UNIVERSITÉ DE NAMUR

Looking back at the impacts of Tor's end-of-life policy

Jules Dejaeghere ▸ Lionel Goffaux ▸ Hosam Elkoulak ▸ Florentin Rochet ▸

▸ University of Namur

17th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2024)

July 19th, 2024, Bristol, UK

Until 2019

- 6000 relays
- Oldest version in the network: ~6 years old
- 85 different versions
- 5 Tor version series maintained

Read more [1]

After 2019

- Exclude EoL relays periodically
- Exclude unsupported version series
- At most 2 Tor version series maintained

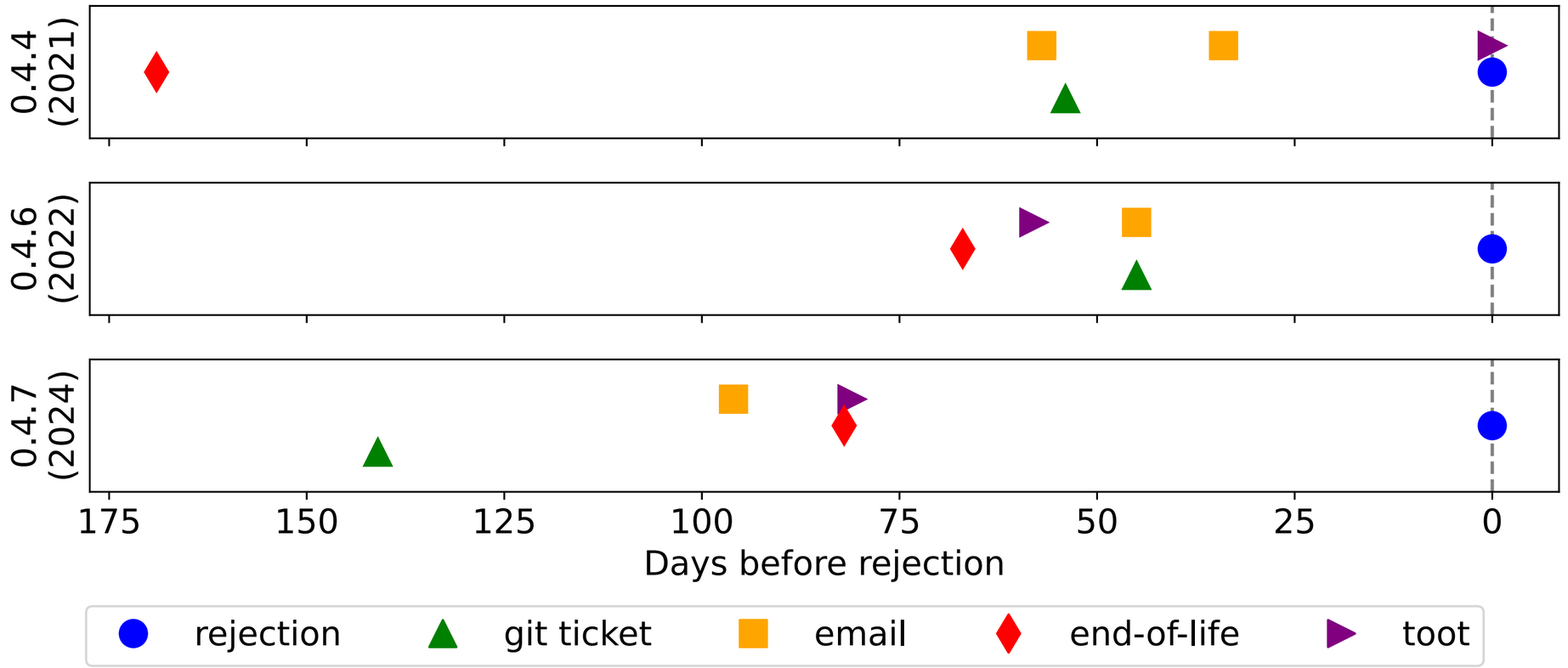
Read more [1]

How exclusion currently works

1. Announcements made on mailing list and fediverse
2. Targeted emails sent to relay operators
3. Relays rejected based on fingerprint and/or version at authorities

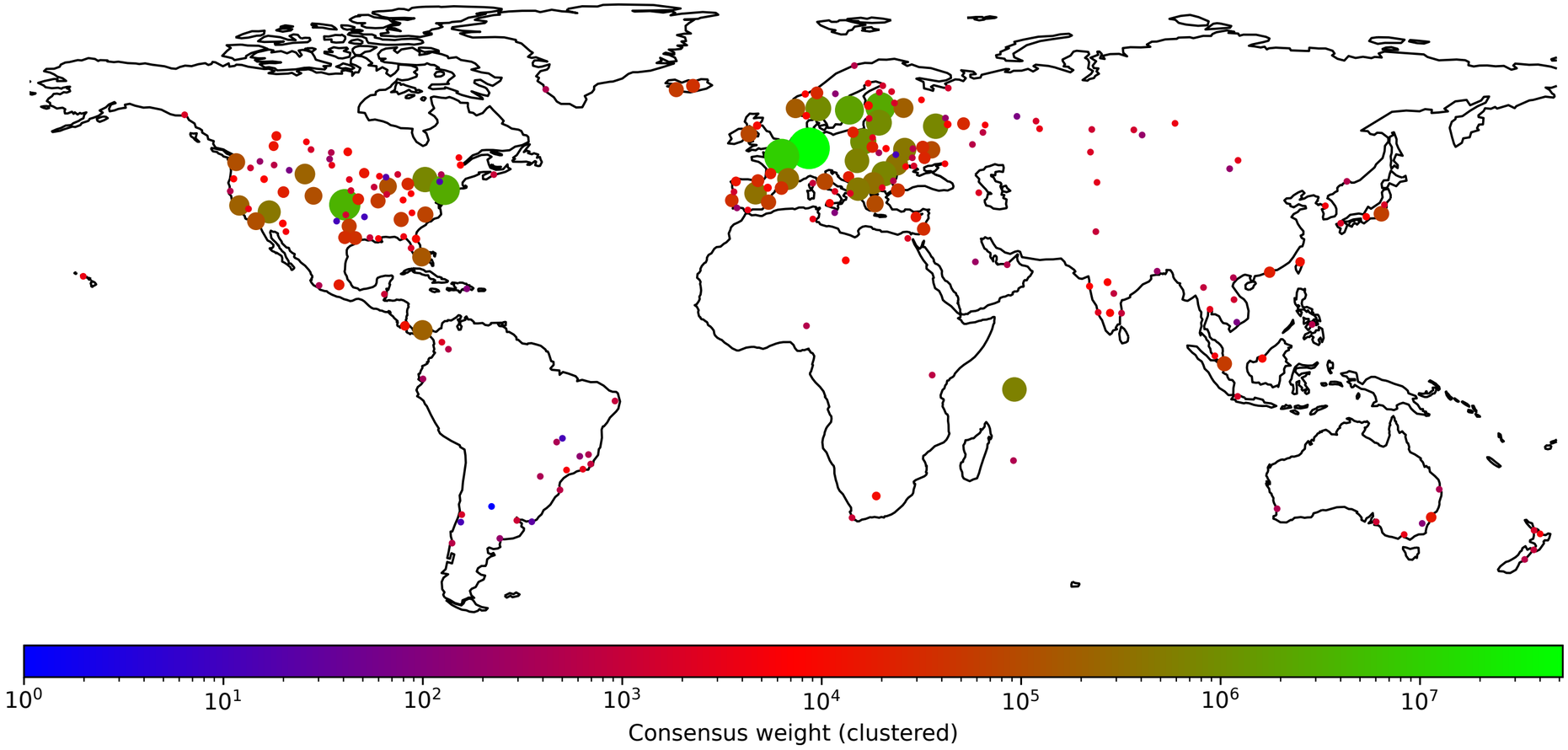
More relays to reject leads to more people to contact

Exclusion timeline



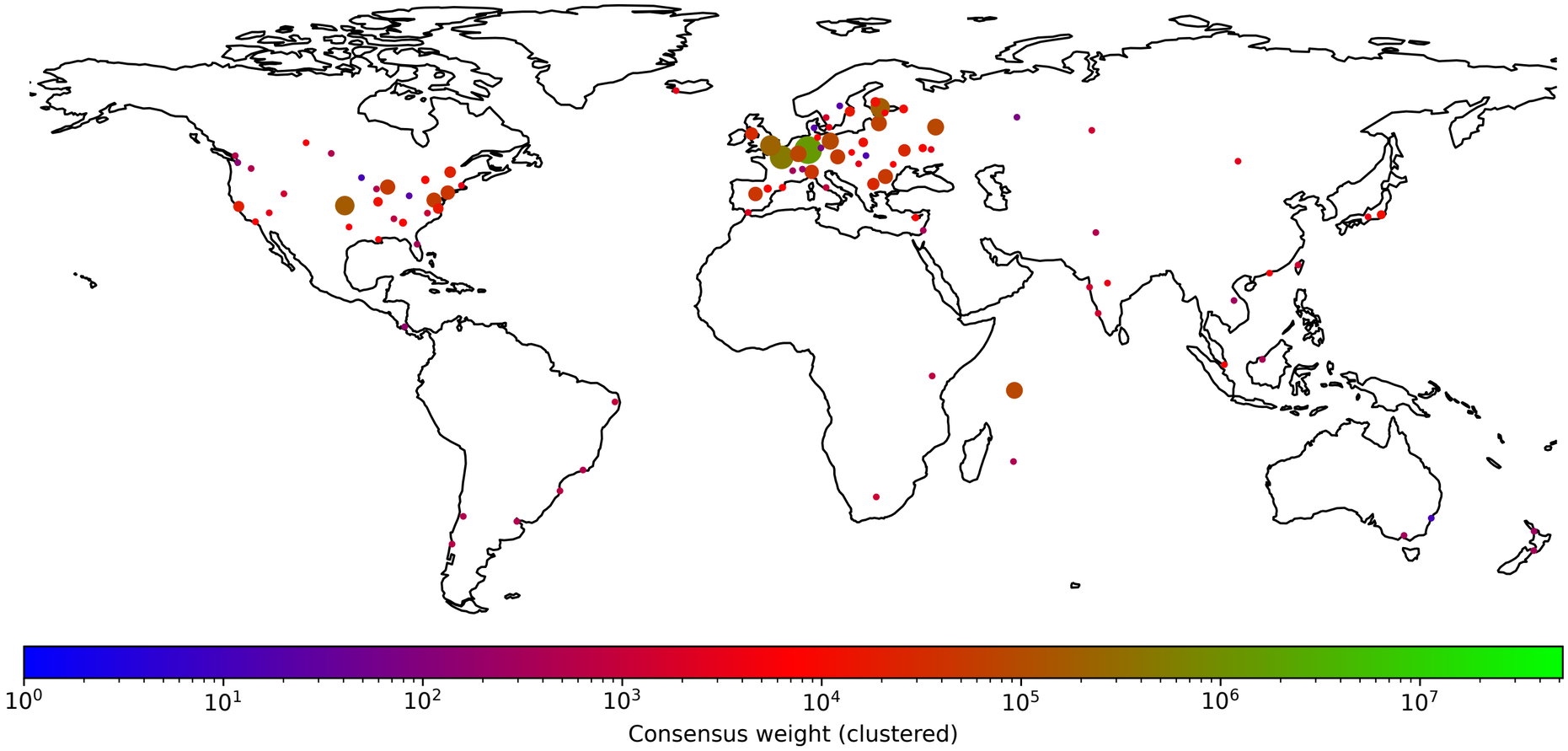
Timeline of the actions taken for different exclusion rounds

Overview of an exclusion round (2021)



All relays from consensus 2021-11-30T12

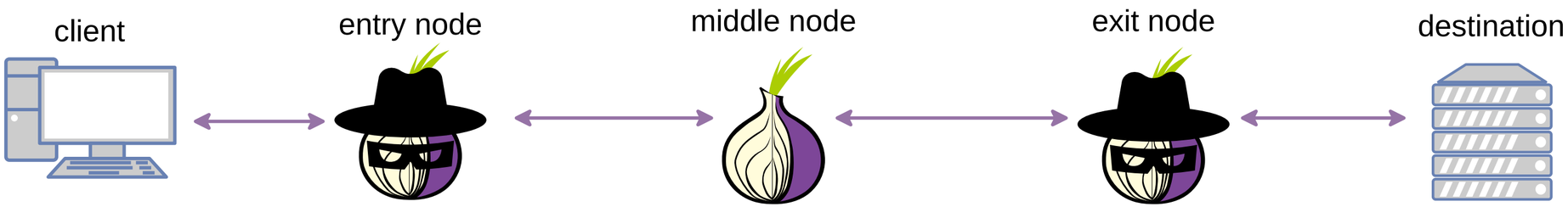
Overview of an exclusion round (2021)



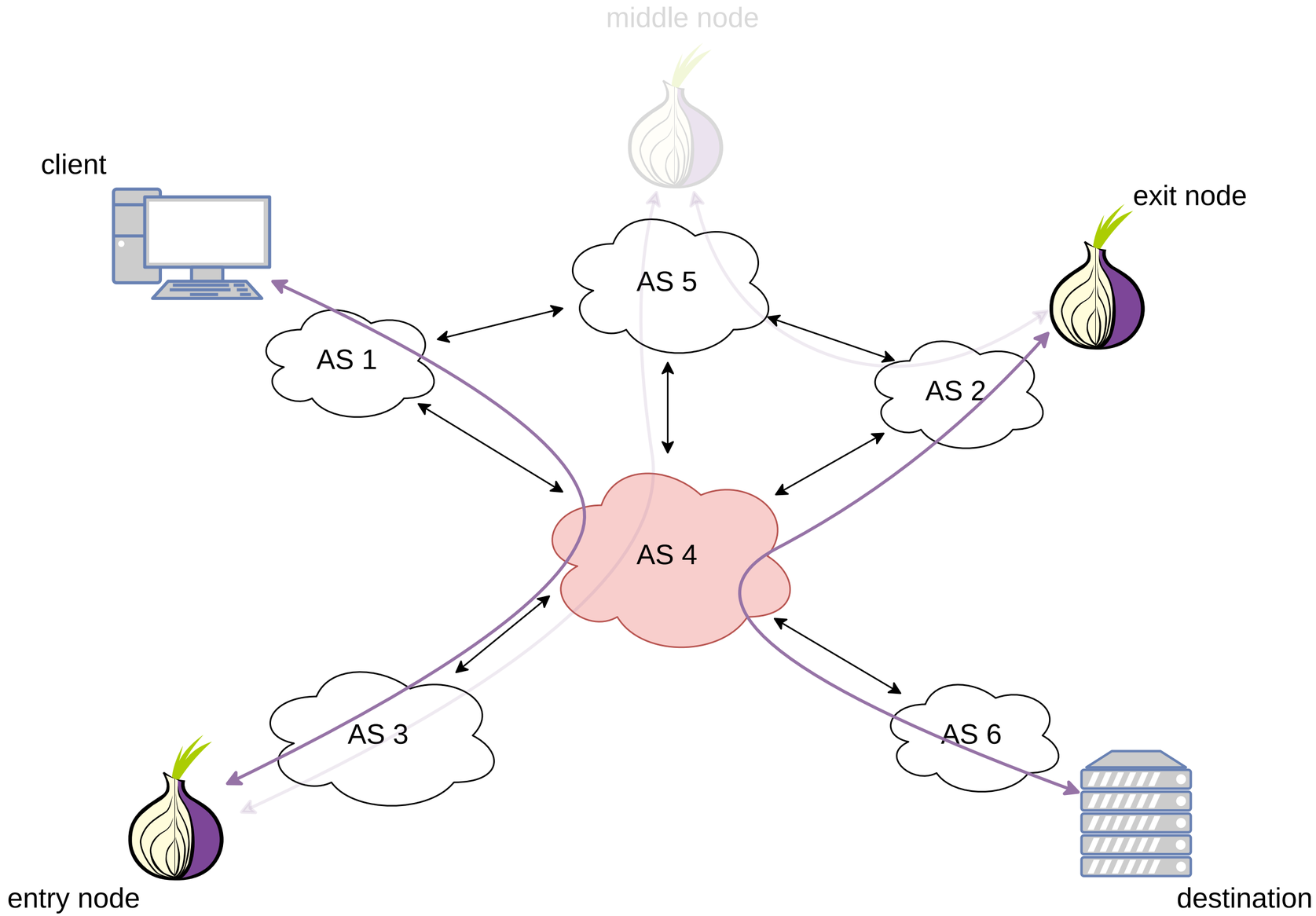
Relays listed for exclusion at 2021-11-30T12 (4.32% of consensus weight)

Common adversaries

Relay adversary



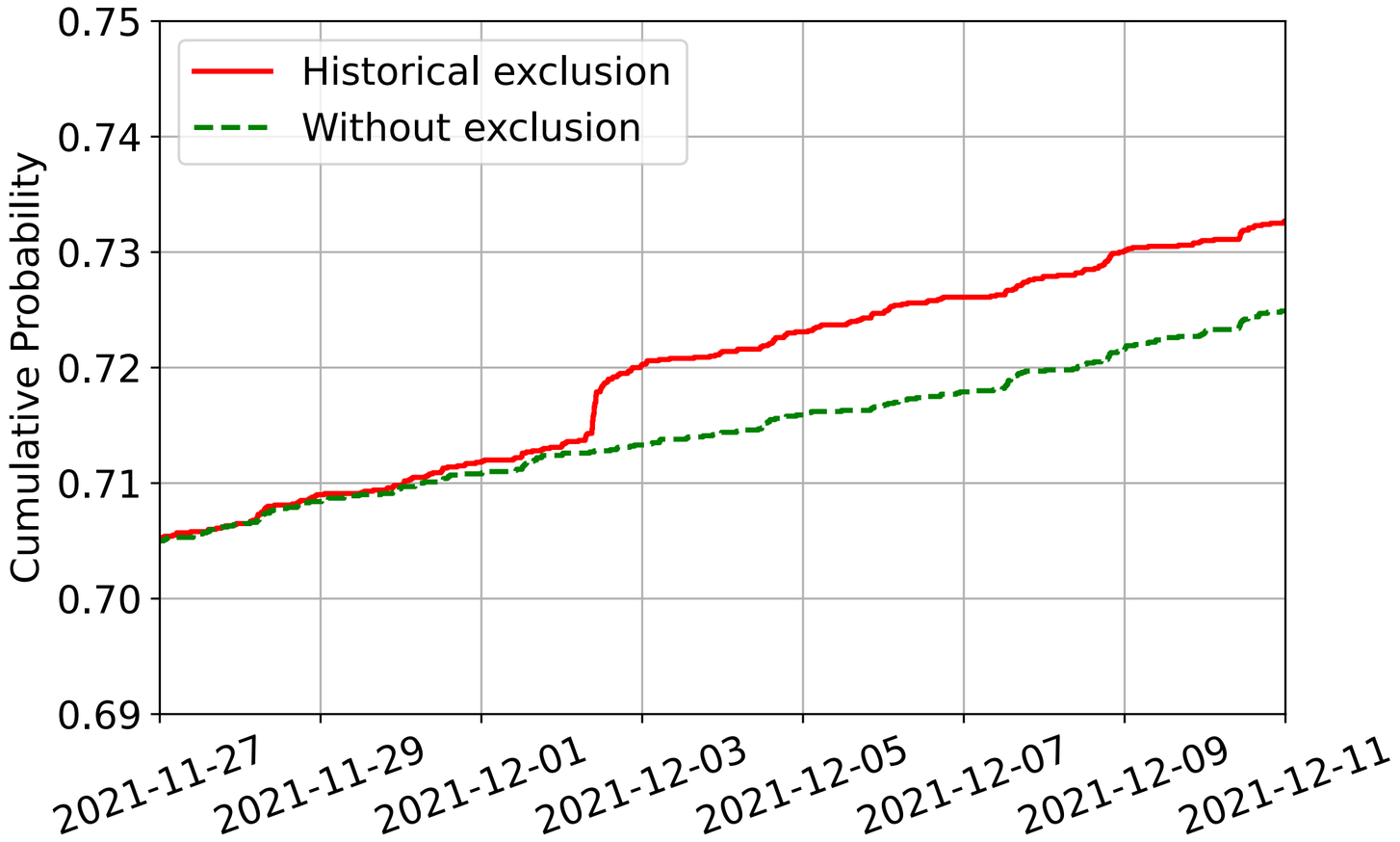
Network-level adversary



Computing the anonymity impact

- Simulate the Tor path selection algorithm for a set of clients at different locations
- Consider an adversary with realistic resources
- Simulate for one month arround the exclusion time
- If the adversary is on both ends of the circuit, then the client is compromised

Guard churn might be the biggest issue



Probability of path compromise with top-3 ASes malicious

How can we deal with the churn or reduce it?

We cannot get everyone up-to-date

- Engaging with every relay operator takes time
- Not all relays bring the same contribution to the network

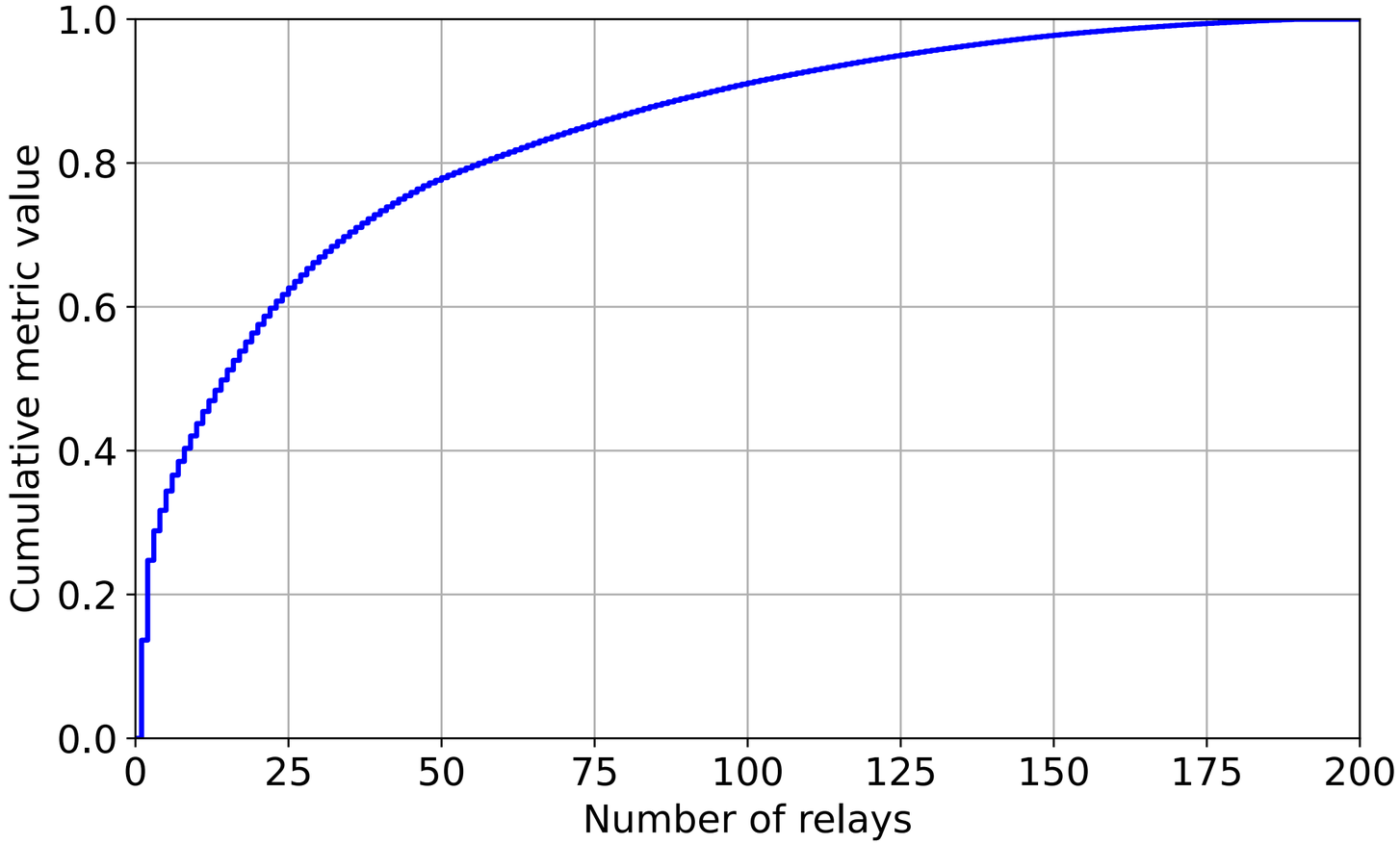
Quantifying relay contribution against adversaries

Quantifying relay contribution against relay adversary

If excluding a relay improves the power of the adversary, then that relay contributes to the network's resilience against the adversary.

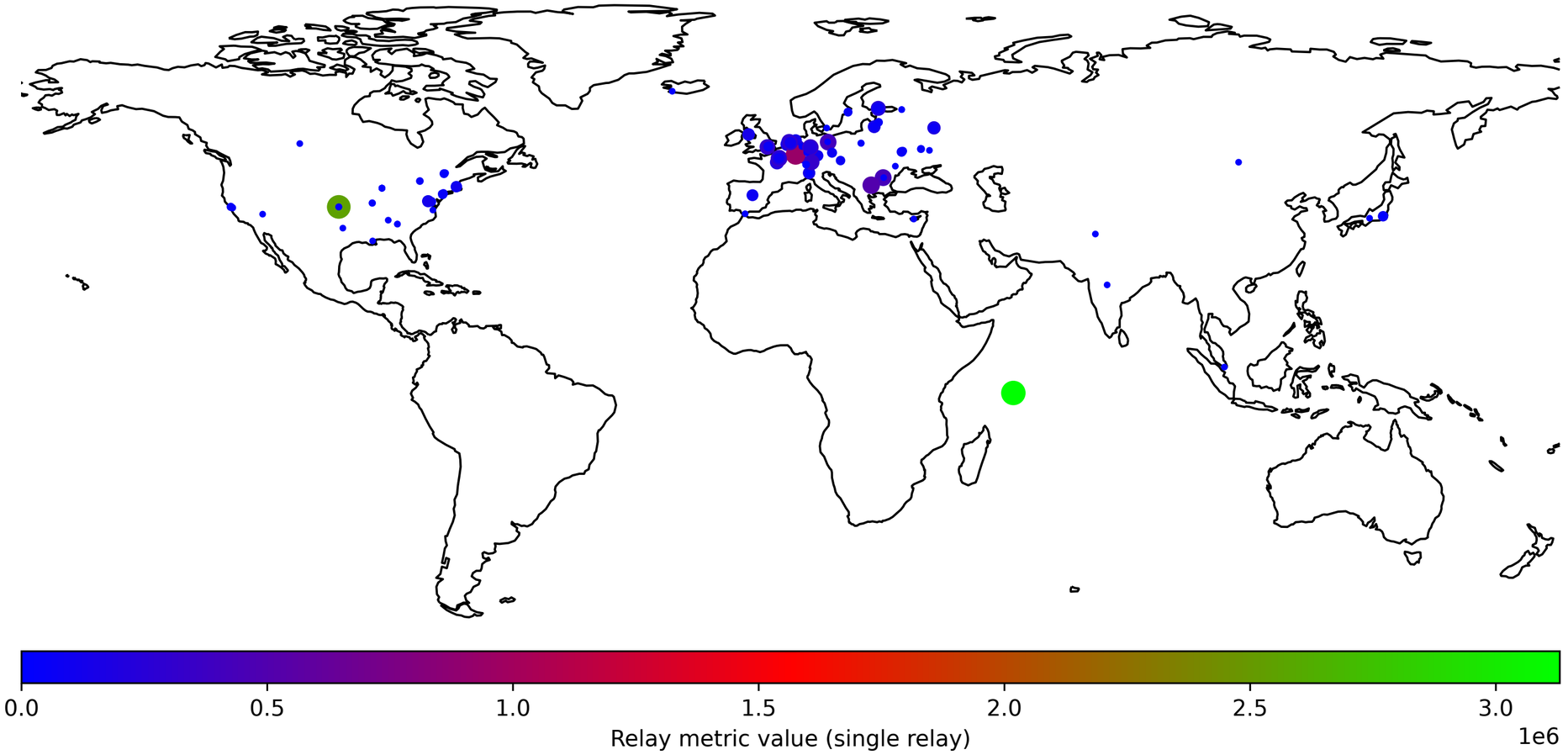
Related to the bandwidth and connectable relays (subnets and family).

Quantifying relay contribution against relay adversary



Cumulative value for the relay metric for relays set for exclusion on 2021-11-30T12

Quantifying relay contribution against relay adversary

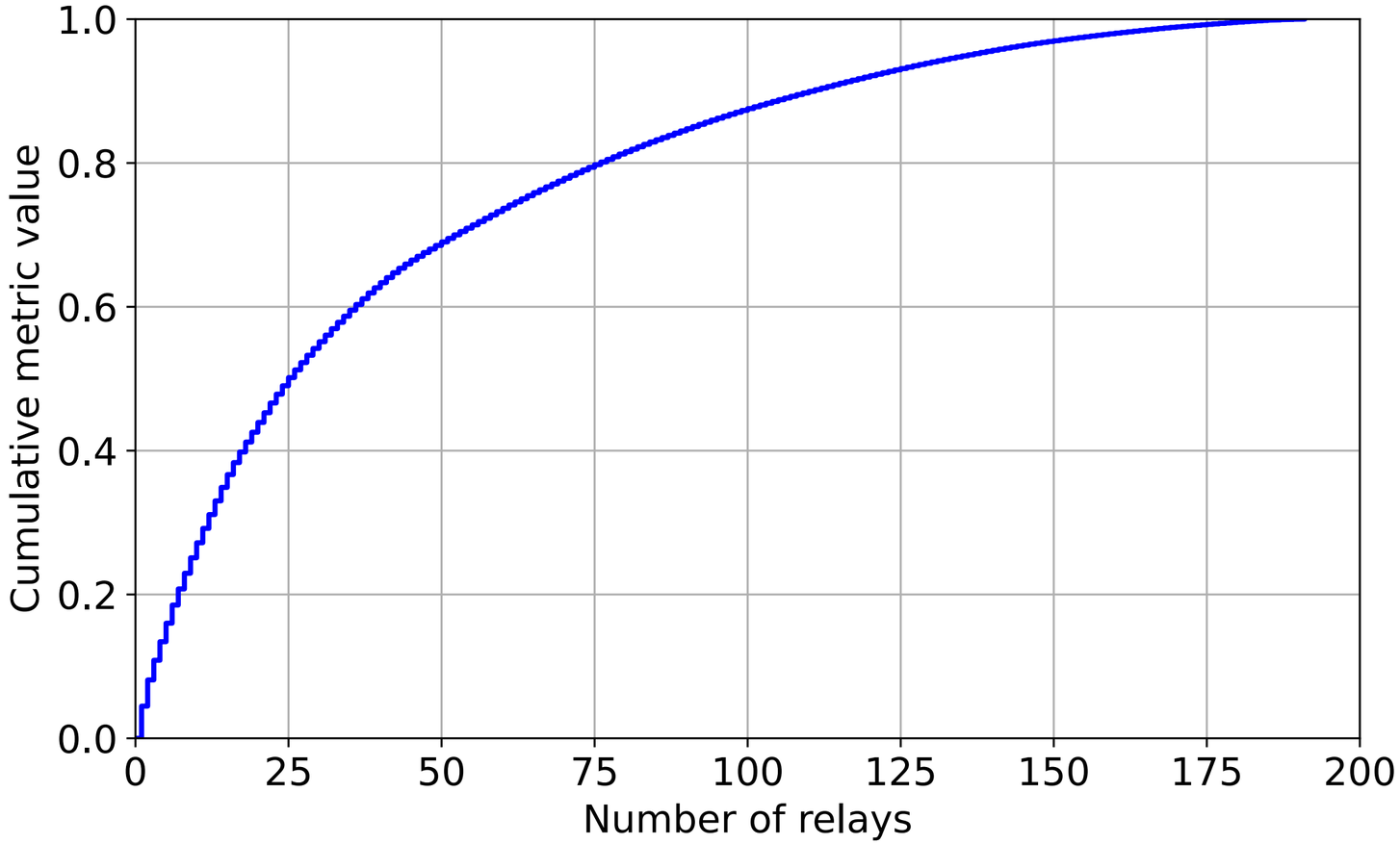


Relay metric value for relays set for exclusion on 2021-11-30T12

Quantifying relay contribution against network adversary

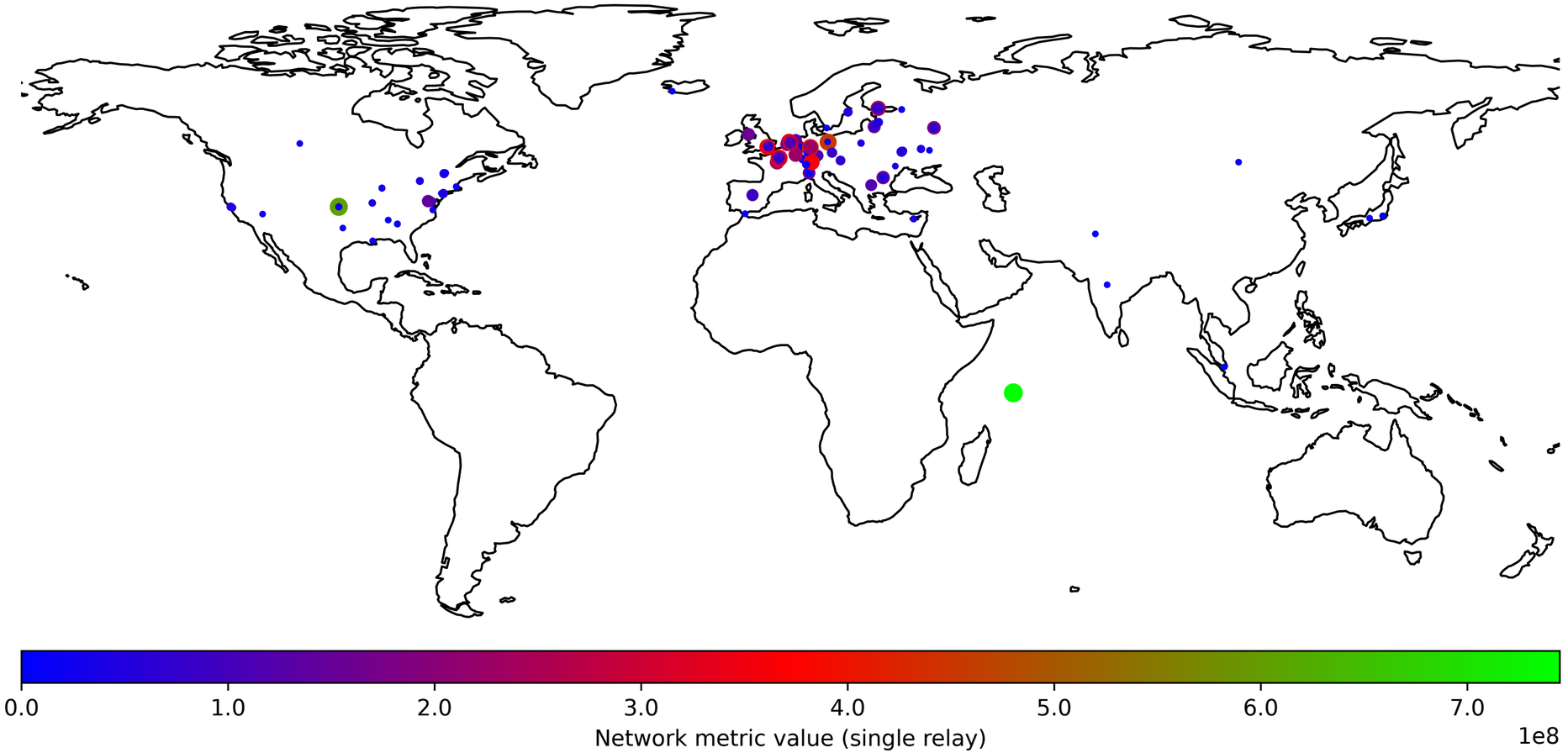
A relay that provides a substantial amount of bandwidth without flowing through the same network-level entity on both ends contributes significantly to the network's resilience.

Quantifying relay contribution against network adversary



Cumulative value for the network metric for relays set for exclusion on 2021-11-30T12

Quantifying relay contribution against network adversary



Network metric value for relays set for exclusion on 2021-11-30T12

We cannot get everyone up-to-date

- Engaging with every relay operator takes time
- Not all relays bring the same contribution to the network

What kind of governance do we want?

Looking back at the impacts of Tor's end-of-life policy

Jules Dejaeghere ▸ Lionel Goffaux ▸ Hosam Elkoulak ▸ Florentin Rochet ▸

▸ University of Namur

17th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2024)
July 19th, 2024, Bristol, UK

CyberExcellence project, grant 2110186
funded by the SPW Recherche

References

[1] Goulet, D. 2019. Removing End-Of-Life Relays from the Network Tor Project. *Tor Blog*

[2] The Tor Project 2023. Expectations for relay operators - The Tor Project - Policies.