The Report of the Coordination Committee
- APNIC ISIF Project

24 August, 2023

Tsinghua University

APNIC FOUNDATION

APAN56 Colombo Sri Lanka 21- 25 August, 2023 Visit Sri Lanka

Outline

- Basic Information
- Objectives and Achievements
- Collaborative Community
- Knowledge Sharing Works
- Deliverables and Dissemination
- Budget and Expenses
- The Extension Project
- The Technical Committee Report

清華大學 Tsinghua University

APNIC FOUNDATION

Basic Information

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

清華大學 Tsinghua University

APNIC FOUNDATION

The Project Objectives and Achievements

Objectives	Detail work	Status
Build a collaborative community for enhancing the capacity of NRENs' network operation and measurement	Inviting project partners	17 NRENs and 2 universities
	Setting up project website	Done
	Collaborative work, including regular meetings and discussions	Done
	Platforms development and deployment	See below
Establish a distributed BGP routing monitoring platform and a looking glass platform in the Asia-Pacific region	BGP Routing Information Sharing	15 partners
	Looking Glass Platform	Connect with 7 partners, link to 4 partners
	Tools for operator(dashboard, routing path search, register and alarm email)	Done by August 2023
Deploy a BGP hijacking detection and mitigation system and analyze the robustness of routing in the Asia-Pacific region	Development of prefix hijacking detection	Done by August 2023
	Development of path hijacking detection	Done by August 2023
	Research Paper: region resilience	Done by May 2023
	Research Paper: routing hijacking detection	Done by June 2023
Share knowledge and experience globally	Training events: RPKI, MANRS, DNSSEC, BGPWatch platform	Done by May 2023
	Meeting presentations, paper, technical reports, manuals, etc.	Nearly Done

Collaborative Community – Partnerships

- **19 Partner Organizations joined the project**

  (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)

清華大學 Tsinghua University

APNIC FOUNDATION

Collaborative Community – Partnerships

AARNET APAN-JP BdREN CERNET DOST-ASTI ERNET University of Gottingen HARNET ITB KREONET

LEARN MYREN NREN PERN REANNZ SingaRen University of Surrey ThaiREN TransPAC

清華大學 Tsinghua University

APNIC FOUNDATION

Collaborative Community – Governance Structure

Collaborative Community – Project Teams

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

清華大學 Tsinghua University

APNIC FOUNDATION

Collaborative Community – Partners' Engagement

APNIC ISIF Partner Engagement Feb.24, 2022 - Aug.23, 2023

Partner	Kick-off (24 Feb. 2022)	Bilateral (Mar. 2022)	1st Joint (10 May 2022)	2nd Tech (20 Jun. 2022)	3rd Tech (3 Aug. 2022)	2nd Joint (29 Sep. 2022)	Chairs Meeting (27 Sep. 2022)	Bilateral (Sep.-Dec., 2022)	Paper Discussion (13 Oct. 2022)	Bilateral in-person (24 May 2023)	3rd Joint (19 Jan. 2023)	6th Tech (27 Apr. 2023)	Project Meeting (25 May 2023))	BGP session	Looking Glass	The Last Joint (24 Aug. 2023)
AARNET		YES	YES					YES						YES		
APAN-JP	YES	YES	YES	YES	YES	YES	YES	YES						YES	YES	
BdREN	YES	YES	YES	YES	YES	YES		YES	YES	YES	YES	YES	YES	YES	YES	
CERNET	YES	YES	YES	YES	YES	YES	YES	YES	YES			YES	YES	YES	YES	
DOST-ASTI	YES	YES	YES					YES		YES		YES	YES			
ERNET	YES	YES	YES		YES											
Gottingen	YES			YES		YES		YES								
HARNET	YES	YES	YES	YES	YES	YES		YES			YES	YES		YES		
ITB		YES	YES	YES	YES	YES		YES			YES	YES		YES		
KREONET		YES	YES			YES		YES			YES	YES		YES	YES	
LEARN	YES	YES	YES	YES	YES	YES		YES	YES	YES	YES	YES	YES	YES	YES	
MYREN	YES	YES	YES	YES	YES			YES			YES	YES		YES	YES	
NREN		YES				YES		YES	YES	YES		YES	YES	YES		
PERN		YES	YES	YES		YES		YES	YES	YES	YES		YES	YES	YES	
REANNZ		YES	YES	YES	YES			YES						YES	YES	
SingAREN	YES	YES	YES	YES	YES	YES	YES	YES			YES			YES	YES	
Surrey	YES	YES		YES	YES			YES								
ThaiREN	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	
TransPAC		YES	YES											YES	YES	

清華大學 Tsinghua University

APNIC FOUNDATION

Collaborative Community – Bilateral Meetings

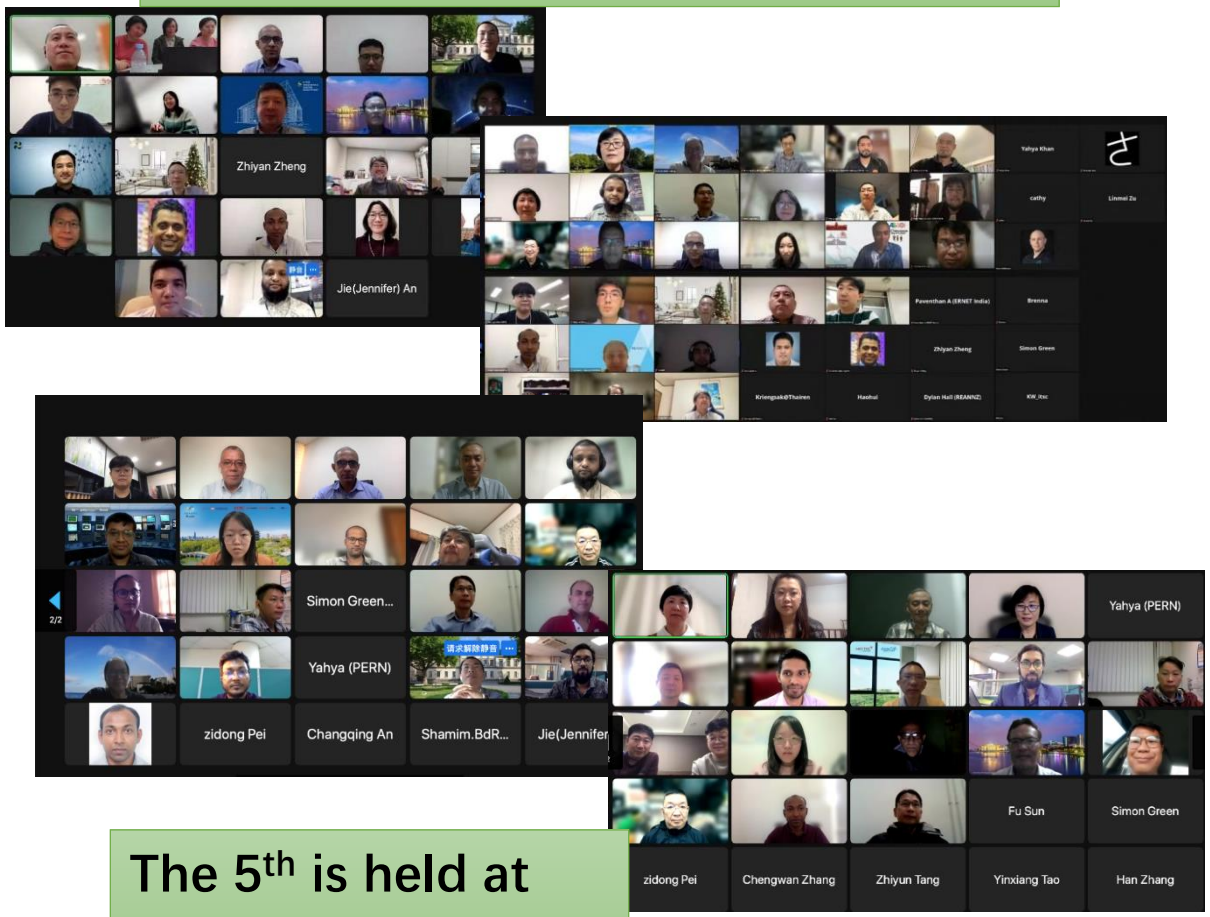
3 Rounds of Bilateral Meetings:
The first round of online bilateral meeting, all 19 partners joined.
The second round of online bilateral meeting, 17 partners joined.
The third round was physical meetings with 6 partners who joined the project meeting in person in May in Beijing.

清華大學 Tsinghua University

APNIC FOUNDATION

Collaborative Community – Committee Meetings

5 Joint Committee Meetings



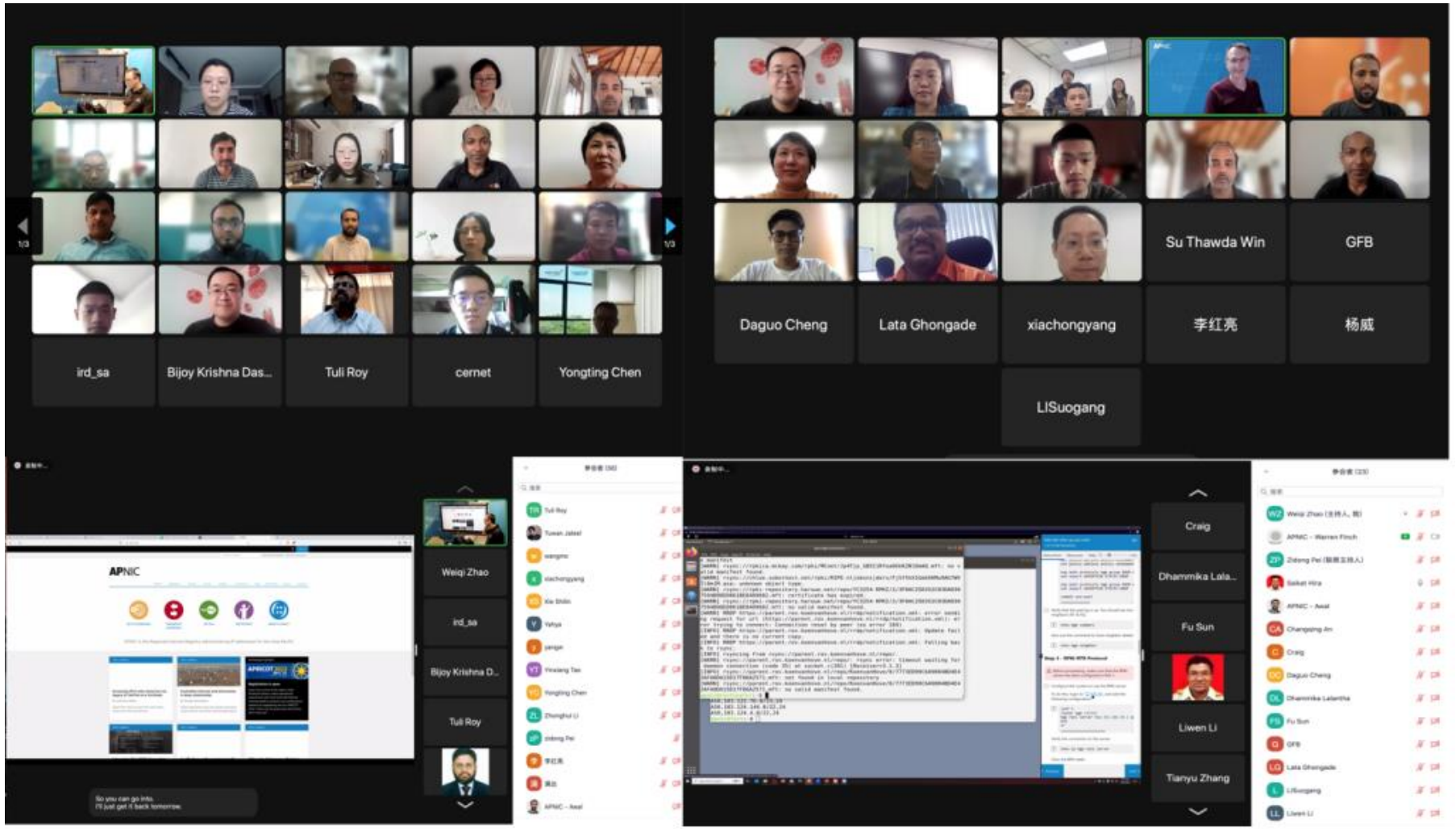
The 5th is held at APAN56 right now.

Technical Committee Meetings

Tsinghua University

APNIC FOUNDATION

Knowledge Sharing – RPKI Online Training



With APNIC Support, this event was open to all besides the project partners, and attracted the participation of 80 engineers and technicians from 19 countries and regions.

清華大學 Tsinghua University

APNIC FOUNDATION

Knowledge Sharing – RPKI & MANRS Training Events at APAN55

RPKI & MANRS Training at APAN55

13th, 15th, 16th March, 2023

Kathmandu, Nepal

Co-organized by:

Tsinghua University, APNIC, APAN, NREN

Sponsored by:

APNIC ISIF Project, APNIC, Tsinghua University

Released Date: 19th January, 2023

Program

(Draft Version 1.0)

Date: 13th, 15th, 16th, March, 2023
Venue: Kathmandu Marriott Hotel (Naxal, Kathmandu, Nepal)
Note. The training event will be conducted in English.

13th March, 2023 (Monday)

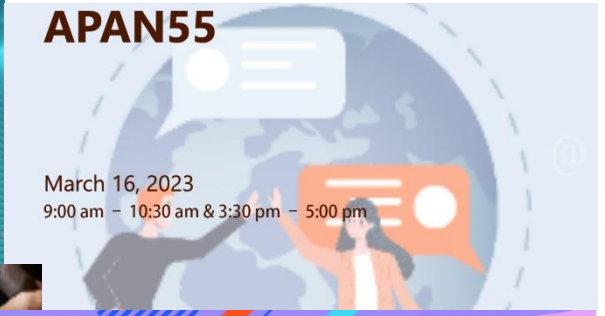
Time (GMT+5:45)	Topic	Trainer
09:00 - 10:30	RPKI - Theory	Dibya Khatiwada APNIC Community Trainer
10:30 - 11:00	Tea/Coffee Break	
11:00 - 12:30	RPKI - Theory RPKI - Hands-on	Dibya Khatiwada APNIC Community Trainer
12:30 - 13:30	Lunch Break	
13:30 - 15:00	RPKI - Hands-on	Dibya Khatiwada APNIC Community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

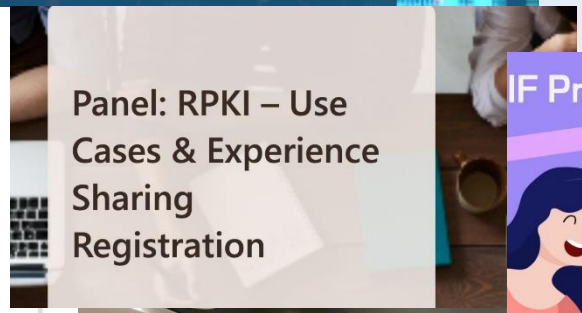
15th March, 2023 (Wednesday)

Time (GMT+5:45)	Topic	Trainer/Speaker
13:30 - 15:00	Panel: RPKI User Cases and Experience eSharing	**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**





With APNIC Support, these events were open to all and a collective of 169 experts and trainees from over 20 countries participated in these sessions.

Knowledge Sharing – DNSSec Training in Beijing

DNSSEC Training
APNIC ISIF Project

Date: 25 May (Thursday)
Venue: Fit 1-312
Program: 09:00-10:30

Program

25 May (Thursday)

DNSSEC Training Trainer: Warren Finch (APNIC)

0830 - 0900	Registration
0900 - 1030	Review: Reverse DNS for IPv6 DNS Security
1030 - 1100	Coffee Break
1100 - 1230	DNSSEC Technical Overview
1230 - 1400	Lunch and Campus Tour II
1400 - 1530	Lab Part 1: DNSSEC Validation DNSSEC Signing
1530 - 1600	Coffee Break
1600 - 1730	Lab Part 2: Manual DNSSEC Signing Lab Part 3: Automatic DNSSEC Signing

CERNET用户
DNS安全技术培训日程

时间：2023年5月25日（星期四）
地点：清华大学FIT楼 1-312

- 08:30-10:00
  DNSSEC 如何保障域名解析安全—技术原理和安全特性
  主讲人：刘保君（清华大学网络科学与网络空间研究院助理教授、博士生导师）、陆超逸（清华大学网络科学与网络空间研究院博士后）
- 10:00-10:50
  基于域名系统的安全检测与应急响应技术
  主讲人：张甲（清华大学网络科学与网络空间研究院副研究员）
- 10:50-11:10
  会间休息
- 11:10-12:00
  HTTPS 部署中的安全挑战与解决方案
  主讲人：张一铭（清华大学网络科学与网络空间研究院博士后）
- 12:00-14:00
  午餐
- 14:00-17:30
  DNSSEC 实际操作培训（培训语言为英文）
  主讲人：Warren Finch（亚太互联网络信息中心APNIC高级网络分析师、技术培训师）

With APNIC Support, the onsite participants are more than 60, and online above 1000.

清華大學 Tsinghua University

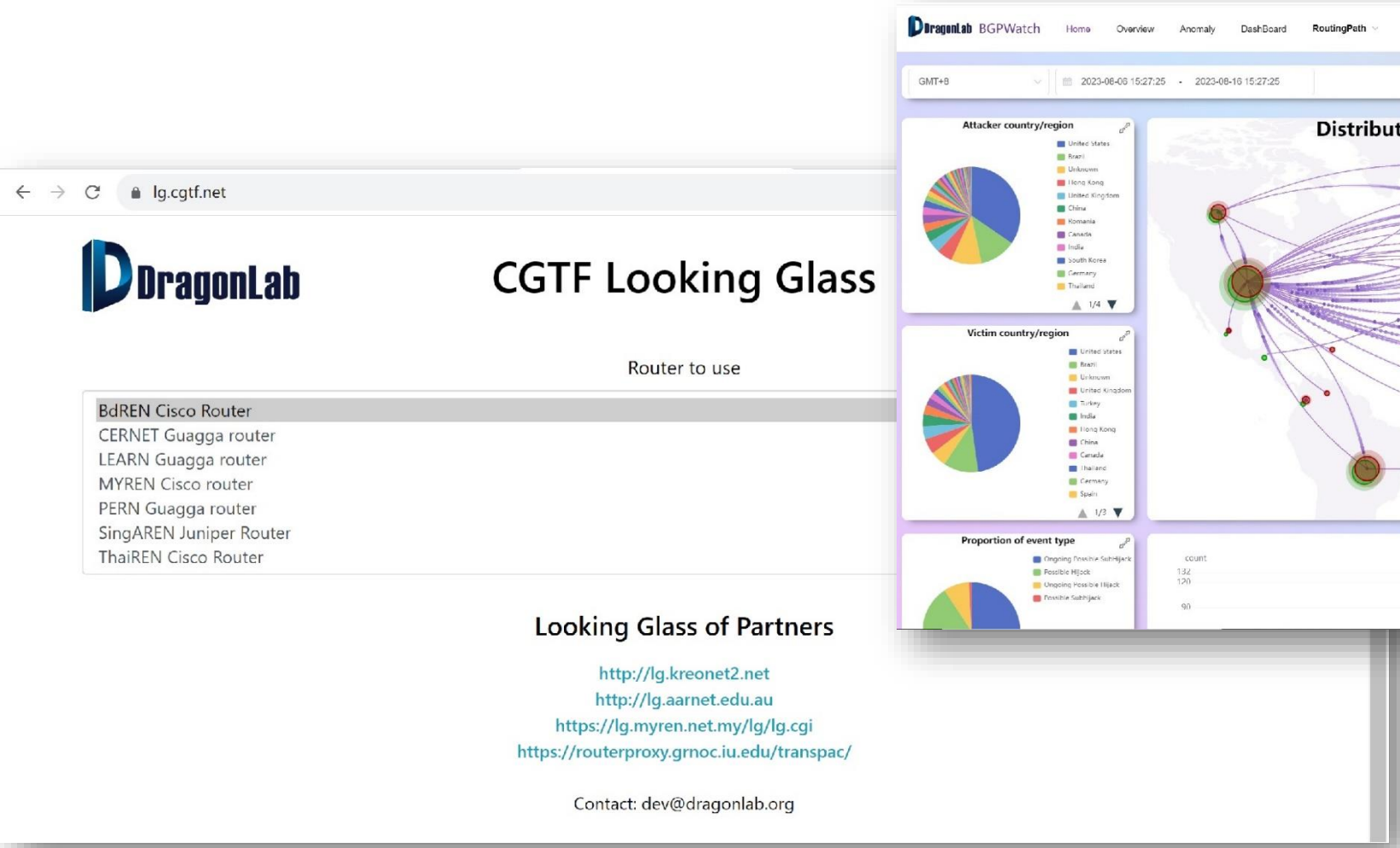
APNIC FOUNDATION

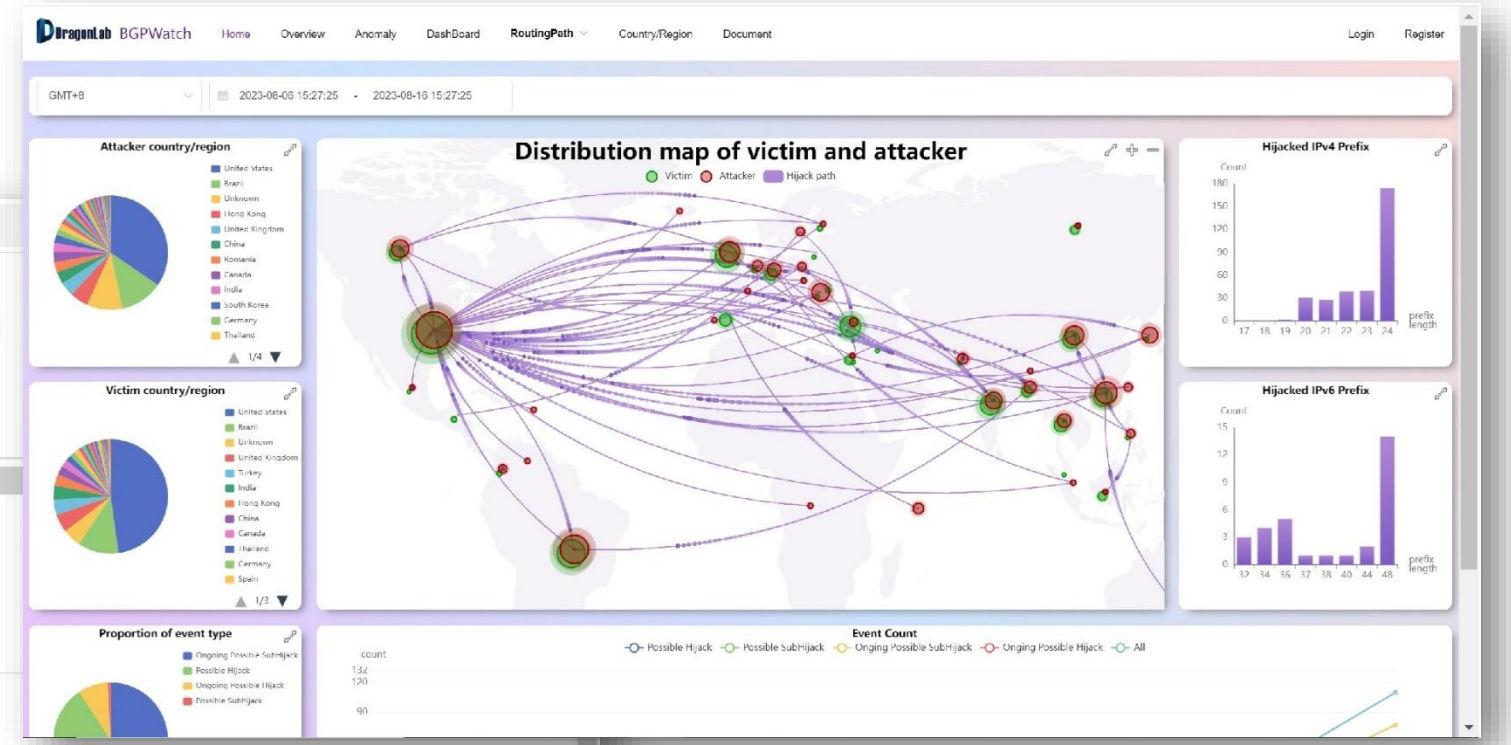
Knowledge Sharing – CompTIA Certificates

- With BdREN's support, investigation of CompTIA Certificates courses was finished, and after receiving the confirmation with APNIC Foundation, we were allowed to use APNIC ISIF Project funds to support our NREN partners' engineers to enroll the CompTIA Certificates courses.
- Finally, 24 enrollments for the selected courses have done with APNIC Foundation's help, the codes are sent to each participant too.

No.	Organization	Name of Student	Courses
1	DOST-ASTI	Tommy Aydalla, Jr.	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
2	DOST-ASTI	Jhonnel Borga	Network+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
3	ThaiREN	Mr. Nattanakit	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
4	ThaiREN	Mr. Wachira Chaowalit	Security+ Exam Voucher CertMaster Learn + Labs, CertMaster Practice
5	BdREN	Kamrul Hasan Shakil	Security+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
6	BdREN	Md. Ariful Islam Arman	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
7	ERNET	Hari Krishna Atluri	Security+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
8	ERNET	Yashwant Reddy R	Security+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
9	HARNET	KW Pong	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
10	HARNET	Wai-Man Cheung	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
11	LEARN	Tuwan A. Jaleel	Security+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
12	LEARN	W.D. Dhammika Lalantha	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
13	MYREN	Ridzwan Mohamed	Network+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
14	MYREN	Abd Hamid Ariffin	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
15	NREN	Mr. Nirajan Parajuli	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
16	NREN	Ms. Binita Kushum	Security+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
17	CERNET	Linmei Zu	Network+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
18	CERNET	Zidong Pei	Linux+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
19	CERNET	Jiaxing Zhang	Linux+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
20	CERNET	Wenbing Liu	Cloud+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
21	CERNET	Zhiyan Zheng	Security+ Exam Voucher CertMaster Learn + Labs, CertMaster Practice
22	CERNET	Yongting Chen	Linux+ Exam Voucher, CertMaster Learn + Labs, CertMaster Practice
23	PERN	Waqas Masood	Security+ Exam Voucher CertMaster Learn + Labs, CertMaster Practice
24	PERN	Fawad Raza	Security+ Exam Voucher CertMaster Learn + Labs, CertMaster Practice

Platforms and System – BGPWatch and Looking Glass

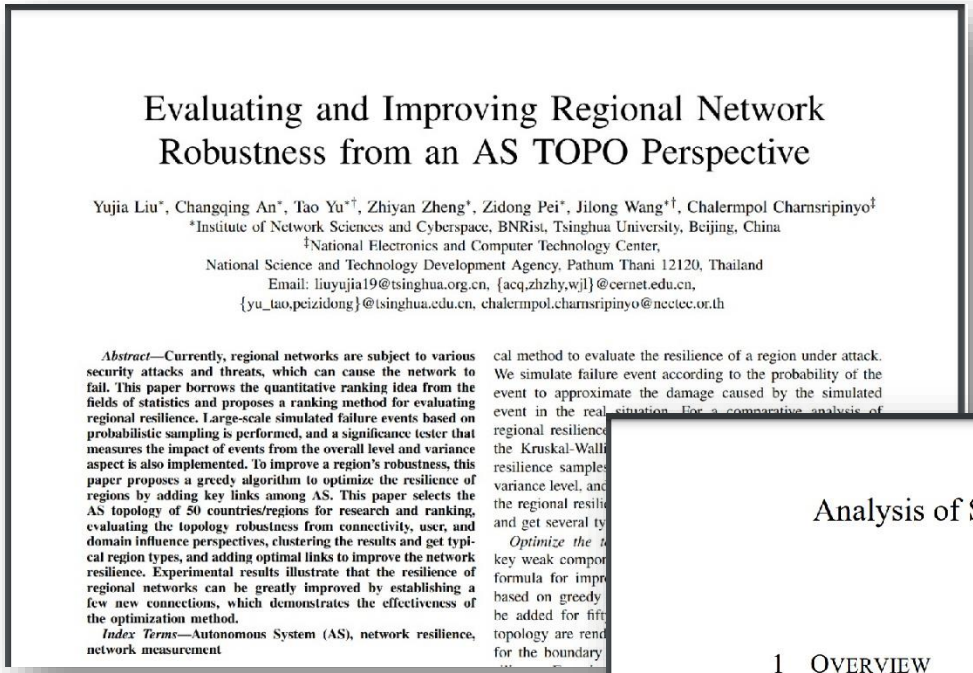




Tsinghua University

APNIC FOUNDATION

Platforms and System – Two Research Papers and One Report



Evaluating and Improving Regional Network Robustness from an AS TOPO Perspective

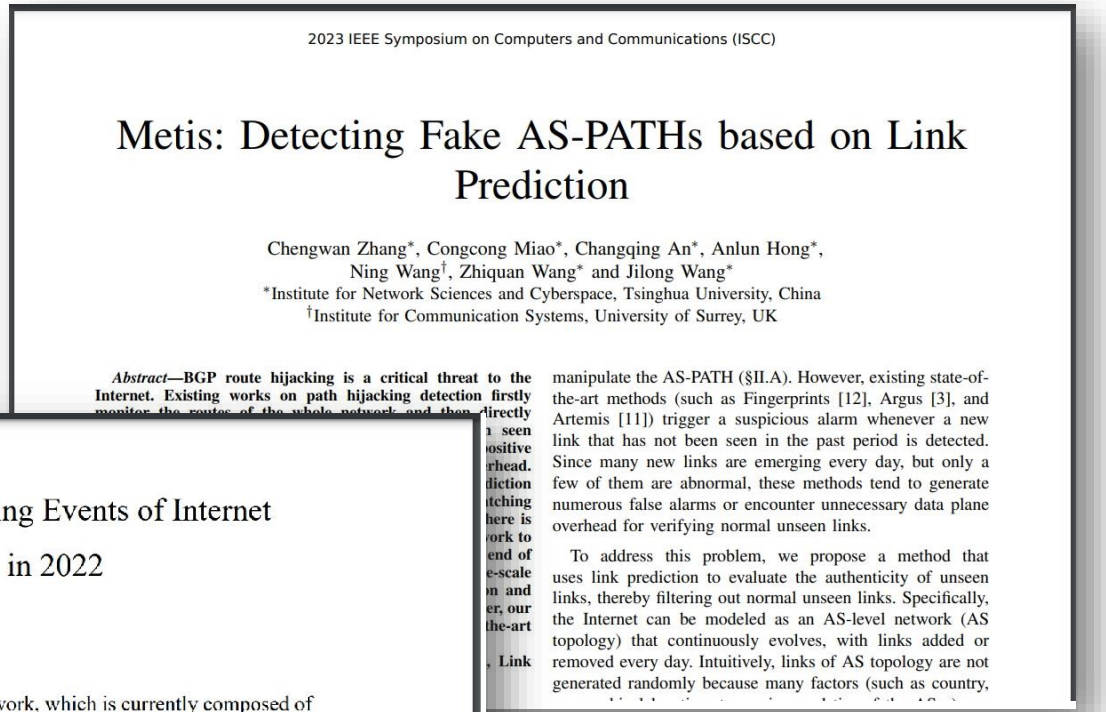
Yujia Liu*, Changqing An*, Tao Yu*†, Zhiyan Zheng*, Zidong Pei*, Jilong Wang*†, Chalermpol Charnsripinyo‡
*Institute of Network Sciences and Cyberspace, BNRist, Tsinghua University, Beijing, China
‡National Electronics and Computer Technology Center,
National Science and Technology Development Agency, 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**

cal 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 the Kruskal-Walli resilience samples variance level, and the regional resili and get several ty

Optimize the t key weak compor formula for impr based on greedy be added for fift topology are rend for the boundary



2023 IEEE Symposium on Computers and Communications (ISCC)

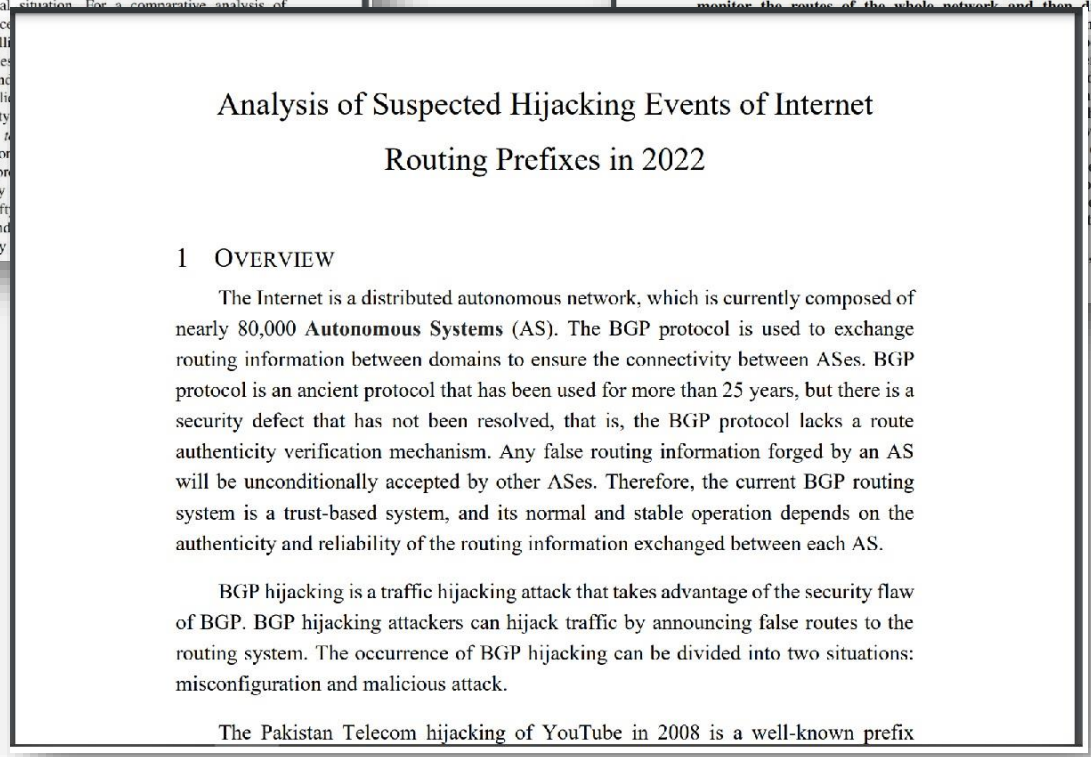
Metis: Detecting Fake AS-PATHs based on Link Prediction

Chengwan Zhang*, Congcong Miao*, Changqing An*, Anlun Hong*,
Ning Wang†, Zhiquan Wang* and Jilong Wang*
*Institute for Network Sciences and Cyberspace, Tsinghua University, China
†Institute for Communication Systems, University of Surrey, UK

***Abstract*—BGP route hijacking is a critical threat to the Internet. Existing works on path hijacking detection firstly monitor the routes of the whole network and then directly**

manipulate the AS-PATH (§II.A). However, existing state-of-the-art methods (such as Fingerprints [12], Argus [3], and Artemis [11]) trigger a suspicious alarm whenever a new link that has not been seen in the past period is detected. Since many new links are emerging every day, but only a few of them are abnormal, these methods tend to generate numerous false alarms or encounter unnecessary data plane overhead for verifying normal unseen links.

To address this problem, we propose a method that uses link prediction to evaluate the authenticity of unseen links, thereby filtering out normal unseen links. Specifically, the Internet can be modeled as an AS-level network (AS topology) that continuously evolves, with links added or removed every day. Intuitively, links of AS topology are not generated randomly because many factors (such as country,



Analysis of Suspected Hijacking Events of Internet Routing Prefixes in 2022

1 Overview

The Internet is a distributed autonomous network, which is currently composed of nearly 80,000 **Autonomous Systems** (AS). The BGP protocol is used to exchange routing information between domains to ensure the connectivity between ASes. BGP protocol is an ancient protocol that has been used for more than 25 years, but there is a security defect that has not been resolved, that is, the BGP protocol lacks a route authenticity verification mechanism. Any false routing information forged by an AS will be unconditionally accepted by other ASes. Therefore, the current BGP routing system is a trust-based system, and its normal and stable operation depends on the authenticity and reliability of the routing information exchanged between each AS.

BGP hijacking is a traffic hijacking attack that takes advantage of the security flaw of BGP. BGP hijacking attackers can hijack traffic by announcing false routes to the routing system. The occurrence of BGP hijacking can be divided into two situations: misconfiguration and malicious attack.

The Pakistan Telecom hijacking of YouTube in 2008 is a well-known prefix

清華大學 Tsinghua University

APNIC FOUNDATION

Knowledge Sharing – Platform Demonstration

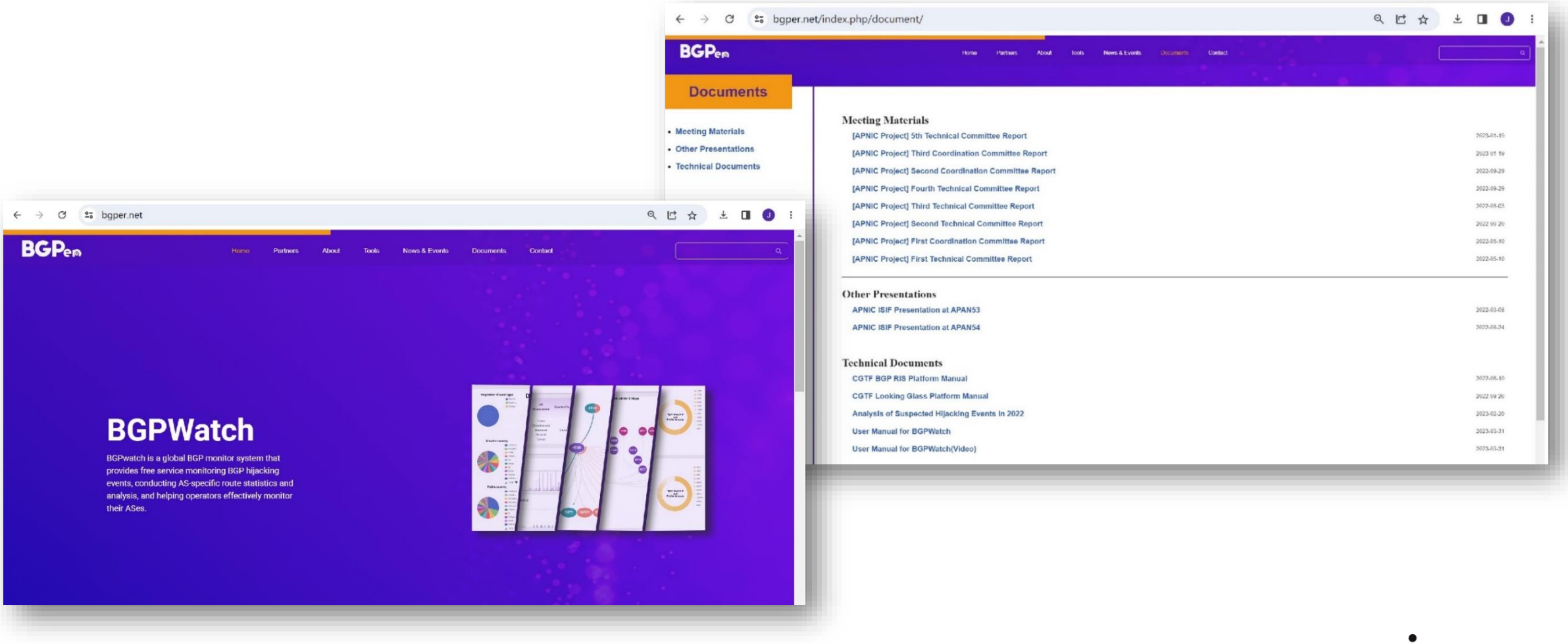
https://www.cgtf.net/wp-content/uploads/2023/07/BGP-Watch-Video-V4.mp4

BdREN team worked with Tsinghua team for writing the user manual and making video demonstration.

清華大學 Tsinghua University

APNIC FOUNDATION

Deliverables and Dissemination – Project Website

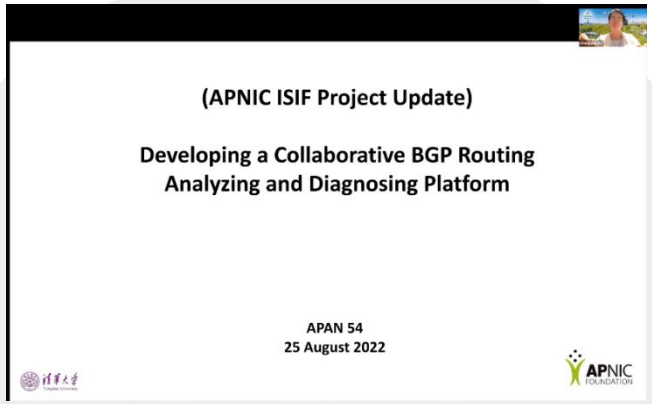


清華大學 Tsinghua University

APNIC FOUNDATION

Deliverables and Dissemination – Presentations

APAN53



APAN54

APAN55

TNC23

APAN56

IGF 京都 KYOTO 2023

The application for an on-site booth was approved by IGF2023 last week. (8-12 Oct., 2023, in Kyoto, Japan)

清華大學 Tsinghua University

APNIC FOUNDATION

Budget and Expense - Consolidated

Consolidated Budget

	ISIF Asia Impact Grant	Applicant's in-kind contribution	Expenditure of ISIF Asia Impact Grant	Remarks
Training session (one-day offline) / backup plan	46,680		44,097.48	The costs associated with engagement conducted by the project team internationally (including travel)
Professional development and collaborative work	72,000		73,273.05	The costs associated with training and professional development for the staff project team
Support Services Fees	31,320		32,629.50	This cost is related to hosting, translation, office supplies, tax, adminitration fee, website, and so forth.
Human Resources of Project Coordination Committee/technical support/Secretariat		41,700		The cost of project management work conducted by the project coordination team members in China will be covered by Chinese funding resources, including 'Joint IPv6 Project'.
The regular participation of the 12 international partner organization (listed in 'Joint IPv6 Project')		10,800		The 12 international partner organizations listed in 'Joint IPv6 Project' could get half financial support from 'Joint IPv6 Project' funding for their regular participation in ISIF proposal activities.
The service fee of cloud server		9,000		This cloud server will be used for this ISIF grant proposal for 18 months, the service fee is around 9,000USD (500USD/month x 18 months).
The travel expenses of one-day offline event for 4 Chinese team members		8,160		This will be covered by 'Joint IPv6 Project'.
Total	150,000	69,660	150,000	

Acknowledgement:
AARNET,
APAN-JP,
REANNZ,
And TransPAC
(APAN Routing WG)
fully contributed to the project without using any ISIF funds.

KREONET and **SingAREN** contributed to the project by using partial project funds.

APNIC FOUNDATION

Budget and Expense - Training

Training Session / Backup Plan						
One-day Offline Training Session at APAN meeting (38,680 USD)						
Description	**Unit**	**# of units**	**Unit rate(in USD)**	**Budgeted(in USD)**	**Spent(in USD)**	**Remarks**
APAN registration fee	per person	17	400	6,800	**36,180.59**	This proposal is planned to organize one-day offline training session at APAN54 or APAN55 and four half-day online training sessions. Regarding one-day offline training session (**38,680 USD**), it is planned to cover the costs of NOC engineers from developing countries/economies, including APAN registration fee, travel and diem for 4-day APAN meeting (3 nights) to encourage the communication with APAN and APNIC community. The total number of unit is 17 including 15 NREN NOC engineers from 13 developing countries/economies(as some have more than one NREN), and two expertises. It is planned to cover the working hour costs fo two expertise as well. If the COVID-19 pandemic situation would get worse. a back-up plan is also prepared as below.
International travel(airfare)	per person	17	1,000	17,000		
Diem(meals, hotels, local transportation)	per person per day	4 days and 17 persons	160	10,880		
Expertise	half-day sesion	2	2,000	4,000		
Four Half-day Online Training Session (8,000 USD)						
Expertise	half-day session	4	2,000	8,000	0	
The Training for CompTIA Certification						
CompTIA Certification				**0**	**7,916.89**	
Sub-total				**46,680**	**44,097.48**	

清華大學 Tsinghua University

APNIC FOUNDATION

Budget and Expense – Community Engagement

Professional development for the staff project team

Description	Unit	#of units	Unit rate(in USD)	Budgeted(in USD)	Spent(in USD)	Remarks
Regular participation of periodically activities of professional development for platform deployment, testing and sharing	per month, per organization	9	1,800	16,200	**60,128.35**	It's expected that 9 NREN partner organizations in Asia Pacific region which are not involved in 'Joint IPv6 Projects'. In some countries/economies, there are more than one NREN organizations. The estimated working time in the whole project is one month each organization, and the average monthly cost is 1,800USD.
	per month, per organization	12	900	10,800		This is the half-cost of 12 international partner organizations involved in 'Joint IPv6 Project' which could cover the other half-costs of their regular participation in all activities of this ISIF proposal .
Expertise participation of monthly activities of professional development for platform development, sharing and training	per month, per expertise	10	3,000	30,000		It's planned that the expertise work from partner organizations will be invited, and the total estimated working hours in the whole project is 10 months, the average monthly cost is 3,000USD.
Collaborative documentation work of papers, reports, etc.,	per month, per person	6	2,500	15,000	**13,144.70**	This includes analizing data, writing, editing, proof-reading, etc. The estimaged working hours in this whole project is 6 months and the average monthly cost is 2,500USD.
Sub-total				**72,000**	**73,273.05**	

清華大學 Tsinghua University

APNIC FOUNDATION

Budget and Expense – Other Support Services

Support Services Fees				
Description		**Budgeted(in USD)**	**Spent(in USD)**	**Remarks**
Tax	3.36%	5,040	**4,777.03**	The funding will go to Tsinghua University's bank account in China and be managed by Tsinghua University. There will occur the tax and administration fee.
Administration fee by Tsinghua University	5%	7,500	**7,311.01**	
Domain Name fee		1,000	**8,037.23**	This is the DNS fee for a domain name of the platforms this project will establish.
Technical service(Project website design, development and maintenance)		6,000		This is the related expenses of technical support of establishing and maintaining a project website for technical platforms and information sharing.
English translation & marketing activities in partner organizations		10,000	**10,570.24**	These include manual/instructions, website, news, poster, case study, etc.
Others (meeting tools,etc.)		1,780	**1,934.00**	
Sub-total		**31,320**	**32,629.51**	

清華大學 Tsinghua University

APNIC FOUNDATION

The Extension Project

Name: An Extension of the Ongoing Project ‘Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform’
Duration: 18 months
Funds: 85000USD
Objectives(draft):
to continue enhancing the capacity of NRENs' network operation and measurement, community engagement and reaching out for international collaborations. The main works are proposed as the draft as follows:
1) Technical work:
- Develop an integrated Looking Glass platform, which can leverage many Looking Glasses and return data to users, and use Looking Glass to further check routing hijacking at the data plan, and to improve detection accuracy.
- Develop path hijacking detection and routing leak detection, continue to maintain and fix bugs in the BGPWatch platform.
2) Others works:
- Continue community development and engagement, international collaboration and knowledge sharing

清華大學 Tsinghua University

APNIC FOUNDATION

The Report of the Technical Committee

清華大學 Tsinghua University

APNIC FOUNDATION