IETF 118

A Large-scale Measurement of IP Source Spoofing on the Internet

Shuai Wang
Zhongguancun Laboratory

Nov 08, 2023

Outline

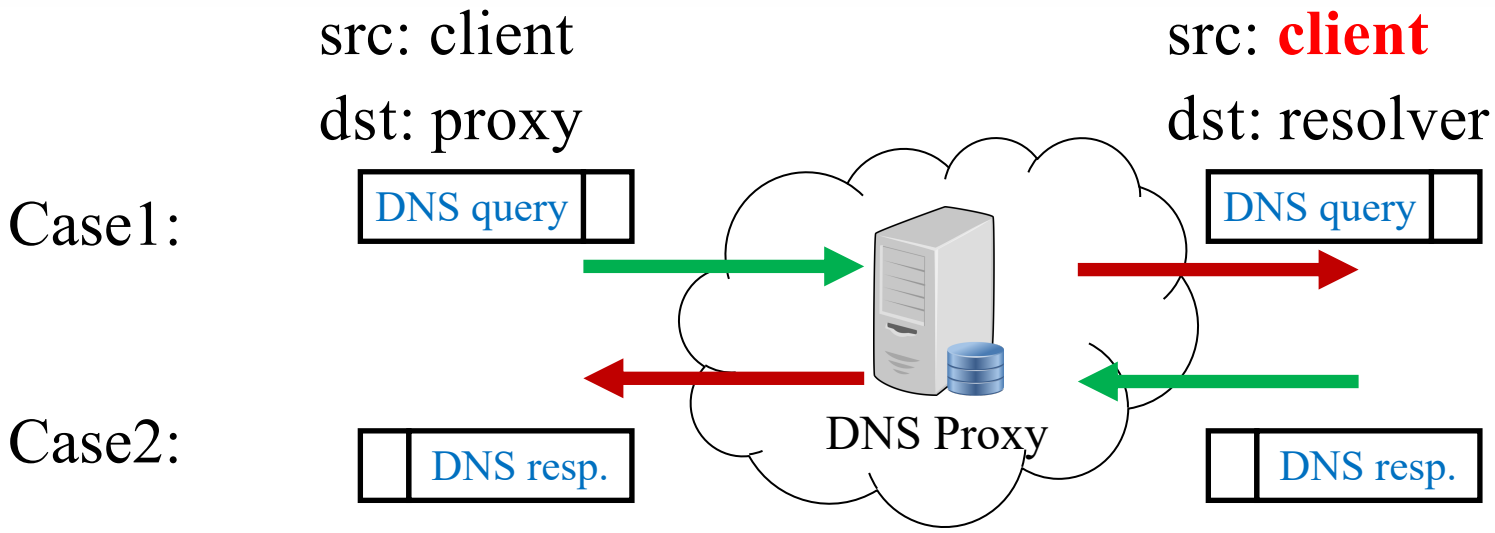
1. Methods of Large-scale Measurement
2. Analysis of Measurement Results
3. Next Steps

Solution 1: DNS Proxy-based Measurement

Key Idea

DNS proxy fails to modify the source address when forwarding DNS requests (or responses), so that the DNS response received by the client comes from another IP instead of the DNS proxy.

- The network where the DNS proxy is located allows to send packets with forged source IP address.



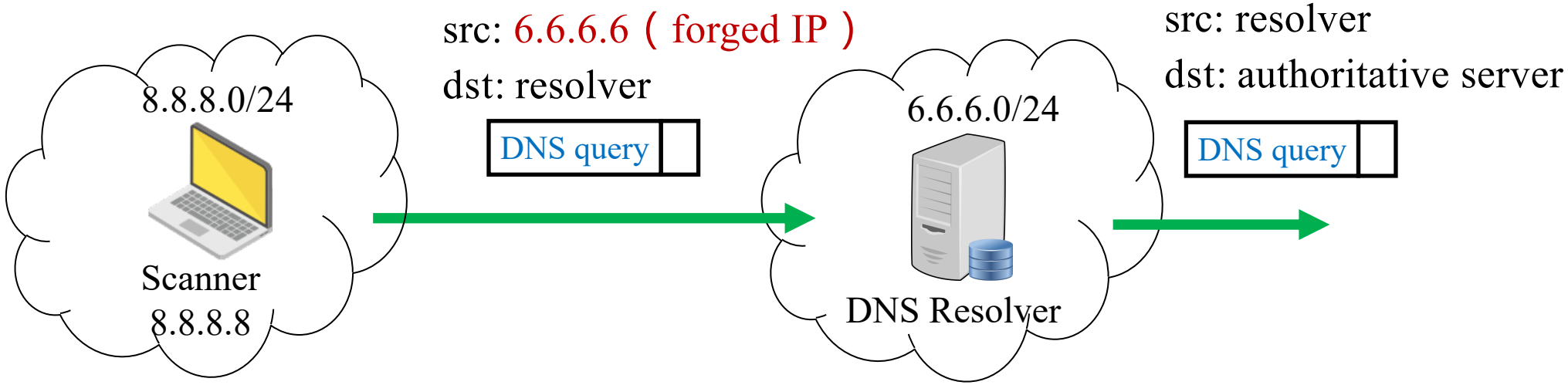
[1] M Kührer, et al., Exit from hell? Reducing the impact of amplification DDoS attacks. Usenix Security'14

Solution 2: DNS Resolver-based Measurement

Key Idea

Send a DNS request with a forged source address to a DNS resolver in the target network, and then check whether the authoritative server receives the DNS request.

- If yes, the target network allows to receive packets with forged source IP address.



NO ISAV!

[1] M Korczyński, et al., Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic. PAM'20
[2] C Deccio, et al., Behind Closed Doors A Network Tale of Spoofing, Intrusion, and False DNS Security. IMC'20

Solution 3: ICMPv6-based Measurement

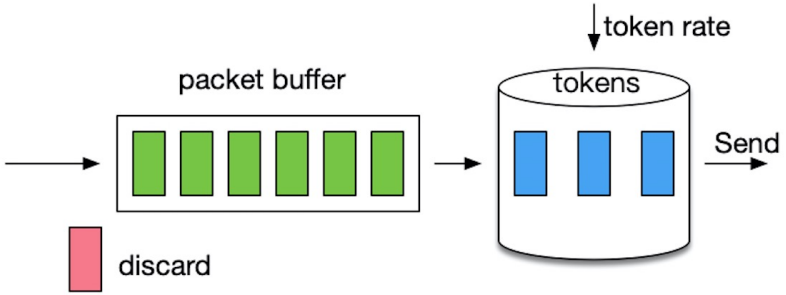
Key Idea

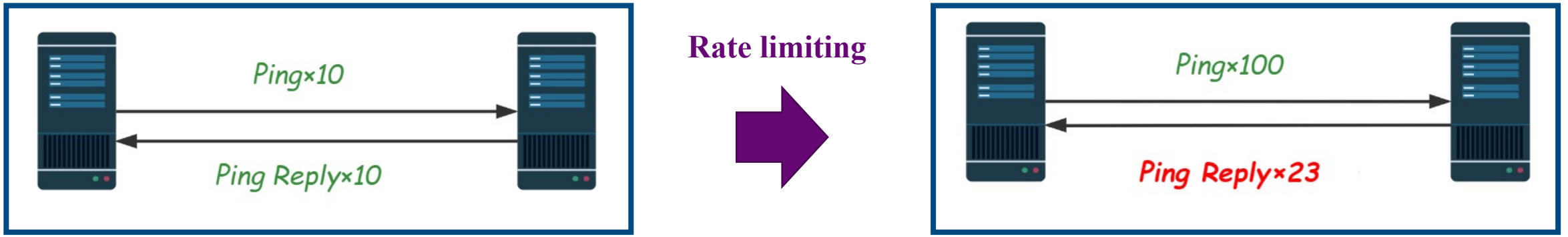
Send ICMPv6 packets with forged source address to the target network, and use the rate limiting mechanism of ICMPv6 as an observer to check whether the spoofed packets are received.

- If fewer ICMPv6 response is received, the target network allows to receive packets with forged source IP address.

ICMPv6 rate limiting

✓As suggested by RFC 4443, in order to limit the bandwidth and forwarding costs incurred by originating ICMPv6 error messages, an IPv6 node MUST limit the rate of ICMPv6 error messages it originates.





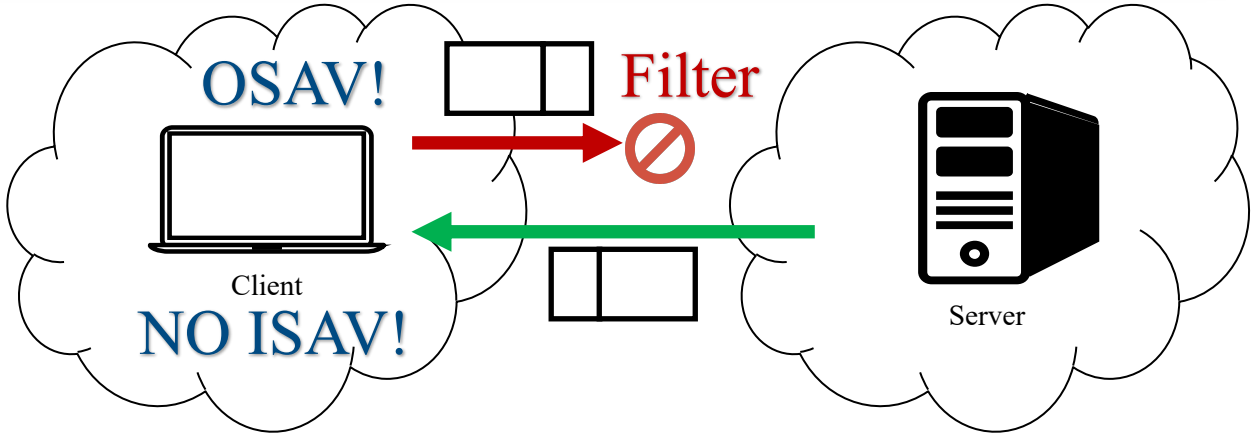
[1] Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. RFC 4443
[2] Long Pan, Jiahai Yang, Lin He, and et. al. Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels. NDSS'23

Baseline: Client-based Measurement

Key Idea

Deploy the client in the target network, and then send packets with forged source address between the client and the controlled server.

- If the spoofed packets sent from the client can be received by the server, then OSAV is not deployed in the target network. Otherwise, OSAV is deployed.
- If the spoofed packets sent from the server can be received by the client, then ISAV is not deployed in the target network. Otherwise, ISAV is deployed.



Measurement client download

File name	Operation system	Architecture	Size
savme-windows-amd64.tar.gz	Windows	x86-64	5.41MB
savme-windows-386.tar.gz	Windows	x86	5.44MB
savme-linux-amd64.tar.gz	Linux	x86-64	5.00MB
savme-darwin-arm64.tar.gz	macOS	arm64	4.91MB

SAVME

SAVME For Windows

SAVME For Linux

SAVME For macOS

Summary of Measurement Methods

Method	Direction	IPv4/ IPv6	Spoofable/ Unspoofable	Inconsistent[2]	Volunteer	Requirements for target network
DNS Proxy-based	outbound	IPv4	spoofable	✗	✗	DNS proxy with bad implementation
DNS Resolver-based	inbound	both	both[1]	√	✗	DNS resolver
ICMPv6-based	inbound	IPv6	both	√	✗	Device with ICMPv6 rate limiting
Client-based (e.g., CAIDA Spoofer)	both	both	both	√	√	✗

[1] For closed resolver, only "spoofable" can be identified; For open resolver, both "spoofable" and "unspoofable" can be identified.
[2] Inconsistent means that the results for different IP addresses in the same AS (or prefix) are different.

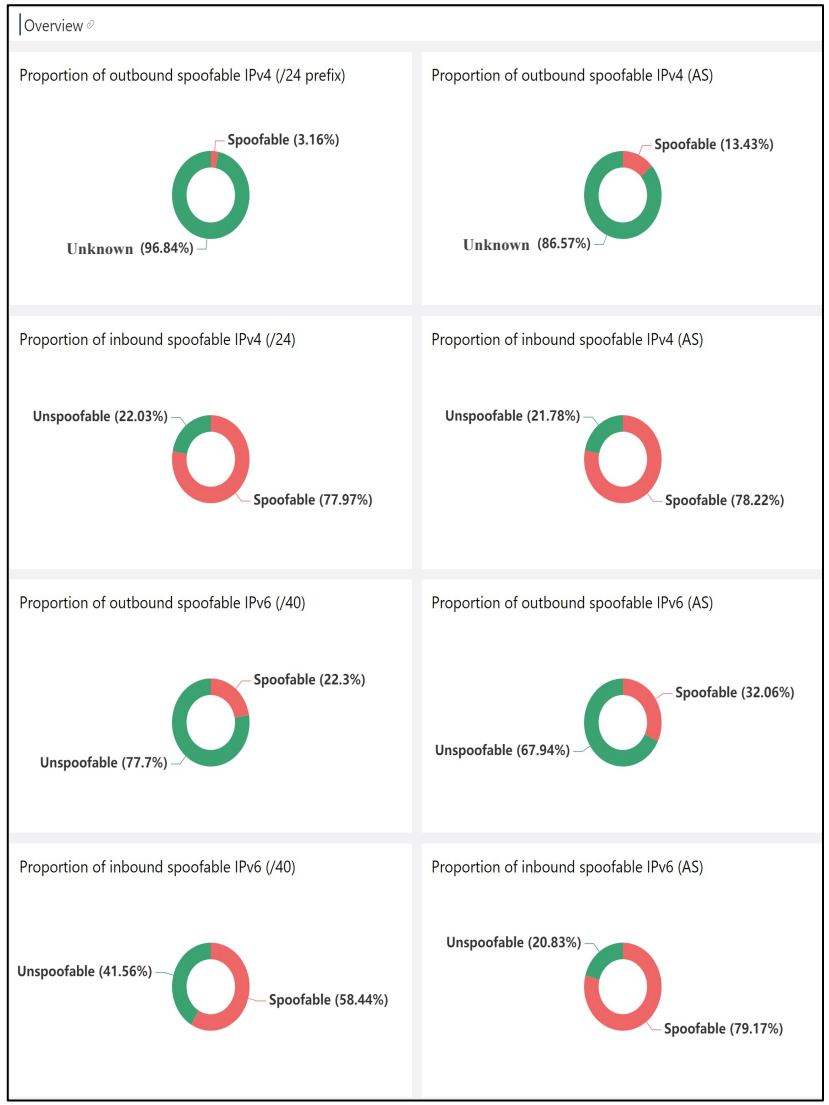
Outline

1. Methods of Large-scale Measurement
2. Analysis of Measurement Results
3. Next Steps

Overview of Measurement Results (1)

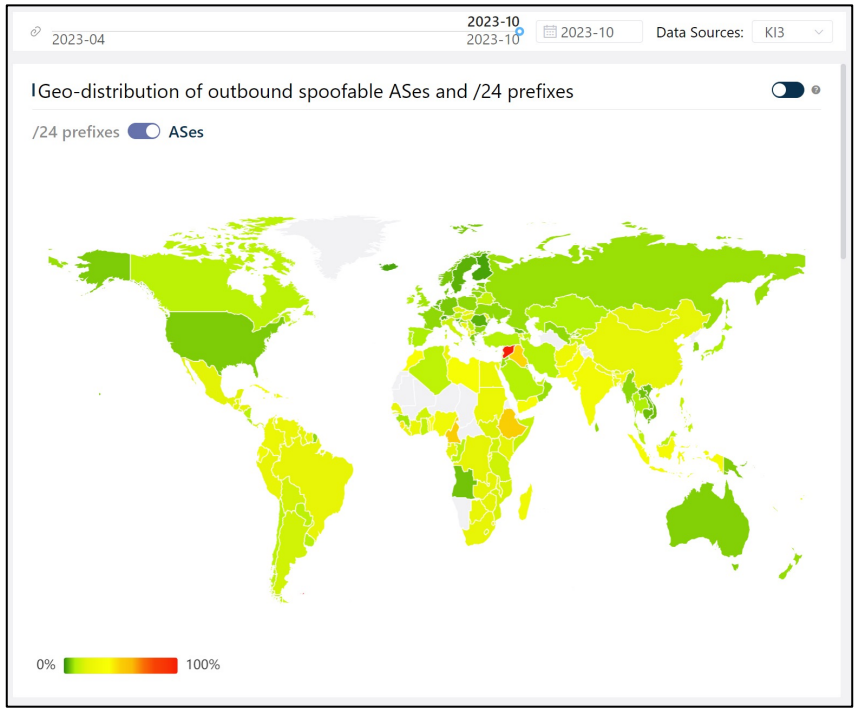
- Publish monthly measurement results of outbound and inbound spoofing for both IPv4 and IPv6
  - ✓ **IPv4 inbound spoofing:** from July 2023 to October 2023
  - ✓ **IPv6 inbound spoofing:** from June 2023 to October 2023
  - ✓ **IPv4 outbound spoofing:** from April 2023 to October 2023
  - ✓ **IPv6 outbound spoofing:** in process
  - ✓ Please visit https://ki3.org.cn for more details
- Proportion of inbound spoofing (~80%) is much higher than outbound (~10%)

> ➢ The ratio of outbound spoofing is calculated by comparing **# of ASes where the destination IP of the DNS request and the source IP of the DNS response are in different /24 prefixes** to **# of ASes that have responding DNS proxies**.
>
> ➢ The ratio of inbound spoofing is calculated by comparing **# of ASes from which our ADNS can receive a DNS request with spoofing IP** to **# of ASes that have responding DNS resolvers**.

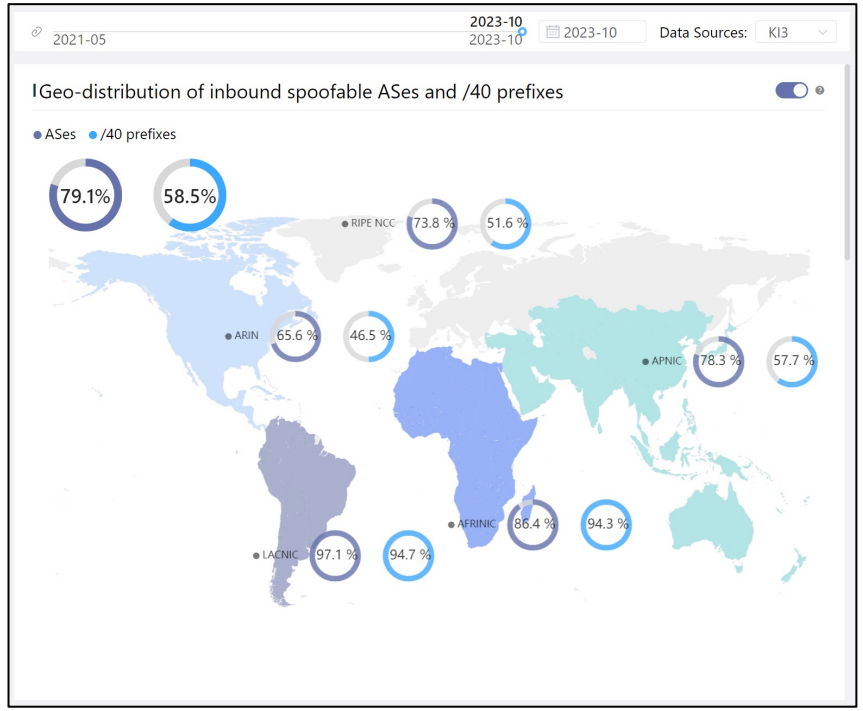


Overview of Measurement Results (2)

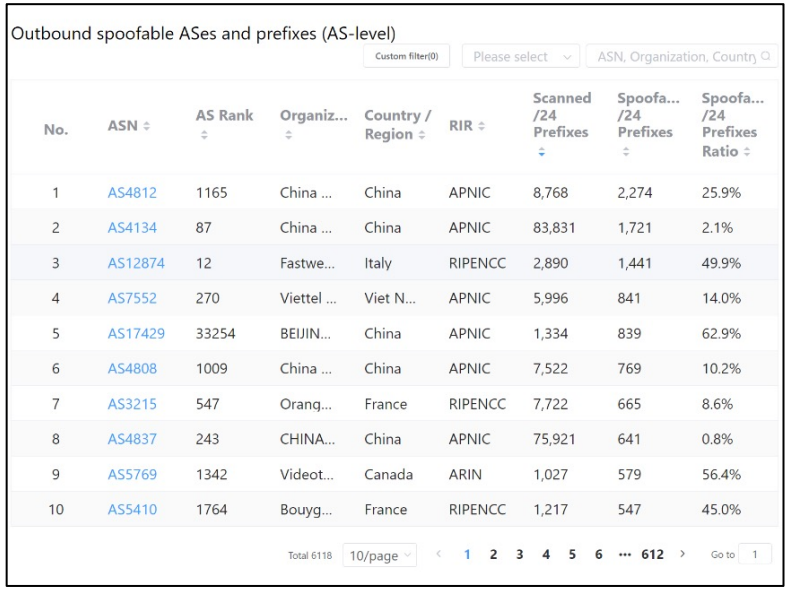
- Show the number of spoofable IP prefixes and ASes in each country/region, and the aggregation results for each RIR
  - ✓Proportion of outbound spoofing ASes in IPv4 is higher in countries in Africa, Asia and South America.
  - ✓Proportion of inbound spoofing ASes in IPv6 is more than 60% in ALL RIRs.



outbound spoofable ASes in IPv4



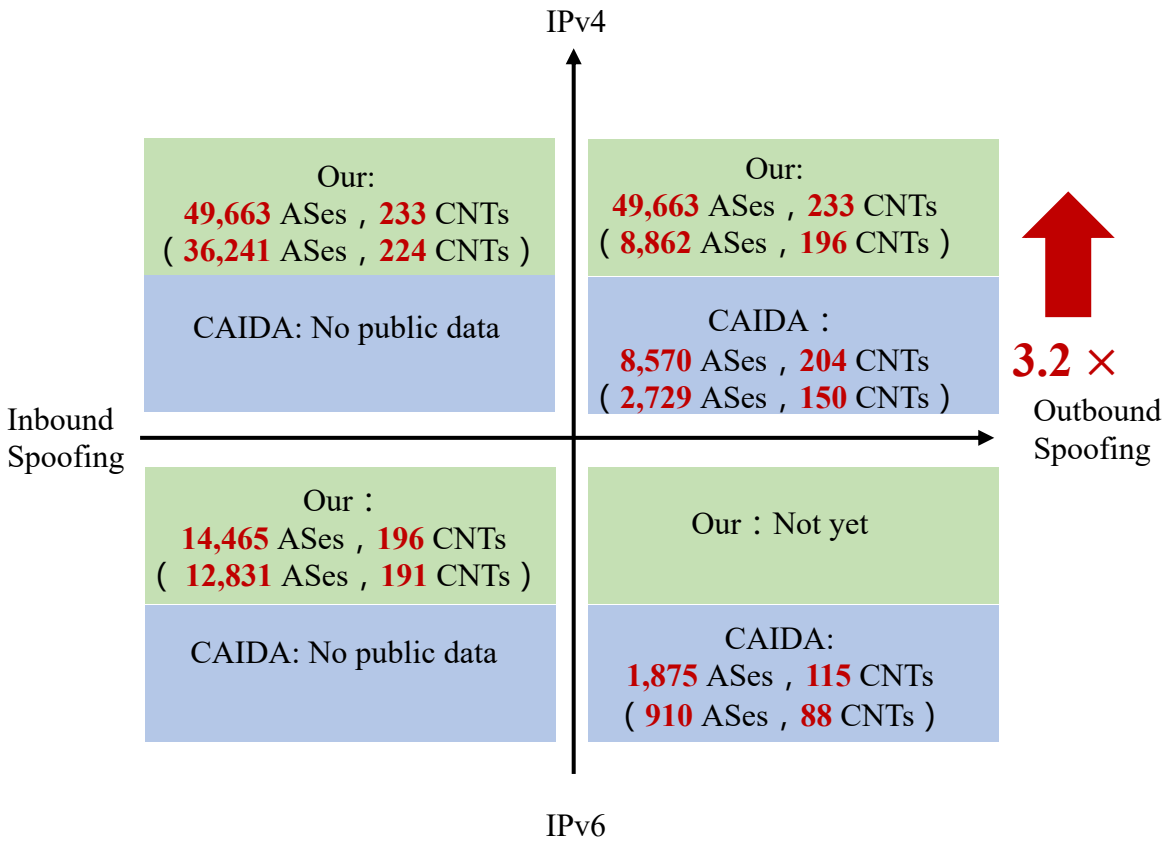
inbound spoofable prefixes and ASes in IPv6


Outbound spoofable ASes and prefixes (AS-level)

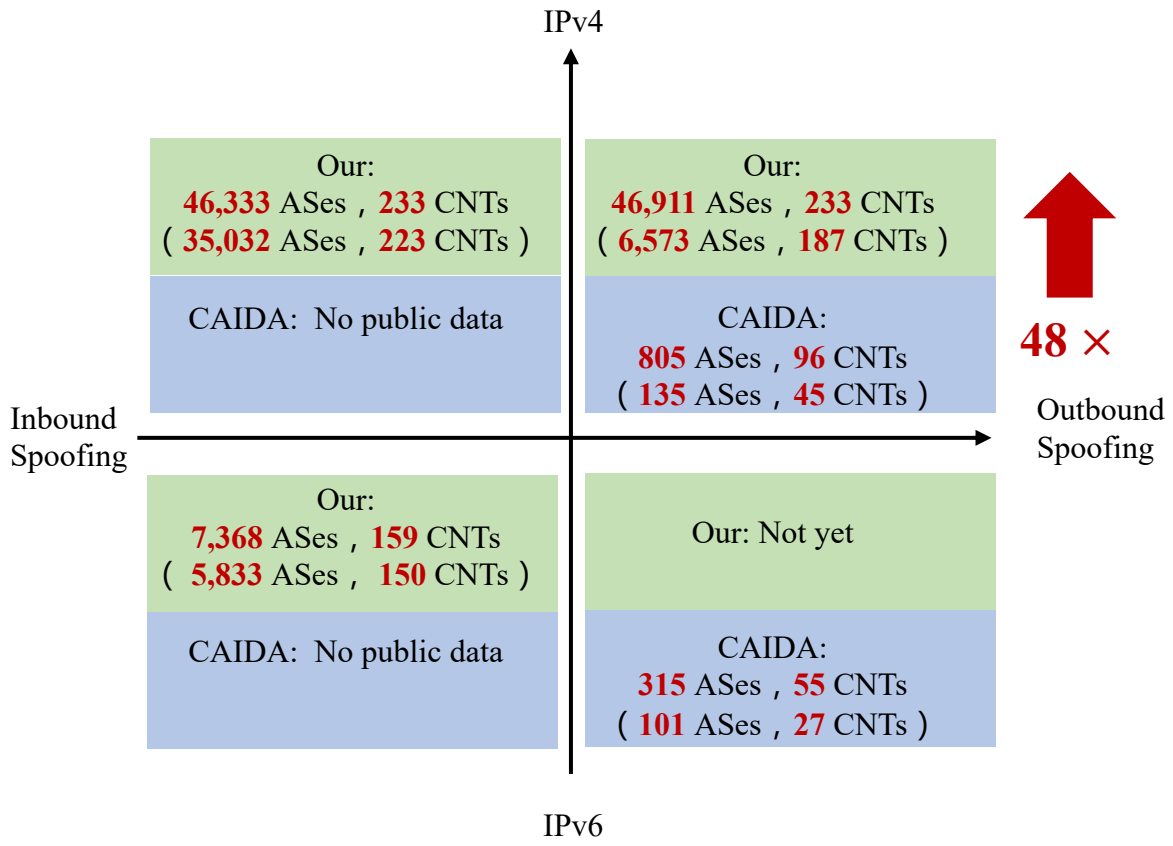
No.	ASN	AS Rank	Organiz...	Country / Region	RIR	Scanned /24 Prefixes	Spoofa... /24 Prefixes	Spoofa... /24 Prefixes Ratio
1	AS4812	1165	China ...	China	APNIC	8,768	2,274	25.9%
2	AS4134	87	China ...	China	APNIC	83,831	1,721	2.1%
3	AS12874	12	Fastwe...	Italy	RIPENCC	2,890	1,441	49.9%
4	AS7552	270	Viettel ...	Viet N...	APNIC	5,996	841	14.0%
5	AS17429	33254	BEIJIN...	China	APNIC	1,334	839	62.9%
6	AS4808	1009	China ...	China	APNIC	7,522	769	10.2%
7	AS3215	547	Orang...	France	RIPENCC	7,722	665	8.6%
8	AS4837	243	CHINA...	China	APNIC	75,921	641	0.8%
9	AS5769	1342	Videot...	Canada	ARIN	1,027	579	56.4%
10	AS5410	1764	Bouyg...	France	RIPENCC	1,217	547	45.0%

List of outbound spoofable ASes in IPv4

Comparison with CAIDA Spoofer (Coverage)



Coverage of total results



Coverage of results in 2023.10

Note 1：The numbers in parentheses are for the networks that allow IP source spoofing

Note 2：Due to ethical concerns, CAIDA does not publish the information of inbound spoofing for a single network. Considering that the client supports both inbound and outbound measurement, the coverage of inbound measurement can refer to its outbound one

Comparison with CAIDA Spoofer (Top 20 countries)

RANK	Our				CAIDA Spoofer			
	Country /Region	# of scanned AS	# of spoofing AS	Spoofing AS (%)	Country /Region	# of scanned AS	# of Spoofing AS	Spoofing AS (%)
1	**Iraq**	119	70	58	Brazil	289	97	33
2	**Pakistan**	170	79	46	Indonesia	18	**6**	33
3	Indonesia	1831	**772**	42	India	28	7	25
4	**Ecuador**	122	42	34	Italy	26	6	23
5	India	1720	579	33	United States	252	53	21
6	**Venezuela**	113	38	33	China	29	6	20
7	**Nigeria**	126	40	31	Netherlands	35	7	20
8	**Colombia**	159	47	29	Mexico	16	3	18
9	**Bangladesh**	879	257	29	Russia	17	3	17
10	Brazil	6768	1810	26	Argentina	18	3	16

RANK	Our				CAIDA Spoofer			
	Country /Region	# of scanned AS	# of Spoofing AS	Spoofing AS (%)	Country /Region	# of scanned AS	# of Spoofing AS	Spoofing AS (%)
11	South Africa	387	101	26	Chile	18	3	16
12	China	889	222	24	Czech Republic	12	2	16
13	**Slovakia**	155	38	24	Canada	32	5	15
14	Mexico	295	69	23	Japan	14	2	14
15	**Moldova**	123	27	21	South Africa	30	4	13
16	Czech Republic	465	96	20	United Kingdom	61	7	11
17	**Argentina**	804	163	20	Germany	41	4	9
18	**Philippines**	173	33	19	Australia	25	2	8
19	**Hungary**	167	31	18	Spain	13	1	7
20	Italy	749	119	15	Turkey	13	1	7

Note 1: Only the IPv4 outbound spoofing results are compared. Both CAIDA Spoofer and our data are from 2023.06 to 2023.10.

Note 2: In order to reduce the bias caused by few samples, only countries with more than 100 scanned ASes are considered in our data, and more than 10 ASes are considered in CAIDA Spoofer data.

Outline

1. Methods of Large-scale Measurement
2. Analysis of Measurement Results
3. Next Steps

Next Steps

- SAVME client software and its deployment
  - ✓Easy use for client software, such as GUI, one-click for measurement, etc
  - ✓Explore how to deploy SAVME clients through crowdsourcing
  - ✓Collaborators are welcome to join us in promoting the SAVME client, which supports fine-grained spoofing measurement.
    - ✓IPv4 /31 - /0 with step size of 1, IPv6 /127 - /0 with step size of 1
- Explore how to conduct a large-scale measurement for IPv6 outbound spoofing
- Explore the misbehaving DNS proxy in more detail, and differentiate between bad DNS proxy and complicated (but normal) DNS system
- …

Thanks!