universität wien

In the Loop:

A measurement study of persistent routing loops on the IPv4/IPv6 Internet

Markus Maier

21. Februar 2024 @ ATNOG 2024/01

universität wien

Wer bin ich?

Markus Maier

Security & Privacy Forschungsgruppe
Fakultät für Informatik; Universität Wien
https://informatik.univie.ac.at/markus.maier

ERIS - Networks and Critical Infrastructures Security Group
SBA-Research
https://www.sba-research.org/team/markus-maier/

ERIS - Networks and Critical Infrastructure
Was machen wir?

- Netzwerk Messungen
  Dedizierter Scanserver @ Nextlayer (https://aim.sba-research.org)

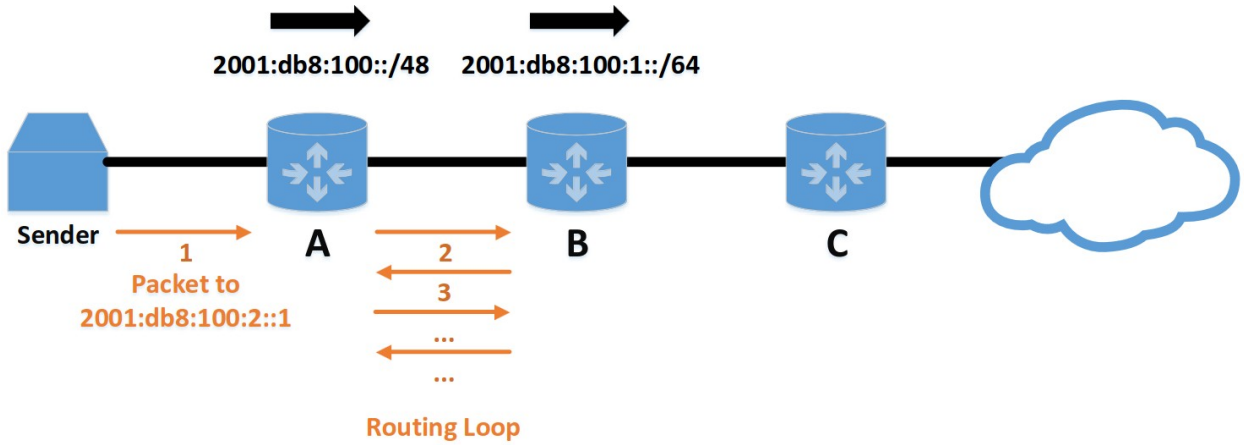
- Mobilfunk Messungen
  Forschungsplattform Mobil Atlas (https://mobileatlas.eu)

- Kritische Infrastruktur (Stromnetz)

- RFC Compliance für Mails (https://www.email-security-scans.org)

Warum Routing Loops?

Terminologie



- Routing Loop:

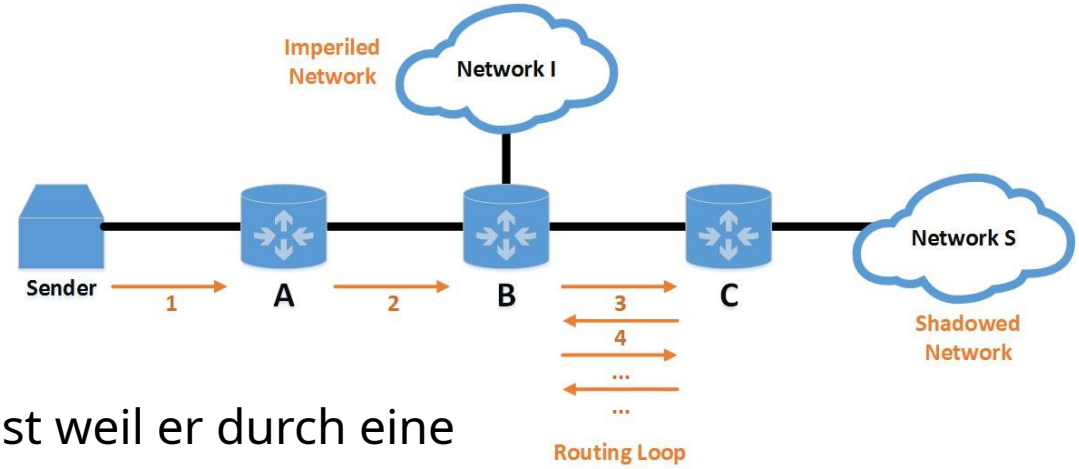
  Ein Paket ist auf dem Weg zu einer Adresse 2001:db8:100:2::1.

  Router A hat eine Route für den Prefix 2001:db8:100::/48 zu Router B.

  Router B behandelt aber nur Prefix 2001:db8:100:1::/64.

  Pakete gehen die Default Gateway zurück → Routing Loop

Terminologie



- Shadowed Network / Prefix:
  Ein Prefix, der nicht erreichbar ist weil er durch eine Routing Loop verdeckt wird.

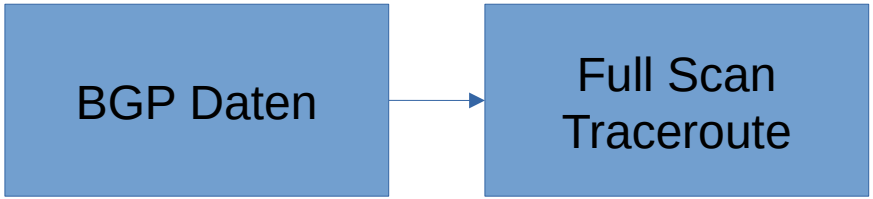
- Imperiled Network / Prefix:
  Ein Prefix mit eine Router einer Routing Loop am Pfad.
  Bei Angriff dieses Routers kann potentiell der Imperiled Prefix ausfallen.

Messaufbau

BGP Daten

CAIDA
Prefix to ASN

Messaufbau

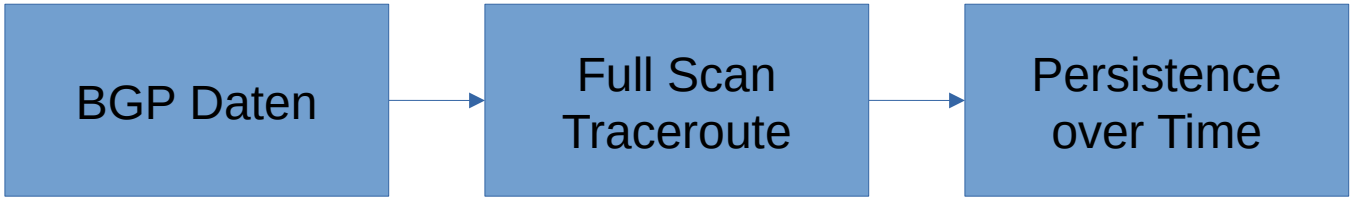


CAIDA
Prefix to ASN

Jedes /24 IPv4
Jedes /48 IPv6

Loop Detection

Messaufbau

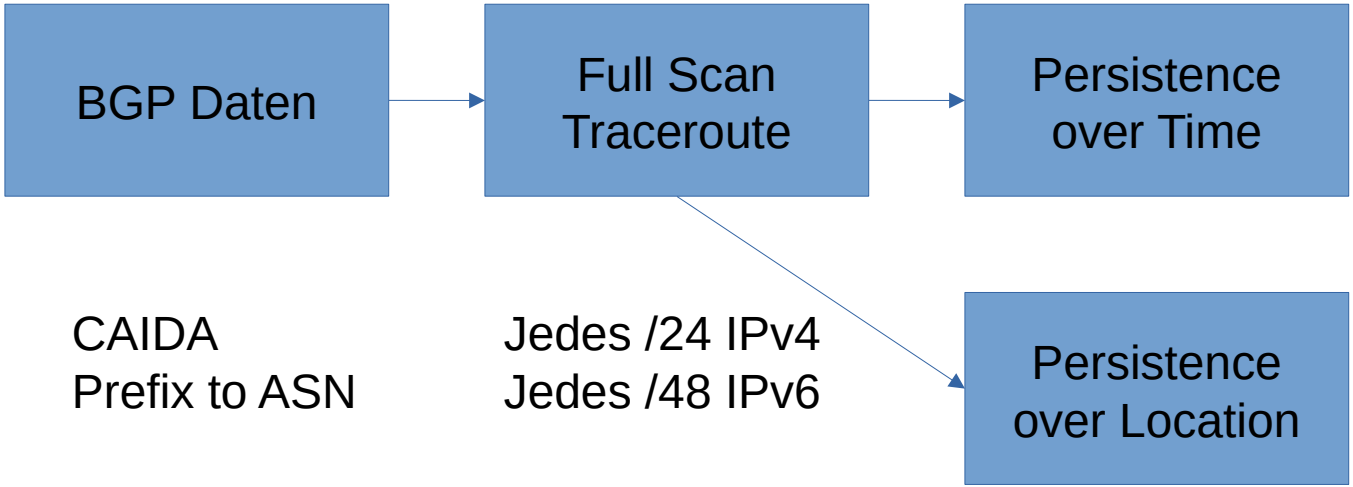


CAIDA
Prefix to ASN

Jedes /24 IPv4
Jedes /48 IPv6

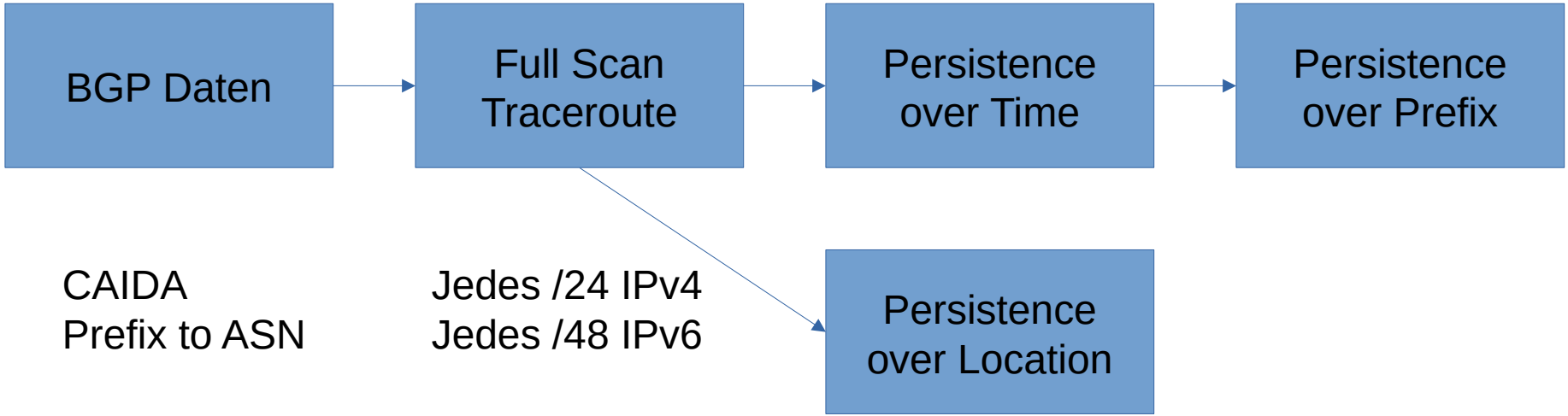
Loop Detection

Messaufbau


BGP Daten
Full Scan
Traceroute
Persistence
over Time
Persistence
over Location
CAIDA
Prefix to ASN
Jedes /24 IPv4
Jedes /48 IPv6
Loop Detection

Messaufbau

Insgesamt:
~3 TB Daten
~26 Tage Messung
Mehrere Tage Berechnung



CAIDA
Prefix to ASN

Jedes /24 IPv4
Jedes /48 IPv6

Loop Detection

Resultate

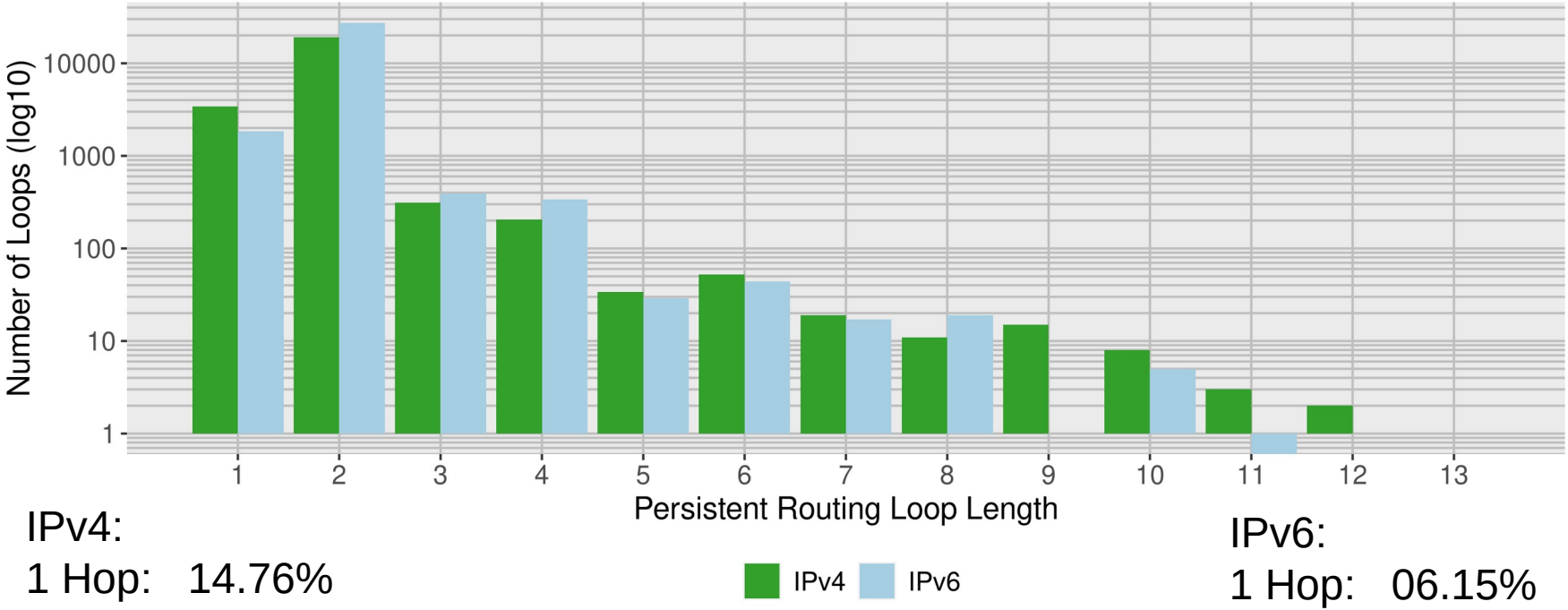
Resultate in Zahlen

Measurement campaign	**Xia et al. (2005)**	**ERIS (2022)**	**ERIS (2022)**
Protocol	IPv4 /24	IPv4 /24	IPv6 /48
Destination prefixes	5,499,518	11,996,245	5,500,185,205
Results			
Routing Loop Candidates	–	34,971	161,284
Persistent Routing Loops	–	23,208	30,090
Involved routers	–	42,035	40,565

Resultate in Zahlen

Measurement campaign	**Xia et al. (2005)**	**ERIS (2022)**	**ERIS (2022)**
Protocol	IPv4 /24	IPv4 /24	IPv6 /48
Destination prefixes	5,499,518	11,996,245	5,500,185,205
Results			
Routing Loop Candidates	–	34,971	161,284
Persistent Routing Loops	–	23,208	30,090
Involved routers	–	42,035	40,565
Shadowed prefixes	135,973	109,178	121,234,603
Imperiled prefixes	42,887	860,991	1,265,045,930

Längen der persistenten Routing Loops



IPv4:
1 Hop: 14.76%
2 Hop: 82.39%
>2 Hop: 02.85%

IPv6:
1 Hop: 06.15%
2 Hop: 91.03%
>2 Hop: 03.65%

universität wien

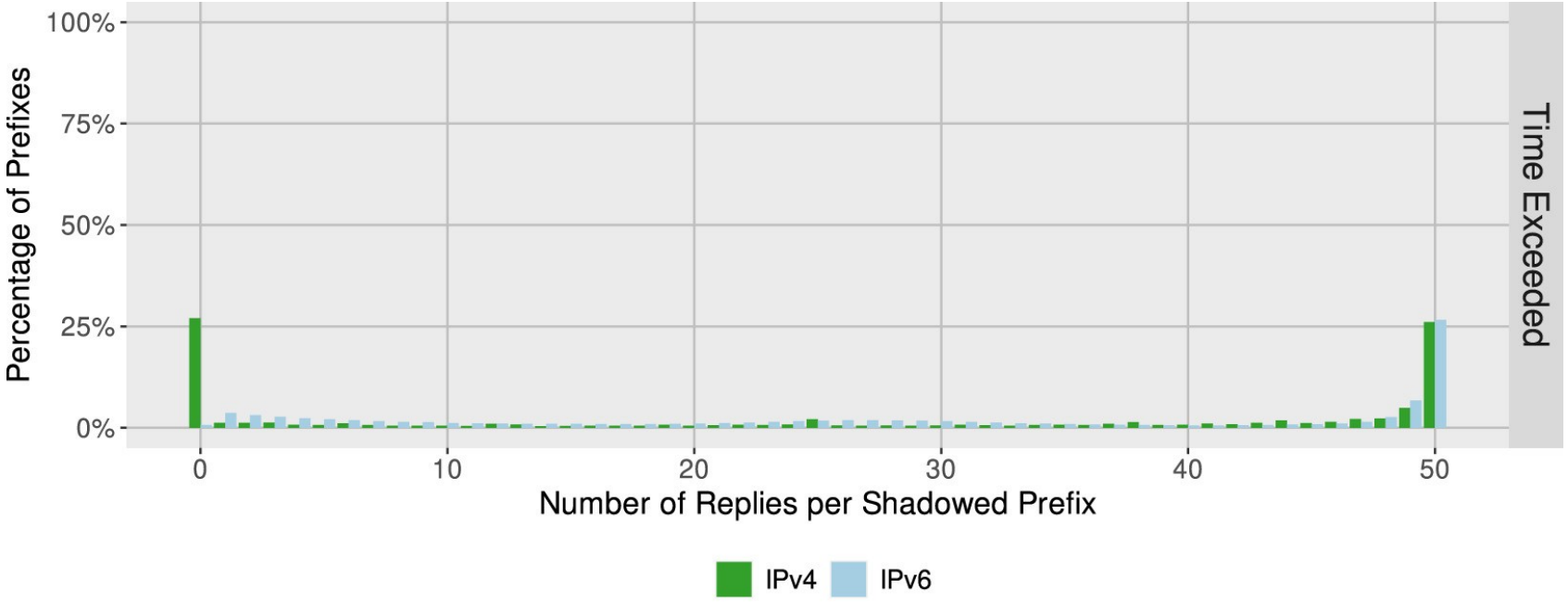
Persistence over Location

Können Loops von überall gesehen werden?

		Observed in		
	Vienna	**Sydney**	**Virginia**	**All locations**
IPv4	23,208	18,542	20,188	17,215
	100%	79.89%	86.99%	74.18%
IPv6	30,090	24,691	26,572	23,274
	100%	82.06%	88.31%	77.35%

Persistence over Prefix

Ist der gesamte Prefix shadowed oder nur die eine Adresse?



AS Attribution

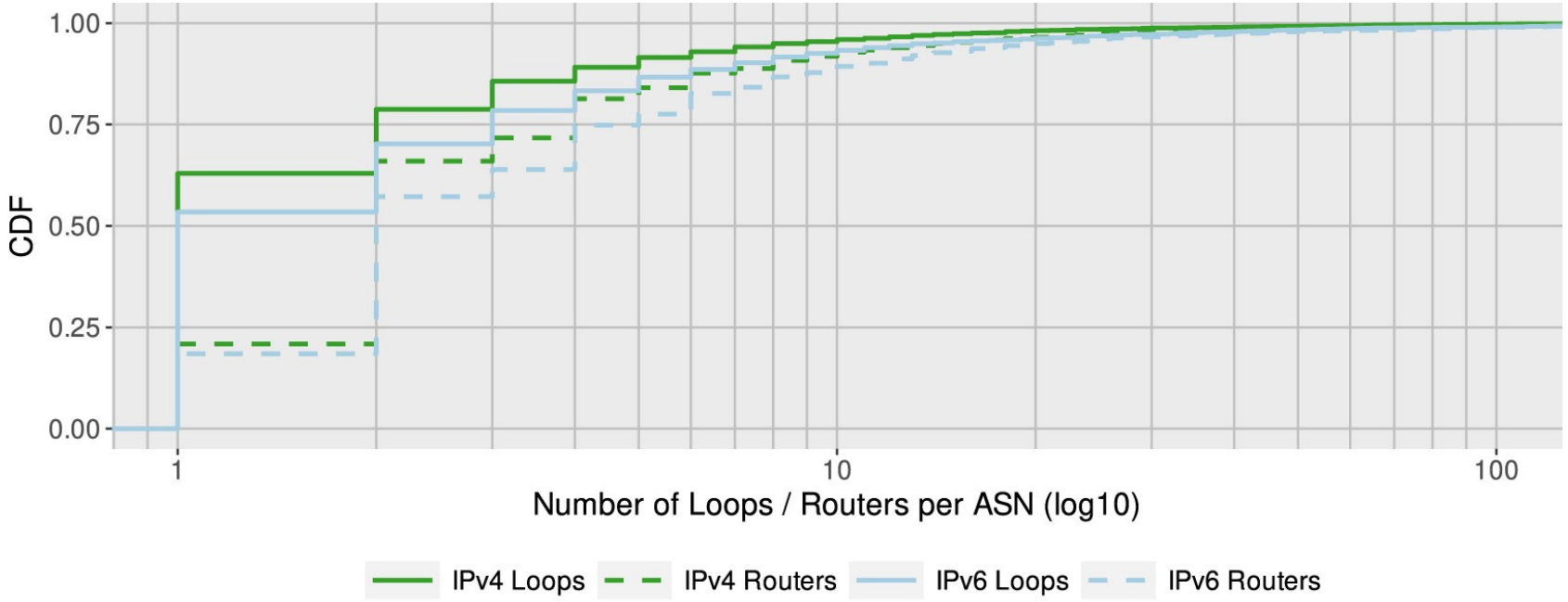
AS Attribution

Wieviele AS sind in einer Loop involviert?

	Xia et al.	IPv4	IPv6
1 AS	94.27%	91.86%	91.06%
(preceding router in same AS)	(67.06%)	(50.54%)	(48.58%)
(preceding router in other AS)	(27.21%)	(41.32%)	(42.48%)
2 ASes	5.35%	7.88%	8.59%
$\geq$ 3 ASes	0.38%	0.26%	0.35%
Total	100%	100%	100%

AS Attribution

Wieviele Loops existieren pro AS?



universität wien

AS Attribution

Wie gefährlich sind Loops für außenstehende AS? (IPv4)

		Imperil			Total
		No ASes	**Invol. ASes**	**Other ASes**	
shadow	Invol. ASes	45.65%	30.52%	6.53%	82.70%
	Other ASes	7.22%	0.59%	9.48%	17.29%
	Total	52.87%	31.11%	16.01%	100.00%

AS Attribution

Wie gefährlich sind Loops für außenstehende AS? (IPv6)

		Imperil			Total
		No ASes	**Invol. ASes**	**Other ASes**	
shadow	Invol. ASes	28.72%	55.29%	6.61%	90.12%
	Other ASes	1.49%	0.08%	8.32%	9.88%
	Total	30.20%	55.37%	14.43%	100.00%

AS Attribution

Netzwerk Klassifikation der AS?

- Zuordnung mittels PeeringDB + ASDB
- IPv4 Loops am häufigsten in NSP Netzwerken (33.12%)
  → eher Core
- IPv6 Loops am häufigsten in Cable/DSL/ISP (44.37%)
  → eher Edge
- uvm.

Key Takeaways

Key Takeaways

- Die meisten Loops sind zwei Hops lang
  → Hauptverdächtiger: fehlende Pull-Up Route

Key Takeaways

- Die meisten Loops sind zwei Hops lang
  → Hauptverdächtiger: fehlende Pull-Up Route
- 76% (IPv4) bzw. 84% (IPv6) der Loops shadown nur eigenes AS
  → geringes Risiko, hohe Eigenverantwortung

Key Takeaways

- Die meisten Loops sind zwei Hops lang
  → Hauptverdächtiger: fehlende Pull-Up Route
- 76% (IPv4) bzw. 84% (IPv6) der Loops shadown maximal eigenes AS
  → geringes Risiko, hohe Eigenverantwortung
- Dennoch gefährden 16% (IPv4) bzw. 14% (IPv6) der Loops
  nicht involvierte AS!

Vielen Dank für die Aufmerksamkeit!

universität wien

Appendix

Links

Link zum Paper
https://www.sciencedirect.com/science/article/pii/S1389128622005345

CAIDA Prefix to ASN (RouteViews)
https://www.caida.org/catalog/datasets/routeviews-prefix2as/

PeeringDB

https://www.peeringdb.com/

ASDB

https://asdb.stanford.edu/

Design der Messungen

- Data Feed von BGP (CAIDA Routeviews)
- Full Scan: ein Traceroute zu einer random Addresse in jedem /24 bzw /48
- Loop Analyse von jedem vollständigem Trace
- Für jede Loop bis zu 10 Zieladdressen auswählen für Persistenz Checks
- Persistence over Time: Nach einem Monat, ausgewählte Addressen tracen
- Persistence over Location: Von zwei weiteren Vantage Points tracen
- Persistence over Prefix: 50 Addressen im Prefix auf TTLe testen

BGP Basis Daten: CAIDA Prefix to ASN (RouteViews)

- BGP Daten als Basis für die Messungen
  Beinhalten ASN Nummer für Prefix -> für später interessant
- Kürzeste Prefixe genommen, überlappende gefiltert.
- Prefixe zwischen /19 und /22 vorbehandelt um Dauer der Messungen zu reduzieren
- 6to4 Prefix gefiltert

Protocol	Prefixes	Prefix Size
IPv4 (Xia.)	5.499.518	/24
IPv4	11.996.245	/24
IPv6	5.500.185.205	/48

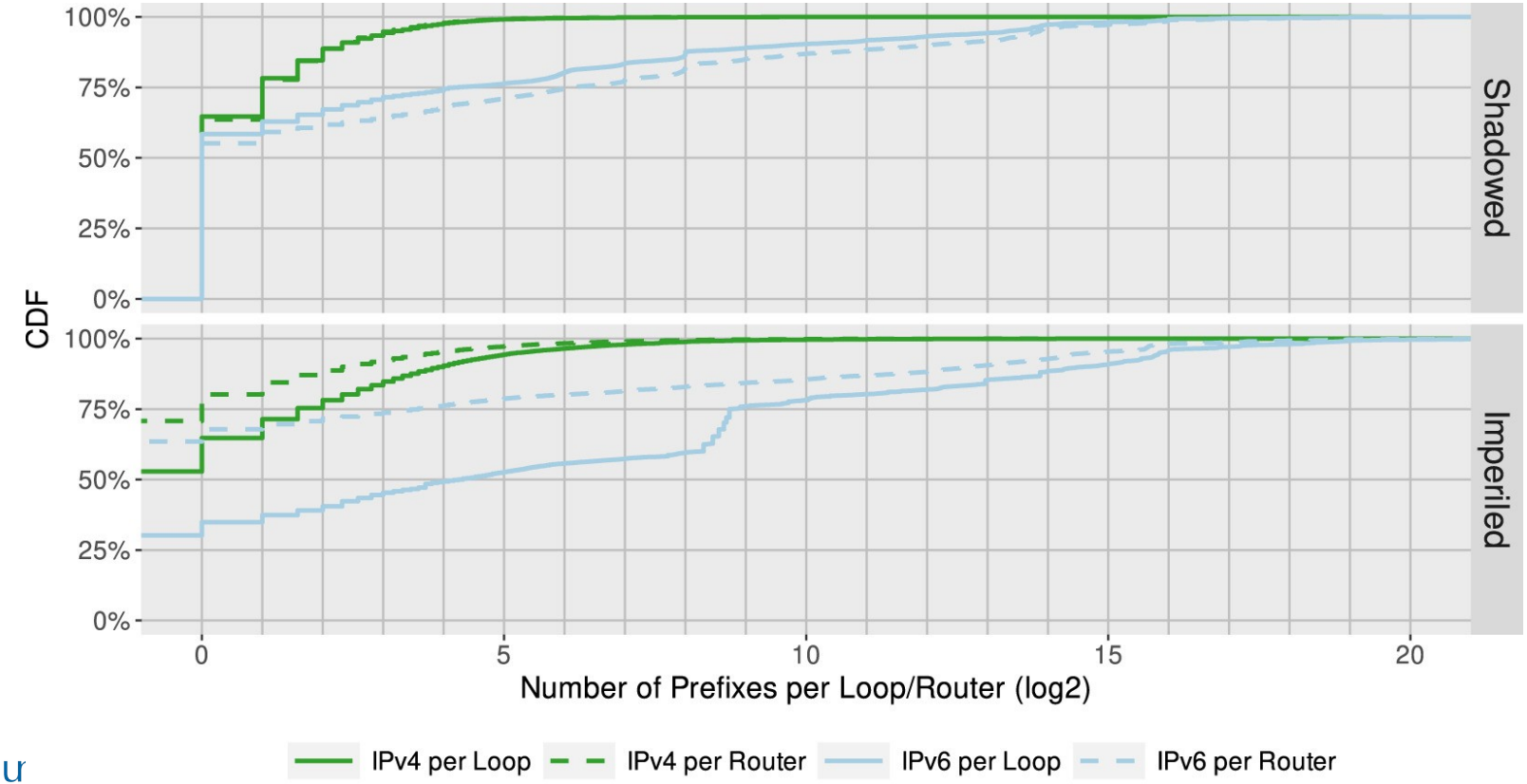
Loop Detection

- Für alle Traceroutes in Full Scan, Persistence over Time / Location
- Wenn nicht alle Hops im Trace vorhanden sind wird rausgefiltert
- Anderer Fehler als TTLe (No Route, Address Unreachable) wird gefiltert
- Von allen Addressen die mehrfach vorkommen, die erste als Loop Start nehmen, Loop Länge ist Anzahl der mehrfach vorkommenden Addressen
- Falls nach der Loop eine neue Addresse gefunden wird, wird rausgefiltert
- IP Addressen der Loop werden sortiert und gehashed um eine ID zu formen

Resultate in Zahlen

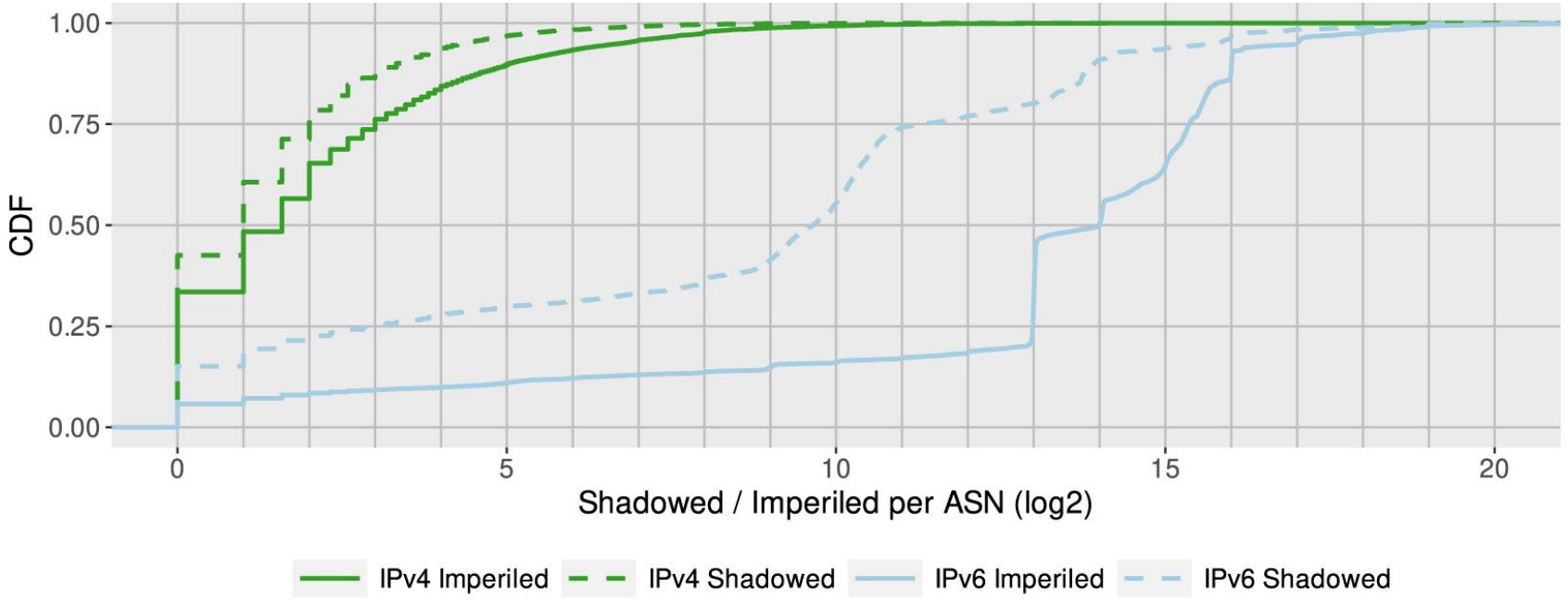
Measurement campaign	**Xia et al. (2005)**	**ERIS (2022)**	**ERIS (2022)**
Protocol	IPv4 /24	IPv4 /24	IPv6 /48
Destination prefixes	5,499,518	11,996,245	5,500,185,205
Results			
Routing Loop Candidates	–	34,971	161,284
Persistent Routing Loops	–	23,208	30,090
Involved routers	–	42,035	40,565
Shadowed prefixes	135,973	109,178	121,234,603
Imperiled prefixes	42,887	860,991	1,265,045,930

Shadowed / Imperiled Pro Loop



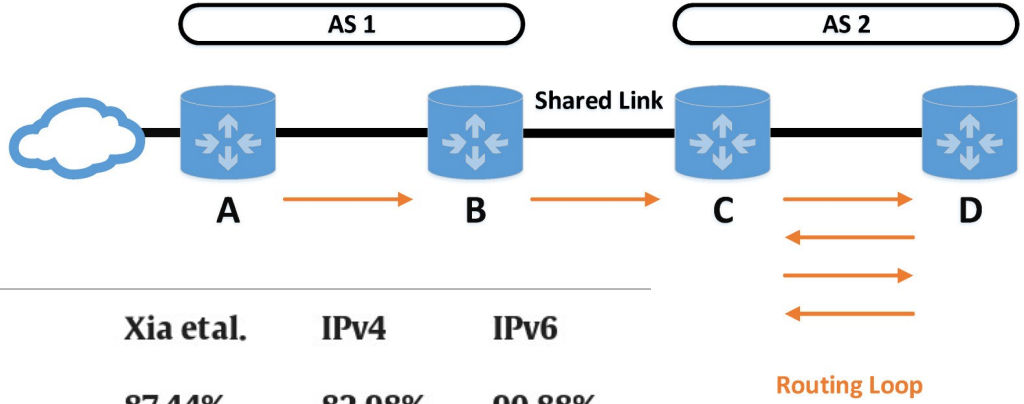
AS Attribution

Wieviele Shadowed / Imperiled Prefixes existieren pro AS?



AS Attribution

Classification Error



	Xia et al.	IPv4	IPv6
Destination AS is involved	**87.44%**	**82.98%**	**90.88%**
(1 address in destination AS)	3.78%	7.17%	8.34%
(≥2 addresses in dest. AS)	83.66%	75.81%	82.53%
No address in destination AS	**12.56%**	**17.02%**	**9.12%**
(Preceding router in dest. AS)	1.47%	0.56%	0.12%
(Preced. router not in dest. AS)	11.09%	16.46%	9.00%
Total	**100.0%**	**100.0%**	**100.0%**