

# A Worldwide View on the Reachability of Encrypted DNS Services

**Ruixuan Li**

*Zhejiang Gongshang University  
Tsinghua University*

**Baojun Liu\***

*Tsinghua University*

**Chaoyi Lu**

*Tsinghua University*

**Haixin Duan**

*Tsinghua University*

**Jun Shao\***

*Zhejiang Gongshang University*



浙江工商大學  
ZHEJIANG GONGSHANG UNIVERSITY

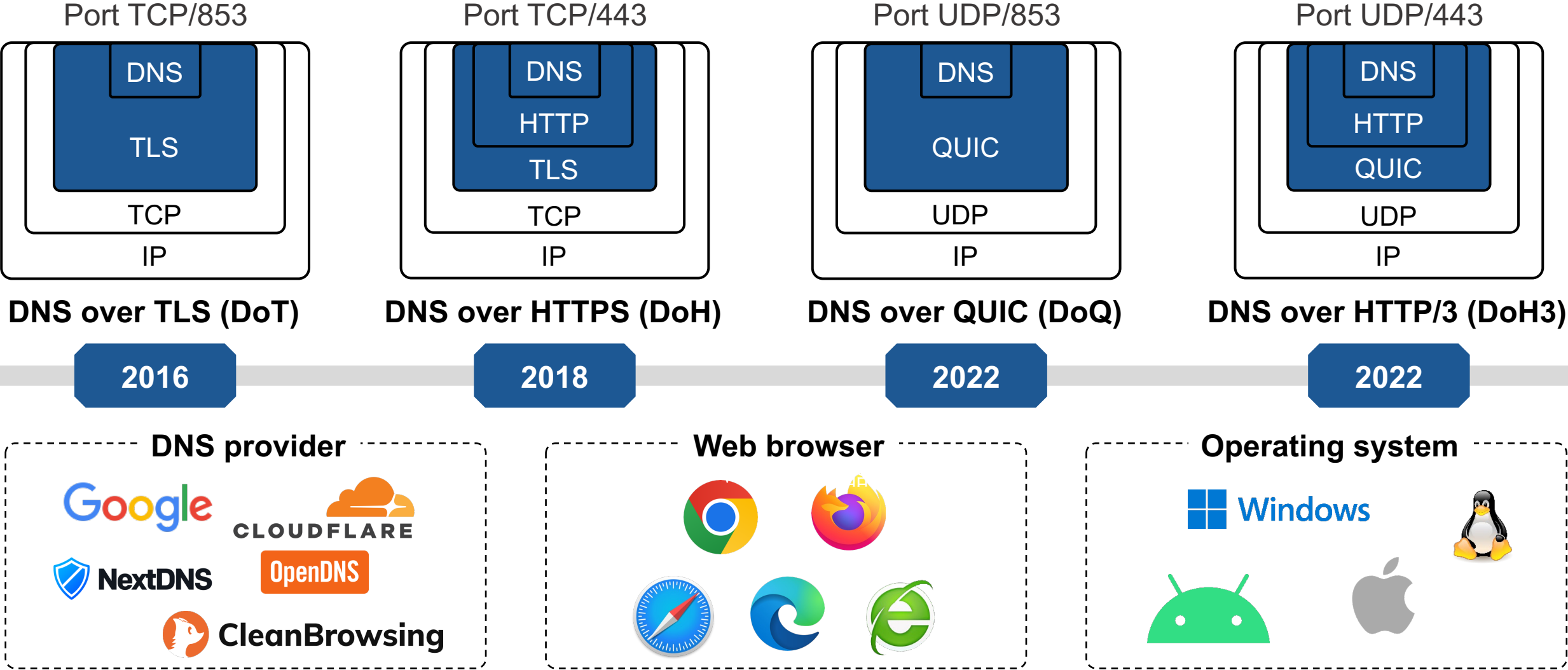


清華大學  
Tsinghua University

\* *Equal corresponding authors*

# Encrypted DNS protocol

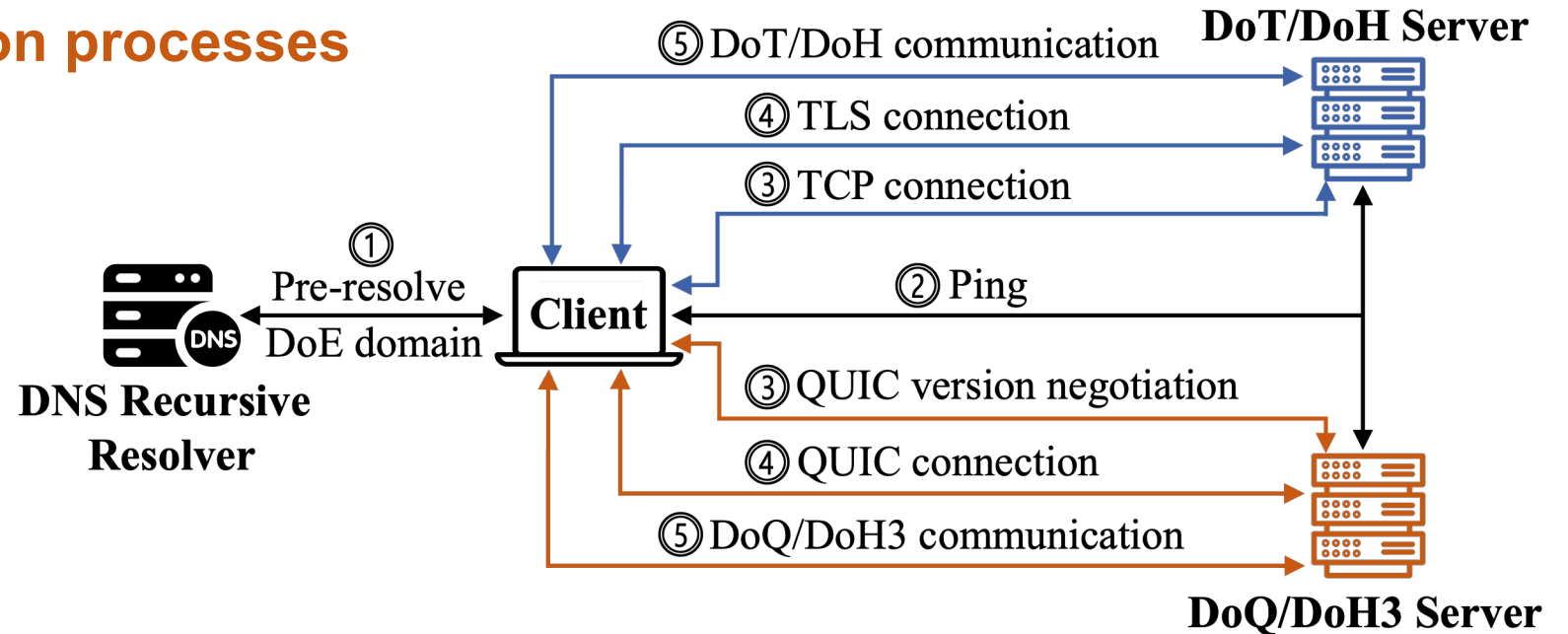
DNS over Encryption (DoE) emerges as emerging technology to mitigate DNS threats



# It is not simple to obtain DoE service

## Complex DoE communication processes

- ❖ multiple network layer
- ❖ multiple handshakes
- ❖ multiple session types



## ISPs block DoE communications to ensure network control



Internet Service Provider Association (UK)



2019 Internet Villains

# Evaluate the reachability of global DoE services

## Challenges

- 1) the community lacks a public comprehensive list of DoE domains
- 2) blocking behaviors may occur at various stages of DoE communication

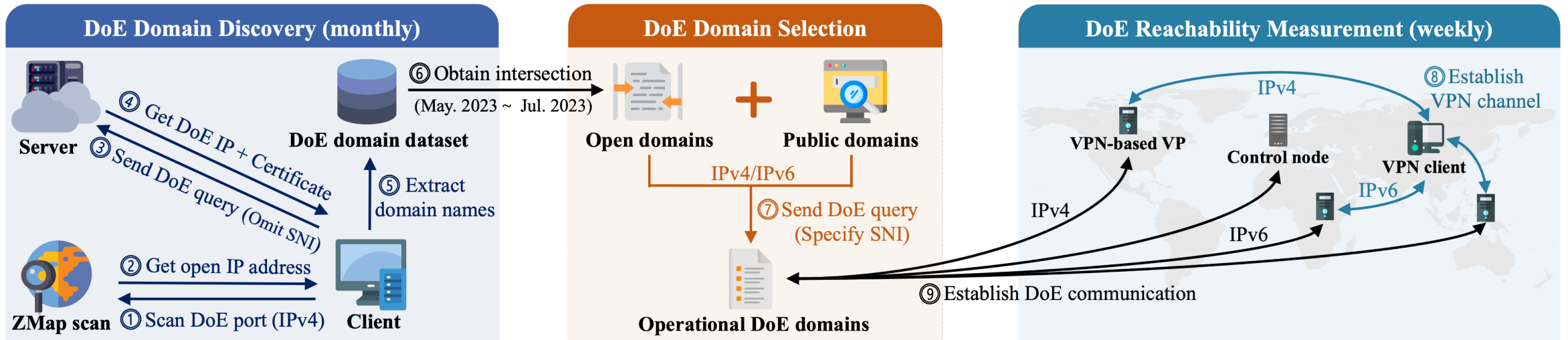
### Previous studies:

- ❖ a limited number of DoT/DoH domains
- ❖ a restricted subset of vantage points
- ❖ lack of blocking type analysis
- ❖ focus on IPv4

### Our study:

- ❖ most comprehensive DoE domain dataset ever
- ❖ vantage points distributed around the world
- ❖ explore DoE blocking types
- ❖ focus on IPv4 and IPv6

# Our global DoE reachability measurement

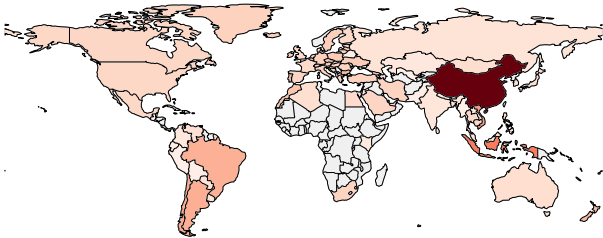


- ❖ **Supported protocols:** DoT, DoH, DoQ, DoH3 (IPv4/IPv6)
- ❖ **Supported blocking type detection:** Pre-resolve, Ping, TCP, TLS, QUIC-VN, QUIC, Response
- ❖ **Vantage point distribution:** 5K VPN nodes, located in 102 countries/regions
- ❖ **DoE domain collection:** 1302 operational DoE domains, 448 of which support IPv6.
- ❖ **DoE reachability monitor:** over 10M DoE queries in two months

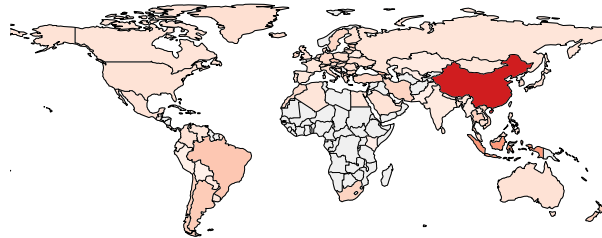
# Global view of DoE service reachability

## Country/region blocking of DoE services

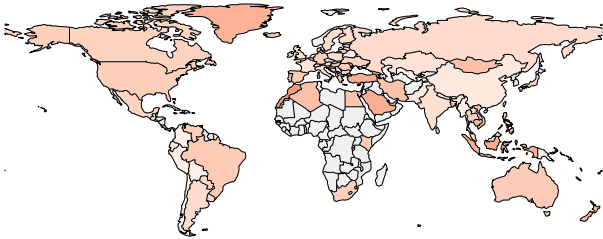
DoTv4



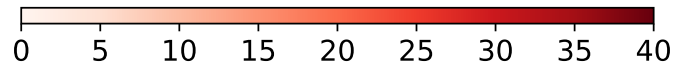
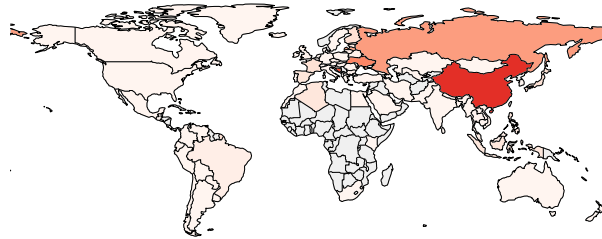
DoHv4



DoQv4



DoH3v4



- ❖ DoE services are poorly reachability in some regions
- ❖ **DoT/DoH** blocking usually occurs in **TCP** sessions
- ❖ **DoQ/DoH3** blocking usually occurs in **QUIC-VN**
- ❖ The reachability of DoE services on **IPv6** is **better**

## Mitigation of DoE blocking: Change DoE service type

1) Change server **IP address** (**59.13%** improvement)

2) Change DoE **protocols** (**63.25%** improvement)

# Thank You For Listening !

---

## A Worldwide View on the Reachability of Encrypted DNS Services

Ruixuan Li, Baojun Liu, Chaoyi Lu, Haixin Duan, Jun Shao

Code and data: <https://port-53.info/data/open-encrypted-dns-servers/>



浙江工商大學  
ZHEJIANG GONGSHANG UNIVERSITY



清華大學  
Tsinghua University