

Poking a Hole in the Wall: Efficient Censorship-Resistant Internet Communications by Parasitizing on WebRTC

Diogo Barradas

Nuno Santos

Luís Rodrigues

Vítor

Nunes

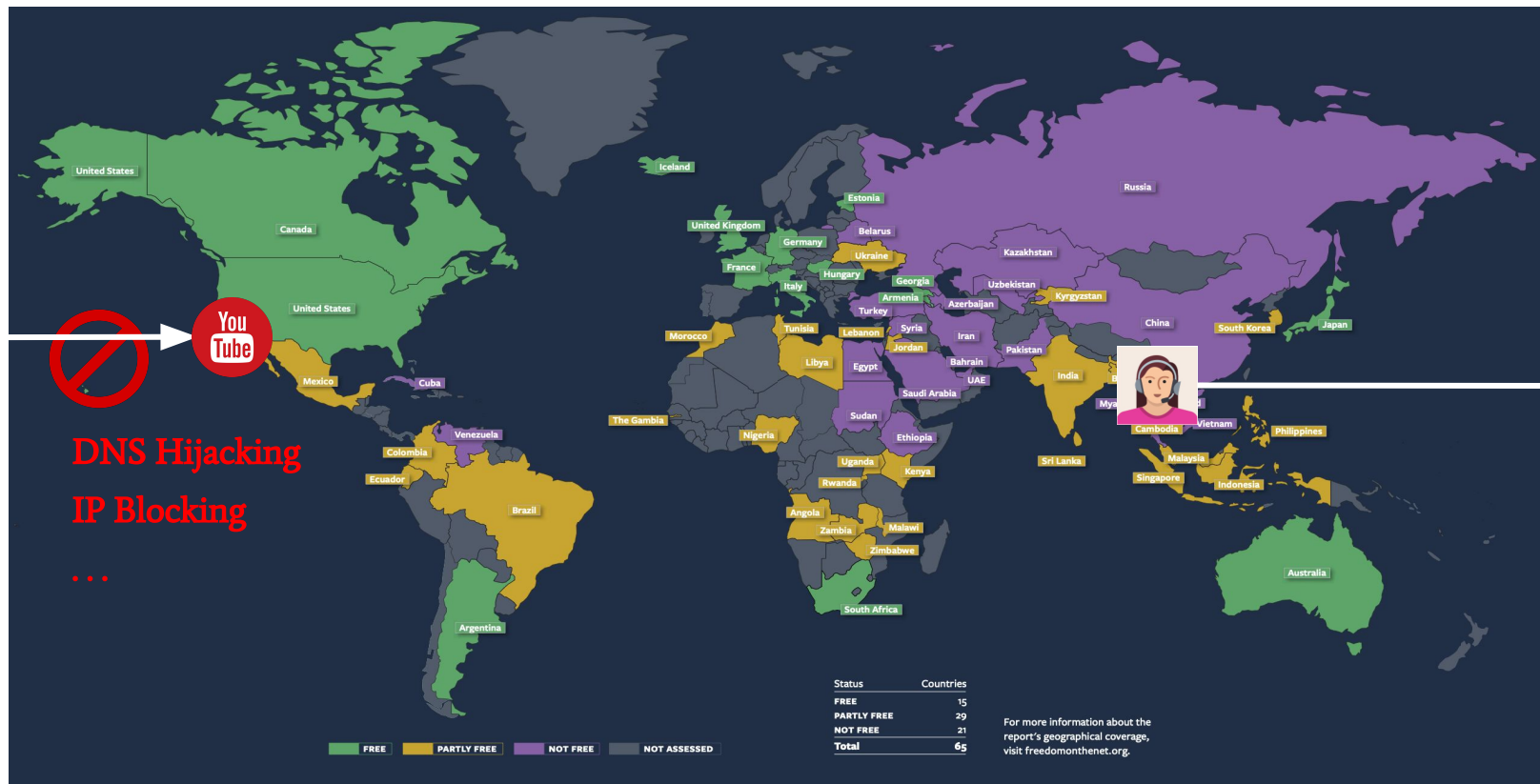
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa



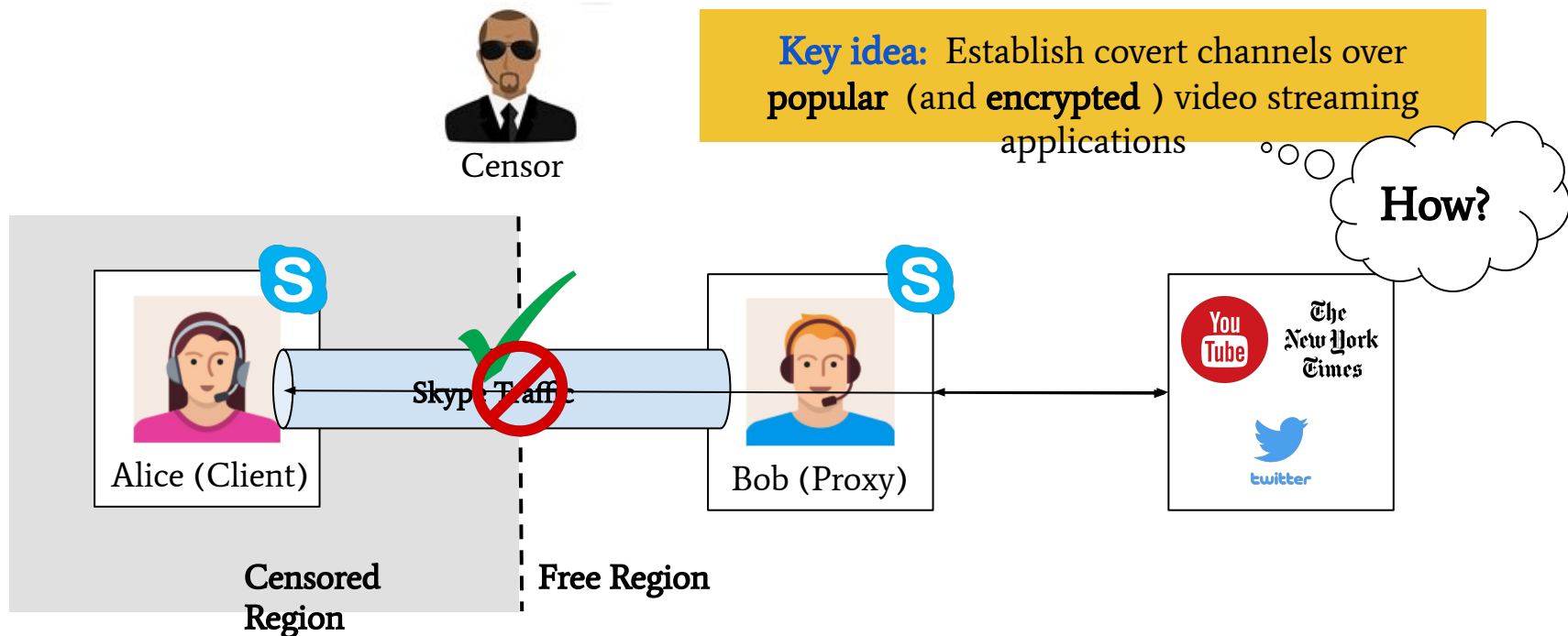
Diogo Barradas, ACM SIGSAC CCS '20



Internet censorship is widespread across the world

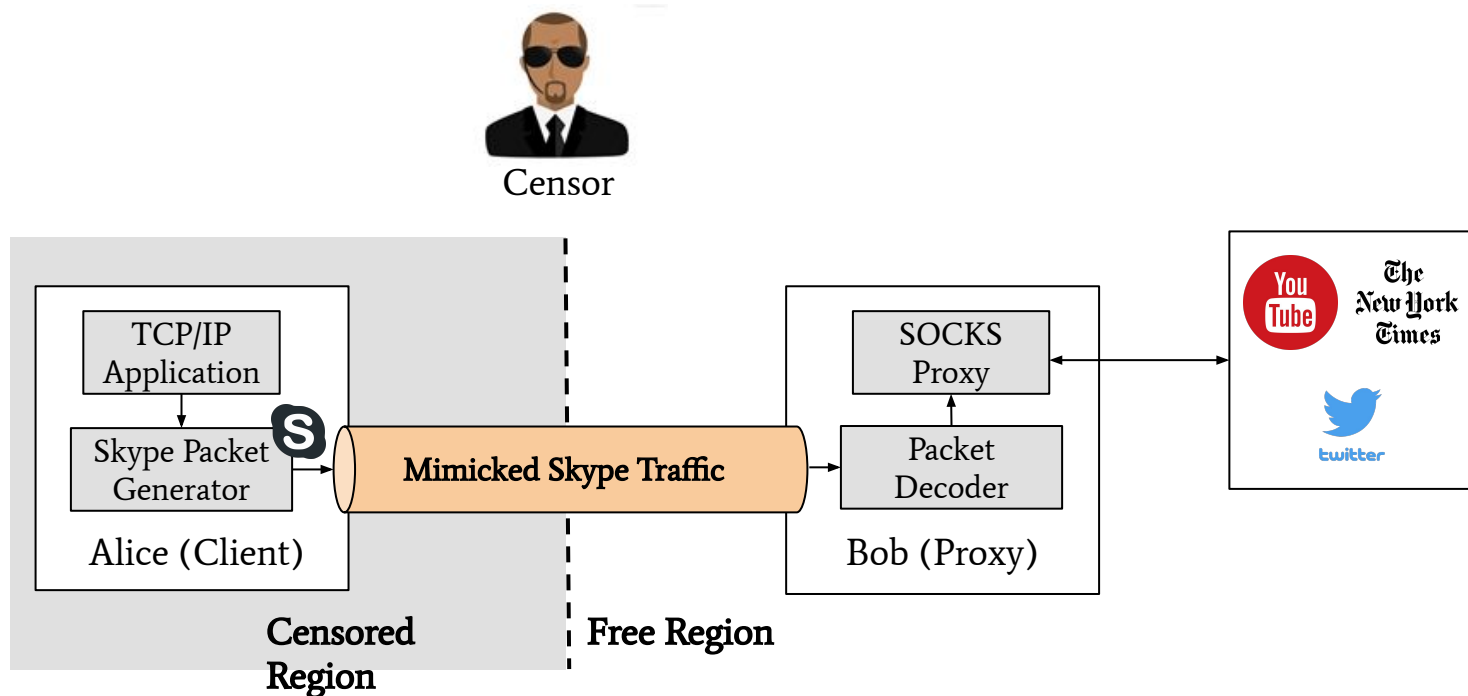


Bypassing censorship with video streams



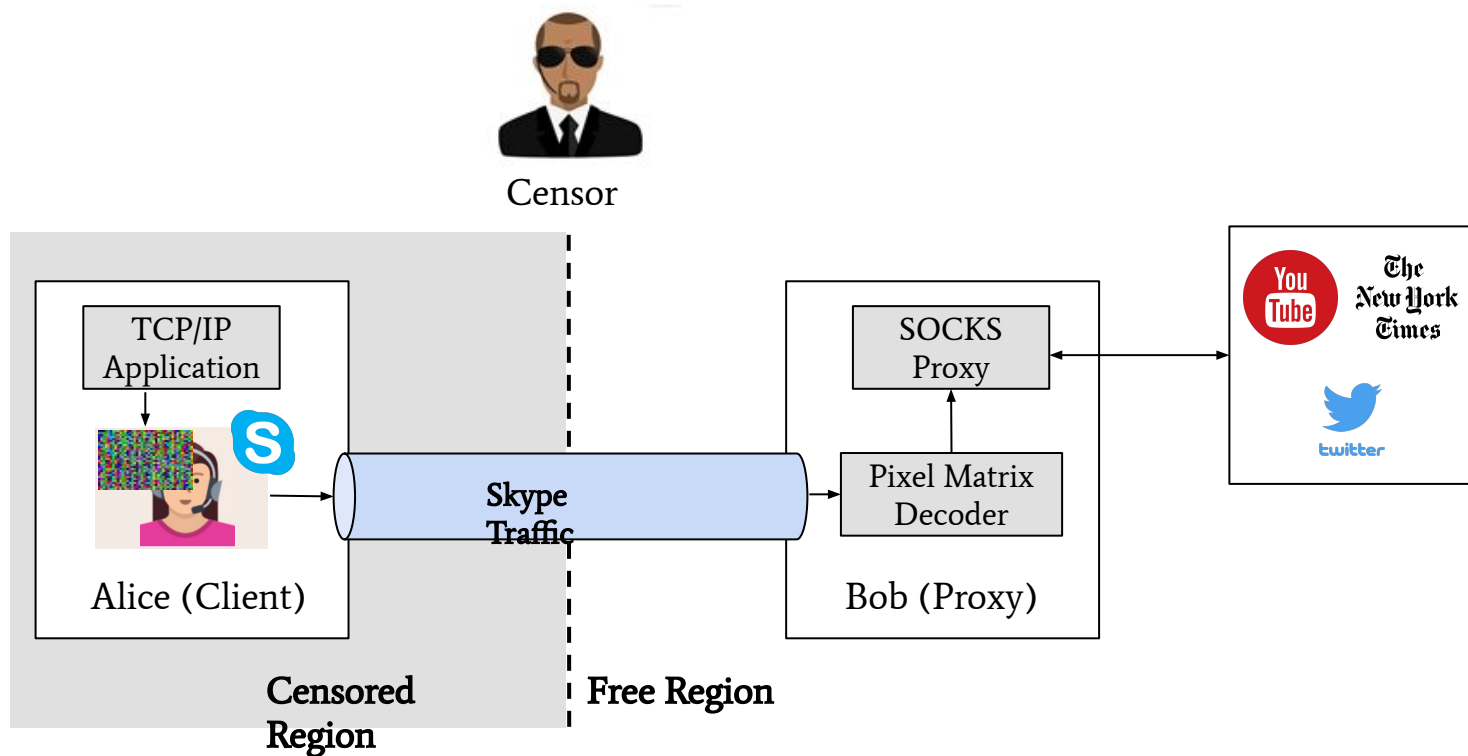
High Throughput / Not secure

Multimedia Protocol Mimicking
e.g. SkypeMorph [CCS'12]

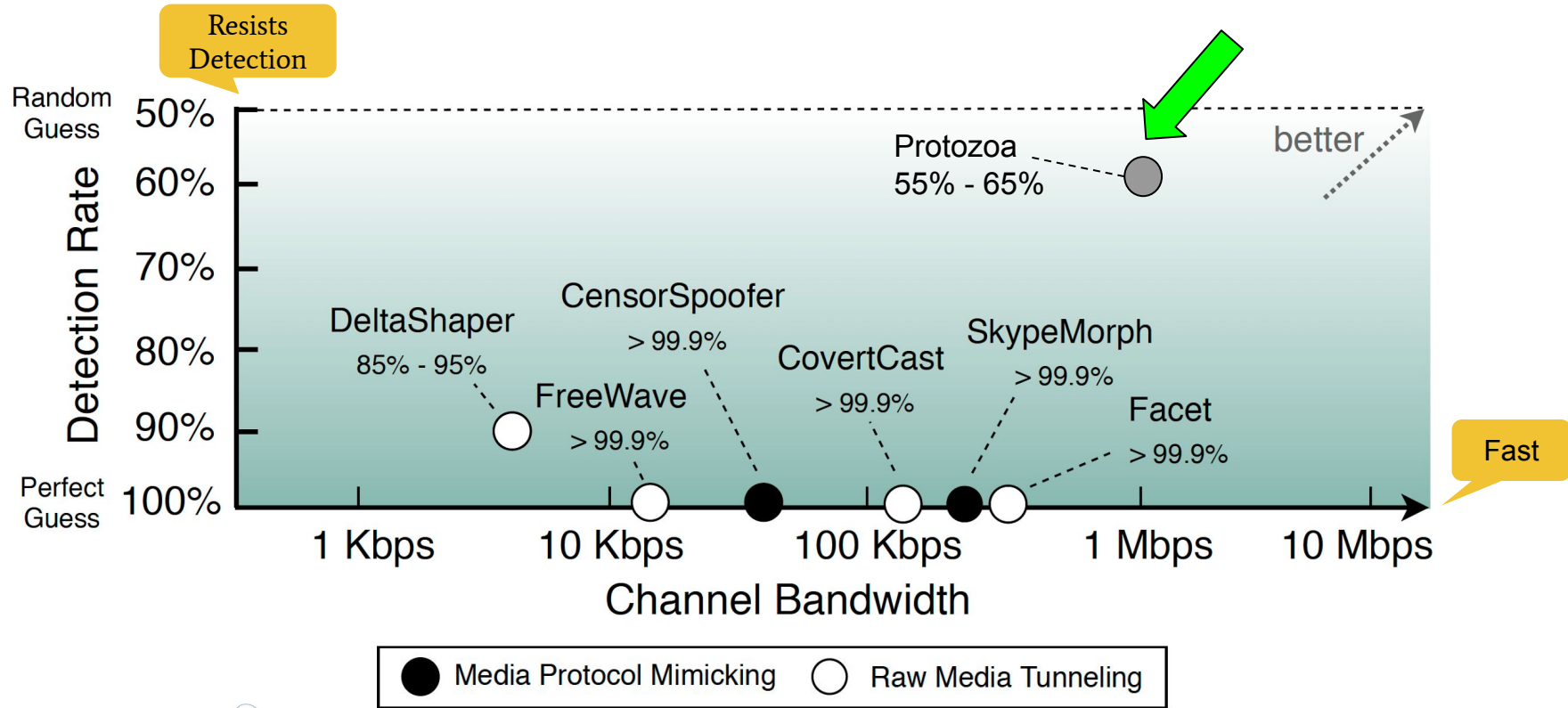


Reasonable Security / Low Throughput

Multimedia Protocol Tunnelling
e.g. DeltaShaper [PETS'17]



Protozoa: High Throughput / Secure



Protozoa's Contributions

- First to leverage **WebRTC video streams** for creating covert channels
 - Allows for the tunneling of arbitrary TCP/IP traffic
- Introduces a new encoding mechanism: **Encoded media tunneling**
 - Instruments the media pipeline in WebRTC stack to replace encoded video
- Works over a range of existing **unmodified WebRTC apps** (e.g., Whereby)
 - Deployed against real censors (China, Russia, India)

Why WebRTC?

- Framework that provides real-time communication capabilities
 - Exposes a set of JavaScript APIs on all major browsers
 - Used by an increasing number of trending applications
 - Open-source



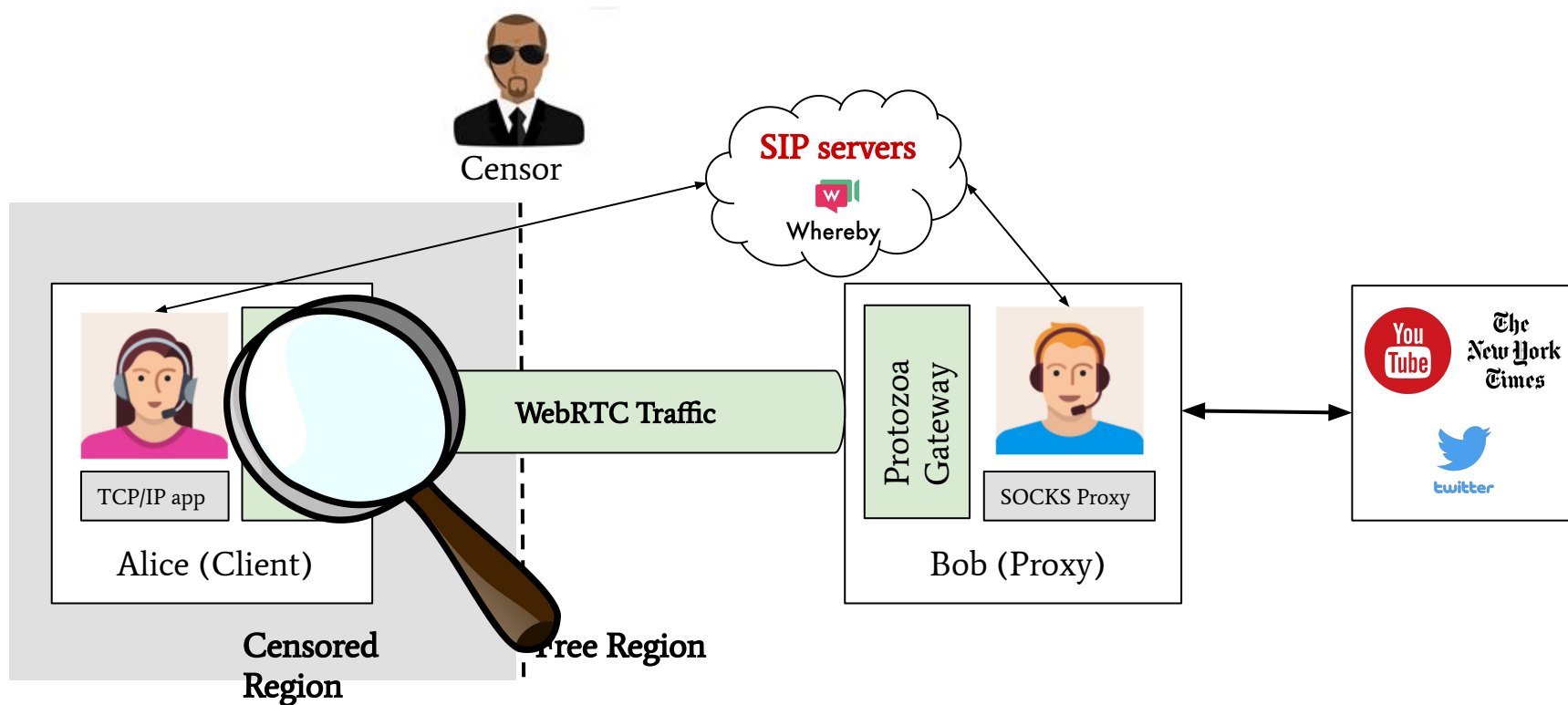
Whereby



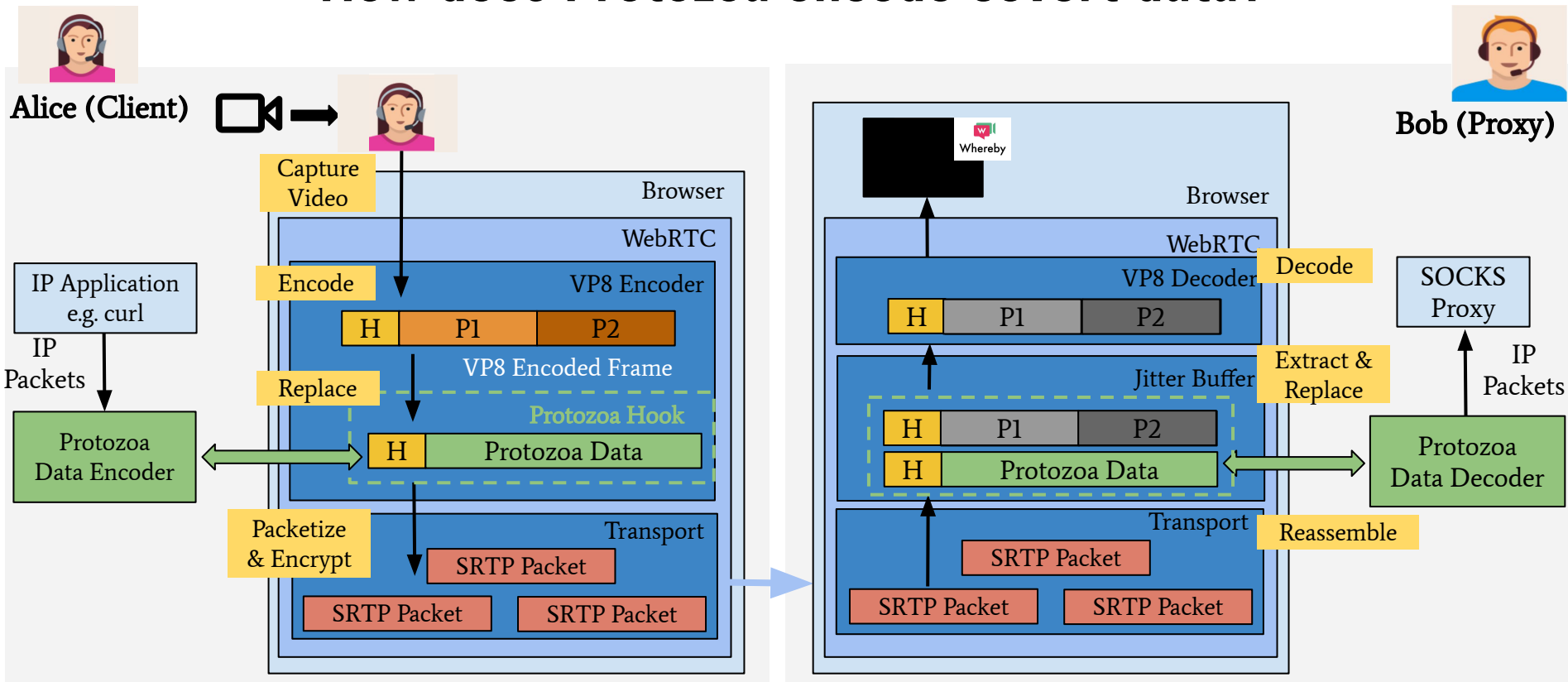
Diogo Barradas, ACM SIGSAC CCS '20



Protozoa's Communication Model



How does Protozoa encode covert data?



Evaluation

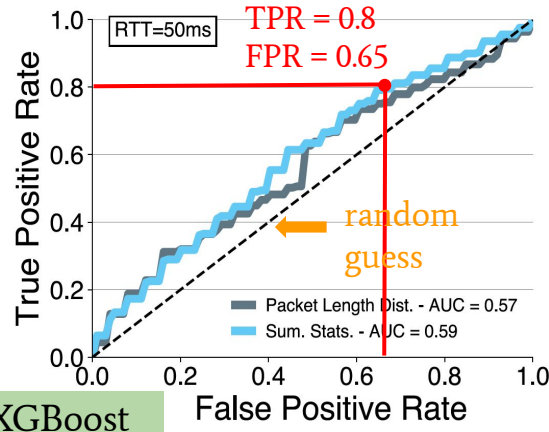
- Varying network conditions
- Varying video profiles
- Varying WebRTC carrier applications

Baseline configuration

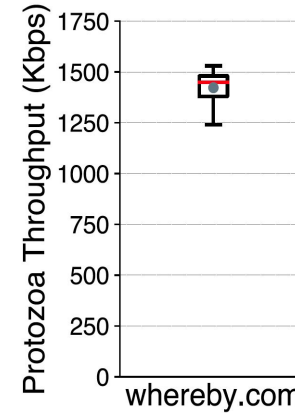
Intra-continental connection (50ms
RTT)
Chat video profile
Whereby.com

Baseline Evaluation

Check the paper for our comprehensive evaluation!



Protozoa is largely indistinguishable from legitimate WebRTC video streams

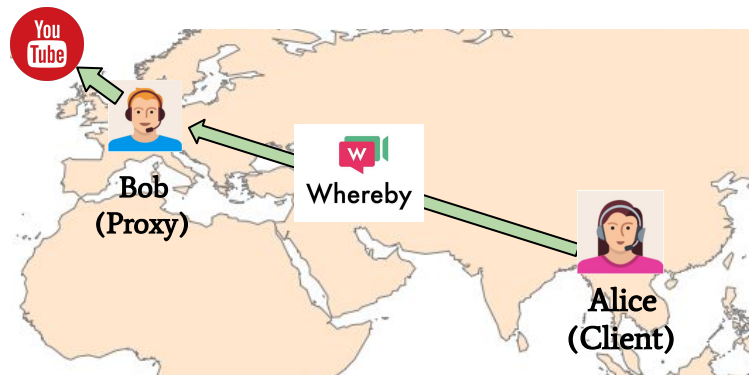


Protozoa achieves up to 1.4Mbps tput (w/ channel efficiency of 99%)

Validation in the Real-World

WebRTC Application	Reachability		
	China	Russia	India
appr.tc	-	✓	✓
aws.amazon.com/chime	✓	✓	✓
codassium.com	✓	✓	✓
coderpad.io	✓	✓	✓
discordapp.com	-	✓	✓
gotomeeting.com	✓	✓	✓
hangouts.google.com	-	✓	✓
messenger.com	-	✓	✓
slack.com	✓	✓	✓
whereby.com	✓	✓	✓

Multiple WebRTC apps are available in countries known to experience Internet censorship



Protozoa makes it possible to access blocked content / services (e.g. YouTube)

Conclusions

- **Protozoa** - a new censorship-resistant system
- Leverages **WebRTC video streams** to tunnel arbitrary TCP/IP traffic
- Introduces a new technique: **Encoded media tunneling**
- Operates over **multiple WebRTC applications**

Our code is available!

`https://github.com/dmbb/protozoa`

Thank You!

`https://web.ist.utl.pt/diogo.barradas`