A Detailed Measurement View on IPv6 Scanners and Their Adaption to BGP Signals

Isabell Egloff, Raphael Hiesgen, Maynard Koch,
Thomas C. Schmidt, Matthias Wählisch

We want to scan the IP address space

Easy.

2^32 IPv4 addresses scanned in 44 minutes

1,7*10^-10 seconds per address

We want to scan the IP address space

Easy. Really?

2^32 IPv4 addresses scanned in 44 minutes
1,7*10^-10 seconds per address

2^128 IPv6 addresses scanned in ??

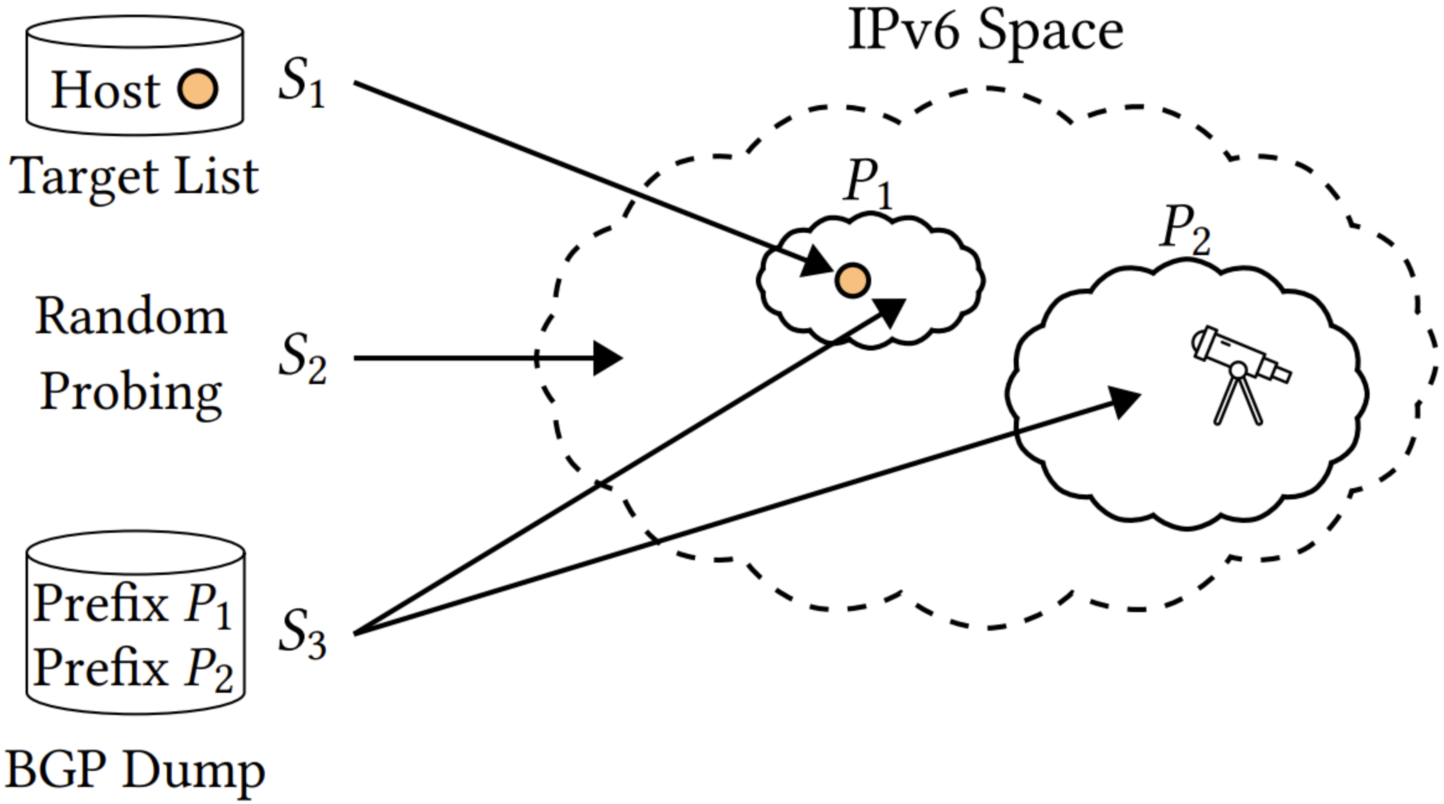
We want to scan the IP address space

Easy. Really?

We will not be able
to scan every IPv6 address!

2^128 IPv6 addresses scanned in ??

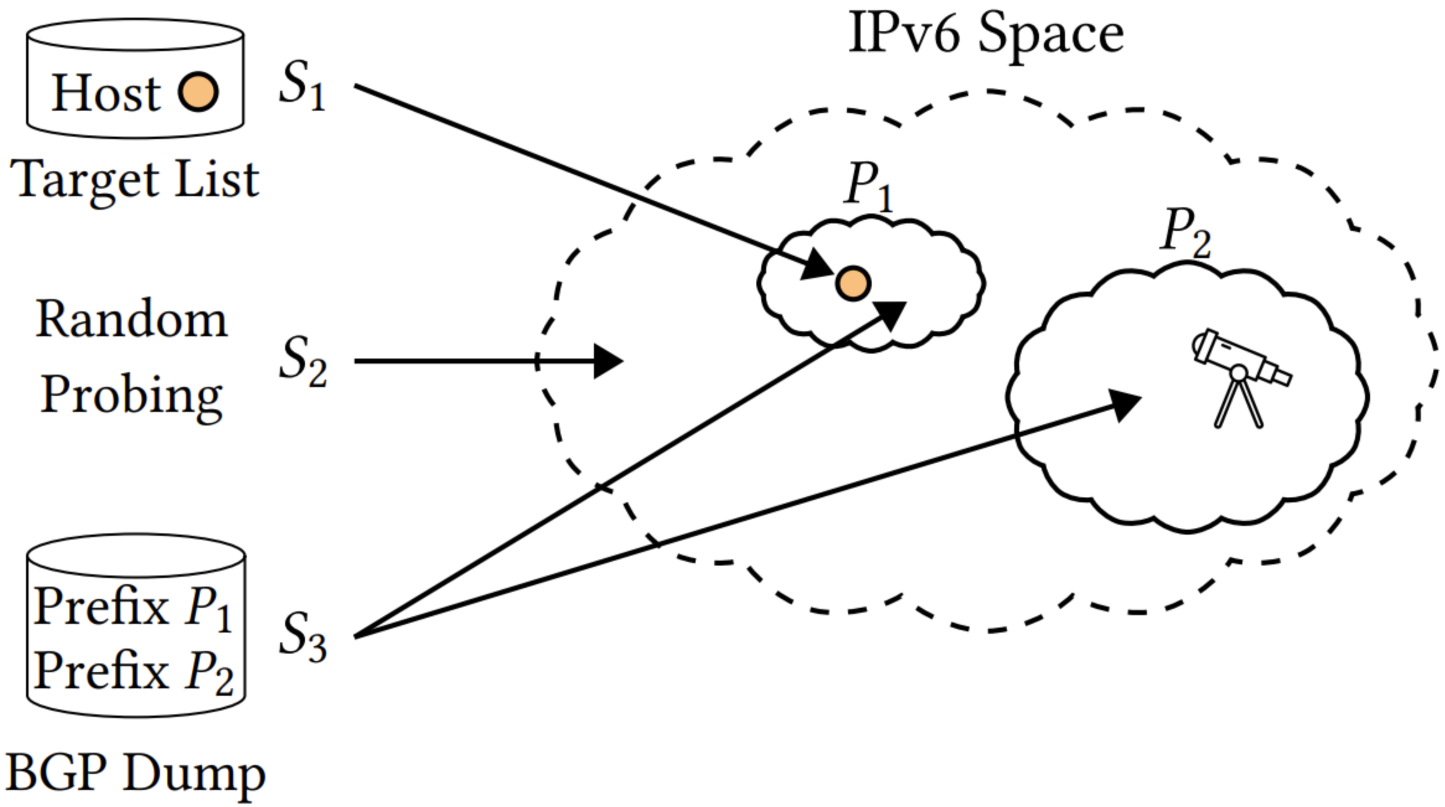
Three approaches to probe IPv6 address space?



Three approaches to probe IPv6 address space?

If we understand IPv6 scanners, we can deploy observation points with more precise focus.

This may reduce costs and increase accuracy.



What is this study about?

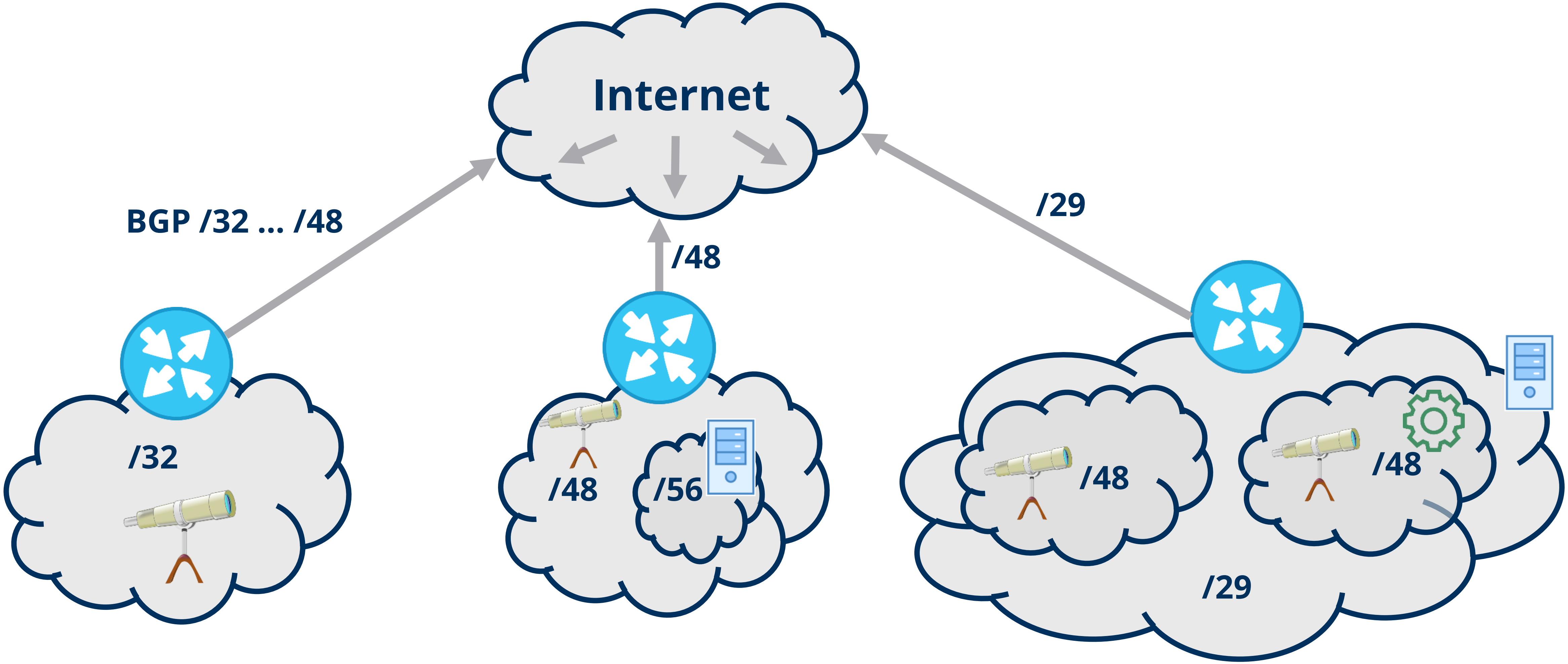
Better understanding of IPv6 scanners.

How should we design IPv6 network telescopes to capture IPv6 scanners?

Which limitations do specific network telescopes have?

Which bias is introduced from the perspective of a telescope?

Our four network telescopes



T1: Passive,
BGP controlled

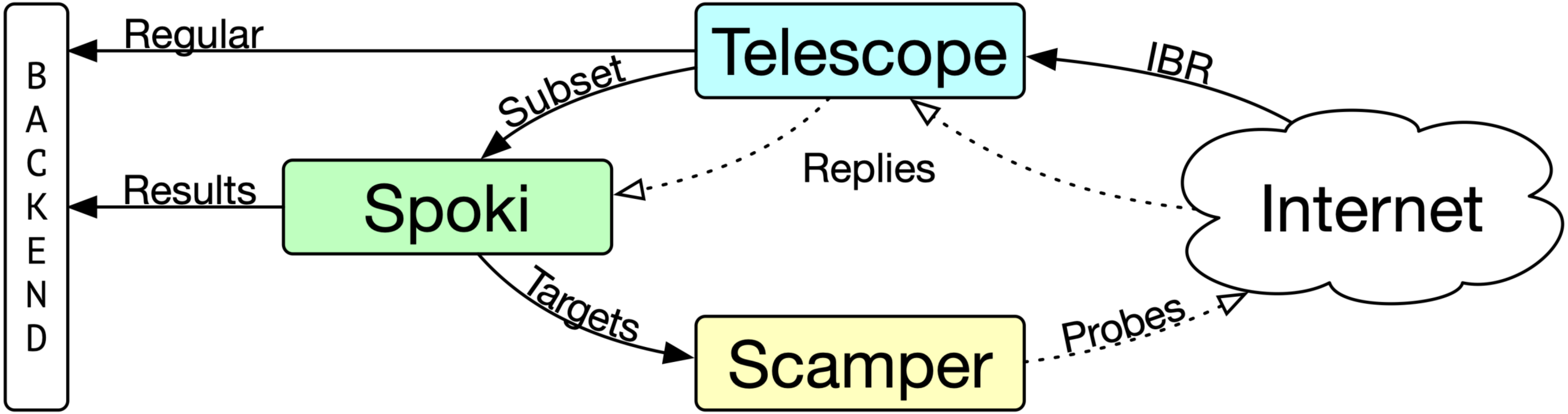
T2: Partially
productive

T3: Silent

T4: Reactive
(TCP)

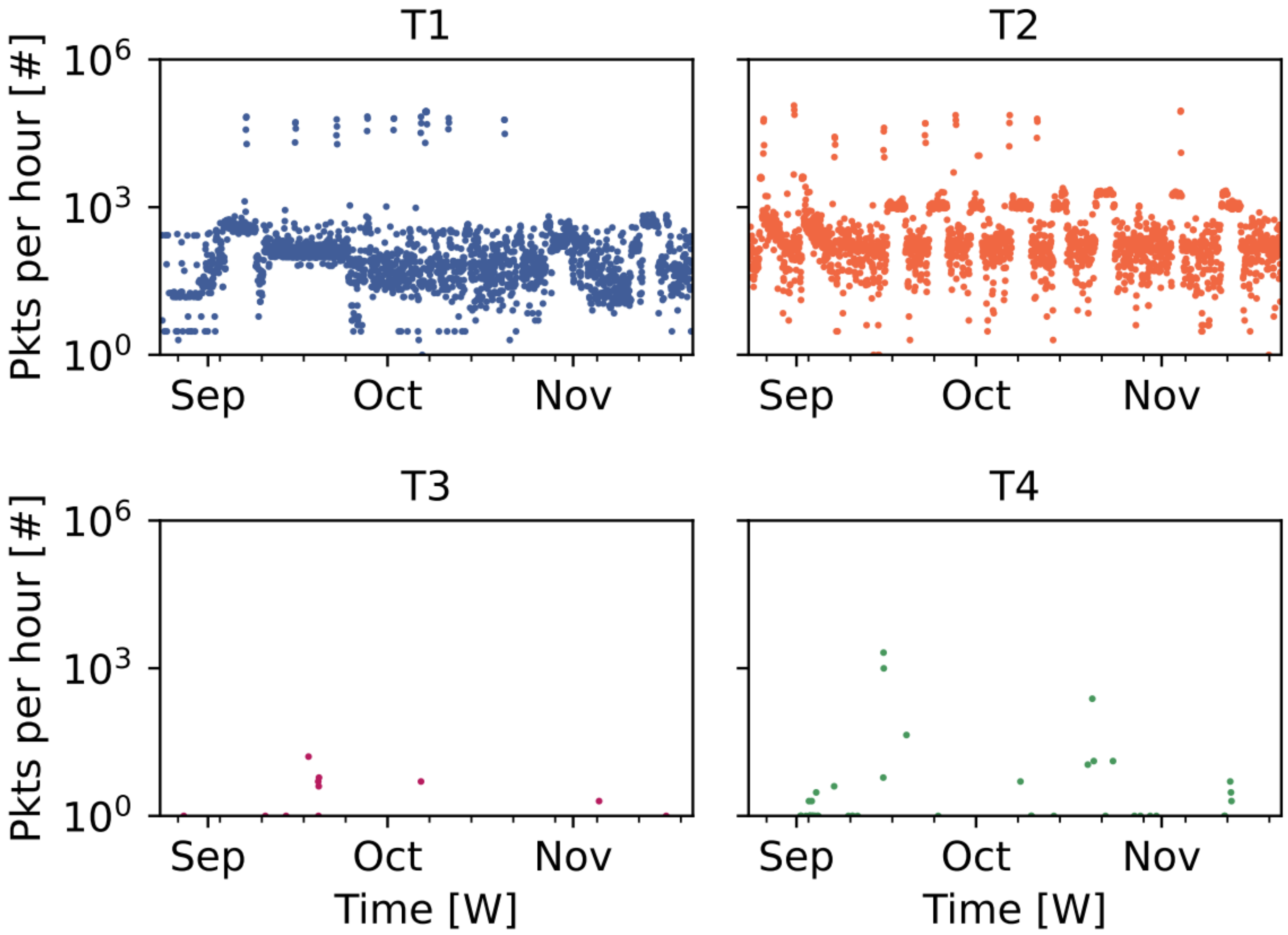
Spoki: Reactive telescope to continue dialog with attacker

- Replies to (stateless two-phase) scanning to explore attack surface
- Asynchronously accepts and matches (2^{nd} phase) connections



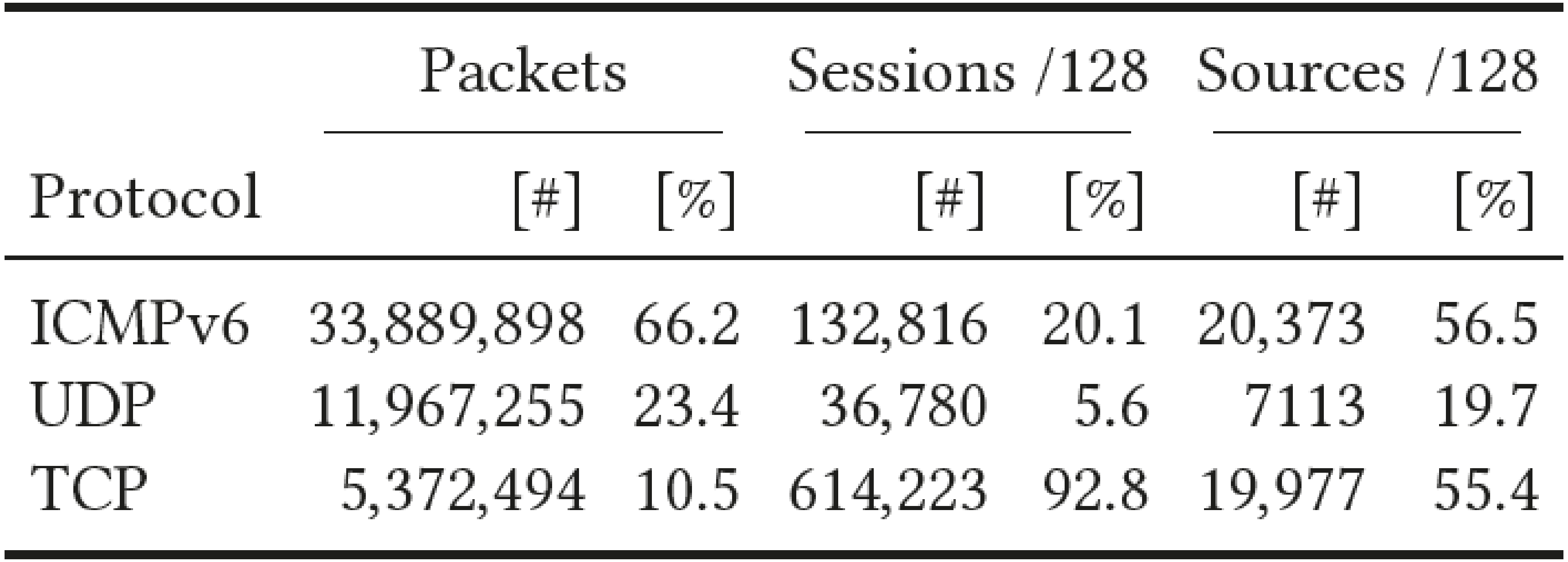
Raphael Hiesgen, Marcin Nawrocki, Alistair King, Alberto Dainotti, Thomas C. Schmidt, Matthias Wählisch,
Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope,
In: *Proc. of 31st USENIX Security Symposium,* pp. 431-448, USENIX Association : Berkeley, CA, USA, August 2022.

Unsolicited traffic across the telescopes during initial observation period of 12 weeks



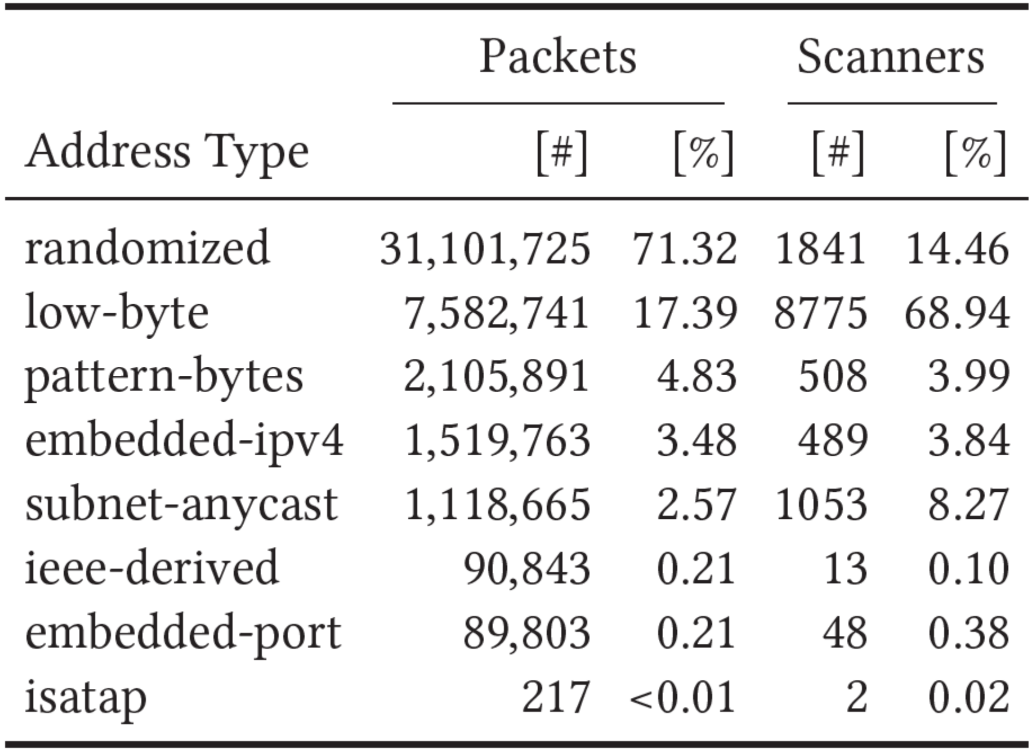
How popular are protocols?

Packets vs. sources vs. sessions

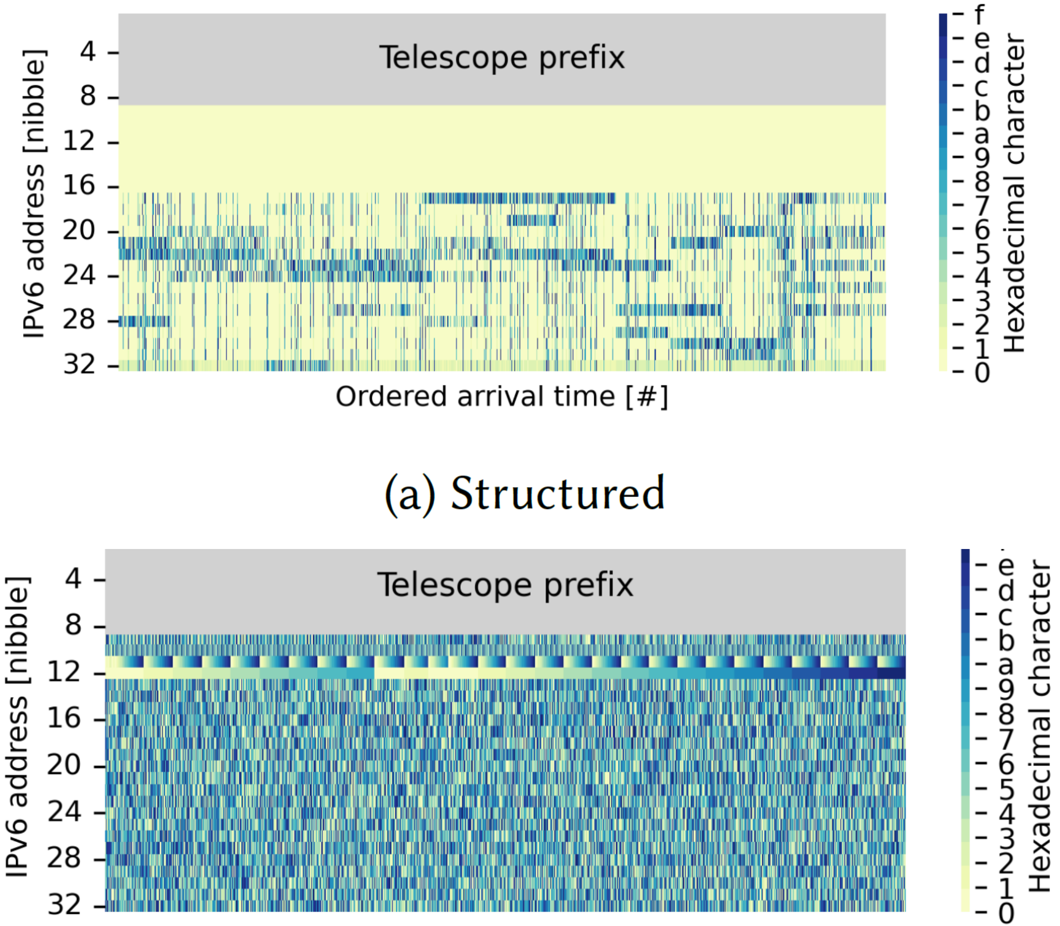


	Packets		Sessions /128		Sources /128	
Protocol	[#]	[%]	[#]	[%]	[#]	[%]
ICMPv6	33,889,898	66.2	132,816	20.1	20,373	56.5
UDP	11,967,255	23.4	36,780	5.6	7113	19.7
TCP	5,372,494	10.5	614,223	92.8	19,977	55.4

Which type of addresses do scanners target?



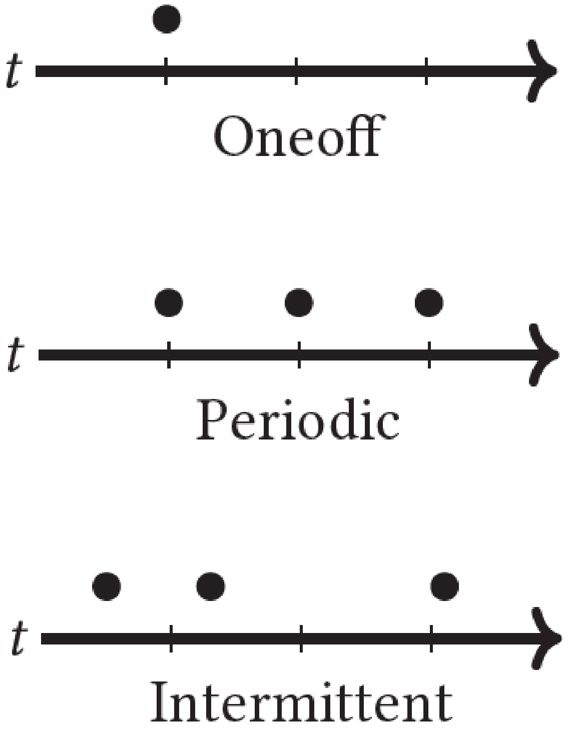
	Packets		Scanners	
Address Type	[#]	[%]	[#]	[%]
randomized	31,101,725	71.32	1841	14.46
low-byte	7,582,741	17.39	8775	68.94
pattern-bytes	2,105,891	4.83	508	3.99
embedded-ipv4	1,519,763	3.48	489	3.84
subnet-anycast	1,118,665	2.57	1053	8.27
ieee-derived	90,843	0.21	13	0.10
embedded-port	89,803	0.21	48	0.38
isatap	217	<0.01	2	0.02



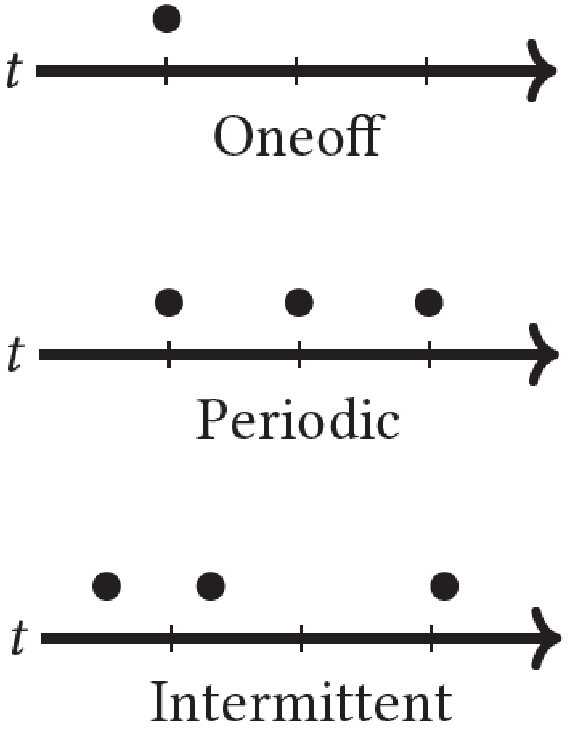
(a) Structured

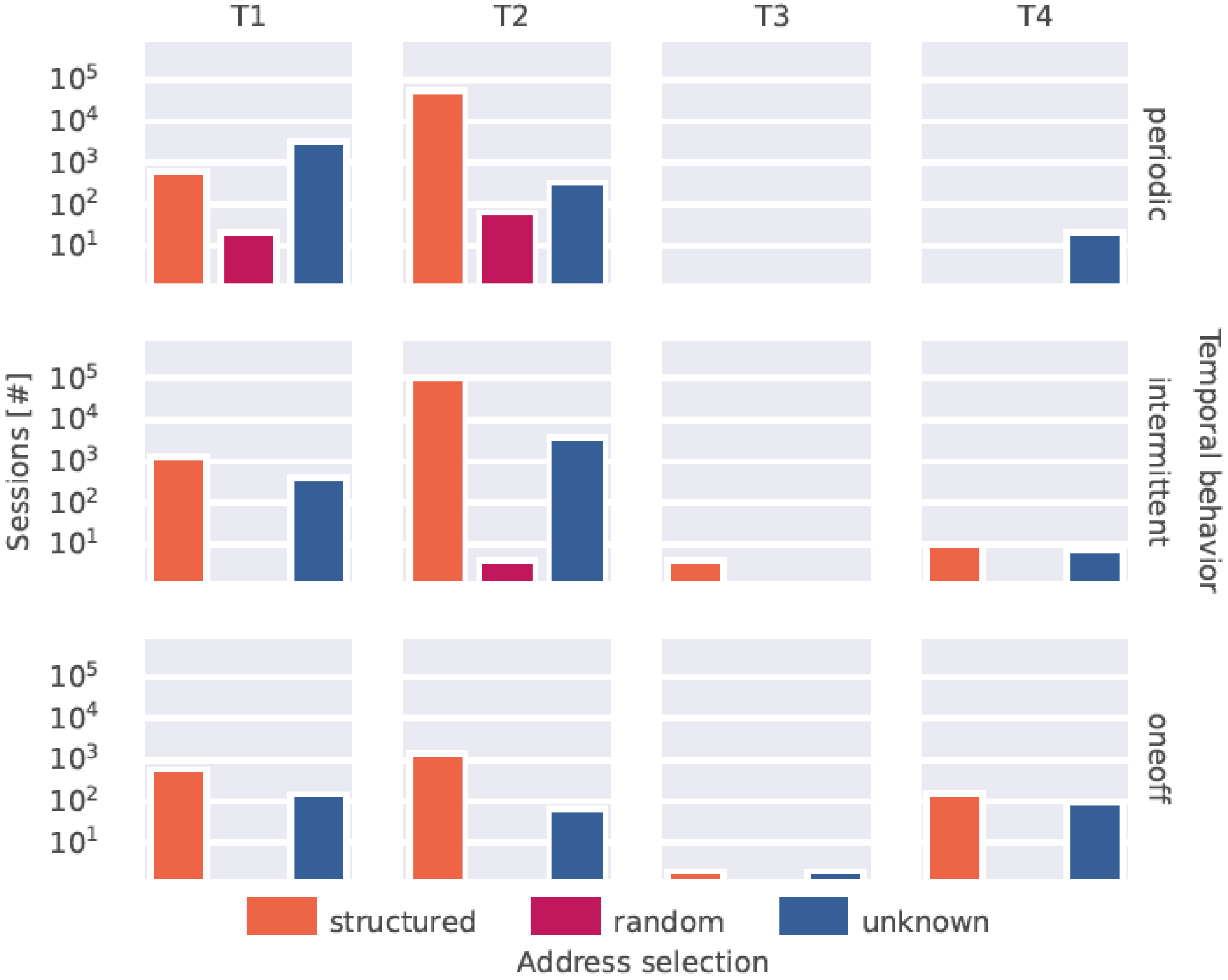
(b) Random

We also classify scanners based on temporal behavior



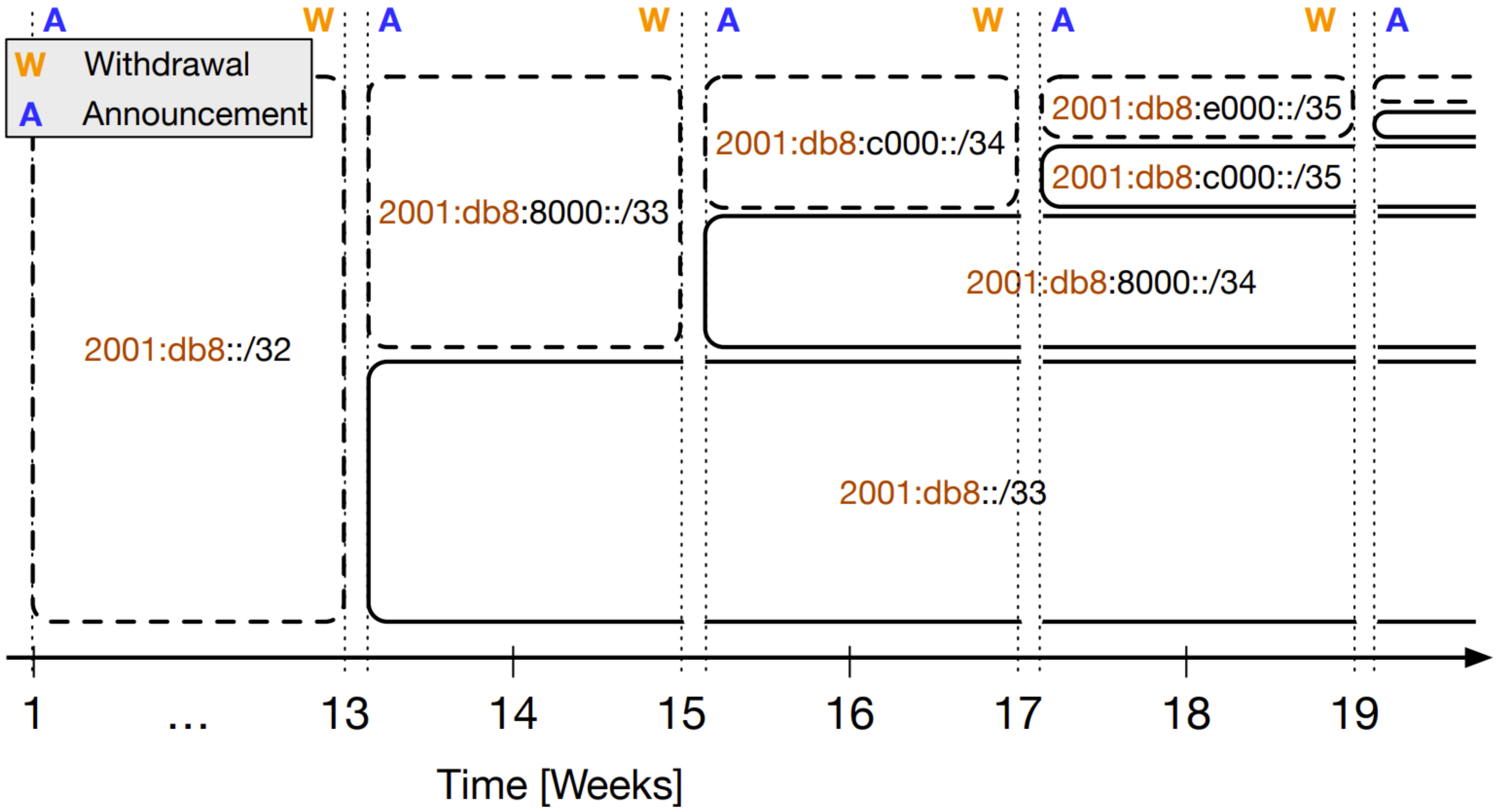
We also classify scanners based on temporal behavior



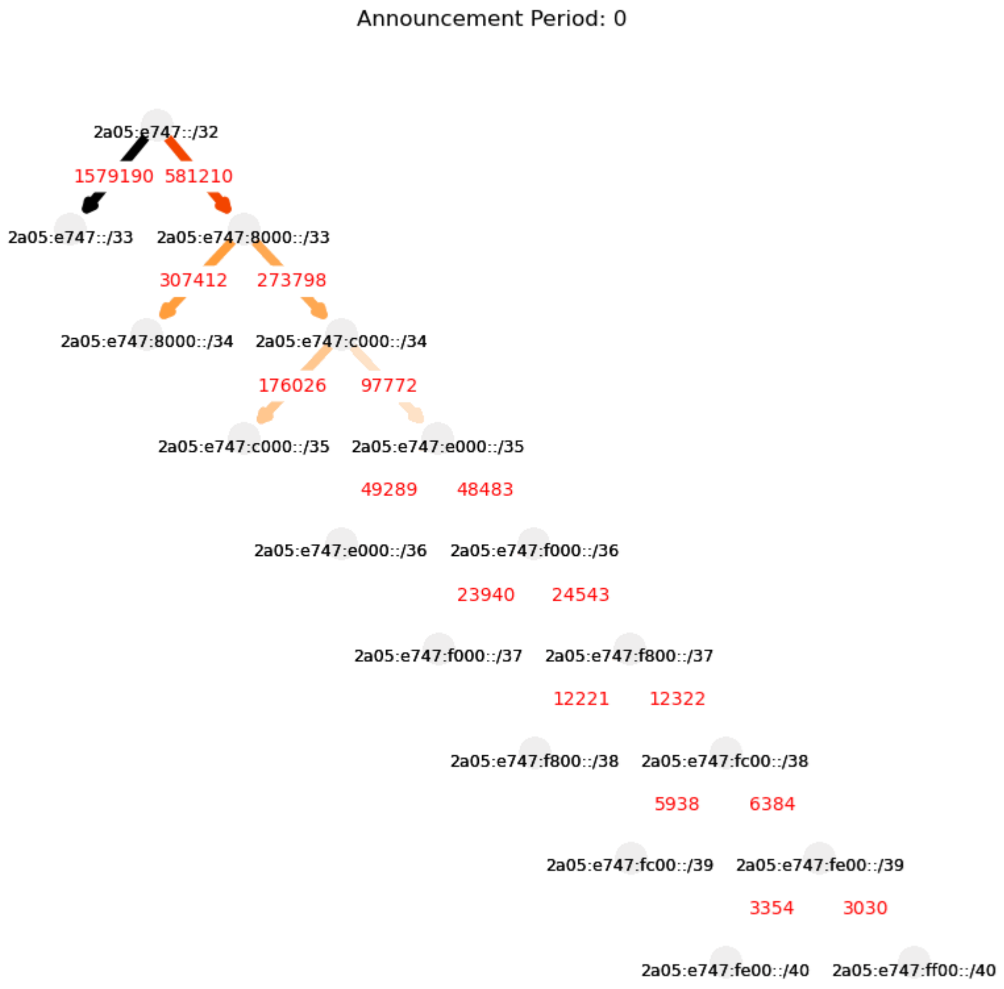


Our method to create BGP signals

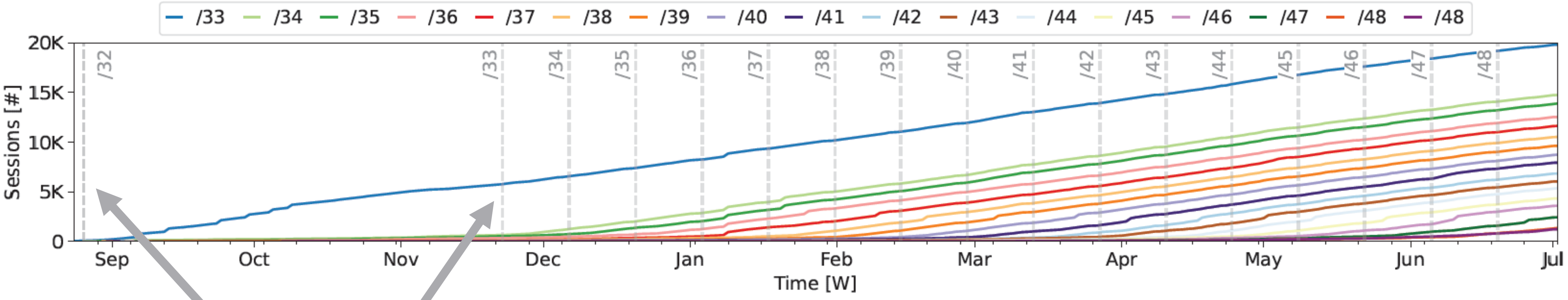
Controlled, passive measurements



How do scanners react on our BGP announcements?



How do scanners react on our BGP announcements?



Start of BGP announcement

As soon as we announce a more specific prefix, scanners start probing this more specific prefix.

Conclusion

How to build an attractive telescope? Network visibility largely depends on announcing the telescope prefix individually in BGP.

Are observations in telescopes unbiased? No. Scanners contact telescopes following external triggers, which in turn means that triggers attract only those scanners that react to them.

Are IPv6 telescopes suitable to monitor DDoS? No. Telescopes commonly monitor DDoS by capturing the backscatter from randomly spoofed attack traffic.