ShorTor

Improving Tor Network Latency via Multi-Hop Overlay Routing

Kyle Hogan
klhogan@mit.edu

Sacha Servan-Schreiber
3s@mit.edu

Zack Newman
zjn@mit.edu

Ben Weintraub
weintraub.b@northeastern.edu

Cristina Nita-Rotaru
c.nitarotaru@northeastern.edu

Srinivas Devadas
devadas@mit.edu

ShorTor is a **routing overlay** for the Tor network that **reduces latency** between relays on a circuit while **maintaining Tor's security** guarantees.

ShorTor: Roadmap

Multi-hop overlay routing:

- ➔ in the wild
- ➔ on Tor?

Security of ShorTor:

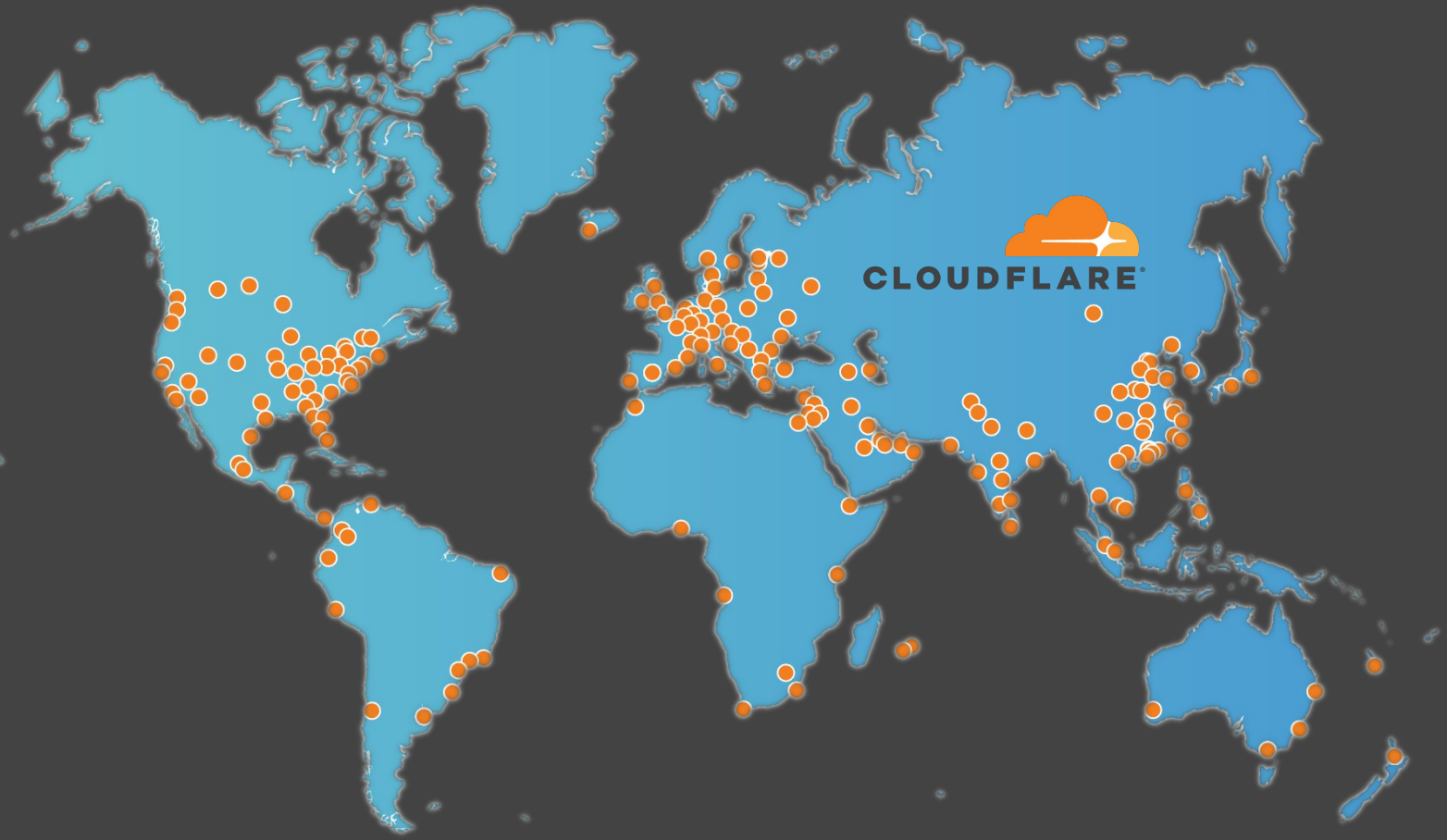
- ➔ via selection
- ➔ adversarial advantage

Performance of ShorTor:

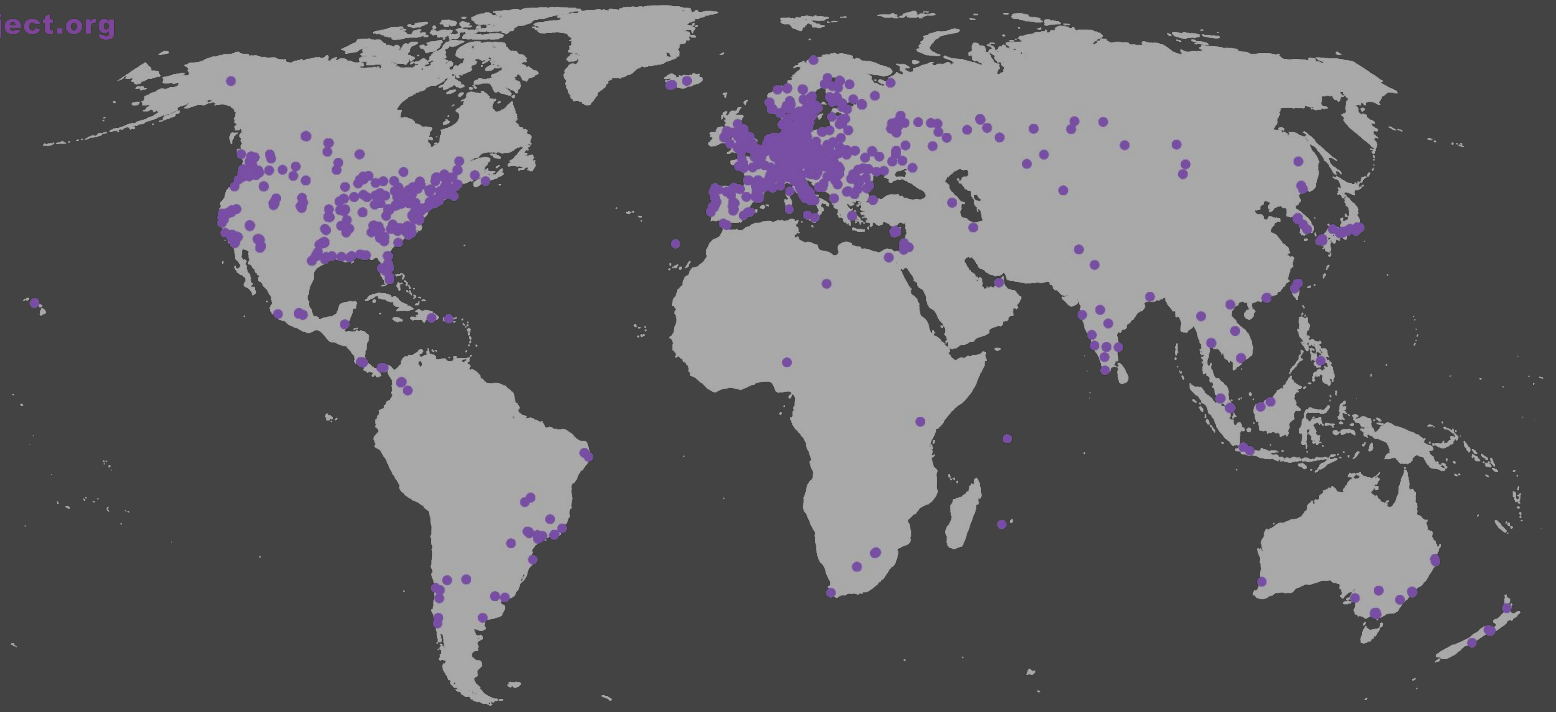
- ➔ measured latency
- ➔ page load times

Multi-hop Overlay Routing


Argo Smart Routing
Congestion Avoidance
Routing decisions using
real-time network conditions
User
Origin
CLOUDFLARE
Cloudflare Data Center
Internet node / hop

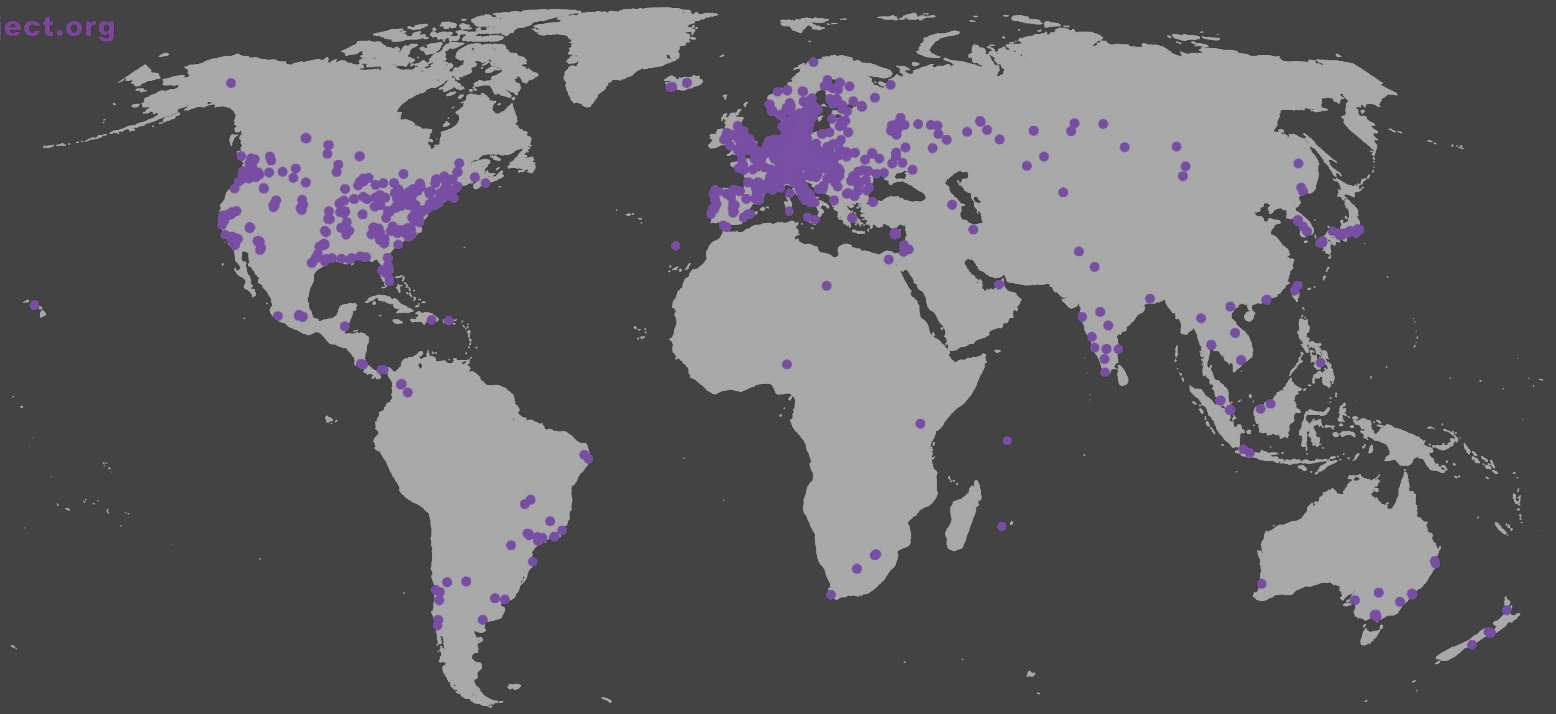

CLOUDFLARE

TorProject.org



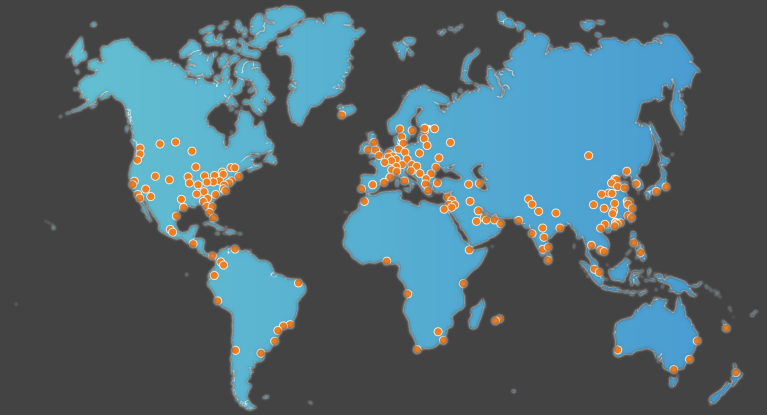
Tor is *also* a widely distributed network that routes traffic around the globe

TorProject.org



Can Tor benefit from multi-hop overlay routing?

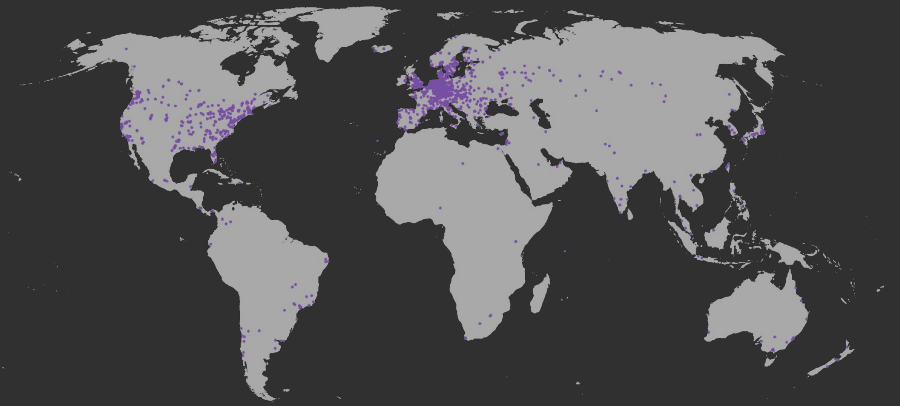
Cloudflare



(very) large scale

- ➔ 270 datacenters in 100+ countries
- ➔ 142 Tbps

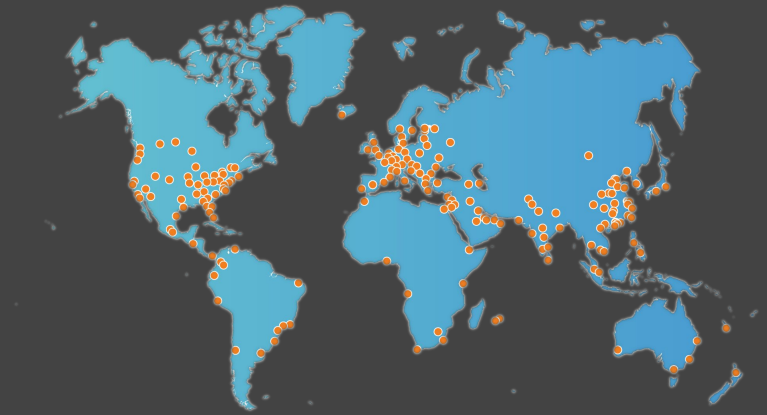
Tor



(relatively) small scale

- ➔ 7000 servers in 81 countries
- ➔ 700 Gbps

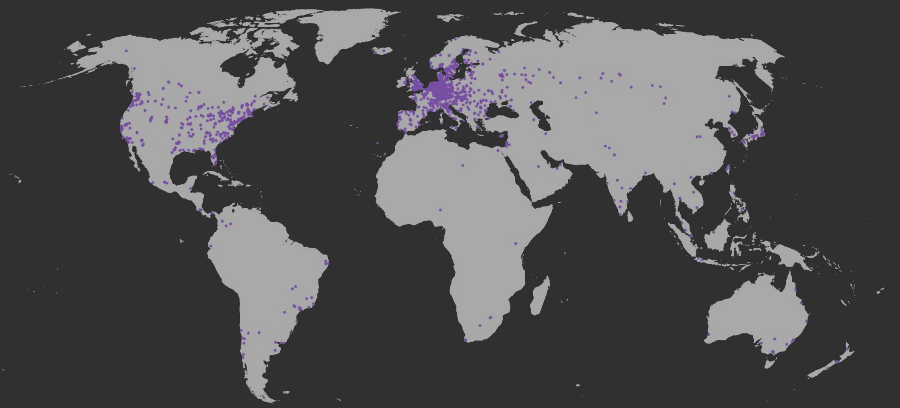
Cloudflare



Optimized server placement

➔ directly connected to **10,500** networks

Tor



Volunteer run servers

➔ relays in **1028** autonomous systems

Tor's network is **substantially smaller** than a CDN and is **not optimized** for fast routing

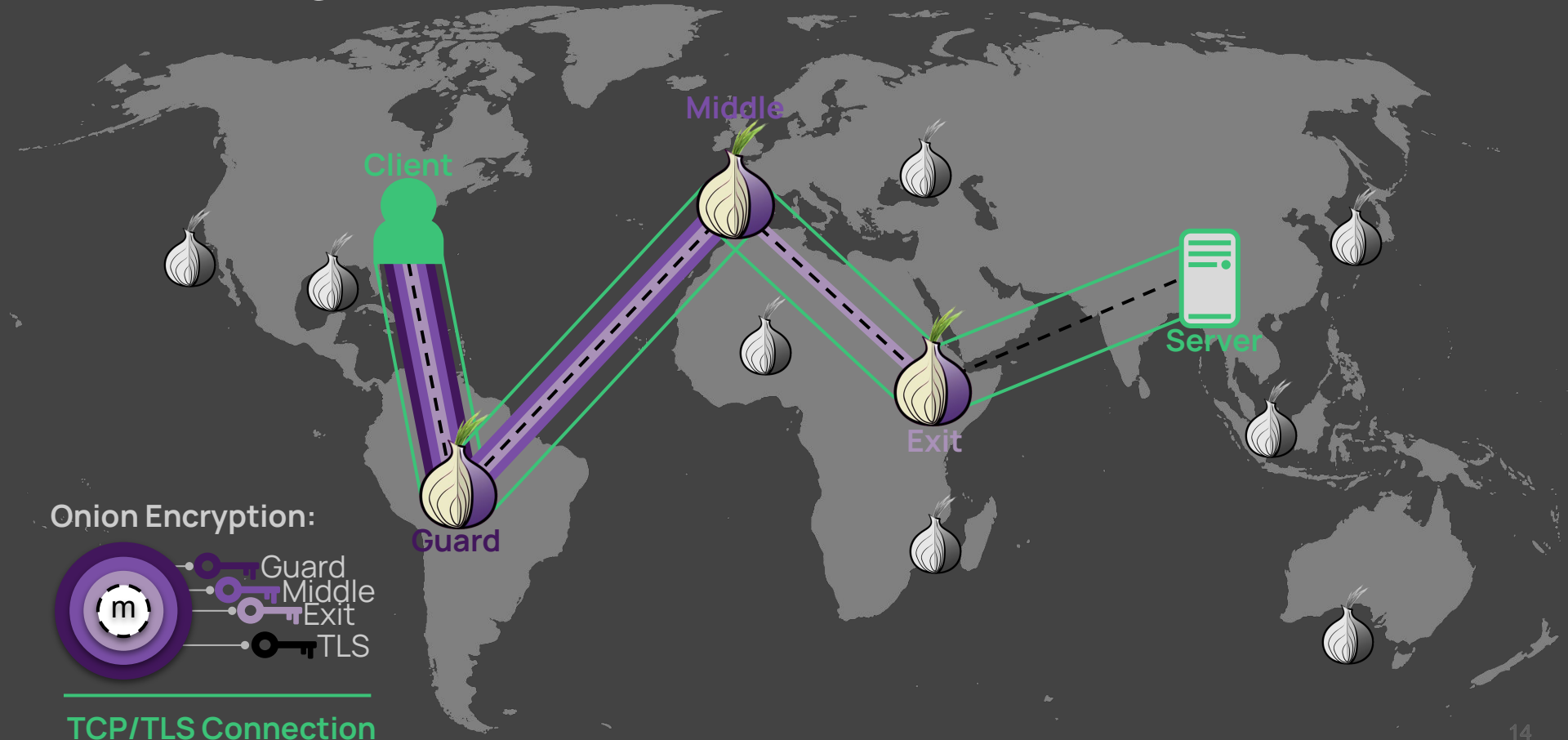
Tor's network is **substantially smaller** than a CDN and is **not optimized** for fast routing

but it can still see **substantial reduction in tail latency** using multi-hop overlay routing

ShorTor

multi-hop overlay routing on the Tor network

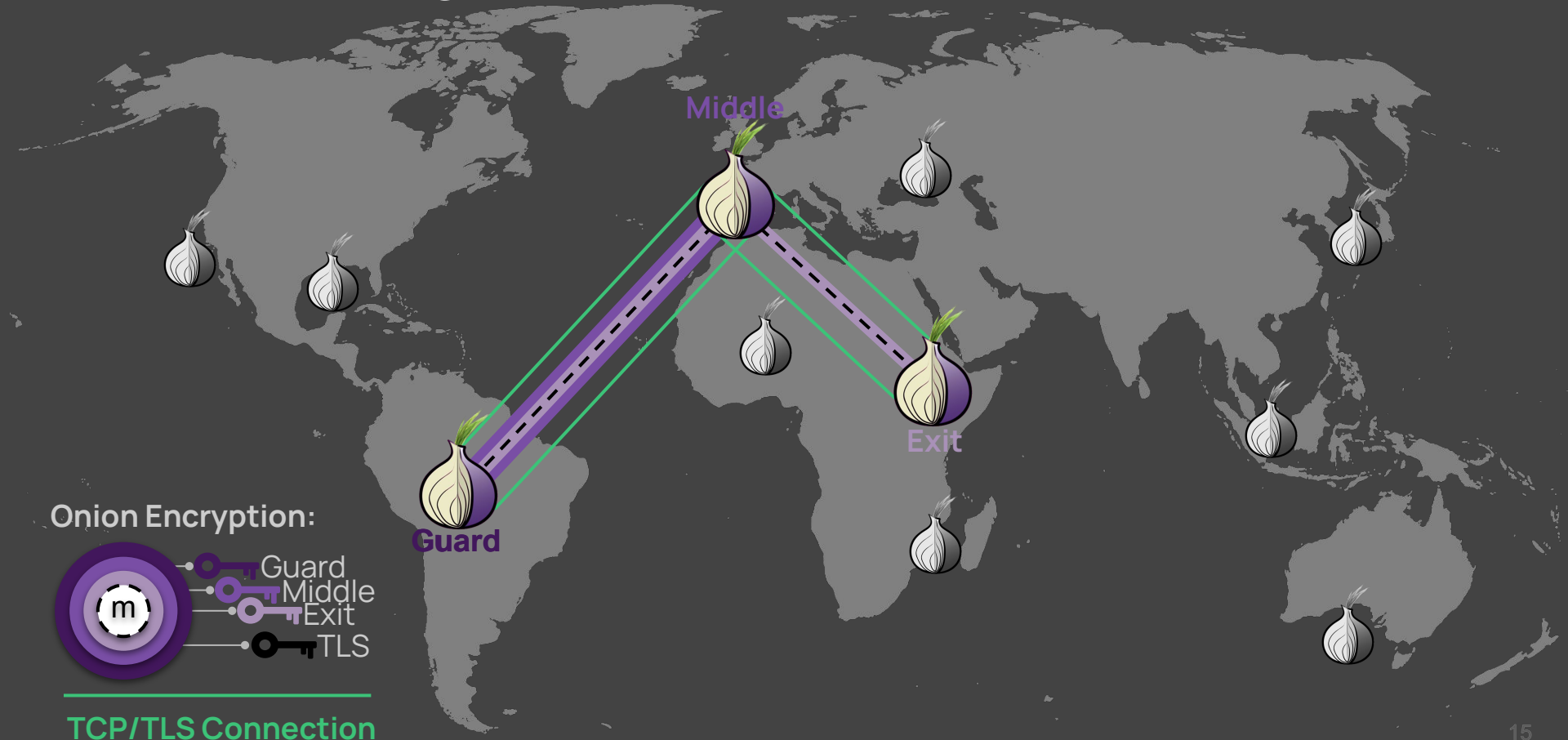
Tor routing without ShorTor: already an overlay!



Onion Encryption:

TCP/TLS Connection

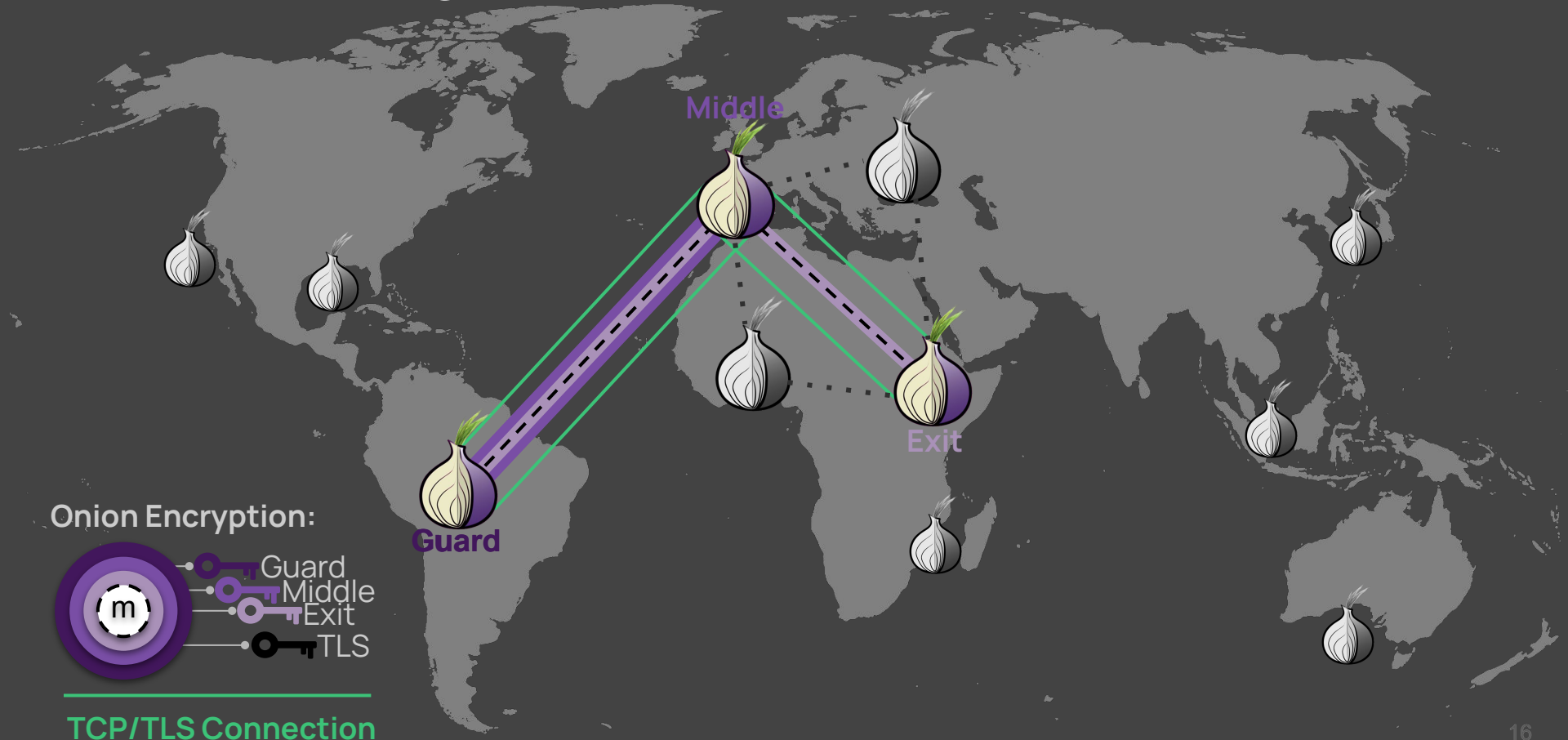
ShorTor routing: between relays *only*



Onion Encryption:

TCP/TLS Connection

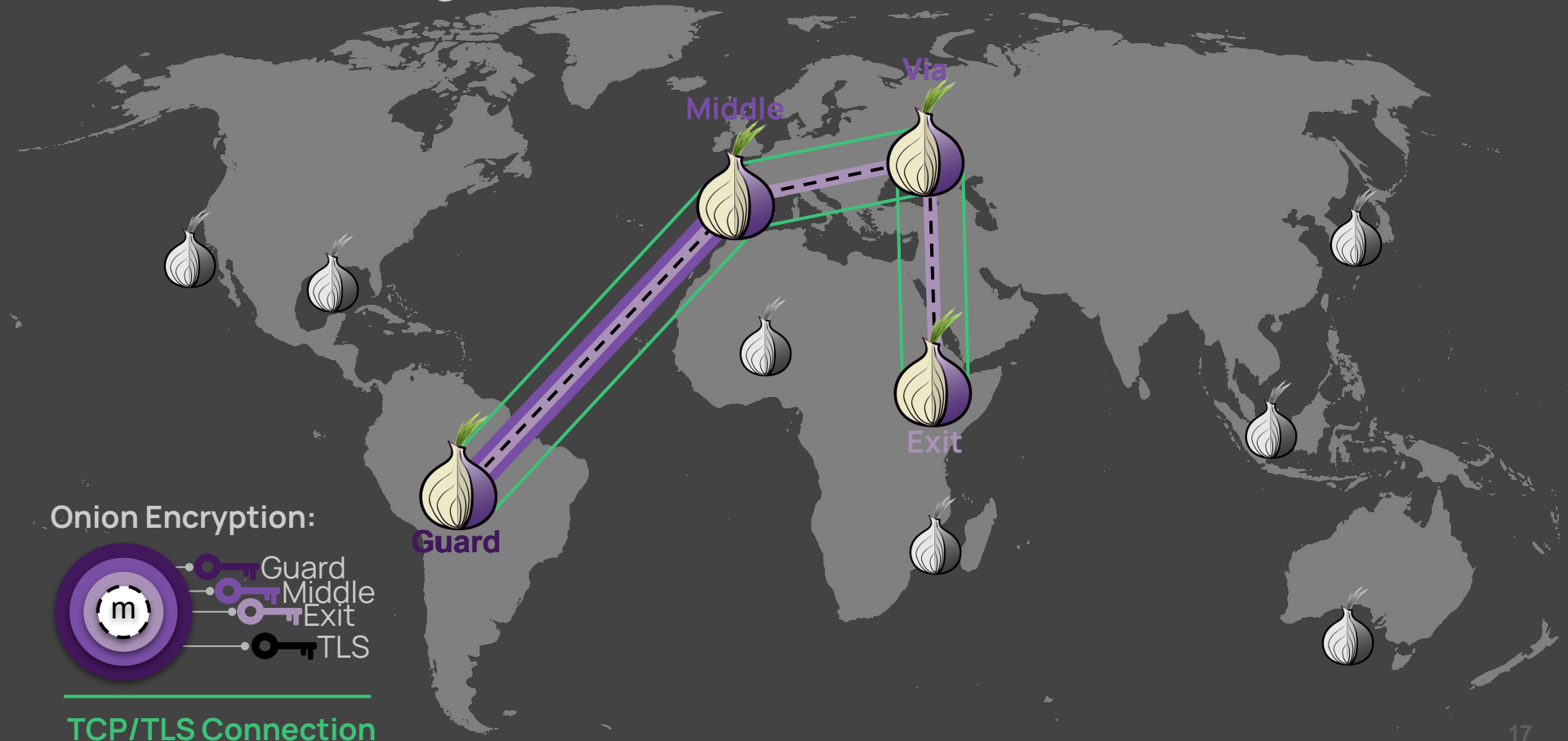
ShorTor routing: test alternative routes



Onion Encryption:

TCP/TLS Connection

ShorTor routing: select the fastest



Onion Encryption:

TCP/TLS Connection

Security

anonymity & adversarial relays

ShorTor: client anonymity

Server-side **only**:

- ➔ applied to **pre-existing** circuits
- ➔ via selection is dependent on relay location, **not client location**

ShorTor gives adversarial relays **no advantage** in distinguishing individual Tor clients.

ShorTor: traffic analysis by adversarial vias

Client identity is not the only anonymity concern in Tor:

➔ adversarial relays may use **traffic analysis** to learn which website is visited

ShorTor: traffic analysis by adversarial vias

Client identity is not the only anonymity concern in Tor:

➔ adversarial relays may use **traffic analysis** to learn which website is visited

Goal: relays cannot **artificially increase** the probability they are chosen as a via

ShorTor: traffic analysis by adversarial vias

Client identity is not the only anonymity concern in Tor:

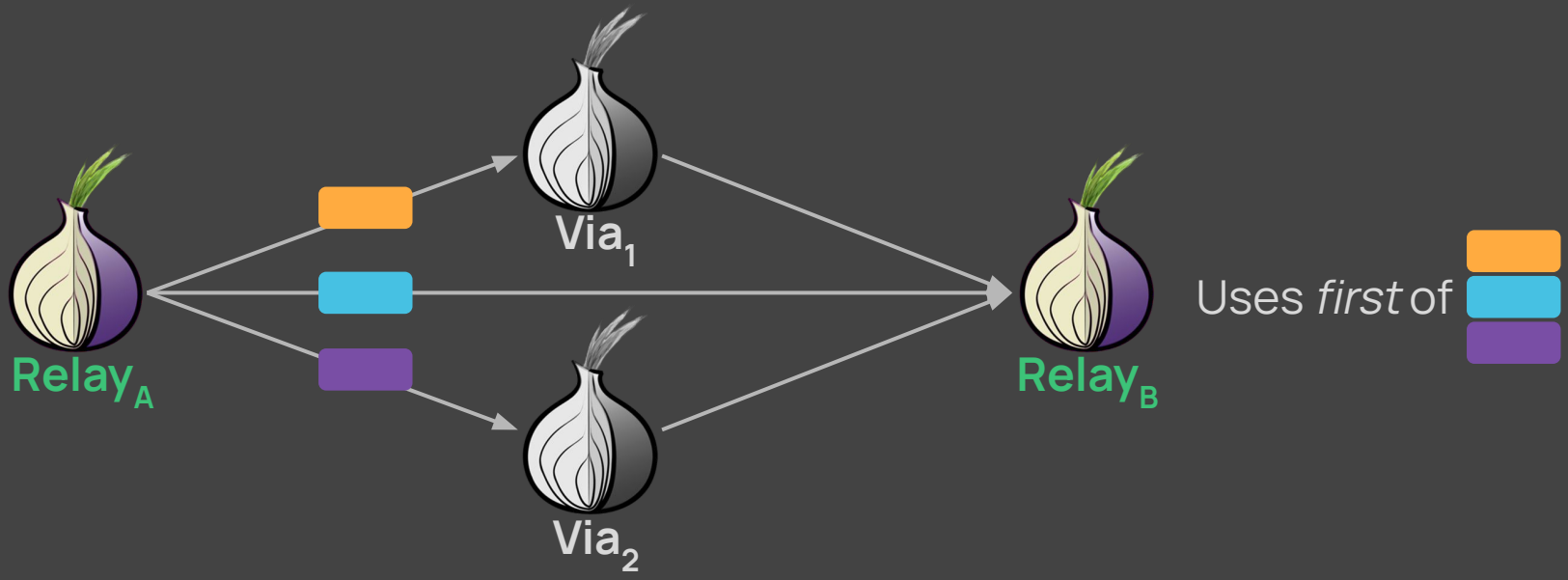
➔ adversarial relays may use **traffic analysis** to learn which website is visited

Goal: relays cannot **artificially increase** the probability they are chosen as a via

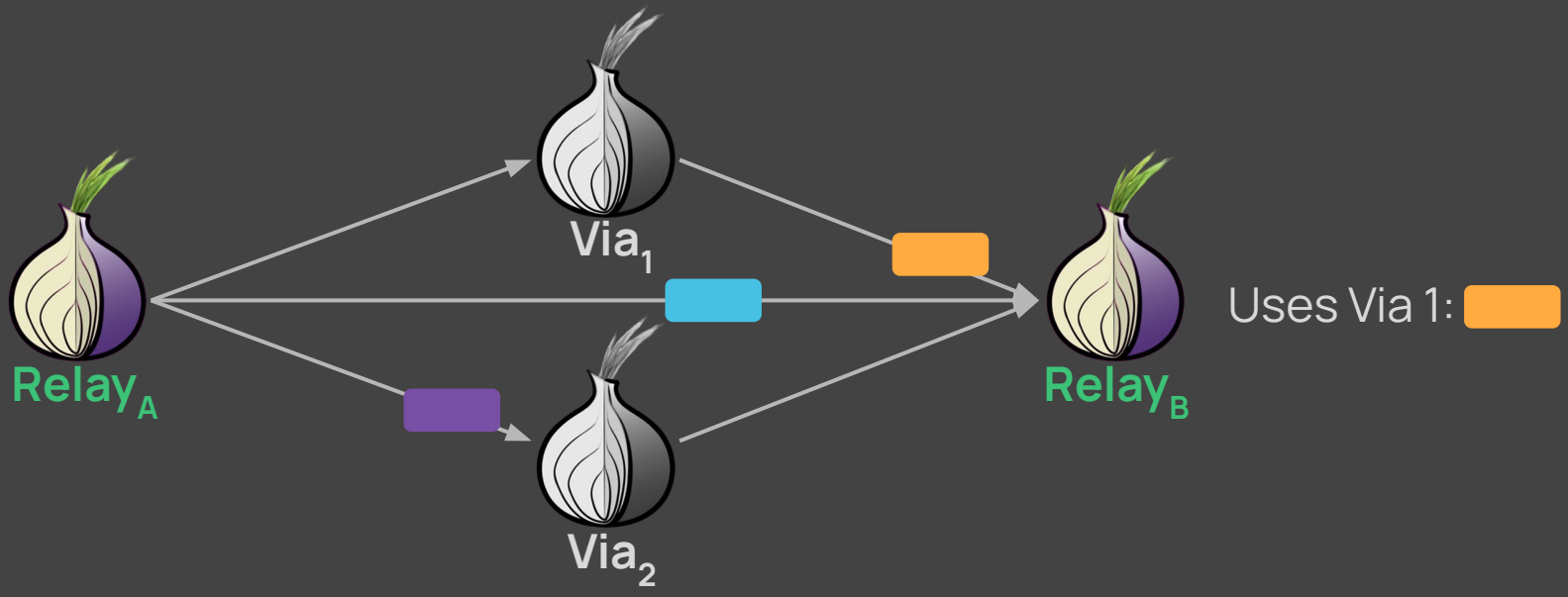
Adversarial vias:

- ➔ selection probability based on measured latency, **not reported latency**
- ➔ adversarial relays must be **fast** to increase odds
- ➔ how? **data races**

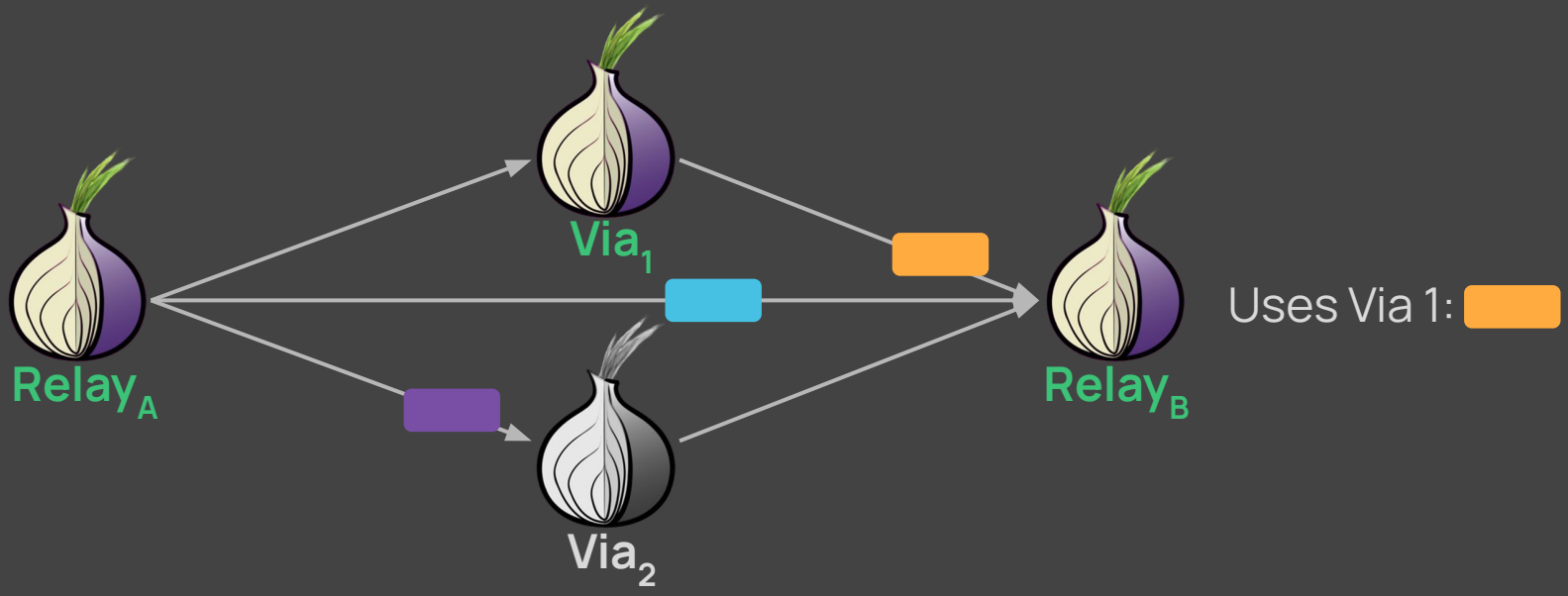
Data Races: via selection



Data Races: via selection



Data Races: via selection



No clock synchrony assumption! Vias are only able to win by **actually** having lowest latency

In ShorTor, relays **cannot forge** their latency:

Reduced latency increases probability of selection as a **via relay**,
higher capacity increases probability of selection as a **circuit relay**.

In ShorTor, relays **cannot forge** their latency:

Reduced latency increases probability of selection as a **via relay**,
higher capacity increases probability of selection as a **circuit relay**.

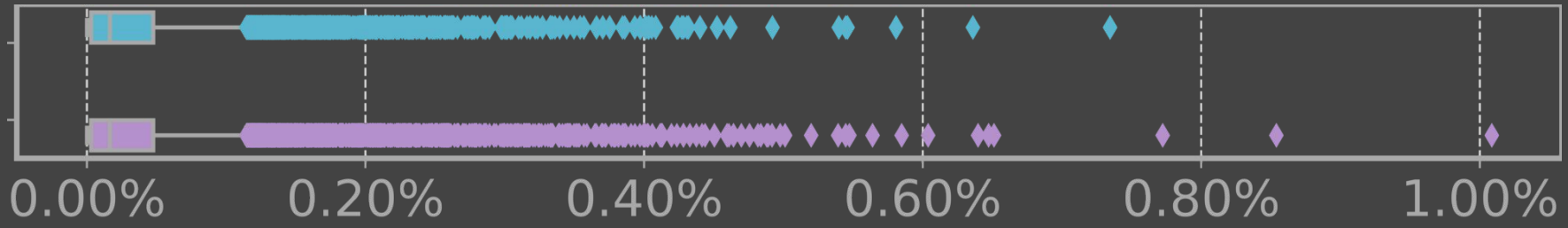
Increased selection probability correspondingly increases the
total fraction of Tor traffic that a relay can observe.

Adversarial Vias: global network share

What fraction of client circuits can a relay observe in **baseline Tor** vs. **ShorTor**?

Adversarial Vias: global network share

What fraction of client circuits can a relay observe in **baseline Tor** vs. **ShorTor**?

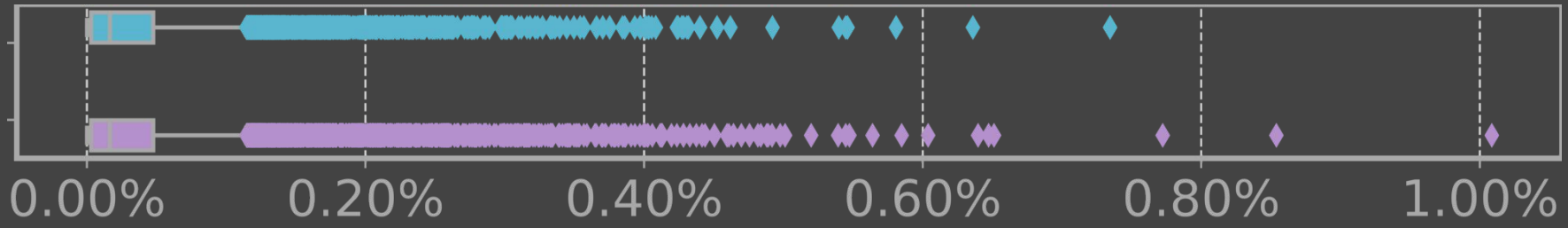


maximum network share held by an **individual** relay: **0.7%** vs **1.0%**

based off 2M circuits selected according to Tor's path selection algorithm

Adversarial Vias: global network share

What fraction of client circuits can a relay observe in **baseline Tor** vs. **ShorTor**?



maximum network share held by an **individual** relay: **0.7%** vs **1.0%**

total network share of **all** relays in
Germany: **1.1%** vs **1.4%**
FVEY: **0.45%** vs **0.47%**

based off 2M circuits selected according to Tor's path selection algorithm

Performance

reduced tail latencies on the Tor network

Evaluating ShorTor: measured latency

Evaluating a routing protocol like ShorTor requires **real network conditions**.

Problem 1: ShorTor is server-side and we don't own (many) Tor relays

Problem 2: the Tor network doesn't look much like the regular internet

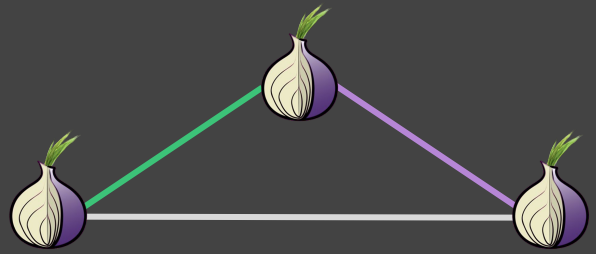
Evaluating ShorTor: measured latency

Evaluating a routing protocol like ShorTor requires **real network conditions**.

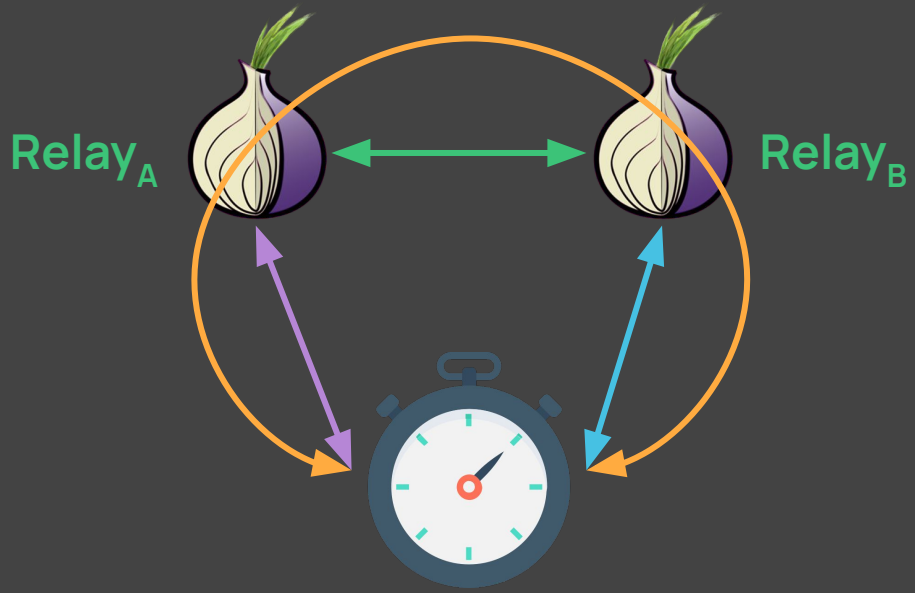
Problem 1: ShorTor is server-side and we don't own (many) Tor relays

Problem 2: the Tor network doesn't look much like the regular internet

Solution: measure **round trip times between Tor relays** we don't control and use these measurements to **find triangle inequalities**



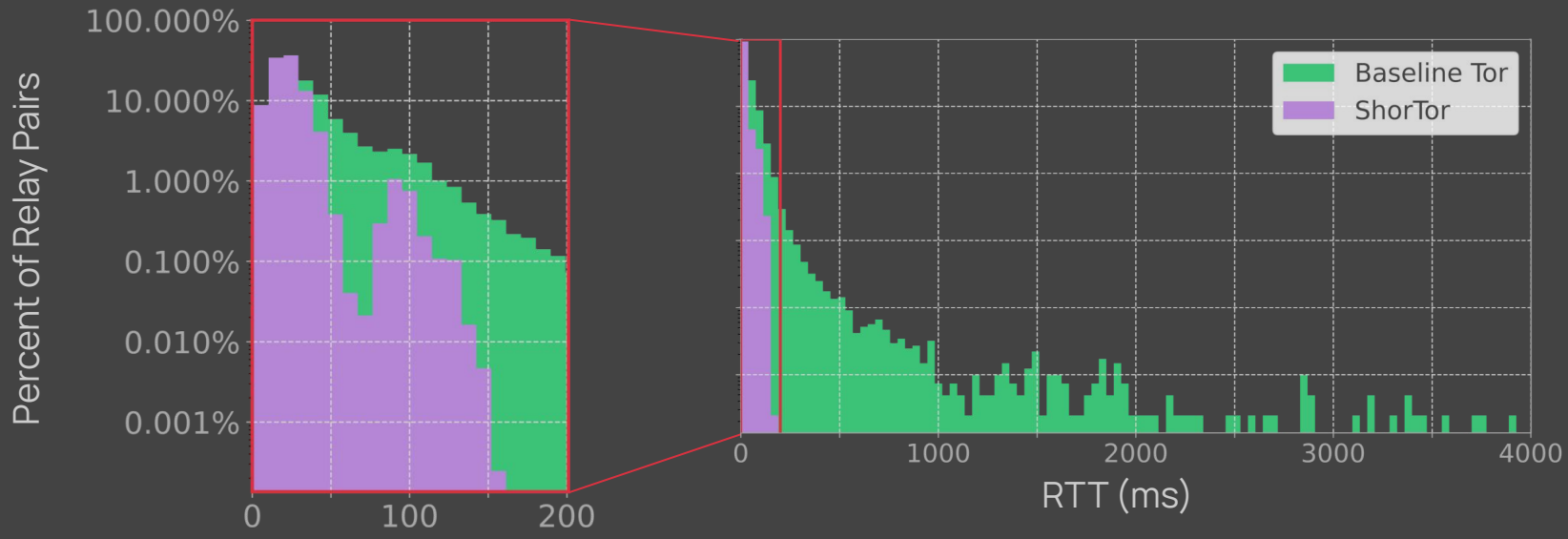
Measured Latency: 400k pairs of 1000 largest relays



$$\text{Relay}_A \longleftrightarrow \text{Relay}_B = \text{RTT}_{AB} - (\text{RTT}_A + \text{RTT}_B)/2$$

Frank Cangialosi, Dave Levin, and Neil Spring. "Ting: Measuring and exploiting latencies between all Tor nodes." *IMC* 2015.

Measured Latency: 400k pairs of 1000 largest relays



Percent of relays pairs seeing a given RTT in Baseline Tor vs. ShorTor

Page Load Times: impact of RTT on user experience

Loading a webpage involves **many** round trips.

When loading `nytimes.com` over Tor:

50 ms network delay caused **1.66 s** increase in PLT
100 ms network delay caused **2.34 s** increase in PLT
150 ms network delay caused **15.80 s** increase in PLT

Page Load Times: impact of RTT on user experience

Loading a webpage involves **many** round trips.

When loading `nytimes.com` over Tor:

(5.04% of ShoTor circuits) 50 ms network delay caused **1.66 s** increase in PLT
(1.66% of ShoTor circuits) 100 ms network delay caused **2.34 s** increase in PLT
(0.04% of ShoTor circuits) 150 ms network delay caused **15.80 s** increase in PLT

Tor sees **~2M daily users**, each building at least one circuit.

based off 2M circuits selected according to Tor's path selection algorithm

ShorTor is a **server-side routing overlay** for the Tor network that **reduces tail latencies** while **maintaining anonymity**.

Absent from this talk:

Incremental deployment:

➔ ShorTor works pretty well even with relatively low support

MATor security analysis:

➔ ShorTor exacerbates anonymity loss from location aware path selection

Integration with Tor:

➔ ShorTor is minimally invasive and low overhead

ShorTor is a **server-side routing overlay** for the Tor network that **reduces tail latencies** while **maintaining anonymity**.

Questions?

Kyle Hogan (klhogan@mit.edu)