Aggregation & Analysis of IPv6 Prefixes at Internet-Scale

by Philipp Nowak

066.937 Software Engineering & Internet Computing
June 2024

~$ Synopsis

- Empirical measurement with custom software
- **Goal:** Network structure on the IPv6 internet
- **Challenges:**
  - large search space / scale
  - no direct access to targets + no global ground truth
  - measurement artefacts in real-world networks

~# Background

~$ Internet Measurements

- Collect **data** from other **real-world networks**
- **Why?** Empirical evidence (e.g. InfoSec)
- **Feasibility in Practice:**
  - > **IPv4 solved:** exhaustive, minutes-hours
  - > **IPv6 unsolved:** non-exhaustive due to 128-bit search space

~$ Existing methods for IPv6

- None provide results similar to IPv4 methods (yet)
- Various approaches
  - > focus on specific subsets (routers, edge networks)
  - > side channels (DNS, NTP) + address prediction
  - > combine existing sources (hitlist)
  - > **awareness of structure**

~# Goals & Contributions

~$ Synopsis of Research Questions

> Can prefixes be **meaningfully aggregated** with this data?

> Is it possible to predict **more valuable scanning regions** from results of previous rounds in practice? **How well?**

> How can we **store & update** this data in a distributed system?

~$ Novelty

- **Combination** of existing ideas
  - > **feedback** mechanism (reuse results from previous rounds)
  - > more granular measurement of **interesting** areas
  - > prefix **aggregation** using routing **topology** (Hobbit)
  - > focus on **networks**, not single addresses
- **Dynamic** probing focus on **variable-size subnets**

~$ Scientific Methods

- **Literature Review**
- Experiment Design
- Execution of **Experiments**
- **Quantitative & Qualitative Evaluation** of results

~# Proposed Method

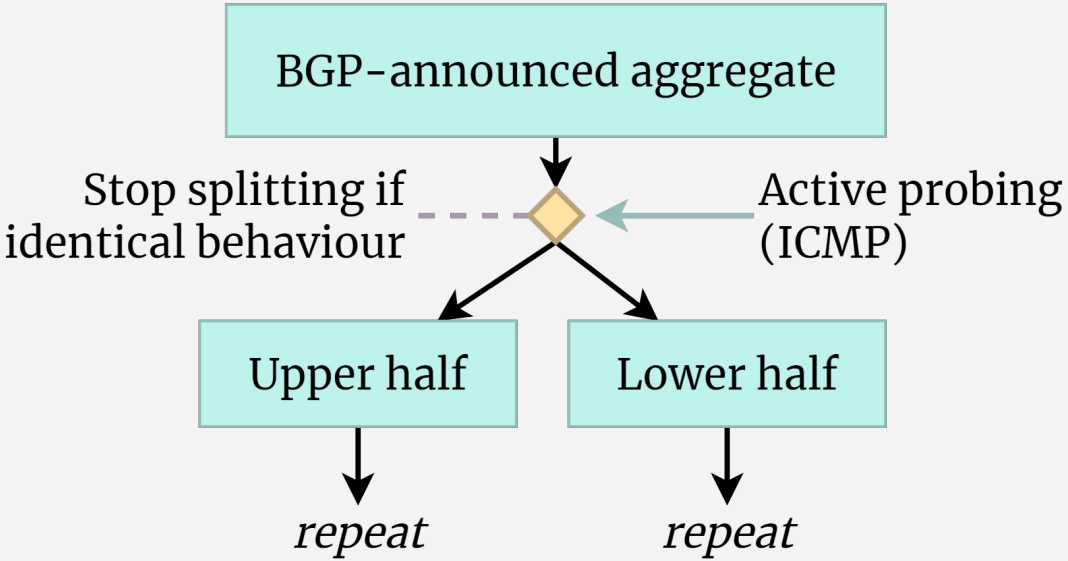
~$ Key Ideas

- Design for **entire internet**
- Operate on **networks** (*“big picture”*)
- **Feedback** from past measurements
- **Prioritise** more interesting regions

~$ Why are regions meaningful?

- Network **hierarchy** organised by address **prefix**
  - e.g. address **2001:db8:cafe**:0::701
- Parameter: **prefix length** (bits) – e.g. /48
  - **cannot** be directly observed from address or public traffic

~$ How do we identify candidate regions?



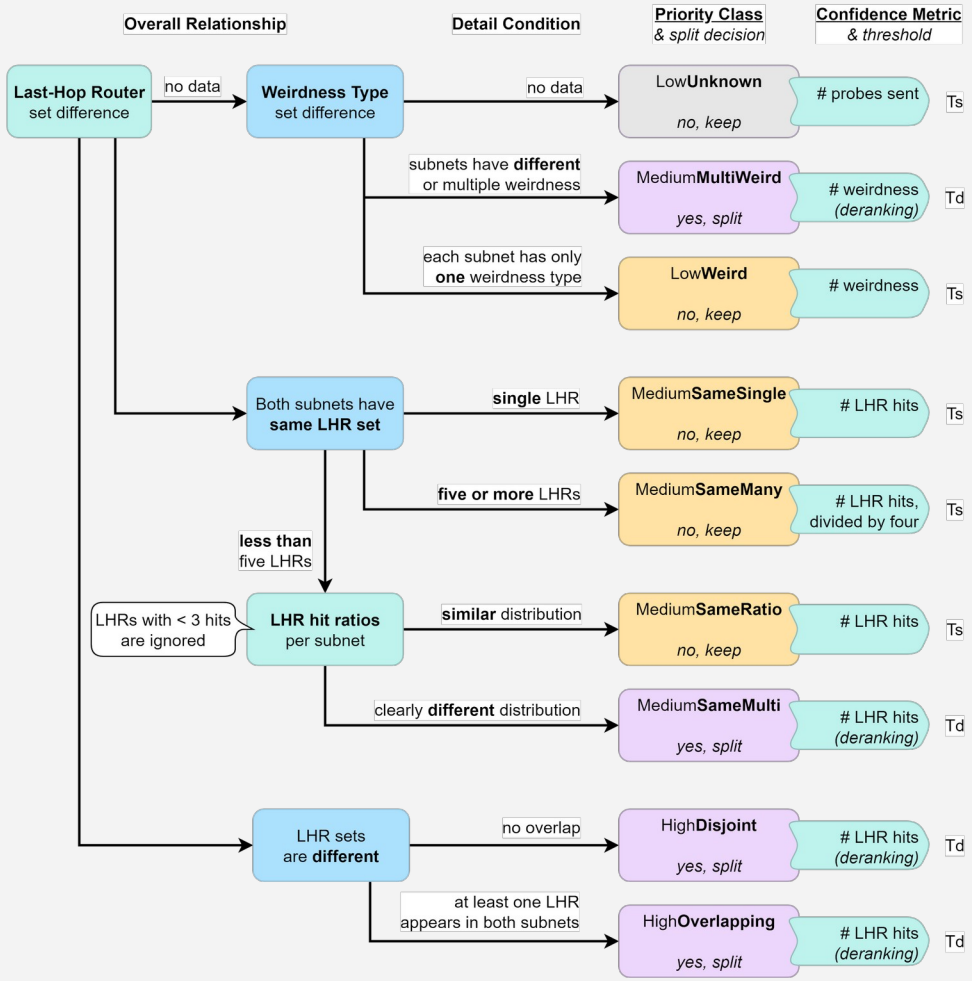
~$ What is identical behaviour?

- Determine **(last) router** responsible for network *[1]*
  - > ICMP error responses (e.g. network unreachable)
  - > **fallback:** Traceroute
- Compare across **halves**
  - > **one router:** trivial
  - > **multiple routers & weird responses:** difficult / heuristics

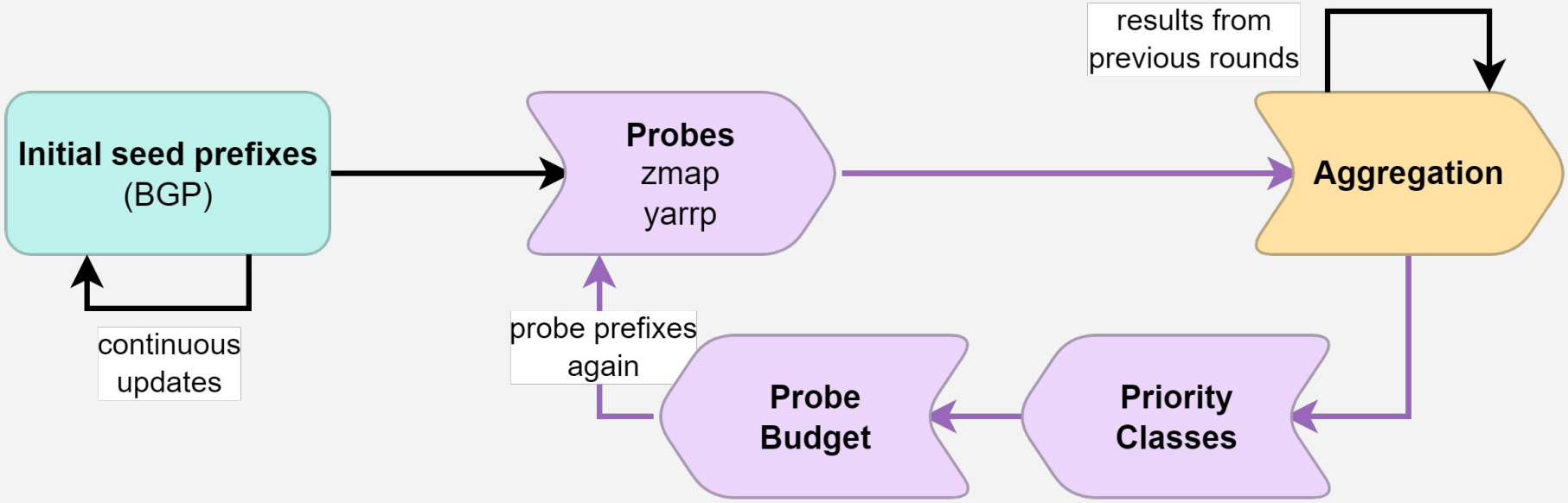
[1] Lee and Spring 2016 (Hobbit)

~$ Split Logic

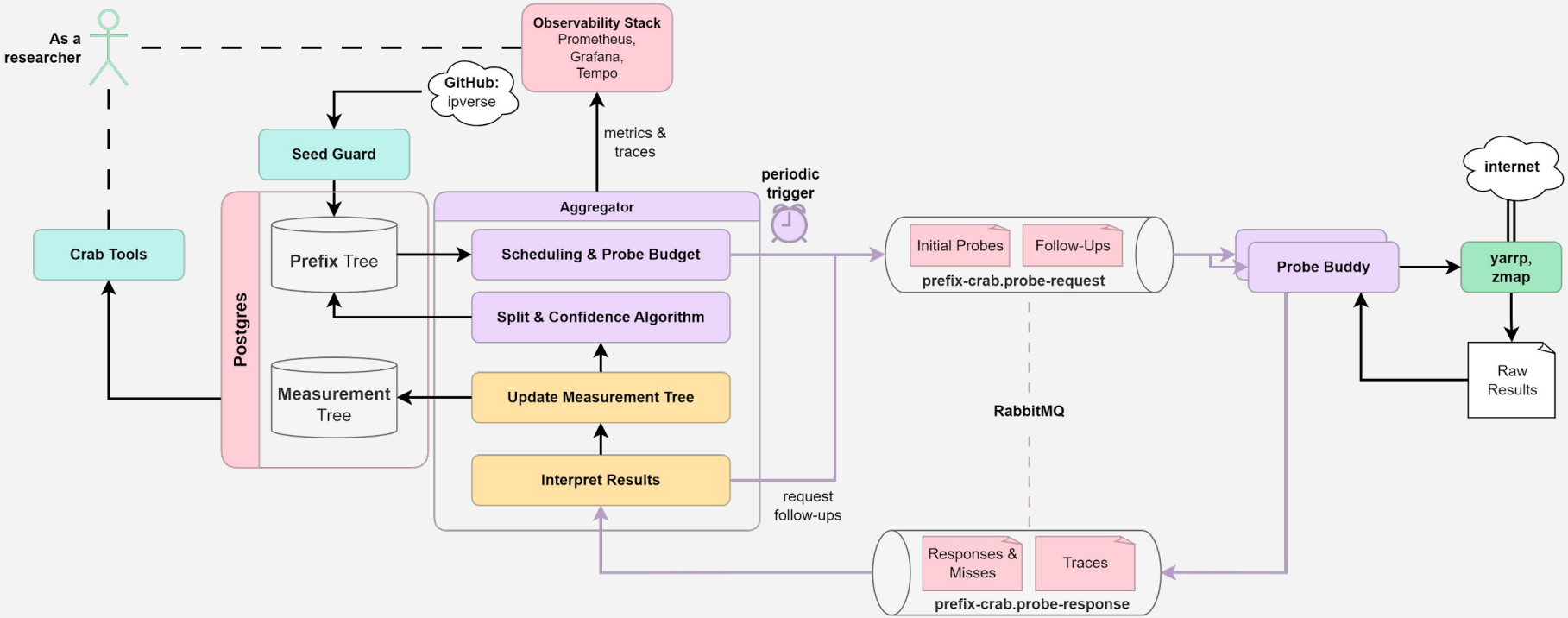
-> Thresholds



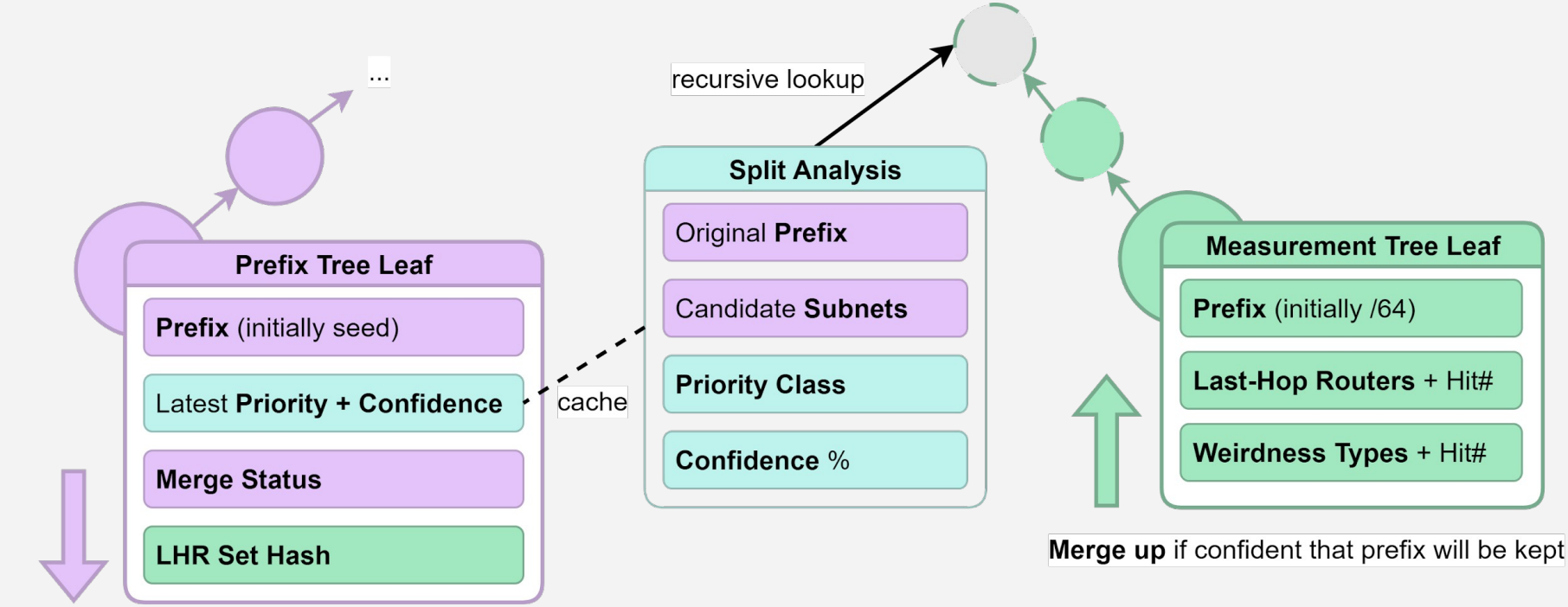
~$ Process Overview



~$ Architecture



~$ Split Decision



~# Does this work?

~$ Measurements

- **U-*:** university network (23 days)
- **AT-10:** most Austrian networks (1.5 months)
- **AT-11:** repeated for evaluation (10 days)

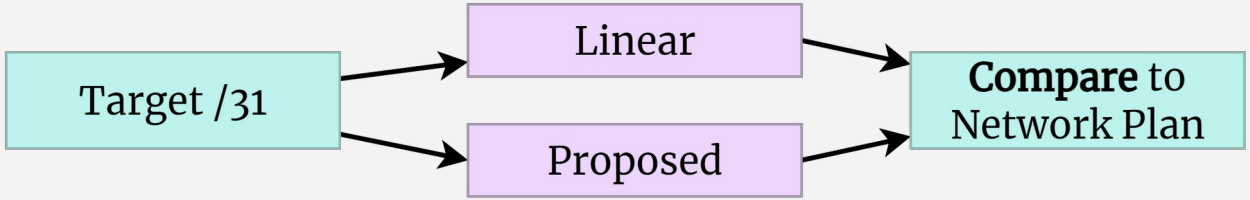
~$ Evaluation Overview

- A) *Discovery* comparison to **linear probing**
- B) **Stability** analysis across AT-* measurements
- C) **Qualitative** metrics interpretation

~$ Evaluation A

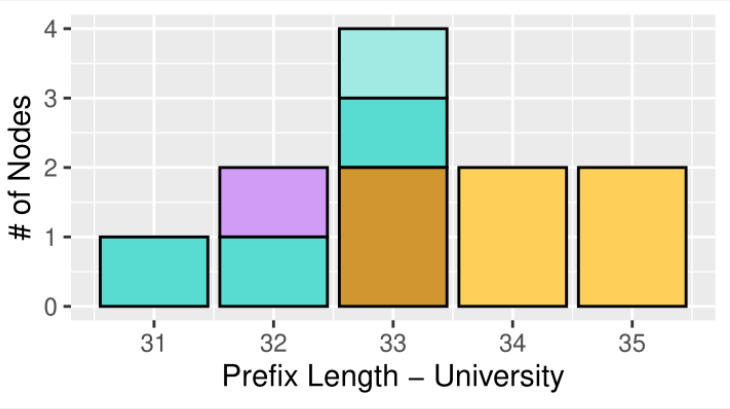
/48 in use?	yes **(linear)**	no **(linear)**
yes **(true)**	5 (+1)	19 (-1)
no **(true)**	0 (±0)	131 048 (±0)

- **Benchmark** against linear
  - > 16 probes to each prefix half (linear: /48)
- **Outcome:** not worse, one additional true positive
  - > **same total probe#** overall
  - > more granular structure found

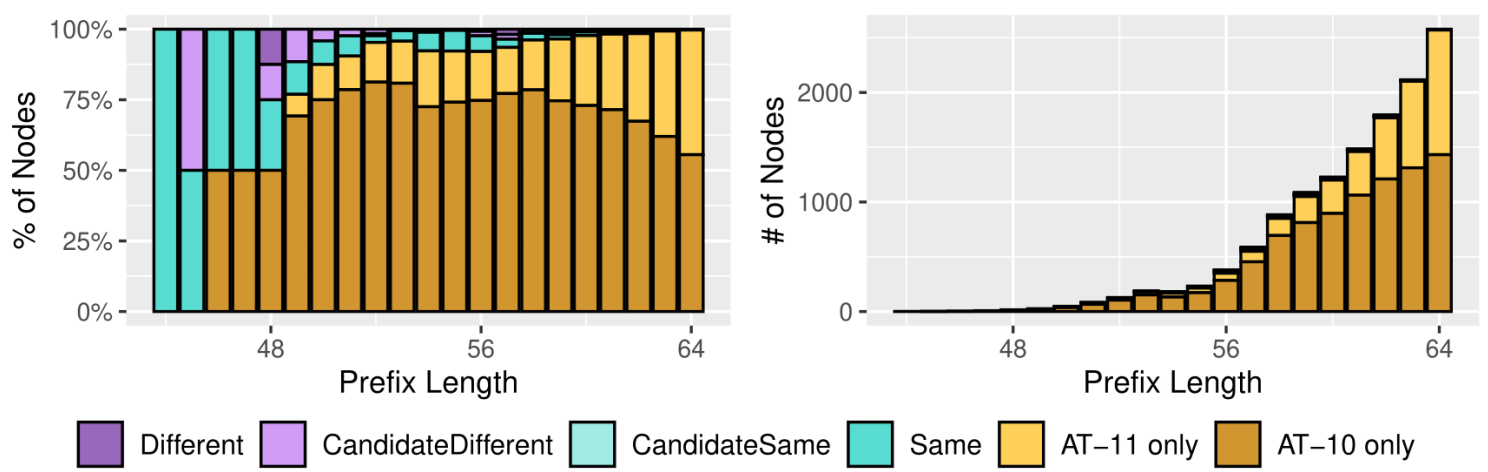


~$ Evaluation Results

- Tree **stability** (AT-10 vs. AT-11)
  - > university

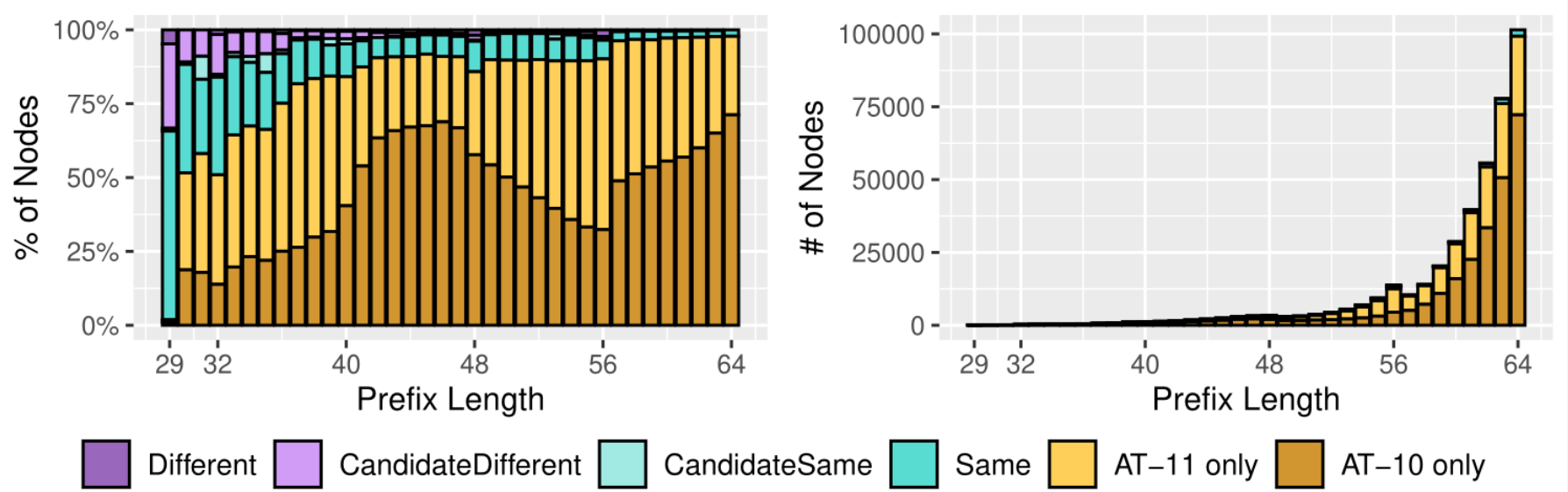


>



~$ Evaluation B (Excerpt)

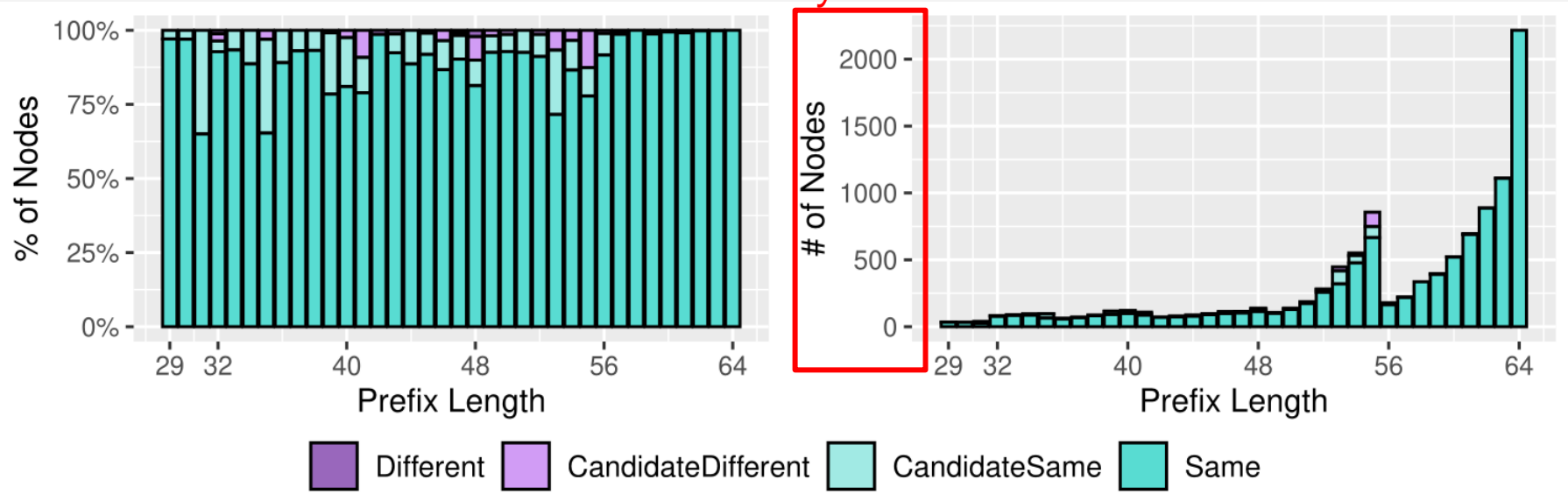
- Tree **stability** (AT-10 vs. AT-11) - overall



~$ Evaluation B (Excerpt)

- Tree **stability** (AT-10 vs. AT-11) *excl.* multiple routers

tiny fraction of data set!

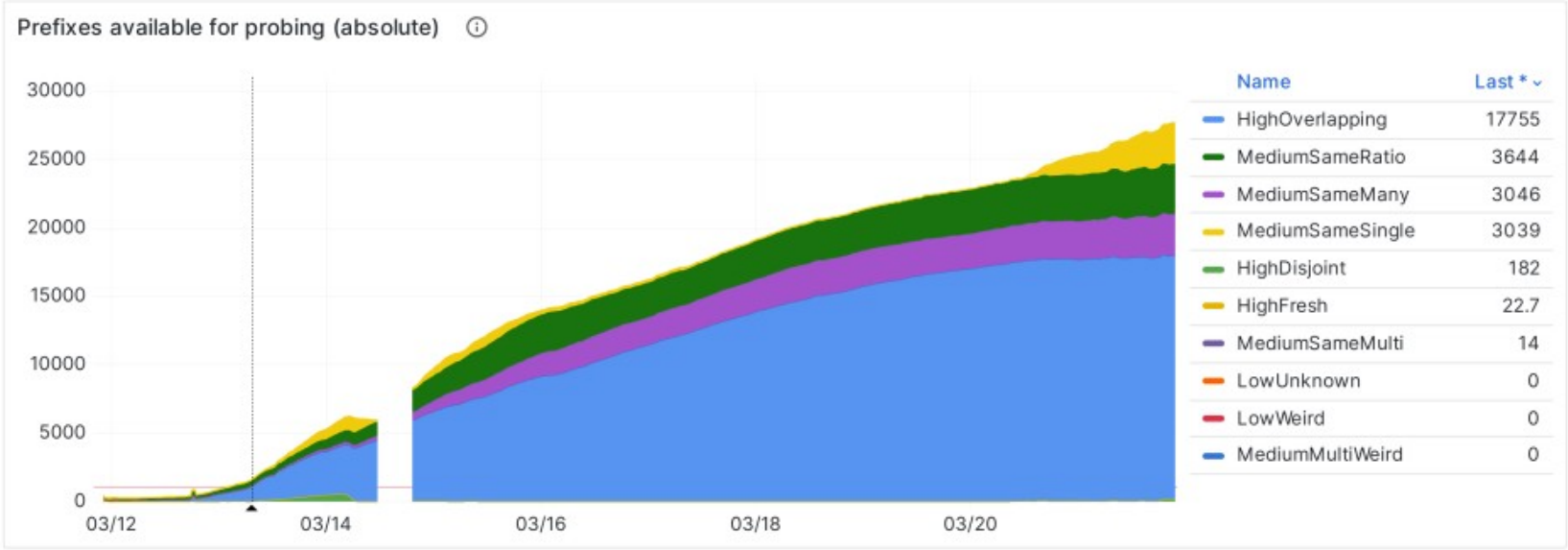


~$ Evaluation C (Excerpt)

- Priority Class vs. # changes over prefix lifetime

Last Priority Class	AT-10				AT-11			
	Nodes	0	1	+	Nodes	0	1	+
High – Overlapping	77%	95	3	1	70%	97	1	0
High – Disjoint	2%	99	0	0	5%	99	0	0
Medium – Same, single	4%	99	1	0	8%	99	0	0
Medium – Same, multiple	0%	19	29	51	0%	56	42	2
Medium – Same, ratio	12%	75	19	6	14%	89	9	2
Medium – Same, many	5%	59	34	7	3%	56	42	2
Medium – Same, multi-weird	0%	0	100	0	0%	0	100	0
Low – Weird	0%	89	8	3	0%	88	12	0
Low – Unknown	0%	100	0	0	–			

~$ Evaluation C (Excerpt)



(a) Number of prefixes available for probing, attributed to priority classes. The horizontal line indicates the per-round prefix budget of `1620` for reference.

~$ Interpretation

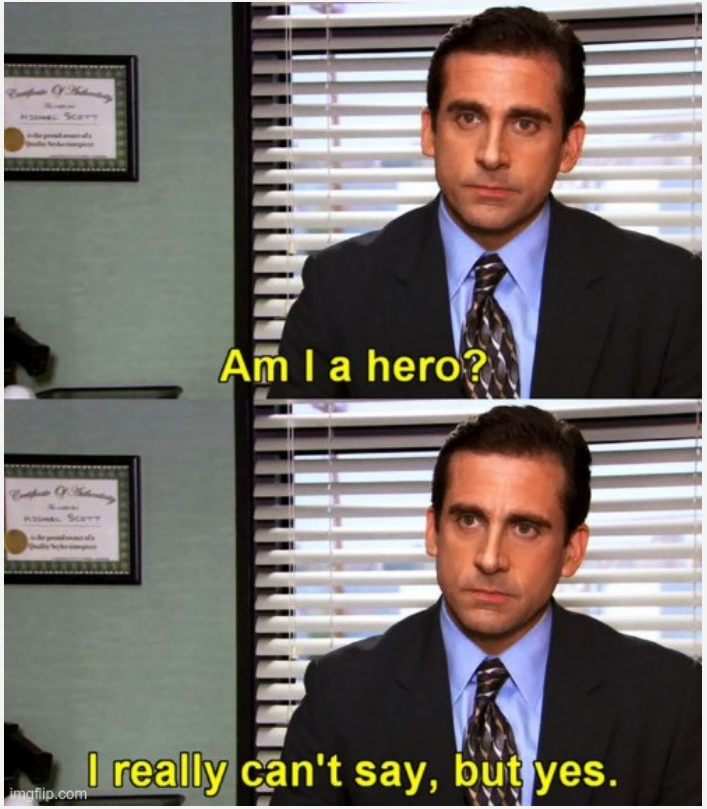
- **Measurement artefacts** & weird setups problematic
  - > some networks degraded mostly to /64s -> large % of budget
- Results at **high granularity** mixed
  - > **limiting** depth (e.g. /56) might allow greater breadth & quality

~$ Interpretation

- Good performance with **single router** on both halves
  - > **not** very commonly observed
- Method **not worse than linear**
  - > clear potential to **reveal more** with same probe budget

~# In Summary

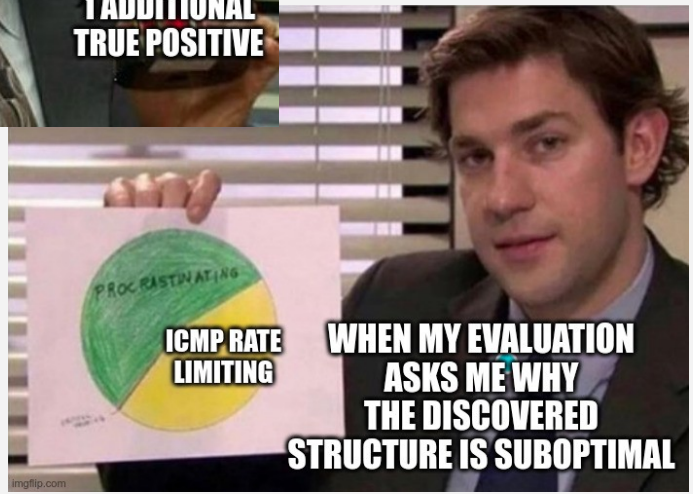
- idea seems promising
- *further work needed*

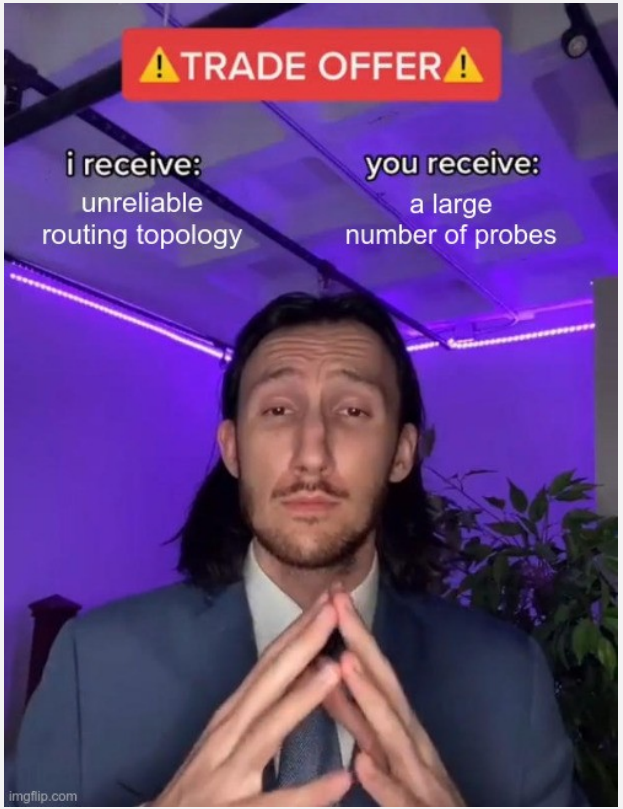


~# Questions?

~# In Summary


1 ADDITIONAL
TRUE POSITIVE
imgflip.com


PROCRASTINATING
ICMP RATE
LIMITING
WHEN MY EVALUATION
ASKS ME WHY
THE DISCOVERED
STRUCTURE IS SUBOPTIMAL
imgflip.com


⚠TRADE OFFER⚠
i receive:
unreliable
routing topology
you receive:
a large
number of probes
imgflip.com

~# In Summary


I DISCOVER STRUCTURE VERY WELL
OK NAME ONE THING YOU'RE IMPROVING
I HAVE ONE ADDITIONAL TRUE POSITIVE FOR A TOTAL OF 6/24
That's on me, I set the bar too low.
imgflip.com


Here are two pictures. One is your METHOD The other is a garbage dump in the Philippines. Can you tell which is which?
This one's the dump.
They're both your METHOD
imgflip.com