an prefix address. For example: 1.0.205.0/24. The system will return routing rtree of it.

- Exactly matched prefix in routing table
- Need to improve interactivity

清華大學 Tsinghua University

APNIC FOUNDATION

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

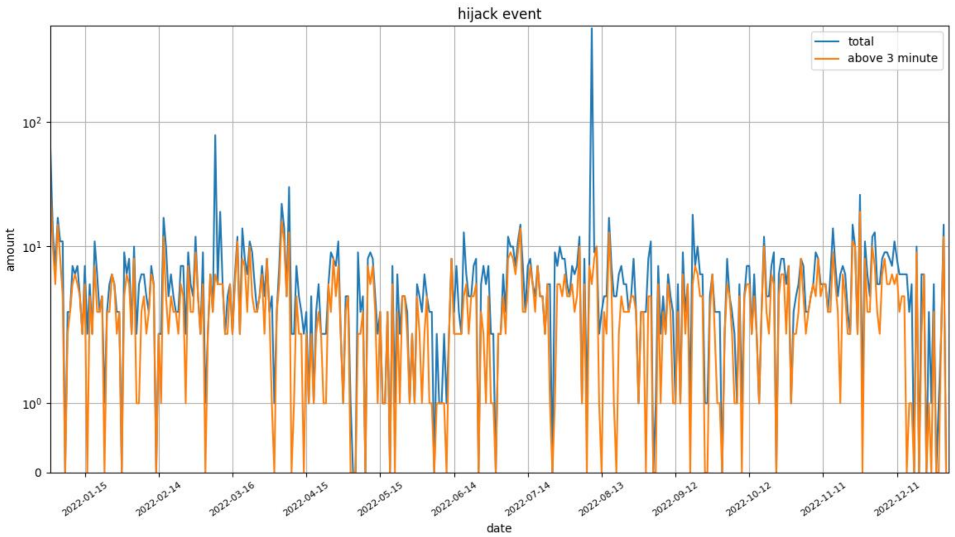
- Accepted by NOMS 2023
- https://github.com/thudragonlab/Resilience

Tsinghua University

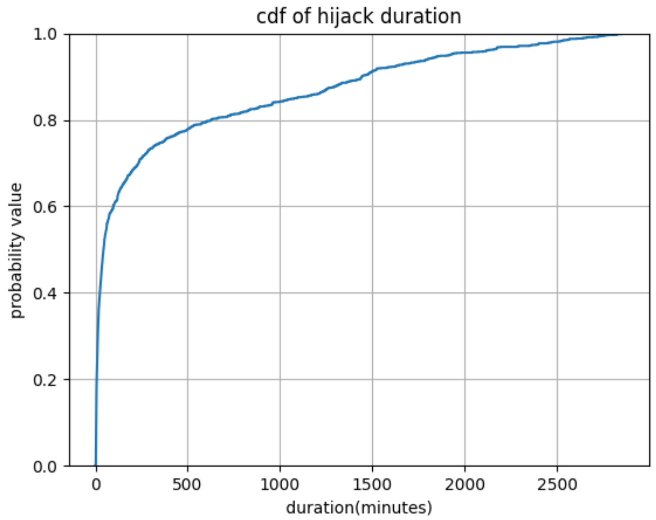
APNIC FOUNDATION

Prefix Hijacking Annual Report (Draft)

Daily Events



length distribution of hijacked IPv4 prefix



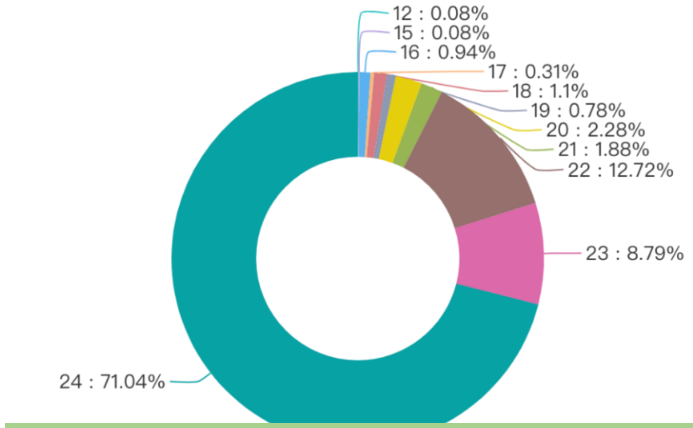
Duration Distribution

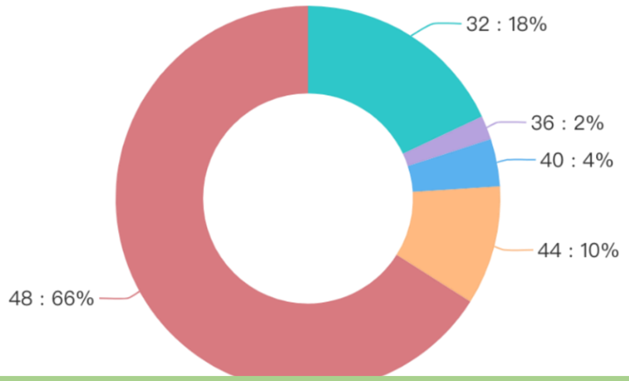
60% under 100m

80% under 500m =8.33h

length distribution of hijacked IPv6 prefix

Hijacked IPv4 prefix Distribution



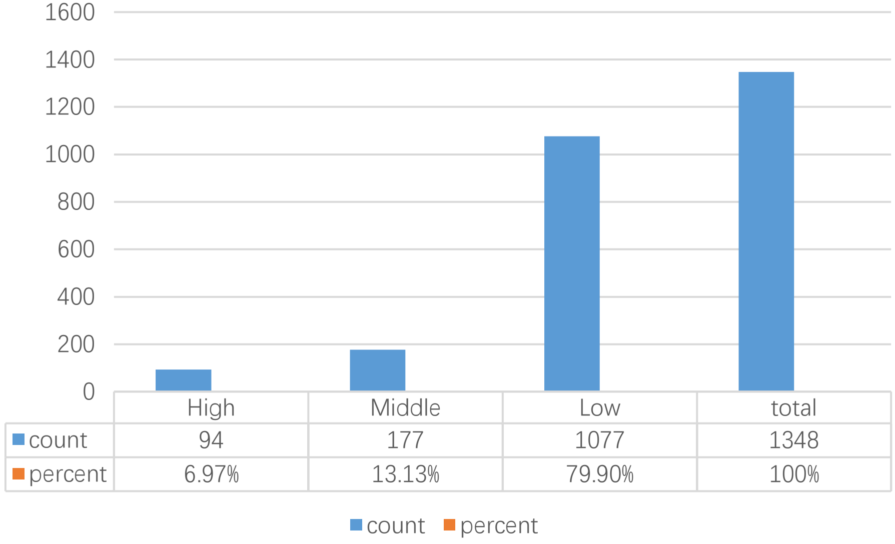


Hijacked IPv6 prefix Distribution

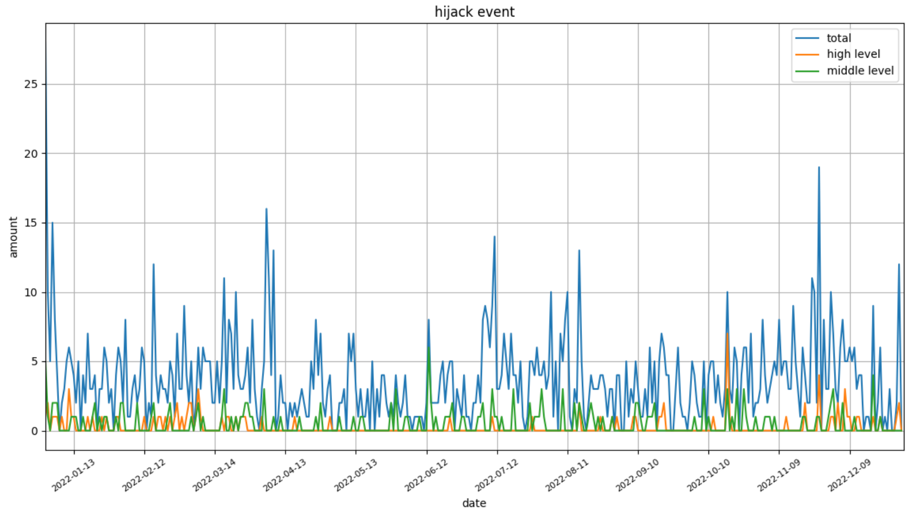
- The draft versions will be shared with project partners for your comments before they are released in March

Prefix Hijacking Annual Report (Draft)

Event of each level

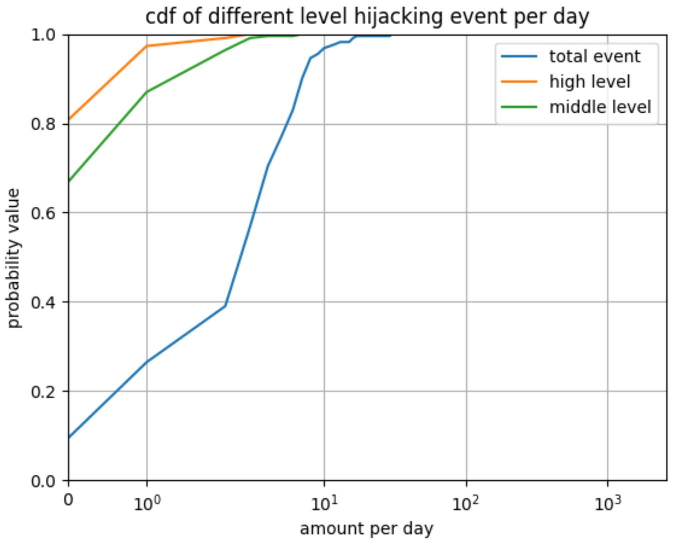


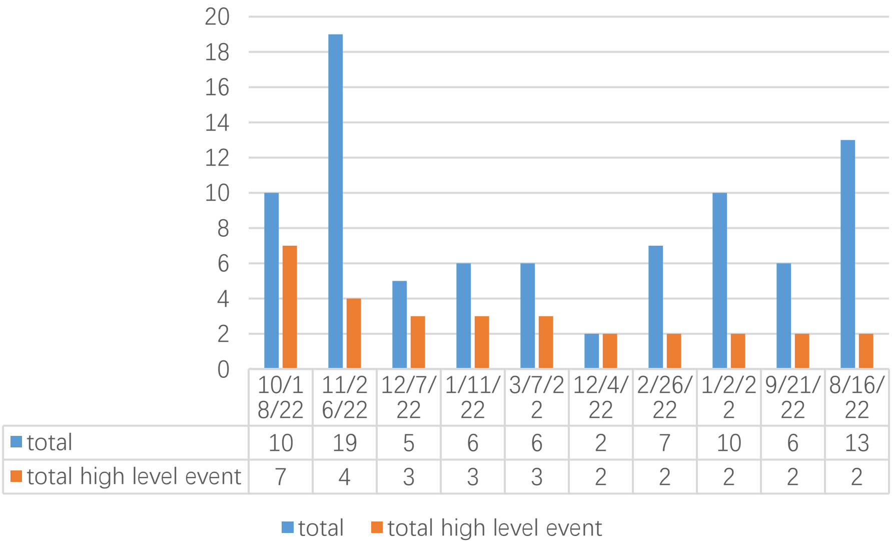
	High	Middle	Low	total
count	94	177	1077	1348
percent	6.97%	13.13%	79.90%	100%



Daily event of each level

Daily event Distribution

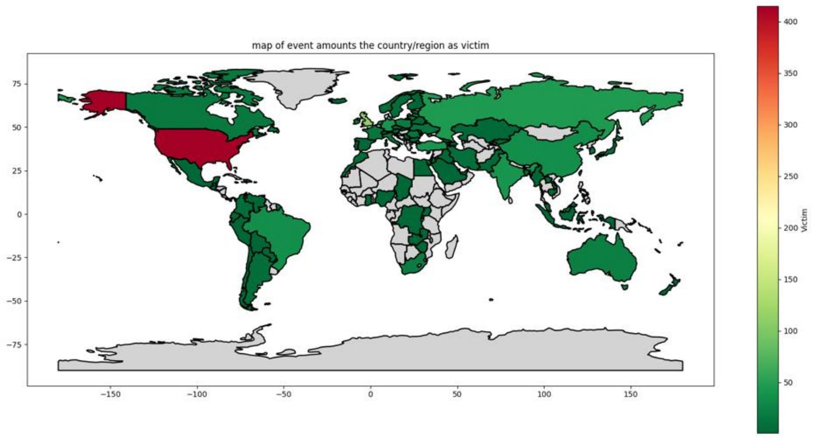


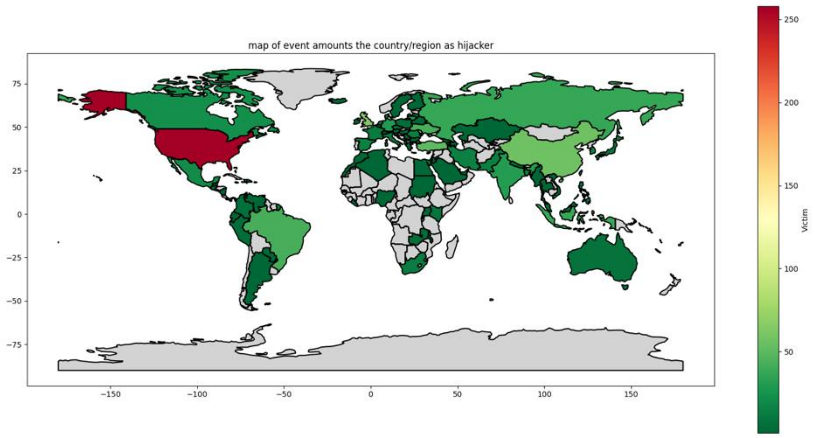


	10/18/22	11/26/22	12/7/22	1/11/22	3/7/22	12/4/22	2/26/22	1/2/22	9/21/22	8/16/22
total	10	19	5	6	6	2	7	10	6	13
total high level event	7	4	3	3	3	2	2	2	2	2

TOP 10 high level events

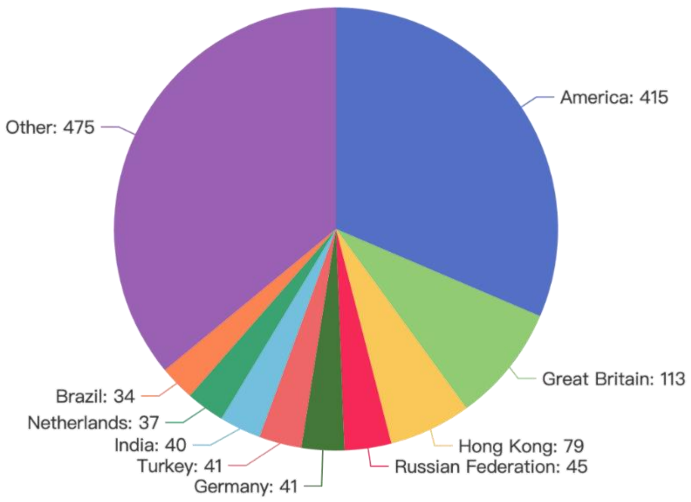
Prefix Hijacking Annual Report (Draft)





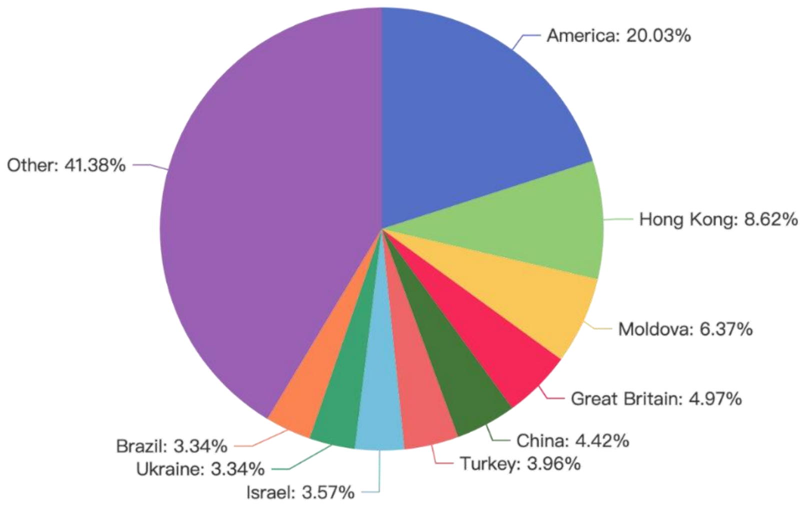
distribution of event amounts the country/region as victim

Distribution of events by country as victim



distribution of event amounts the country/region as hijacker

Distribution of events by country as hijacker



Future Work

- Refining/Bug Fixing
- 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
- Monthly /weekly summary
- Knowledge sharing
- Documents

Comments/Suggestions

- ??

Thanks!