



ODNS Clustering

Unveiling Client-Side Dependency in Open DNS Infrastructure

Wenhao Wu¹³, Zhaohua Wang², Qinxin Li¹³, Zihan Li¹³, Yi Li², Jin Yan⁴, Zhenyu Li¹⁵✉

¹ICT,CAS, ²CNIC,CAS, ³UCAS, ⁴CNNIC, ⁵Zhongguancun Laboratory

Background & Motivation

Many DNS servers do not resolve DNS queries by themselves

- DNS forwarding behavior causes complex dependency

- Dependency between forwarder and forwarder
- Dependency between forwarder and resolver

- Dependency causes potential risks

Single-point failure, Amplify malicious behaviors, Entrances for Attacks

How to characterize the dependencies among ODNS

ODNS servers with dependence naturally form clustered structure

Methodology: ODNS Clustering

Concept: What is ODNS Cluster

- Collection of upstream servers and forwarders with dependencies.
- Example: S1-S6 are divided into two ODNS clusters. Servers S1-S3 in Cluster 1 and S4-S6 in Cluster 2.

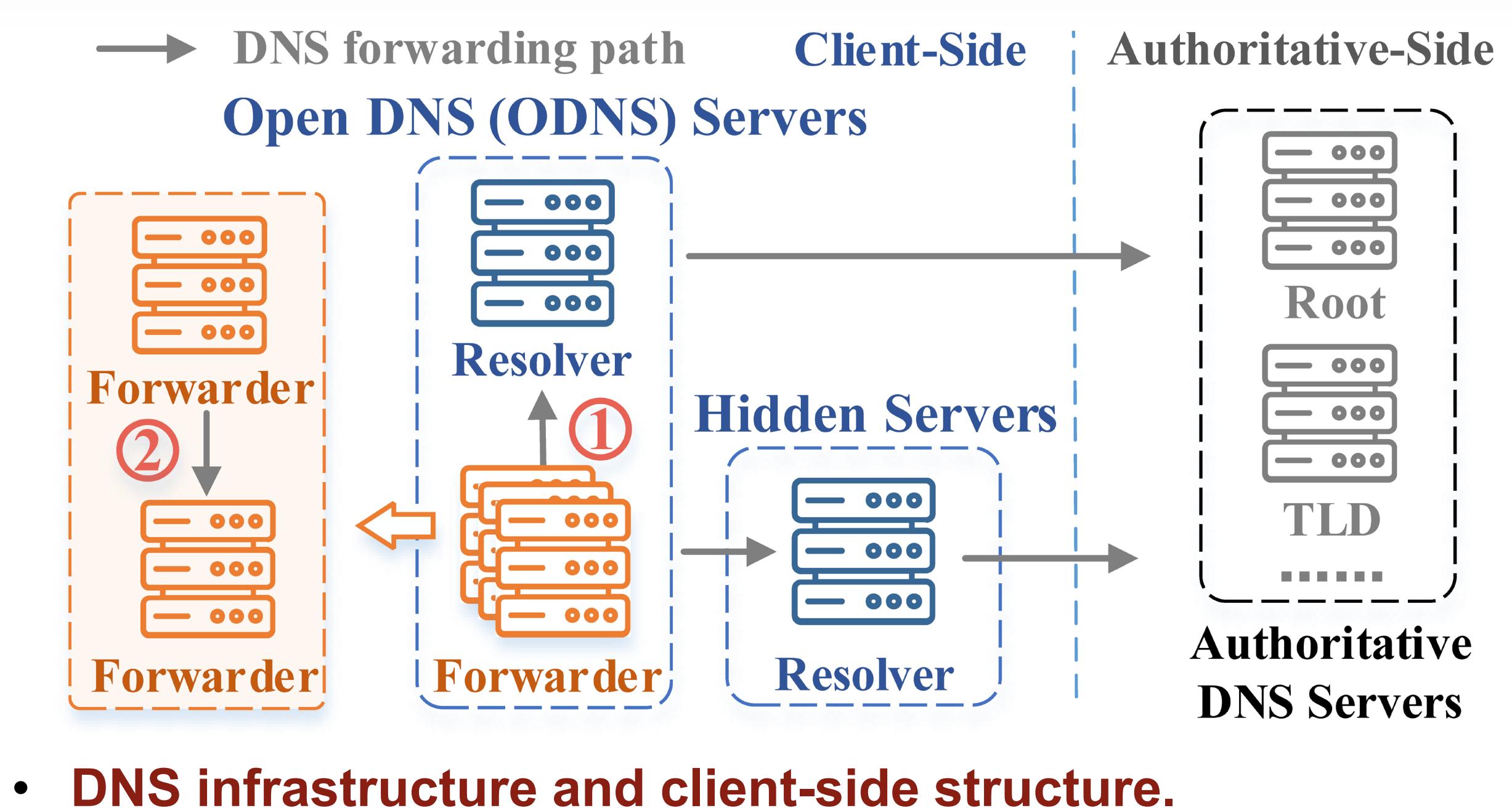
Methodology: Divide DNS servers into multiple clusters

- Servers are clustered by A record (S1-S3 get 0.0.0.1, S4-S6 get 0.0.0.2)

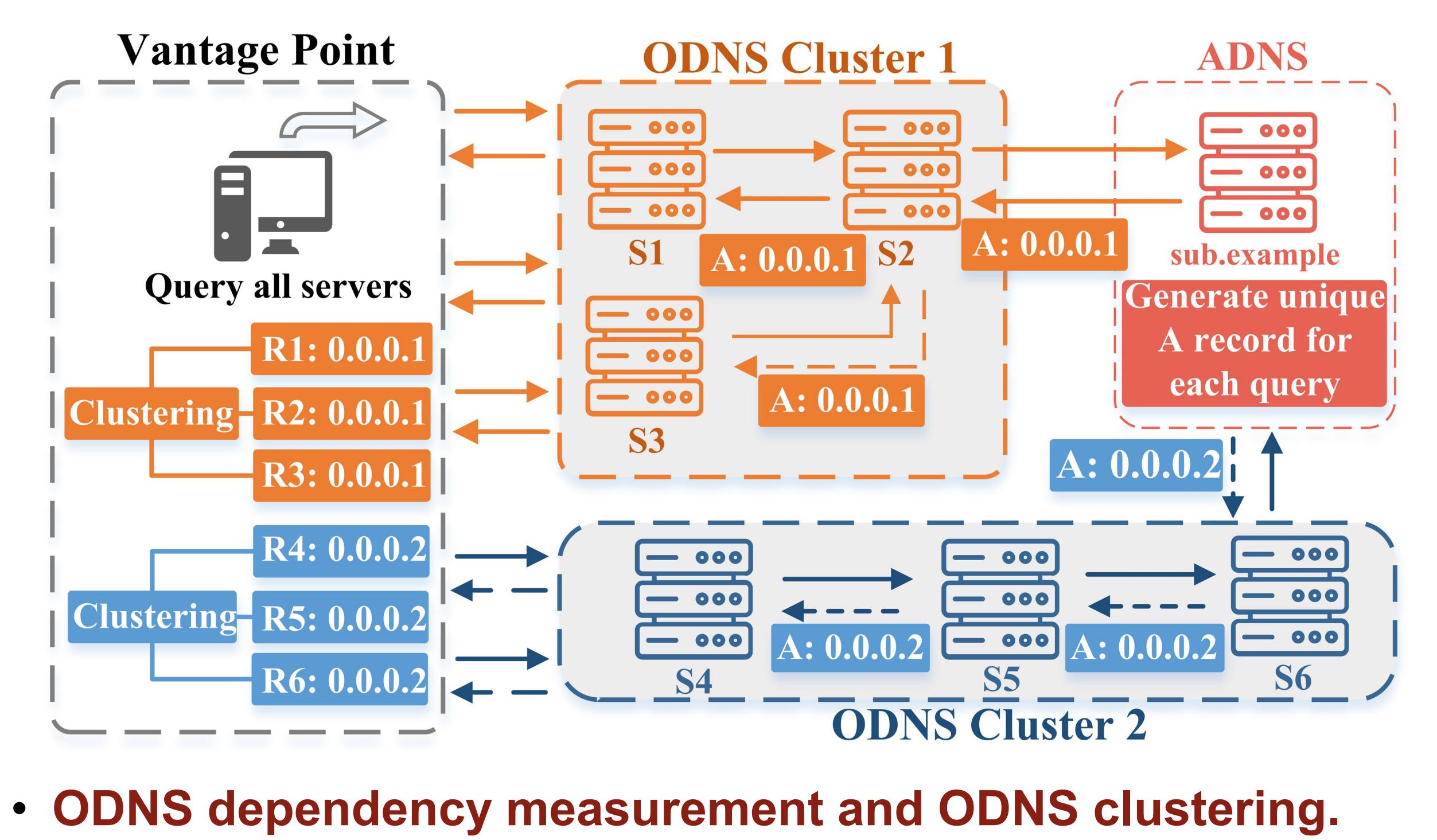
Controlled ADNS for specific domain. Generate unique A record for each query (e.g. 0.0.0.1, 0.0.0.2)

Vantage Point

Send A queries for specific domain to each ODNS servers, and collect the responses.



• DNS infrastructure and client-side structure.

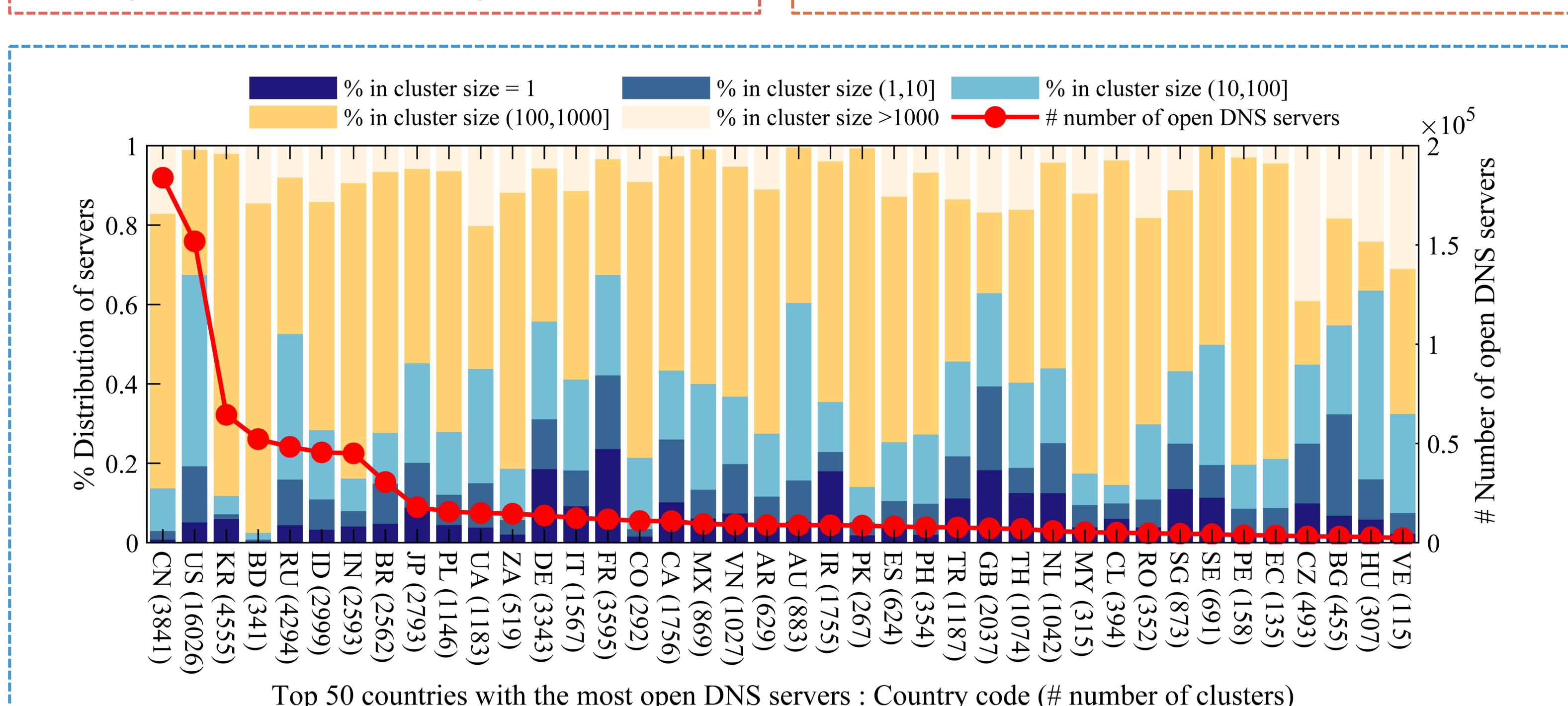
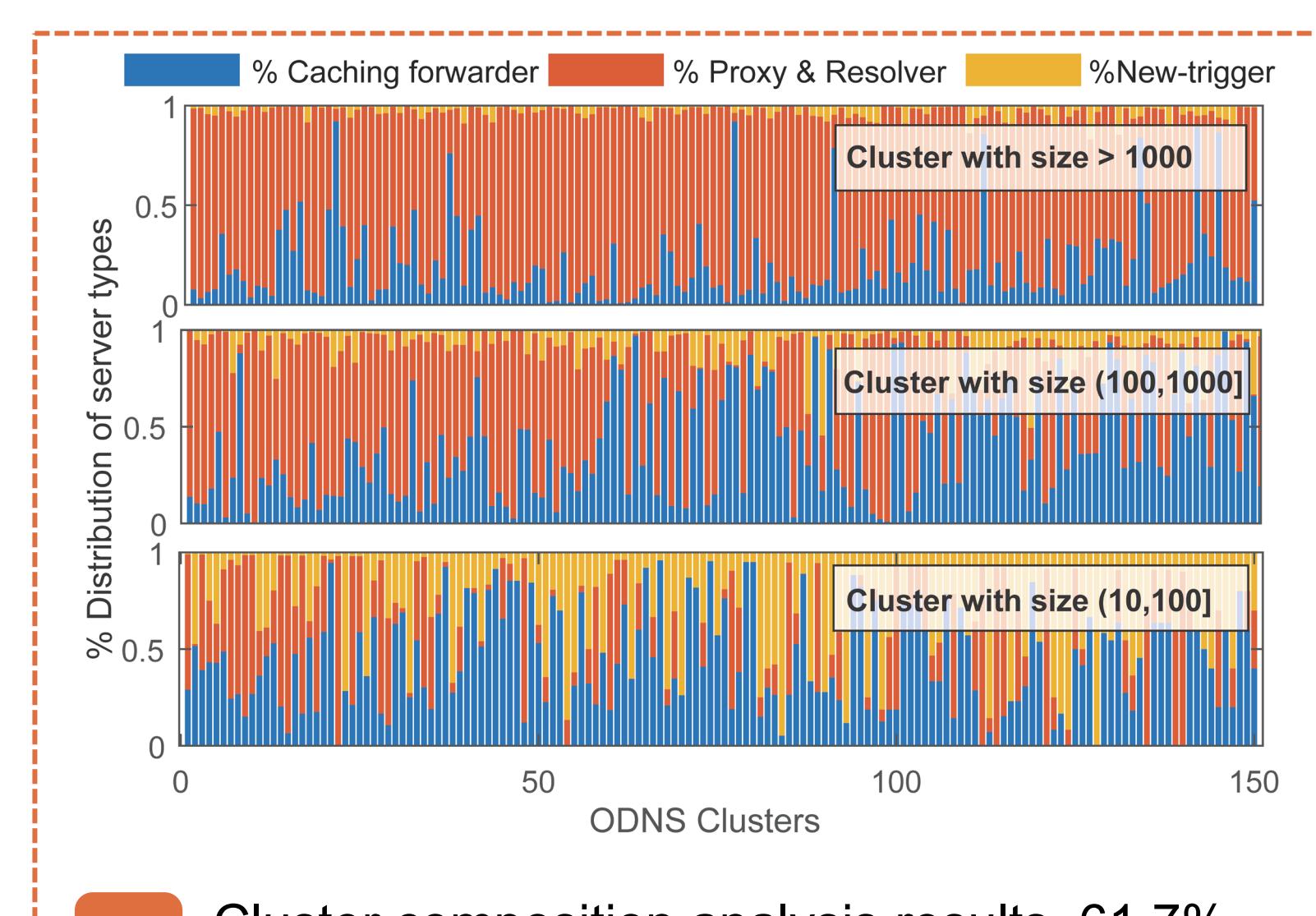
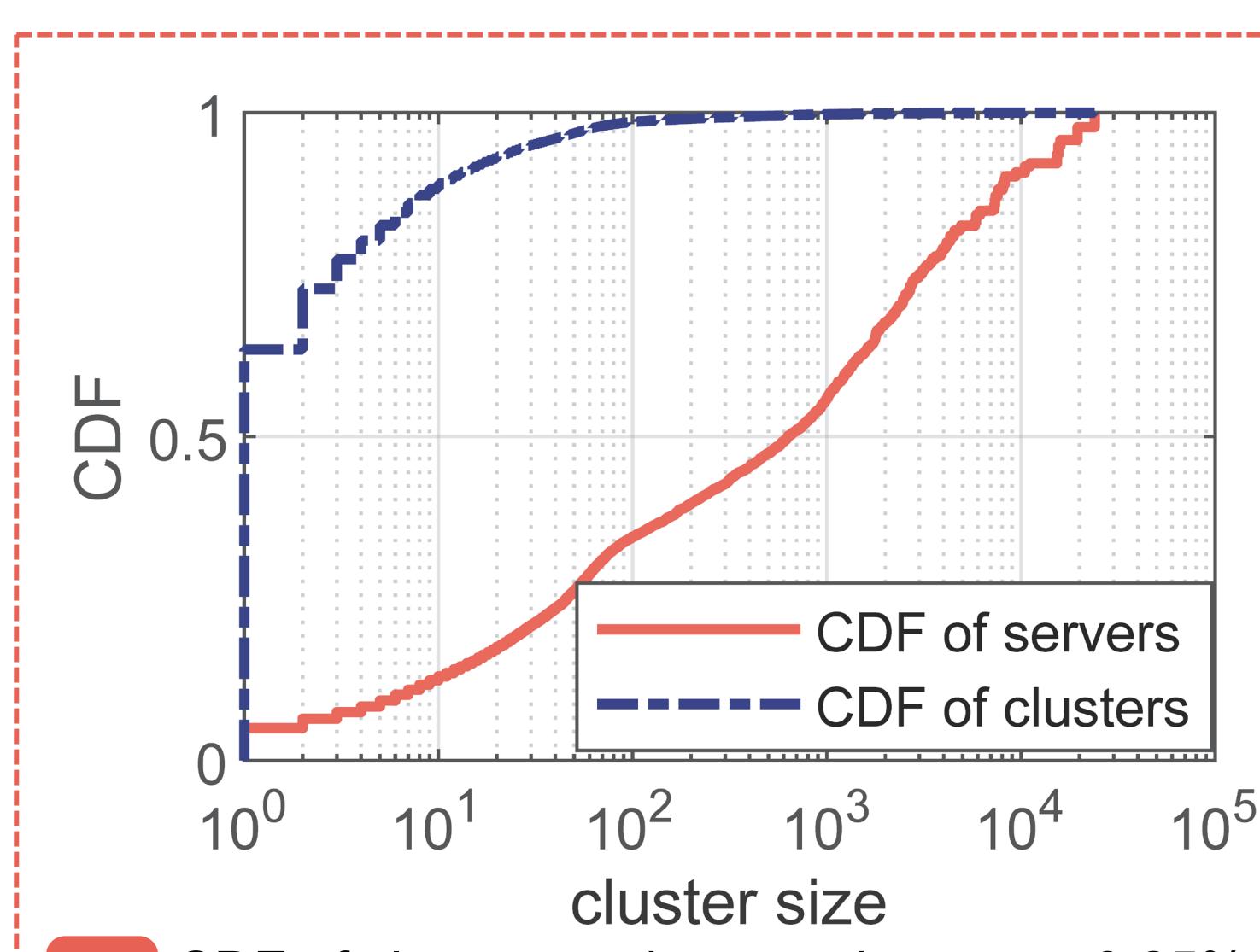


• ODNS dependency measurement and ODNS clustering.

Measurement & Analysis: Million-scale ODNS servers in the wild form only 81,636 clusters

Key Observations

- Cluster Size Bias** 95% open resolvers exhibit dependencies on others for name resolution. The distribution of cluster size is heavily biased.
- ODNS Server Types** About 61.7% of forwarders are non-caching proxies, which may be leveraged by attackers to attack the upstream resolvers.
- Geolocation Bias** Cluster size distribution varies significantly across countries, implying differences in DNS infrastructure.
- Network Centralized** Clusters that are led by major public DNS servers cover 47% open DNS servers.
- Problematic Clusters** 9% of the ODNS servers direct web requests to the wrong destinations.



Provider	# of clusters	% covered rate
Google	268	27.99%
Cloudflare	228	9.76%
OpenDNS	46	5.33%
Yandex.DNS	118	4.24%
Others	—	4.63%

4 Clusters for top public DNS. Popular public resolvers lead a large portion of open DNS servers. The use of Anycast results in multiple clusters for one public DNS provider.

Response Type	Subcategory	# of clusters
Success	Parked Domain	218
	Filtered/Blocked	60
	Error Page	72
	Others	29
Redirection	Malicious	65
	Normal	101
No Response	—	3648
Error	—	2864

5 Response type statistics for unexpected A record in problematic clusters. 65 clusters (affecting 1581 ODNS servers) led users to potentially malicious pages.