

## Problem & Motivation

- ▶ Tor provides **anonymity** to millions of users.
- ▶ Low-latency anonymity systems are vulnerable to **traffic correlation attacks**.
- ▶ Strong passive adversaries, such as large **autonomous systems (AS)**.
- ▶ Current analyses mostly based on **BGP updates**.
- ▶ With **RIPE Atlas** and **traceroute** this needs to be re-evaluated.
- ▶ **Placement of measurement nodes** in the same ASes as Tor network nodes.

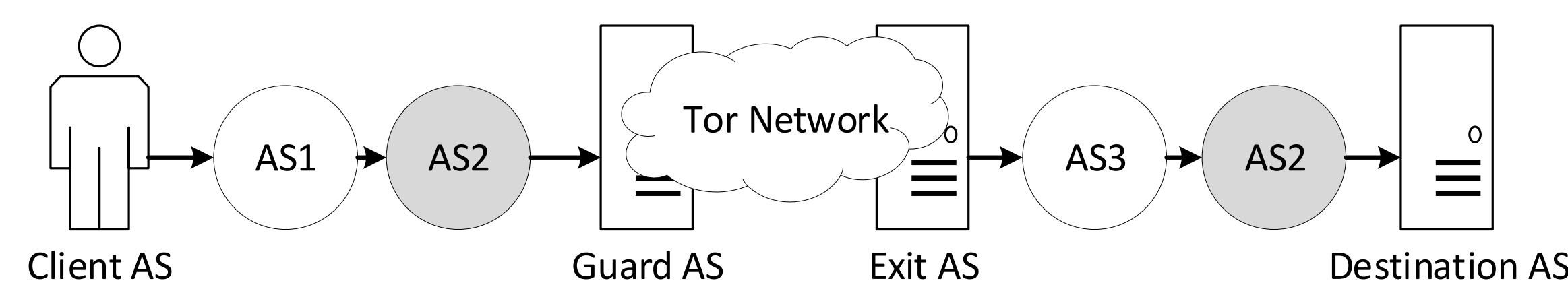


Figure 1: AS2 in a possible position for a traffic correlation attack

## Tor Relays & RIPE Atlas

- ▶ Tor relays (approx. 6,500) are globally distributed.

	Relays	Diff. AS	BW (Gbit/s)
All Relays	6,509	1,104	418.07
Exit Relays	1,000	275	112.90
Guard Relays	2,415	470	254.61

Table 1: Tor relay overview

- ▶ RIPE Atlas measurement probes (approx. 10,000) are also globally distributed.
- ▶ Partially, in the same autonomous systems.

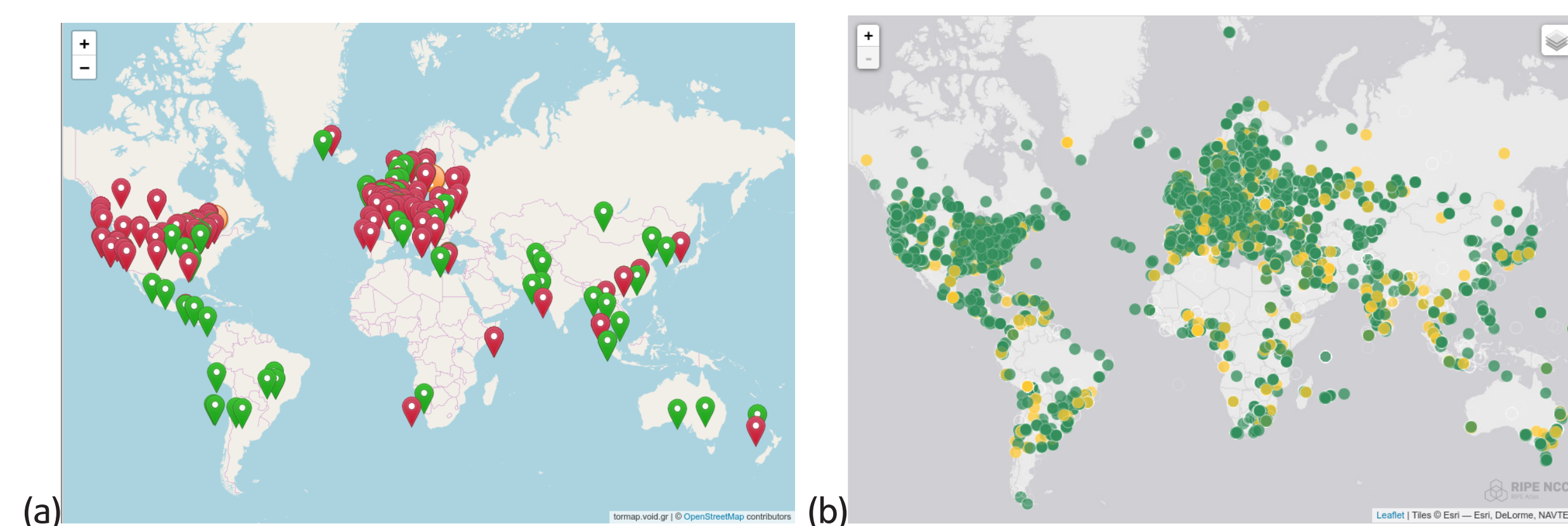


Figure 2: Visualization of Tor relays (a) and RIPE Atlas coverage (b)

- ▶ RIPE Atlas probes cover a substantial amount of ASes with Tor relays.
- ▶ For Tor exit relays it is 41% of total exit probability.
- ▶ For Tor guard relays it is 83% of total exit probability.

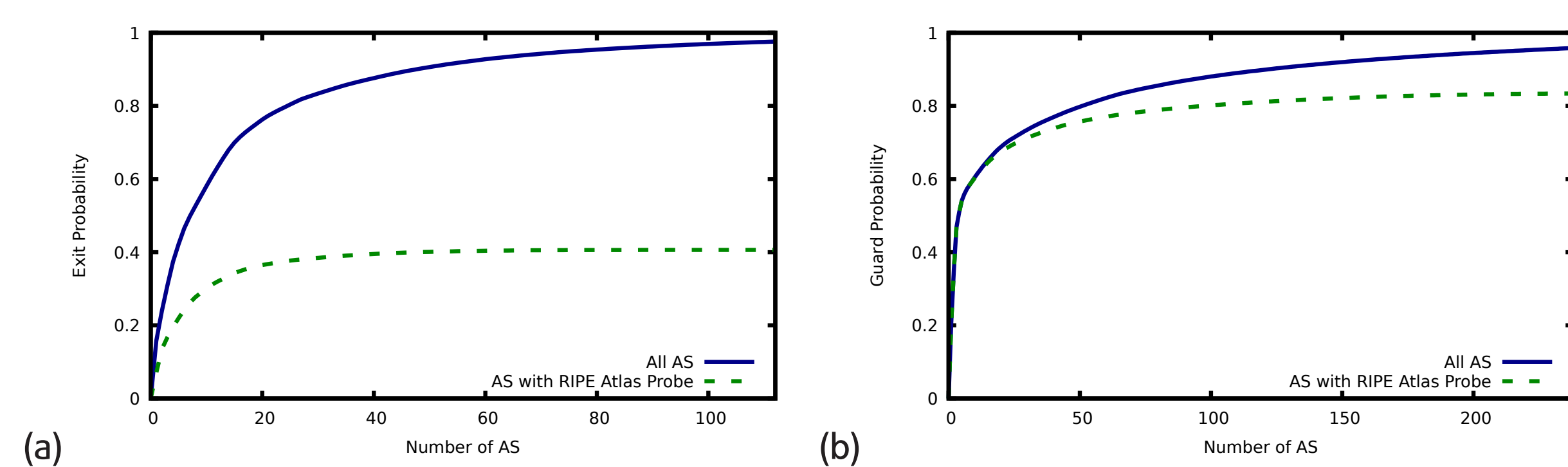


Figure 3: Accumulated percentage of (a) exit, and (b) guard probability with the number of autonomous systems

- ▶ Numbers could be increased:
  - ▶ Add 10 selected probes, cover 87% exit probability.

## traceroute Measurements

- ▶ Executed traceroute commands on RIPE Atlas probes.
  - ▶ Placed in AS with Tor relays.
- ▶ Four different directions of measurements.
- ▶ From Top client ASes to Top destination ASes.

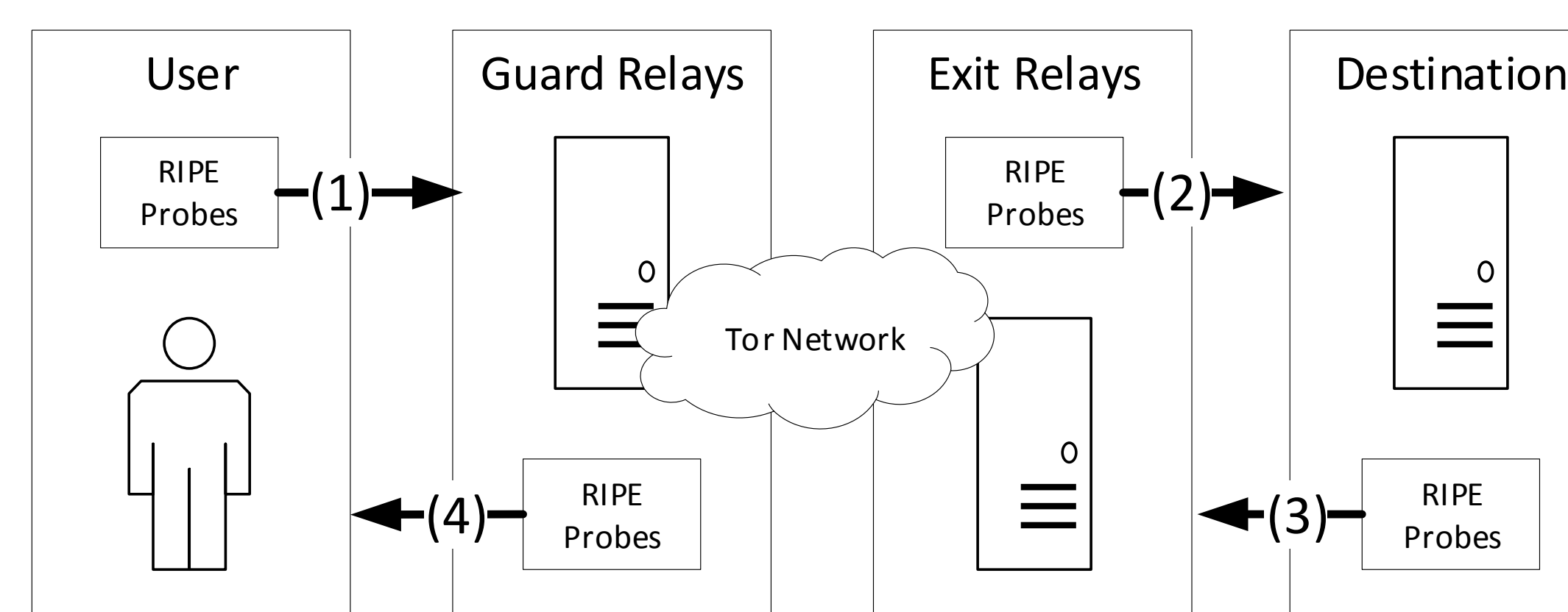


Figure 4: Four different directions of active RIPE Atlas traceroute scans

## Evaluation

- ▶ Identified ASes with high probability to be on guard side as well as exit side (from single client AS to top destination ASes).

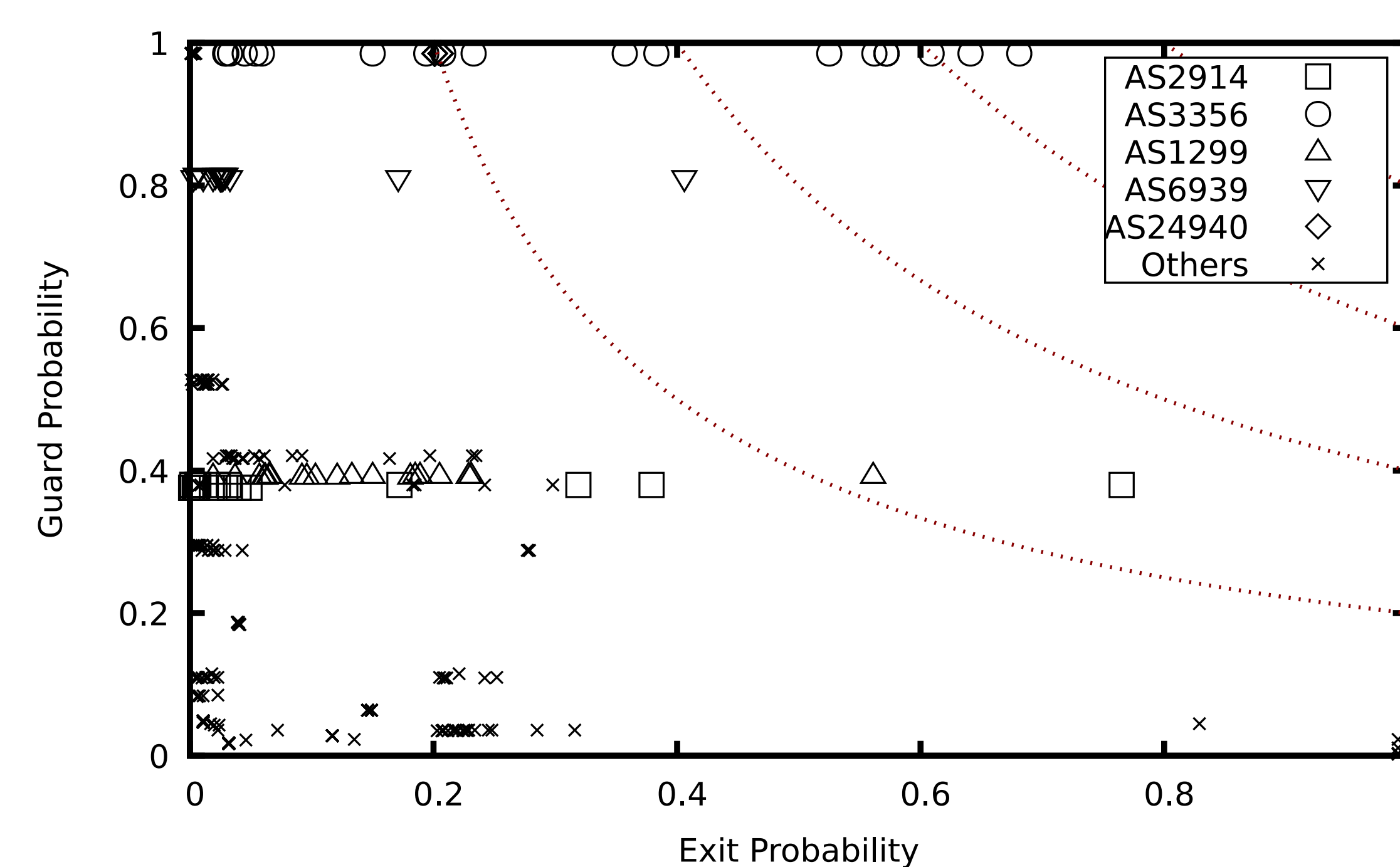


Figure 5: Combined probability of ASes appearing on the client and destination path

## Conclusion

- ▶ A **novel way to analyze the network routes** taken by traffic from and to the Tor network.
- ▶ Utilized the **RIPE Atlas** framework.
- ▶ Identified a **small set of ASes which have a great influence** on the total amount of Tor bandwidth.
- ▶ We generated a **valuable additional data source**.