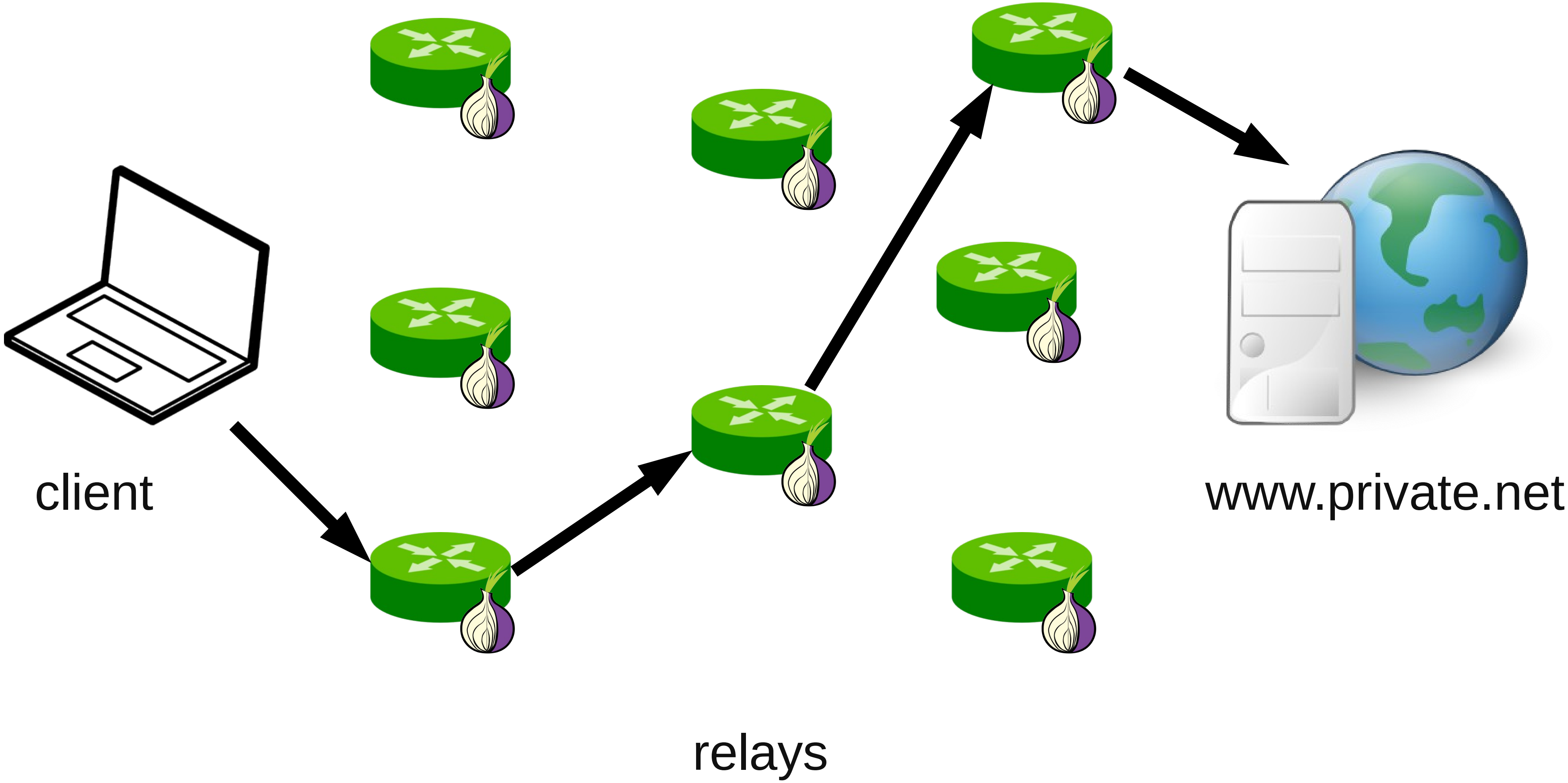
One Fast Guard For Life

Roger Dingledine
Nick Hopper
George Kadianakis
Nick Mathewson

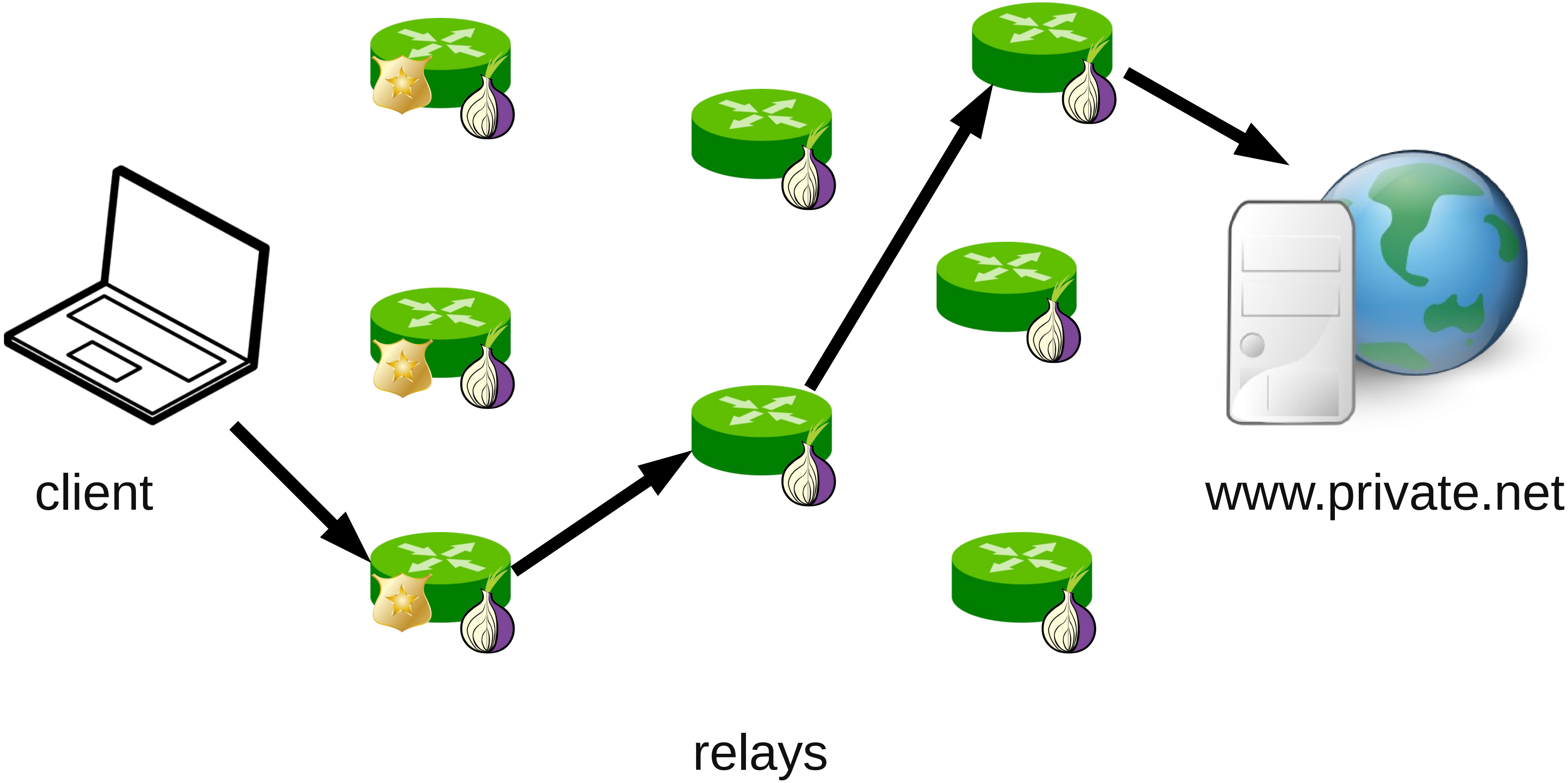
Outline

- ***1) How Tor works now***
- 2) The problems
- 3) How we should fix it

Guards and Tor



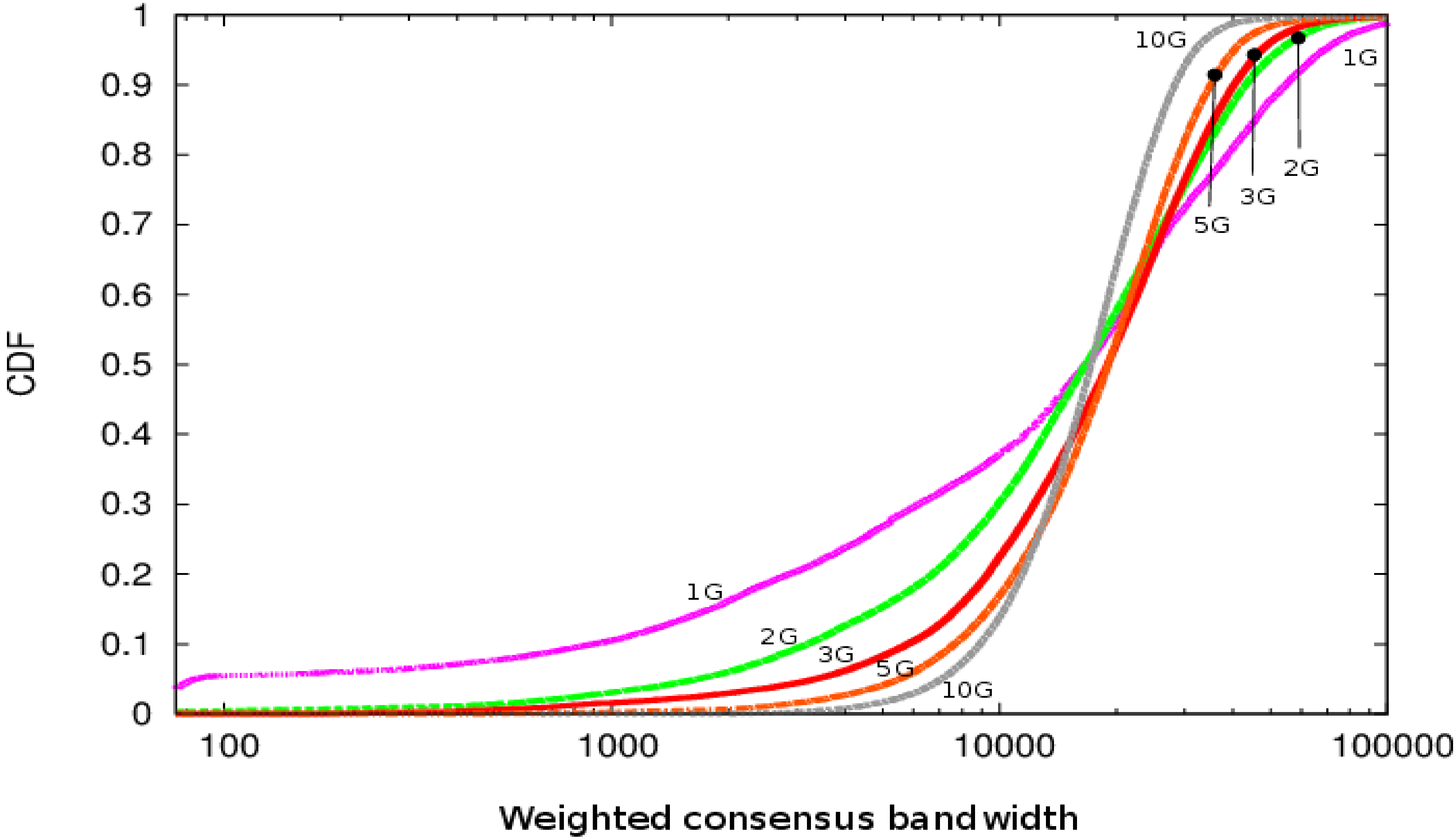
Guards and Tor



Other benefits from guards

- Mitigate “denial of service as denial of anonymity” attacks
- Force ongoing cost by attacker (“raise the start-up cost of attack”)

3 guards, to reduce variance



Load balancing

- Problem: nodes that have been guards for a long time accrue load (so they get slower and slower)
- Fix: clients rotate to new guards every 45ish days to load balance

Outline

- 1) How Tor works now
- ***2) The problems***
- 3) How we should fix it

Problem 1: guard rotation

- Every time you pick a new guard, it's a new chance to lose
- 6 months is ~12 new guard picks!
- “Attacker with 10% of Tor network for 6 months = 80% compromise rate” – CCS 2013

Pervasive surveillance?

- And don't just think of relay-level adversaries: every new guard is a new set of **network locations** that get to see your traffic too.

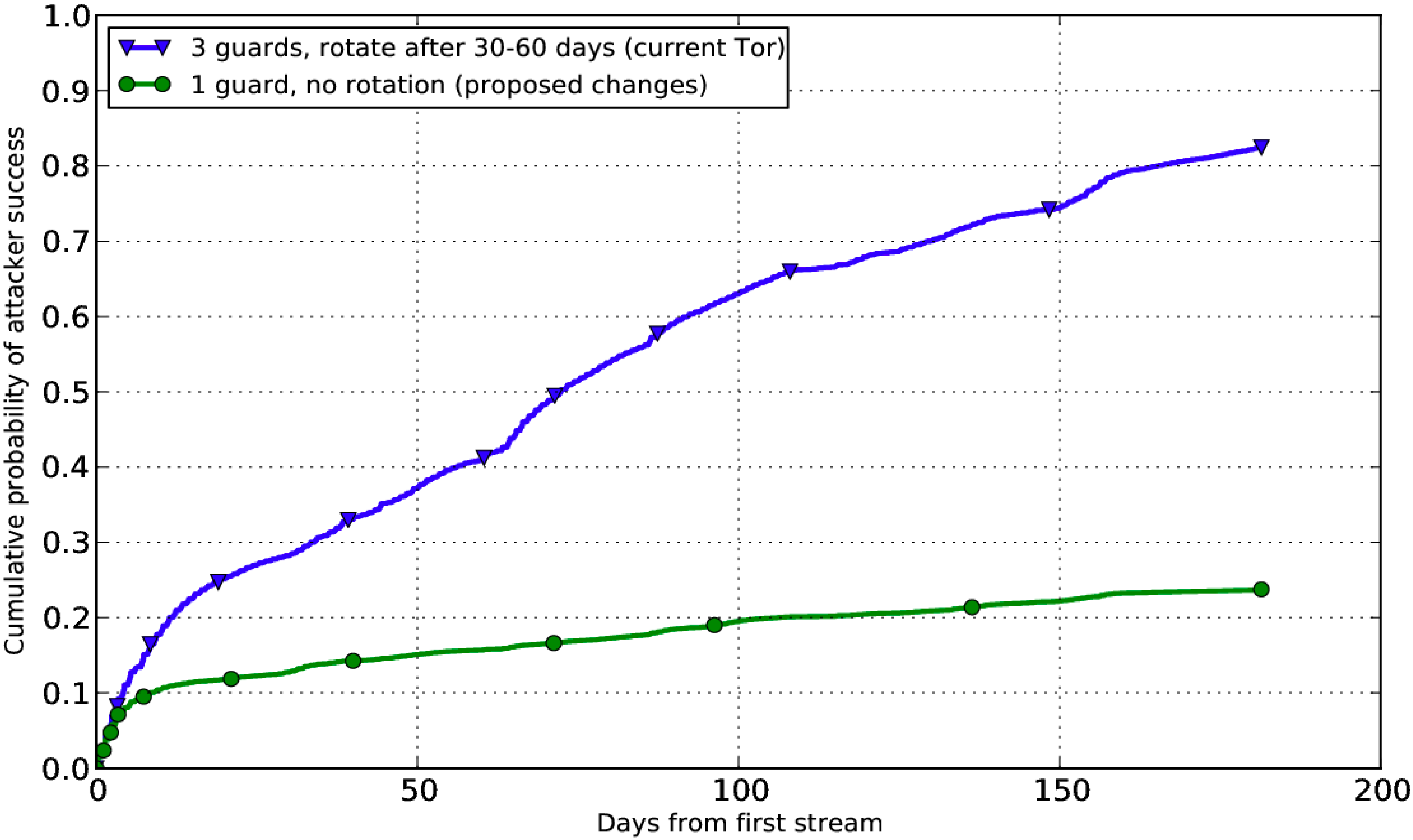
Problem 2: guard fingerprinting

- Every client picks its own set of three guards (out of ~1000).
- A given trio of guards is a nearly unique fingerprint to a local observer.

Outline

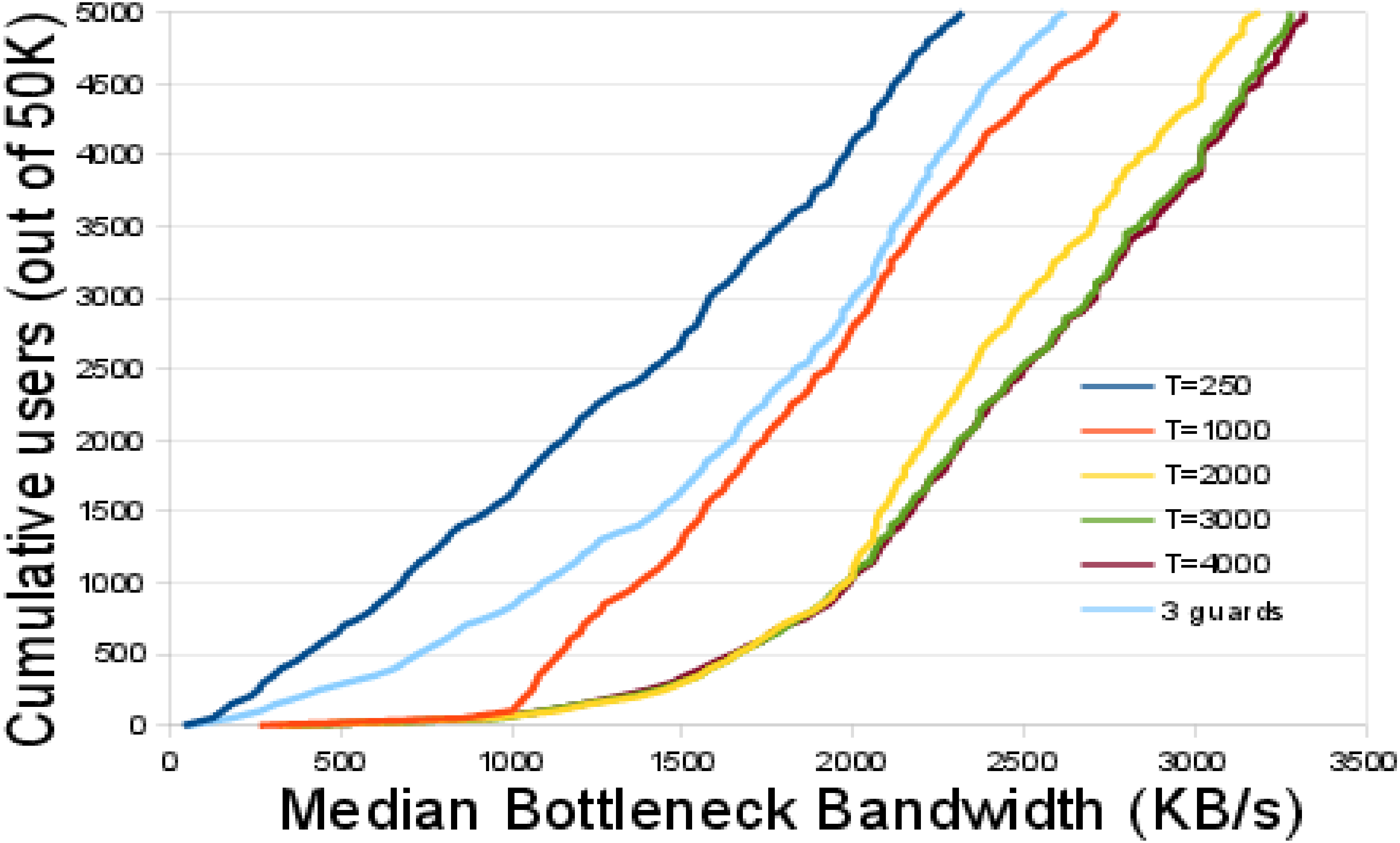
- 1) How Tor works now
- 2) The problems
- ***3) How we should fix it***

Our potential gains



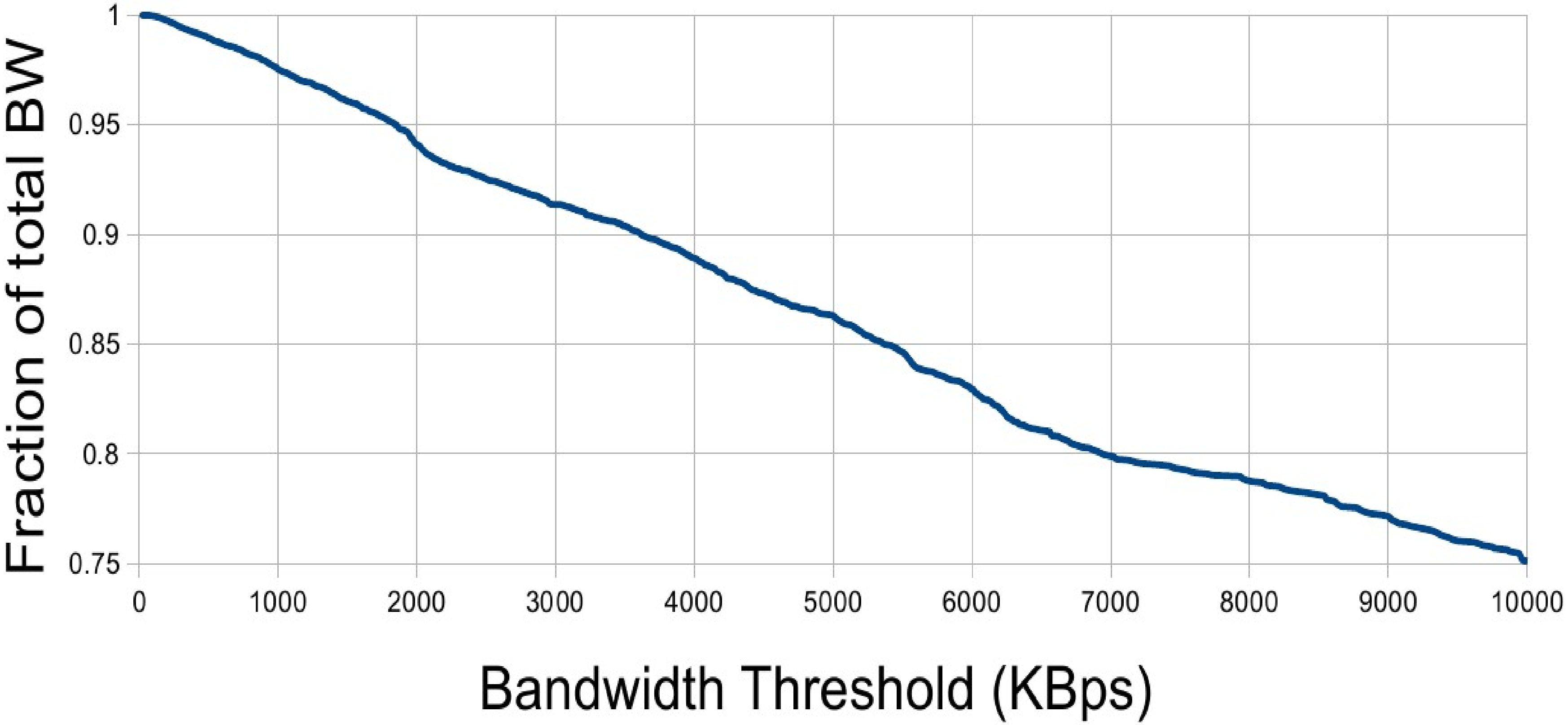
[Johnson+, CCS13]

What if your one guard is slow?



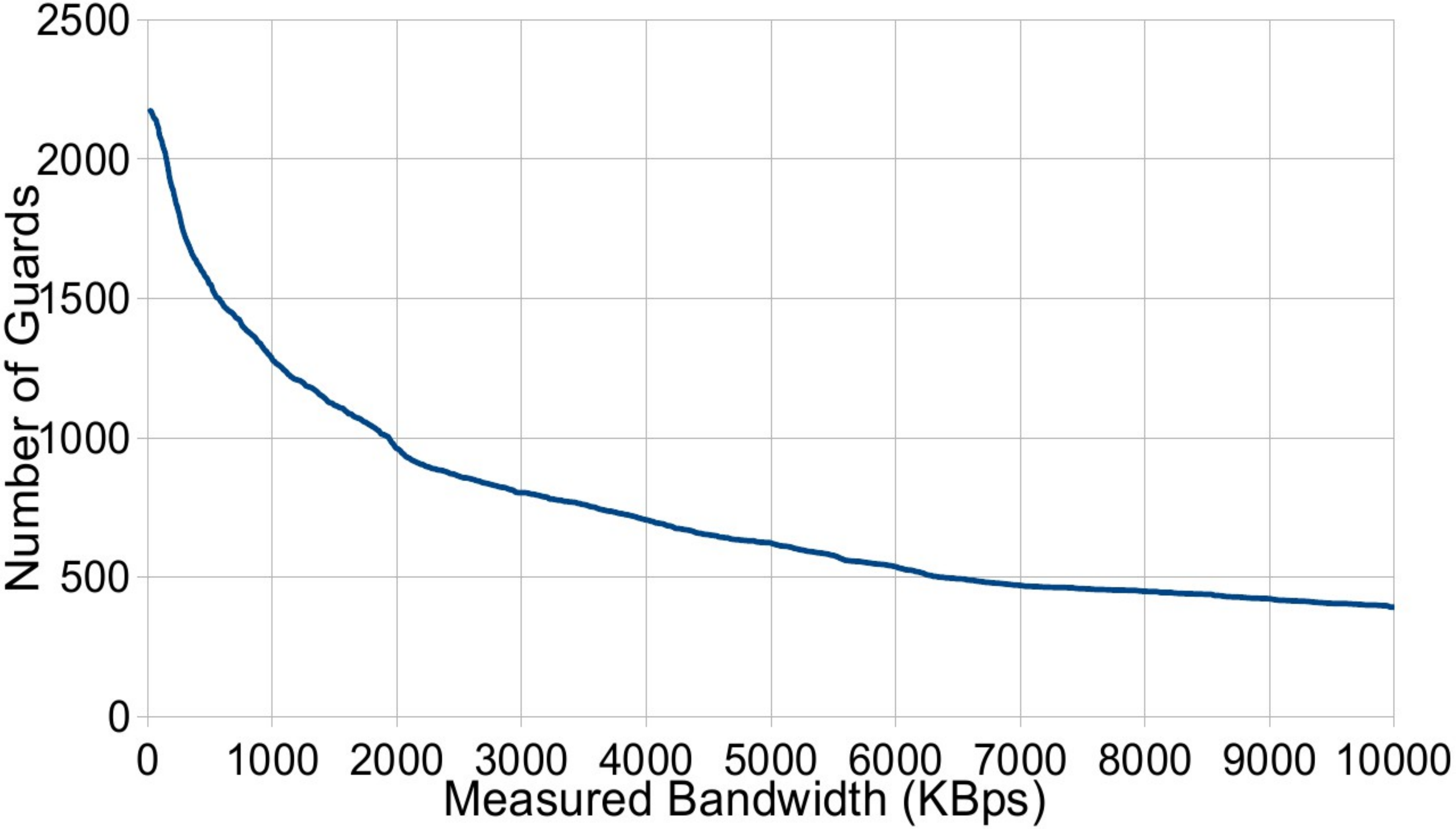
Require guards to have bandwidth ≥ 2MB/s

How much bandwidth do we lose?



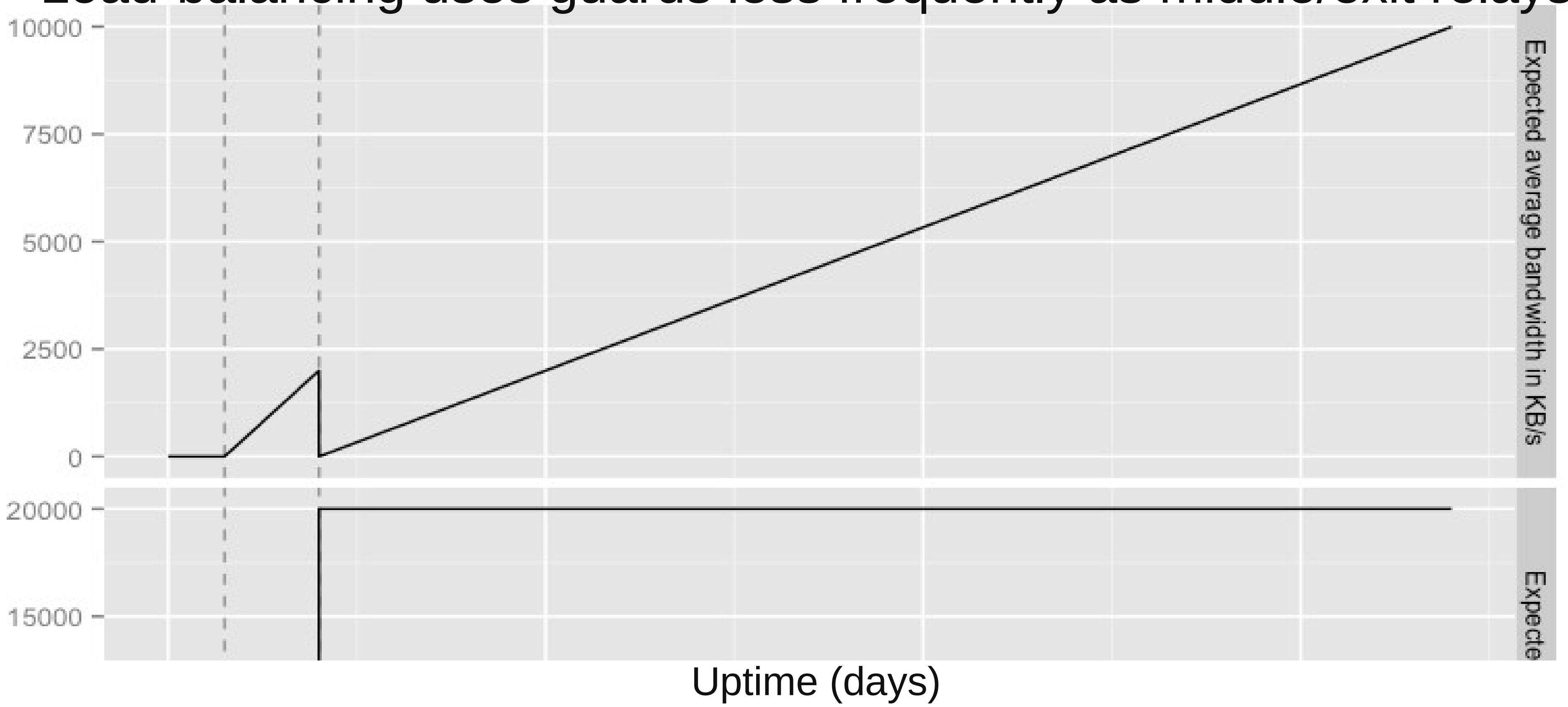
How many guards do we lose?

threshold



Less-Frequent Rotation

Load-balancing uses guards less frequently as middle/exit relays.



Longer rotation period → new guards more underutilized.

Solution: track time as guard; use newer guards in middle more.

Disadvantage: more time to identify/compromise guards

Open problems (1)

- If we keep a single guard for 9 months, how much do we increase vulnerability to e.g. MLATs?
- Due to churn, users will pick a second guard, fragmenting the anonymity set. “Guard buckets”?

Open problems (2)

- Improved guard selection criteria
- Can't do Conflux design anymore :(
- Guard enumeration attacks (“layered guards” seem useful but different)
- “First use of guard = total loss” not really accurate. Profiling?