

Measuring DNS-over-HTTPS Performance Around the World

Rishabh Chhabra, et. Al.
University of Illinois at Urbana-Champaign

IMC '21

Presenter: Junghwan Song

Outline

- Introduction
- Methodology
- Measurement results
- Conclusion

Introduction

- Transition from traditional (unencrypted) DNS to privacy-preserving alternative: Do53 to DoT/DoH
 - Do53: traditional DNS protocol using port 53
 - DoT: DNS-over-TLS
 - DoH: DNS-over-HTTPS

Firefox continues push to bring DNS over HTTPS by default for US users

FEBRUARY 25, 2020 SELENA DECKELMANN

DNS over TLS support in Android P Developer Preview

April 17, 2018

Apple adds support for encrypted DNS (DoH and DoT)

Apple said this week that iOS 14 and macOS 11 will support the DNS-over-HTTPS and DNS-over-TLS protocols.



Written by Catalin Cimpanu, Contributor on June 25, 2020

Microsoft Edge tests fix for DNS-over-HTTPS performance issues

By [Mayank Parmar](#)

March 20, 2021 12:44 PM 0

Chrome 83: rollout of DNS over HTTPS (Secure DNS) begins

MARTIN BRINKMANN May 20, 2020

Google Chrome | 16

DoT v.s. DoH

	DoT	DoH
Supports	<p>OS level support</p> <ul style="list-style-type: none">- Hard to update protocol	<p>App level support</p> <ul style="list-style-type: none">+ App update → protocol update
Port	<p>Port 853 (DoT)</p> <ul style="list-style-type: none">- DNS query, response are exposed by port number+ Easy to block suspicious DoT messages for network operators	<p>Port 443 (HTTPS)</p> <ul style="list-style-type: none">+ Cannot distinguish DoH with HTTPS messages by port number → better user privacy- Either for network operators

Existing works

■ **Can Encrypted DNS Be Fast?**

Austin Hounsel¹(✉), Paul Schmitt¹, Kevin Borgolte², and Nick Feamster³

¹ Princeton University, Princeton, NJ 08544, USA

{ahounsel,pschmitt}@cs.princeton.edu

² TU Delft, 2628 BX Delft, The Netherlands

k.borgolte@tudelft.nl

³ University of Chicago, Chicago, IL 60637, USA

feamster@uchicago.edu

Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web

Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, Nick Feamster

Princeton University

{ahounsel,borgolte,pschmitt,jordanah,feamster}@cs.princeton.edu

An Empirical Study of the Cost of DNS-over-HTTPS

Timm Böttger, Felix Cuadrado, Gianni Antichi, Eder Leão Fernandes,

Gareth Tyson, Ignacio Castro and Steve Uhlig

Queen Mary University of London

- Lacks of global perspective
- Or including other delays (middleboxes, etc.)

Global scale measurements



We wanted to compare DNS-over-UDP (Do53) with DNS-over-HTTPS (DoH) for as many countries as possible

Global scale measurements



We wanted to compare DNS-over-UDP (Do53) with DNS-over-HTTPS (DoH) for as many countries as possible

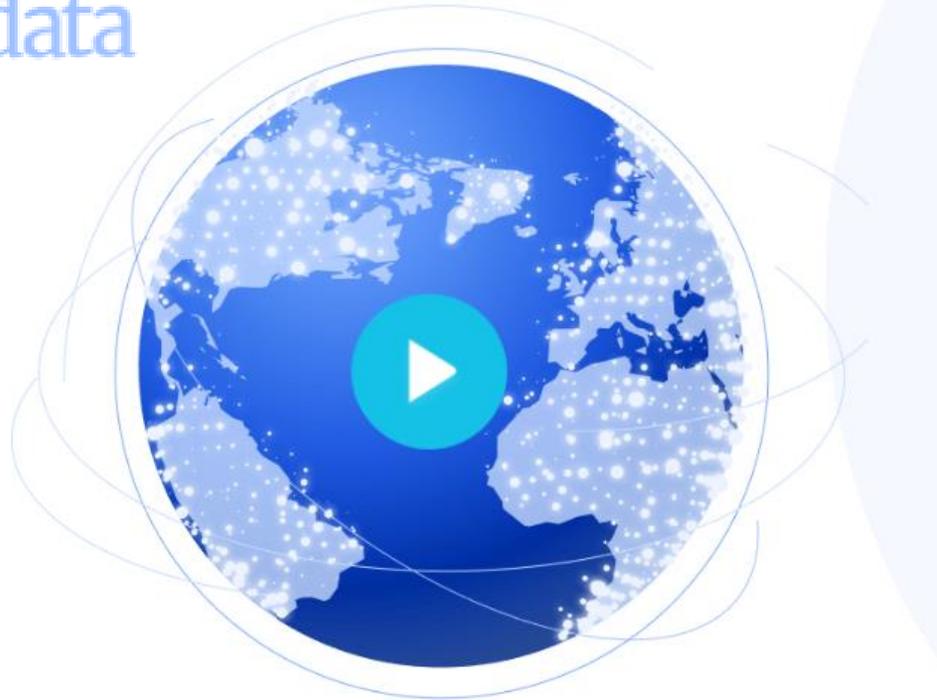
Core questions

- Performance impact of a switch from traditional Do53 or DoH
- Differences across countries and geographical regions
- External factors or variables
- Gap between architecture and performance

Methodology

Obtaining data with “bright data”

bright data



 **RESIDENTIAL PROXY NETWORK**

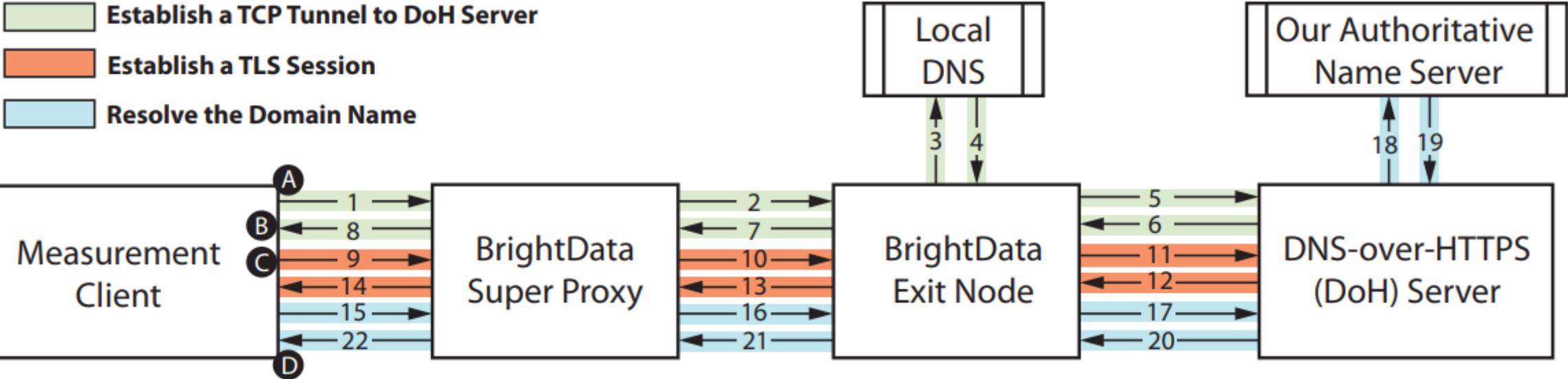
Real Residential Proxies

Avoid restrictions and blocks with the fastest residential proxy network in the industry

- ✓ Target any country, city, carrier & ASN
- ✓ 99.99% uptime - extremely stable
- ✓ 72+ million ethically-sourced IPs

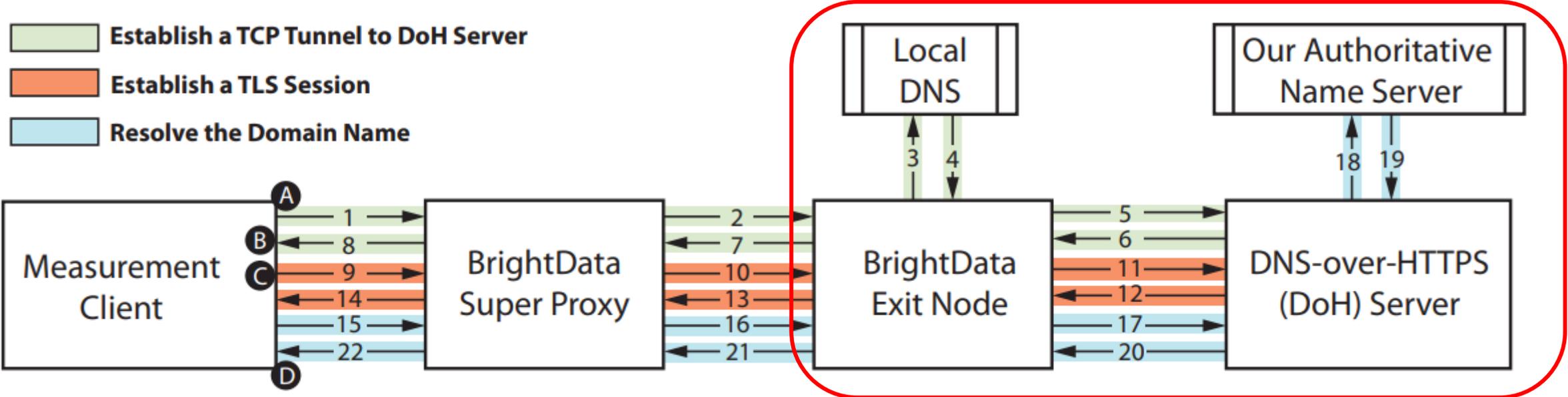
Globally spread

DoH resolution time data



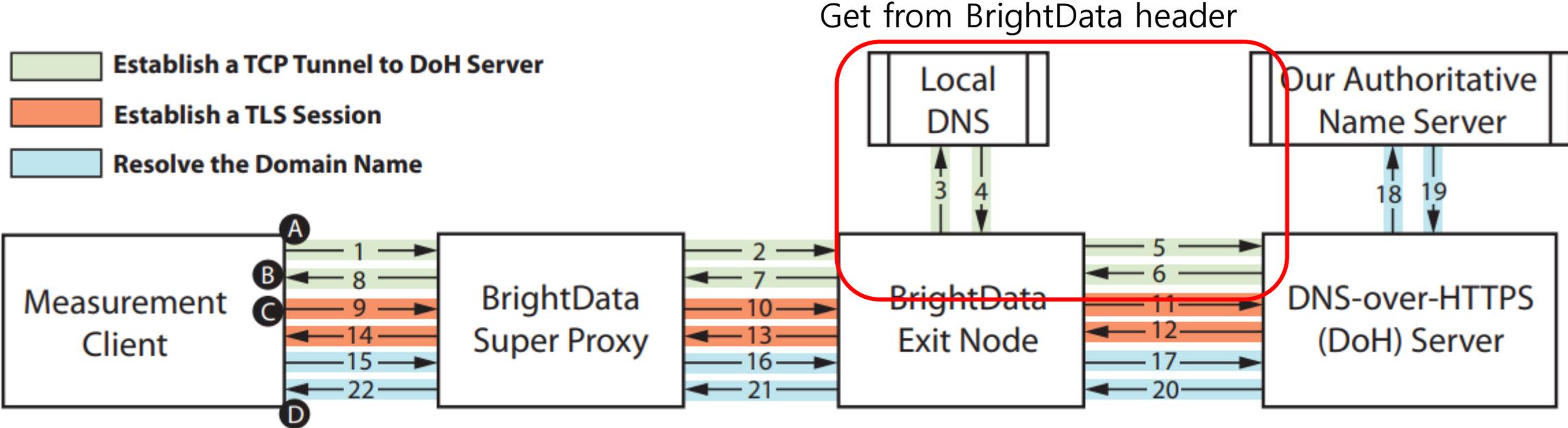
DoH resolution time data

- Establish a TCP Tunnel to DoH Server
- Establish a TLS Session
- Resolve the Domain Name

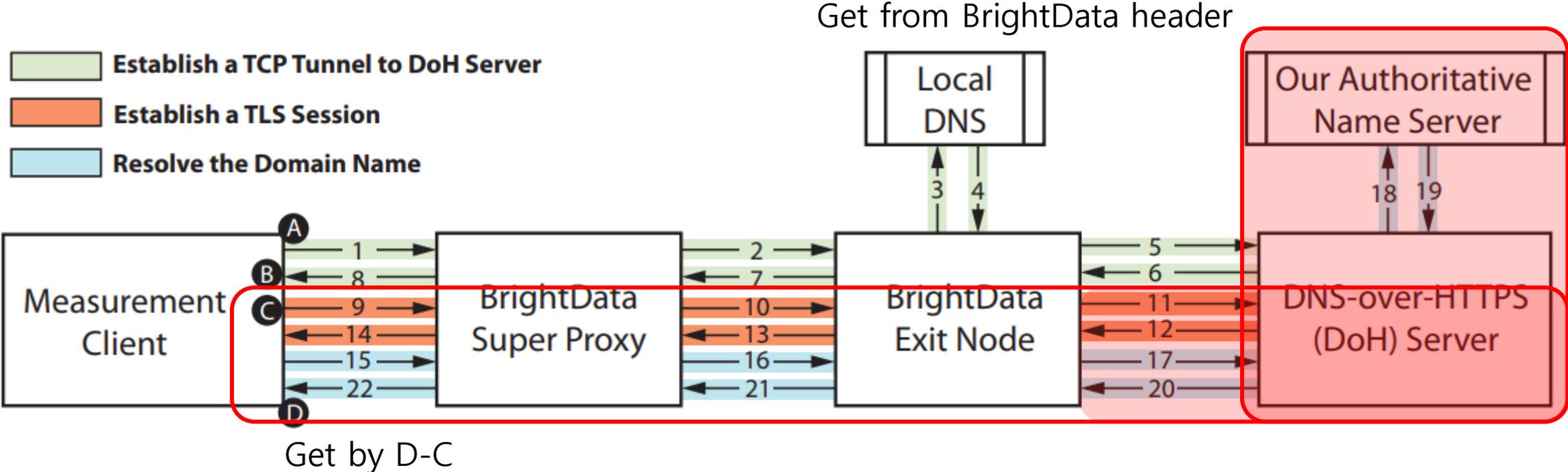


Delays authors wanted

DoH resolution time data

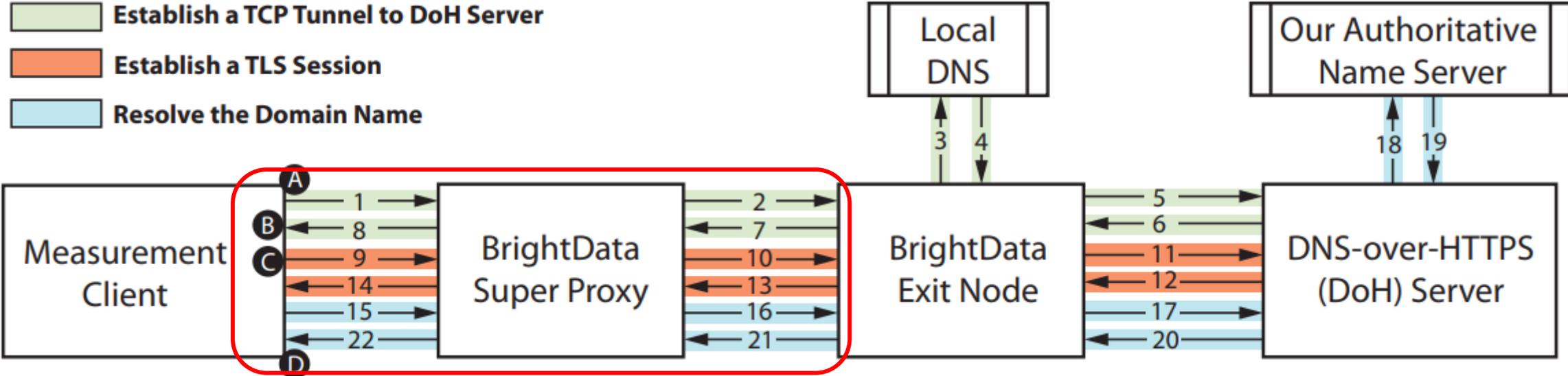


DoH resolution time data



DoH resolution time data

- Establish a TCP Tunnel to DoH Server
- Establish a TLS Session
- Resolve the Domain Name

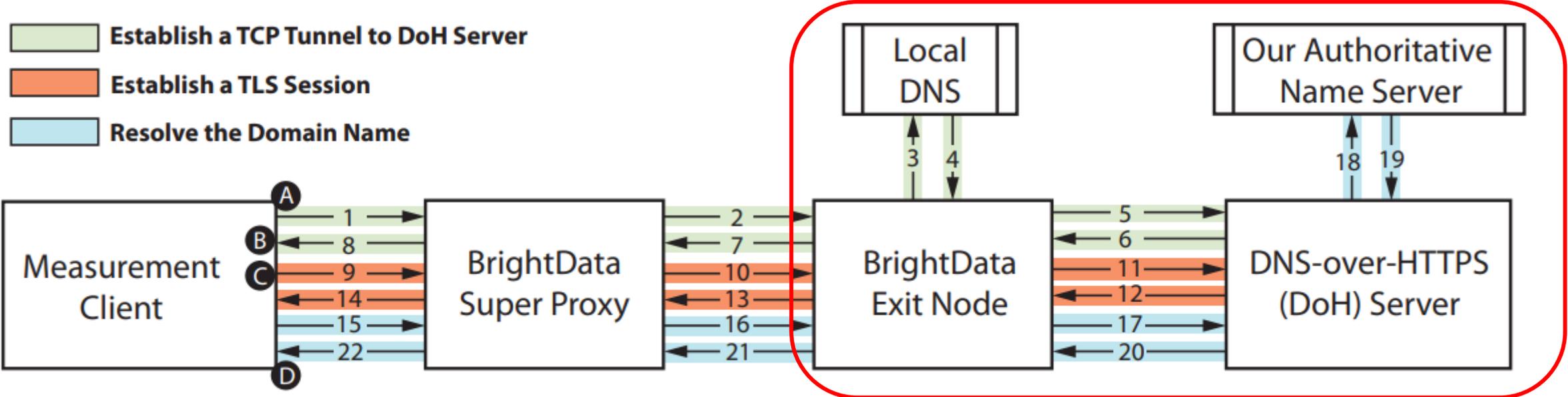


Suppose that RTT between client and exit node is stable

$$RTT = 1+2+7+8 = B-A-BrightData\ header = 9+10+13+14 = \dots\dots$$

DoH resolution time data

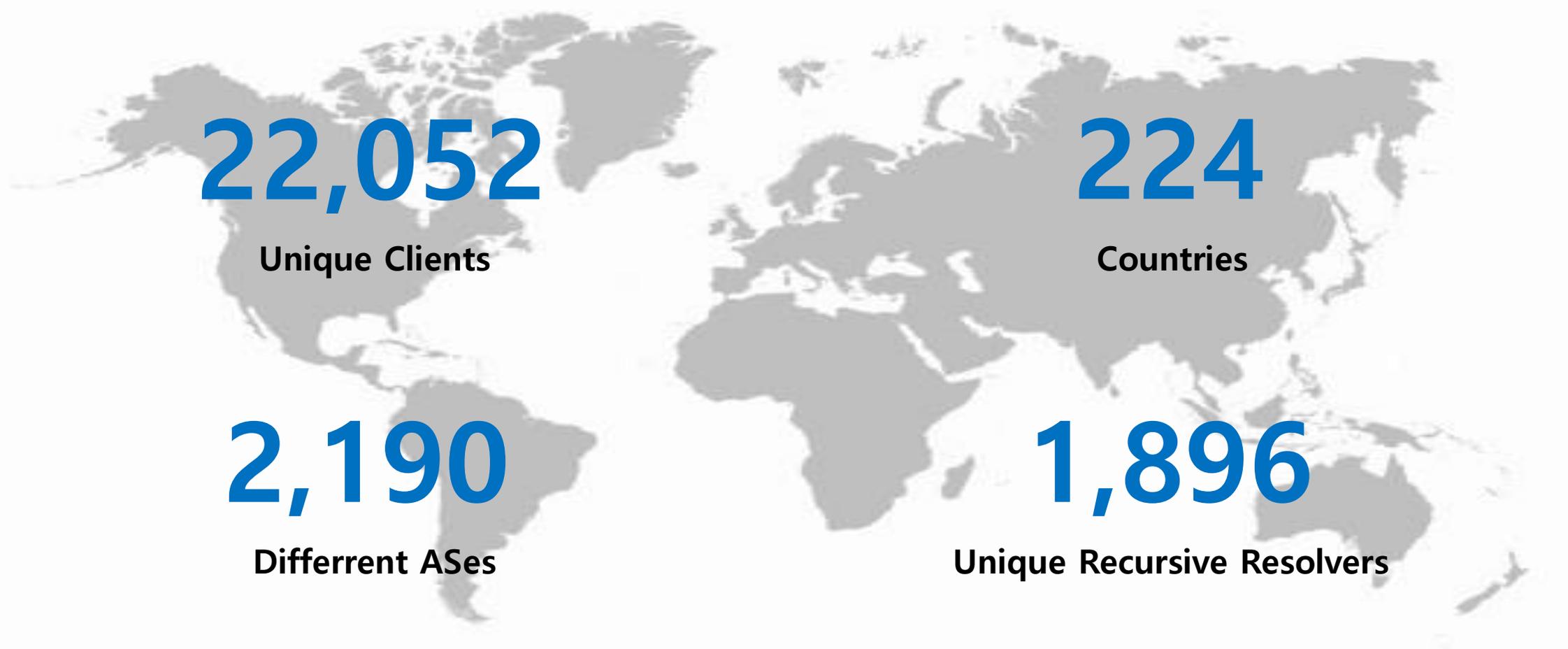
- Establish a TCP Tunnel to DoH Server
- Establish a TLS Session
- Resolve the Domain Name



Delays authors wanted
= D-C-2RTT+BrightData header

Results

Data overview

A light gray world map is centered in the background of the slide. Overlaid on the map are four large blue numbers, each with a corresponding label below it. The numbers are: 22,052 (top left), 224 (top right), 2,190 (bottom left), and 1,896 (bottom right).

22,052

Unique Clients

224

Countries

2,190

Differrent ASes

1,896

Unique Recursive Resolvers

Ground-truth validation

Country	Ireland		Brazil		Sweden		Italy		India		USA	
	DoH	DoHR	DoH	DoHR	DoH	DoHR	DoH	DoHR	DoH	DoHR	DoH	DoHR
Our Method	116	94	193	182	129	122	246	236	254	251	53	25
Ground-Truth	109	85	190	176	131	126	245	238	260	257	52	23
Difference	7	9	3	6	2	4	1	2	6	6	1	2

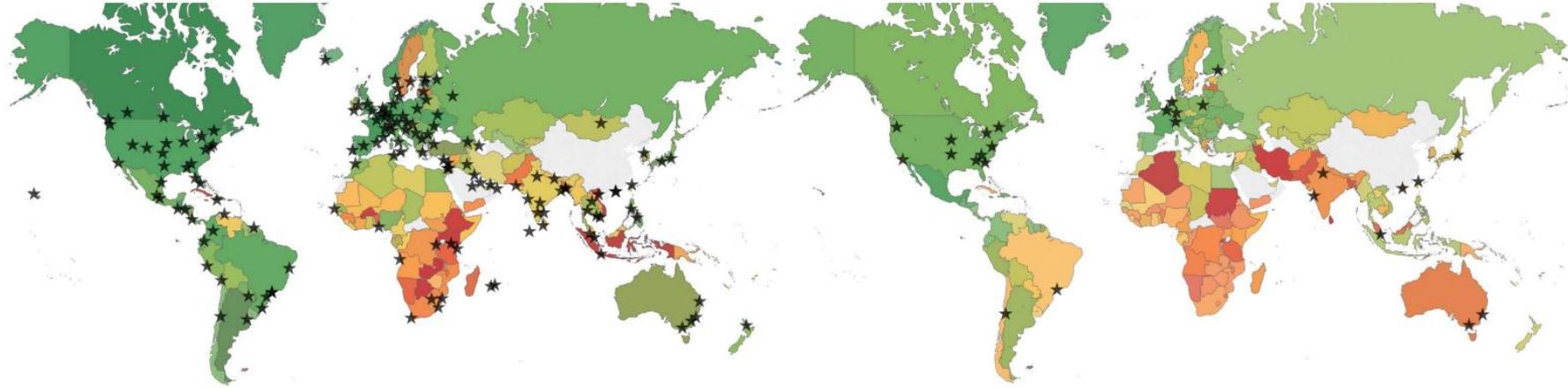
Table 1: Ground-truth Experiments for DoH and DoHR (DoH Connection Reuse)

Country	Ireland	Brazil	Sweden	Italy
Our Method	102	139	131	204
Ground-Truth	102	138	129	203
Difference	0	1	2	1

Table 2: Ground-truth Experiments for Do53

Minor differences between ground-truth and authors' methodology

Global performance



(a) Cloudflare

(b) Google



(c) NextDNS

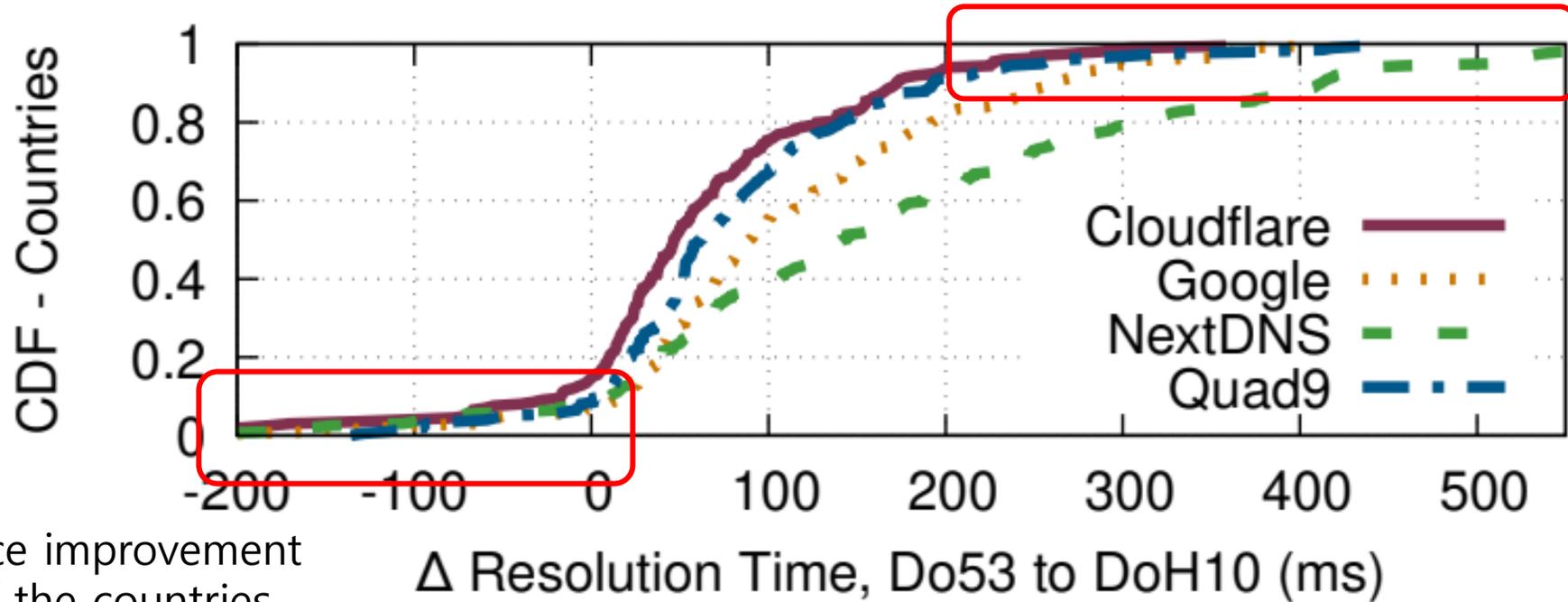
(d) Quad9

Median DoH Resolution Time (ms)



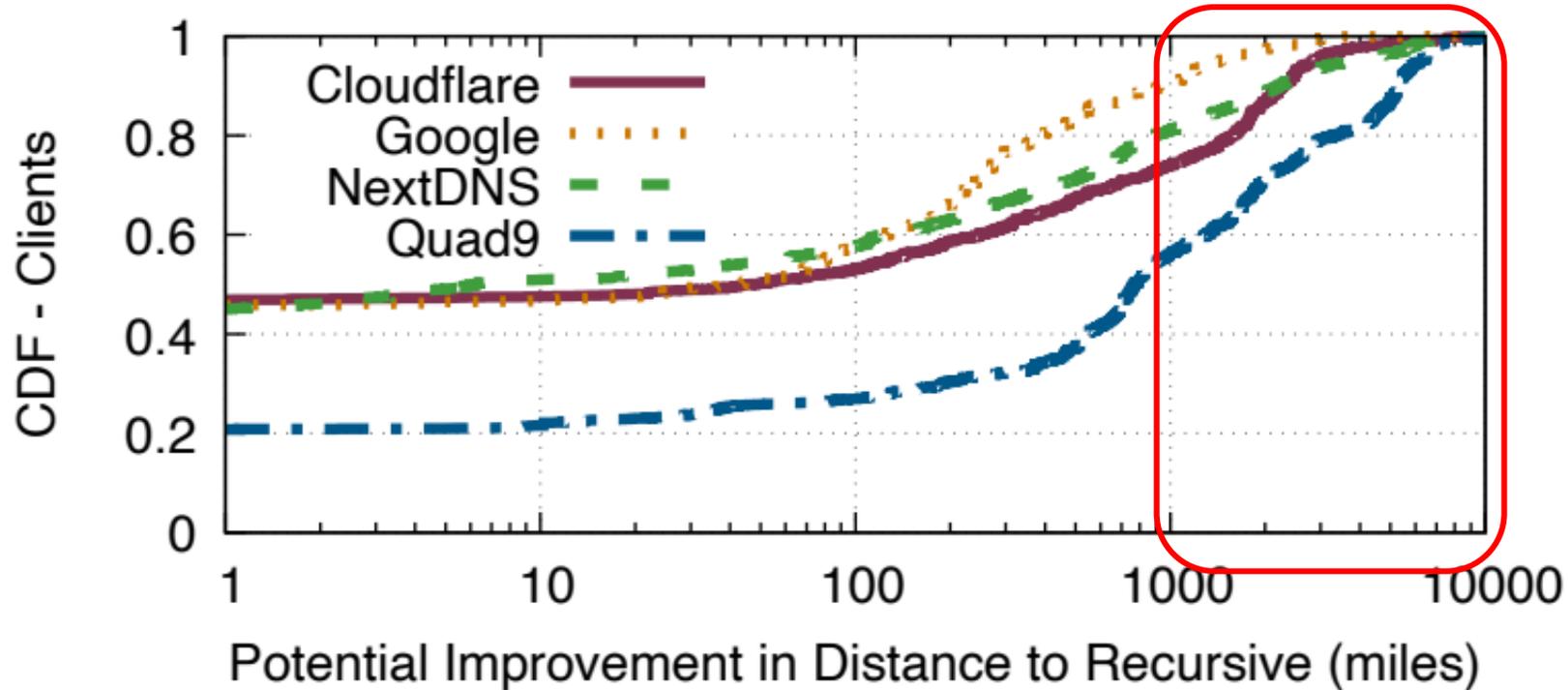
Performance inequality

Might be unacceptable additional delays for 10% of the countries



Performance improvement for 8.8% of the countries

Room for improvement



Potential Improvement: differences between actual PoP and the closest PoP (in the dataset)

→ 10% of Google / 26% of Cloudflare clients can be switched to a PoP at least 1000 miles closer

Conclusion

- Authors conducted global scale measurements with Do53 and DoH
- They shows performance gaps between countries
 - Low Internet infra & economic development will be disproportionately impacted by a unilateral switch to DoH from Do53
- They also shows there is room for improvement